IDP
REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

IDP Número 44 (marzo, 2026)

Universitat Oberta de Catalunya

https://idp.uoc.edu
ISSN 1699-8154

IDP
REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Monográfico sobre la consolidación del trabajo a distancia (coord. Irene Rovira)

Miscelánea, miscellany, miscel·lània

IDP
REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Monográfico: «Sobre la consolidación del trabajo a distancia» (coord.: Irene Rovira Ferrer)

Los artistas digitales en régimen de teletrabajo transnacional: una reinterpretación tributaria a la luz de la transformación cultural digital

Ángel Urquizu Cavallé
Universidad Rovira i Virgili

Fecha de presentación: mayo 2025
Fecha de aceptación: septiembre 2025
Fecha de publicación: marzo 2026

Resumen

Este artículo analiza el impacto del teletrabajo transnacional en la fiscalidad de los artistas digitales por cuenta ajena, proponiendo una reinterpretación del artículo 17 del MC OCDE a la luz de la transformación digital. Partiendo de una definición funcional del artista digital como aquel que realiza actividad creativa mediante tecnologías y sin presencialidad física, el estudio examina diversos perfiles profesionales (*streamers*, *performers* en XR, músicos virtuales, etc.) que desarrollan su labor en entornos deslocalizados, planteando retos sobre la jurisdicción fiscal competente. Se sostiene que, cuando existe una actuación personal, pública y escénica –aunque sea en formato digital–, puede aplicarse el artículo 17, permitiendo al Estado de recepción gravar la renta. En cambio, si la actividad carece de proyección pública o se limita a tareas técnicas, debería aplicarse el artículo 15, atribuyendo la potestad tributaria al Estado de residencia. El trabajo también analiza los efectos del modelo *Employer of Record* y la figura del empleador económico, proponiendo soluciones interpretativas que eviten la elusión fiscal. Finalmente, se sugiere incluir en futuros convenios fiscales una cláusula que permita considerar actuaciones digitales en directo como realizadas en el territorio donde se reciben, para adaptar el marco convencional a la realidad cultural digital contemporánea.

Palabras clave

artista digital; teletrabajo transnacional; convenios de doble imposición; empleador económico

Digital artists in transnational teleworking regime: a tax reinterpretation in light of the digital cultural transformation

Abstract

This article analyses the impact of transnational teleworking on the taxation of digital artists employed by others, proposing a reinterpretation of Article 17 of the OECD MC in the light of the digital transformation. Based on a functional definition of the digital artist as one who performs creative activity through technologies and without physical presence, the study examines various professional profiles (streamers, XR performers, virtual musicians, etc.) who carry out their work in unlocated environments, posing challenges for competent tax jurisdictions. It is argued that, when there is a personal, public, and scenic performance – even in digital format – Article 17 can be applied, enabling the Receiving State to tax the income. Conversely, if the activity lacks public exposure or is limited to technical tasks, Article 15 should be utilized, vesting the taxing rights in the State of residence. The work also analyses the effects of the Employer of Record model and the economic employer figure, proposing interpretative solutions that avoid tax avoidance. Finally, it is suggested that future tax agreements include a clause allowing digital live performances to be considered as carried out in the territory where they are received, to adapt the conventional framework to contemporary digital cultural reality.

Keywords

digital artist; transnational teleworking; double taxation agreements; economic employer

Introducción

El desarrollo acelerado de las tecnologías digitales y su integración en los procesos creativos ha dado lugar a formas de expresión artística inéditas, en las que el teletrabajo no es simplemente una adaptación, sino la condición natural de producción.

Podemos entender como un artista digital por cuenta ajena en modalidad de teletrabajo a aquel profesional que, en el marco de una relación laboral de carácter dependiente y retribuida, realiza actividades de creación, diseño o producción artística mediante medios digitales y utilizando herramientas tecnológicas especializadas (como *software* de ilustración, modelado 3D, edición audiovisual, realidad aumentada o arte generativo), ejecutando sus funciones de forma no presencial, generalmente desde su domicilio u otro lugar elegido por él, mediante el uso de tecnologías de la información y la comunicación.

Esta figura engloba a creadores que, contratados por empresas o entidades del sector cultural, audiovisual o tecnológico, producen contenidos artísticos digitales desde entornos remotos, ya sea en un entorno propio u otros espacios digitalmente habilitados.

La creciente desmaterialización de las actividades creativas ha transformado profundamente el ecosistema laboral de los artistas, que desempeñan su labor en modalidad de teletrabajo internacional, prestando servicios creativos para entidades situadas en países distintos al de su residencia.

Esta nueva realidad plantea problemas tributarios de considerable complejidad, especialmente en lo que respecta a la determinación de la Jurisdicción competente para gravar las rentas derivadas de tales actividades y a la aplicación de los instrumentos internacionales para evitar la doble imposición.

La tributación de la renta obtenida por los artistas digitales en teletrabajo transnacional depende, esencialmente, de la existencia o no de un convenio para evitar la doble imposición entre el país de residencia del artista y el país en el que se ejercita la actividad artística, así como de la caracterización jurídica de esa actividad, especialmente en función de si se trata de un trabajo por cuenta ajena o autónomo.

El presente estudio analiza la aplicabilidad del artículo 17 del Modelo de Convenio Tributario sobre la Renta y sobre el Patrimonio de la OCDE (MC OCDE), tradicionalmente re-

servado a artistas del espectáculo y deportistas, a la figura emergente del artista digital que desarrolla su actividad en régimen de teletrabajo. Se parte de una lectura funcional del término «artista del espectáculo» conforme al principio de neutralidad tecnológica, examinando cómo determinadas formas contemporáneas de creación digital pueden encajar jurídicamente en dicho artículo. Asimismo, se identifican situaciones prácticas en las que esta calificación resulta procedente, así como los elementos que permitirían desvirtuarla en favor de la aplicación del artículo 15 del MC OCDE.

El fenómeno del teletrabajo artístico digital transnacional plantea desafíos fiscales inéditos que requieren una adaptación de los convenios de doble imposición para reconocer adecuadamente las especificidades del trabajo creativo digital y una revisión de las normas internas de imposición, a fin de calificar adecuadamente a los nuevos artistas digitales y garantizar la seguridad jurídica de sus relaciones laborales transnacionales.

1. Artista digital y teletrabajo en España

La figura del artista digital se inserta en el régimen laboral especial de las personas dedicadas a actividades artísticas (Real Decreto 1435/1985, de 1 de agosto, por el que se regula la relación laboral especial de las personas artistas que desarrollan su actividad en las artes escénicas, audiovisuales y musicales, así como de las personas que realizan actividades técnicas o auxiliares necesarias para el desarrollo de dicha actividad) y queda simultáneamente sujeta a la normativa sobre trabajo a distancia (de acuerdo con la Ley 10/2021, de 9 de julio, de trabajo a distancia).

El artista digital por cuenta ajena en teletrabajo encarna una nueva realidad profesional híbrida, en la que convergen la dependencia laboral, la innovación tecnológica y la deslocalización del proceso creativo (en particular, sobre el teletrabajo en el ámbito tributario, véanse los excelentes trabajos de Mata Sierra, 2024; Mories Jiménez, 2023; y Rovira Ferrer, 2023, 2024a).

El impacto de las tecnologías digitales en las actividades creativas ha supuesto una transformación profunda de los modos de producción, distribución y comercialización de las obras artísticas. Este fenómeno, acelerado por el auge de la inteligencia artificial, las realidades extendidas y los entornos virtuales, ha configurado nuevas modalidades de trabajo artístico en las que el teletrabajo no es una excepción, sino la forma ordinaria de desarrollo de la actividad.

Desde la perspectiva tributaria, esta evolución plantea la necesidad de encuadrar la actividad artística digital más innovadora para describir y clasificar la naturaleza de la actividad artística desarrollada en régimen laboral.

Frente a los perfiles artísticos tradicionales, emerge hoy una amplia tipología de nuevos artistas digitales cuya actividad se desarrolla íntegramente en entornos virtuales y digitales, permitiendo la plena integración en la modalidad de teletrabajo transnacional.

- Diseñadores de experiencias XR (Realidad Extendida), encargados de crear entornos inmersivos en realidad virtual (RV), aumentada (RA) o mixta (RM), trabajando para museos, estudios de videojuegos o plataformas de metaverso.

- Guionistas que han expandido su campo de acción, más allá del cine o la televisión, hacia la escritura de narrativas transmedia, guiones para experiencias de realidad virtual y estructuras narrativas interactivas para videojuegos y entornos inmersivos (con herramientas digitales de coescritura, revisión en línea y plataformas de diseño de experiencias).

- Compositores que, tradicionalmente ligados a la creación musical, ahora trabajan en el diseño de paisajes sonoros para realidades aumentadas, composiciones adaptativas para videojuegos o experiencias sonoras tridimensionales para entornos de metaverso.

- Músicos y cantantes que graban en remoto y participan en conciertos virtuales en plataformas inmersivas, realizando actuaciones musicales en realidades mixtas (espacios físicos y virtuales) y colaborando en proyectos musicales de NFT sonoros.

- Artistas de inteligencia artificial creativa, que utilizan redes neuronales, redes generativas antagónicas (GANS) y algoritmos generativos para crear obras visuales, sonoras o interactivas, contratados en laboratorios de arte digital o como «artistas residentes» en empresas tecnológicas.

- Diseñadores de espacios virtuales en el metaverso, especializados en construir mundos virtuales compar-

tidos, para espacios y plataformas interactivas (como Decentraland, Somnium Space, Spatial o The Sandbox) que desempeñan su actividad principalmente en agencias web3 especializadas en tecnologías descentralizadas, proyectos NFT y soluciones blockchain, o estudios de arquitectura digital.

- *Creative technologist* o programador artístico, que fusiona programación, arte, sonido e interacción mediante tecnologías como sensores, Arduino o IA, en agencias creativas, universidades, centros de innovación y museos digitales.

- Narradores interactivos y diseñadores de experiencias lúdicas, creadores de narrativas no lineales para videojuegos y aplicaciones educativas, en estudios de videojuegos, aplicaciones educativas y proyectos XR, apoyados en plataformas de colaboración digital.

- Artistas de realidad aumentada, creadores de filtros artísticos, prendas digitales y efectos visuales para redes sociales y campañas publicitarias.

- Bioartistas digitales o artistas de datos vivos, que combinan arte, ciencia y visualización interactiva de datos, trabajando en universidades, laboratorios de ciencia y centros de investigación artística.

- *Performers* avatarizados o artistas escénicos virtuales, intérpretes que realizan actuaciones mediante avatares, captura de movimiento y entornos virtuales inmersivos.

- Artistas de música generativa e interactiva, creadores de piezas sonoras que responden dinámicamente a estímulos ambientales o al comportamiento de los usuarios, que trabajan en el sector de videojuegos, instalaciones inmersivas o plataformas de audio interactivo.

En todos estos casos, y muchos otros, el Estatuto del Artista y la normativa laboral vigente en materia de teletrabajo (Ley 10/2021 de trabajo a distancia y Estatuto de los Trabajadores) reconocen explícitamente la viabilidad de que las actividades creativas, incluidas sus modalidades digitales, se desarrollen bajo relación laboral y en régimen de teletrabajo.[1]

La Ley 10/2021 introduce un marco normativo claro que legitima el desarrollo de actividades laborales fuera del espacio físico de la empresa (por voluntad del empleado), a través del uso intensivo de tecnologías digitales.

Además, define el teletrabajo como una forma de trabajo a distancia sustentada en «el uso exclusivo o prevalente de medios y sistemas informáticos, telemáticos y de telecomunicación» (art. 2.1.b), lo que encaja plenamente con las dinámicas propias de las industrias culturales y creativas digitalizadas.

Desde la perspectiva tributaria, resulta imprescindible que el encuadramiento de las actividades artísticas tome en cuenta la naturaleza material de la creación, independientemente de su soporte físico o digital.

El reconocimiento de estas nuevas formas de creación no solo responde a la necesidad de actualizar los criterios de clasificación técnica y tributaria, sino que constituye un elemento esencial para garantizar la protección social de los artistas digitales, fomentar la innovación cultural y asegurar la competitividad del sector creativo en la economía digital contemporánea.

En conclusión, la aparición de nuevos perfiles de artistas digitales, su progresiva integración en relaciones laborales por cuenta ajena y la generalización del teletrabajo como forma ordinaria de desarrollo de la actividad artística, a nivel nacional y transnacional, redefinen profundamente el concepto de actividad artística en el derecho tributario y en el derecho laboral contemporáneo.

2. La tributación de las rentas obtenidas por el artista digital en modalidad de teletrabajo transnacional

Un artista residente en una jurisdicción puede obtener rentas derivadas del ejercicio de sus actividades artísticas en otra jurisdicción, a través de un vínculo laboral

1. El denominado «Estatuto del Artista» no es una ley única codificada, sino un conjunto de medidas legislativas dispersas, basadas en el Informe de la Subcomisión para la elaboración de un Estatuto del Artista y en posteriores reformas legislativas. El 6 de septiembre de 2018, el Pleno del Congreso de los Diputados aprobó por unanimidad el informe de la Subcomisión para estudiar la elaboración de un Estatuto del Artista y del Profesional de la Cultura.

con una entidad situada en la propia jurisdicción o en otra diferente.

En este sentido, en el contexto actual de digitalización del trabajo, se ha consolidado el modelo de contratación a través de un *Employer of Record* (EOR) como una fórmula habitual para facilitar la vinculación laboral transnacional sin necesidad de establecer una entidad legal en el país de residencia del trabajador. Este esquema presenta una triple relación: el empleado (en nuestro caso, el artista digital), el EOR (entidad que actúa como empleador legal formal) y la empresa cliente (empleador operativo o real, quien dirige y se beneficia de la prestación de servicios).

En las situaciones en que el artista digital residente ejerce su actividad personal en otra jurisdicción, analizaremos el tratamiento fiscal de los rendimientos del trabajo dependiente de ese artista digital transnacional cuando es aplicable un Convenio para evitar la doble imposición internacional, en el marco genérico del MC OCDE (OCDE, 2019).

2.1. Aplicación del artículo 17 del Modelo de Convenio de la OCDE

El artículo 17 del MC OCDE relativo a la imposición de las rentas de artistas y deportistas se utiliza en lugar del artículo 15 del mismo Convenio relativo a la imposición de la renta del trabajo por cuenta ajena porque establece una excepción específica al régimen general de tributación de las rentas del trabajo.

En este artículo se establece una posible tributación compartida entre el Estado de residencia del perceptor de las rentas y el Estado de realización de la actividad.

Así, la renta obtenida por una persona física del ejercicio de su actividad en calidad de artista digital y la renta derivada de esa actividad realizada por el artista, aunque no se atribuya al propio artista, pueden someterse a imposición en el Estado donde se realiza la actividad y en el Estado de residencia del perceptor.

En los Comentarios al artículo 17 del MC OCDE (apartado 1, párrafo 3) ya se reconoce que «no es posible formular una definición precisa del término "artista", aunque el apartado 1 cita algunos ejemplos de personas que pueden tener esa consideración. Esta relación de ejemplos no debe considerarse exhaustiva».

En este sentido, de los propios Comentarios podemos extraer unas características básicas para tener la consideración de artista a efectos del propio artículo 17:

1. Ejercicio personal de una actividad artística por cuenta propia o por cuenta ajena.[2]

2. Existencia de un componente escénico o de espectáculo en la actividad realizada.

El término «artista» incluye a quienes actúan personalmente en actividades públicas o mediáticas.[3]

Un artista está estrechamente vinculado a una dimensión pública o performativa de la actividad que realiza (dar espectáculo).[4]

Entre las actividades del artista también se incluyen otras apariciones públicas que estén estrechamente relacionadas con la actuación artística, como entrevistas o anuncios publicitarios.[5]

Además, se incluyen actividades preparatorias que forman parte normal del desempeño del artista como ensayos, entrenamientos y desplazamientos relacionados.[6]

2. Comentarios al artículo 17, apartado 1 (1).
3. «El término "artista" comprende claramente a los artistas escénicos, los actores de cine, y a quienes actúan en un anuncio de televisión». Comentarios al artículo 17, apartado 1 (3).
4. «El artículo puede aplicarse también a las rentas generadas por actividades de carácter político, social, religioso o benéfico, cuando incorporen un elemento de espectáculo». Comentarios al artículo 17, apartado 1 (3).
5. Comentarios al artículo 17, apartado 1 (9.1).
6. «La preparación, a saber, los ensayos y el entrenamiento, forman parte de la actividad normal de los artistas (...). Si un artista (...) percibe una retribución por el tiempo que duran los ensayos, el entrenamiento o por otras actividades preparatorias en un Estado (lo que es frecuente en el caso de artistas y deportistas asalariados (...), la retribución correspondiente, así como la percibida por el tiempo que pase viajando en ese Estado para llevar a cabo las actuaciones, los ensayos y el entrenamiento (u otra preparación similar), estaría comprendida en el ámbito de este artículo». Comentarios al artículo 17, apartado 1 (9.1).

3. Basta con realizar una actividad artística en una única ocasión para ser considerado artista. No se exige profesionalidad ni habitualidad.[7]

Por el contrario, no se consideran como «artistas» a ciertos perfiles técnicos, administrativos o de apoyo, que no participan directamente en la actuación pública o mediática, aunque trabajen en la industria cultural o del espectáculo.[8]

En el caso de personas que desempeñan actividades mixtas se debe analizar la naturaleza de la actividad concreta de esa persona en el país donde tiene lugar la actuación.[9]

En definitiva, el concepto de «artista» a efectos del artículo 17.1 del MC OCDE debe entenderse en función del carácter personal, directo y público de la actividad desarrollada, siempre que esta incorpore un componente escénico o de espectáculo. La calificación no depende de la forma jurídica de la relación, sino de la naturaleza de la intervención y su proyección pública. En este sentido, se excluyen expresamente las actividades meramente técnicas, auxiliares o de producción, aunque se realicen en el entorno artístico. La aplicación del artículo 17.1 permite gravar rentas derivadas de actuaciones que generan valor económico a través de su visibilidad pública, incluso cuando estas se ejerzan de forma ocasional, desplazando así la regla de tributación en el Estado de residencia prevista en el artículo 15.2 del MC OCDE. (En relación con el concepto de artista, a estos efectos, pueden verse los trabajos de Almudí Cid y Serrano Antón, 2005; Calderón Carrero, 2007, págs. 147-151; González-Cuéllar Serrano, 2019; Magraner Moreno, 2019, págs. 14-18; Mora Pérez, 2023, págs. 199-200; Trapé Viladomat, 2014, págs. 520-524).[10]

De esta forma, el artículo 17.1 se aplica a los artistas digitales asalariados cuando hay una intervención directa y personal del artista en una actuación pública o evento digital, es decir, cuando podemos conceptuarlos como «artistas digitales del espectáculo» transnacionales.

En esta calificación, podríamos enumerar los siguientes:

- *Streamers* o creadores de contenido en directo contratados por plataformas o empresas: se dirigen a un público de forma artística o de entretenimiento en tiempo real (por ejemplo: creador que transmite e interactúa en vivo, con presencia audiovisual pública).

- *VTubers* (Virtual YouTubers) empleados por agencias: combinan actuación personal mediada tecnológicamente e interacción pública continuada (por ejemplo: intérprete que presta su voz y gestos a un avatar animado en transmisiones públicas).

7. «La referencia a "un artista (...)" engloba a toda persona que interviene en esa condición, aunque sea en una única ocasión. Así, el artículo 17 puede aplicarse a un amateur que gana un premio dotado de una cuantía económica o a una persona que, no siendo actor, percibe unos honorarios por su aparición, en una única ocasión, en un anuncio publicitario en la televisión o en una película». Comentarios al artículo 17, apartado 1 (9.1).
8. «(...) No será aplicable a un conferenciante visitante (por ejemplo, un antiguo político que percibe unos honorarios como conferenciante invitado), ni a un modelo en el ejercicio de su actividad como tal (por ejemplo, exhibiendo prendas durante un desfile de moda o en una sesión de fotos) y no como artista, ni al personal administrativo o de apoyo (por ejemplo, los operadores de cámaras en el rodaje de una película, los productores, los directores cinematográficos, los coreógrafos, el equipo técnico, los técnicos que viajan con un grupo de músicos, etc.). Entre unos y otros hay una zona ambigua en la que es necesario valorar el conjunto de las actividades de la persona en cuestión». Comentarios al artículo 17, apartado 1 (3). En la misma línea: «El simple hecho de informar sobre una actuación artística (...), o de comentarla, cuando el comentarista no participa de ella, no es asimilable a la actividad de un artista (...) que interviene en esa condición». Comentarios al artículo 17, apartado 1 (9.1).
9. Comentarios al artículo 17, apartado 1 (4).
10. n la Nota relativa a la tributación de artistas y deportistas no residentes del Departamento de Inspección Financiera y Tributaria, Oficina Nacional de Fiscalidad Internacional, de la Agencia Tributaria, de 28 de marzo de 2023, ya se remarca que mediando Convenio Fiscal la expresión artista «exigirá que en su actividad concurra la existencia de un elemento de espectáculo o diversión. Tendrán dicha consideración, por ejemplo, los actores de cine o teatro, los músicos, los *disc jockey* –DJ– o pinchadiscos, etc. (incluyendo las actividades de carácter político, social, religioso o benéfico), cuando incorporen un elemento de diversión o espectáculo. Mediando dicho elemento de espectáculo público celebrado en territorio español, podrían incluirse en esta categoría diversas actividades realizadas por no residentes que han surgido con el desarrollo de nuevas tecnologías y el uso de las denominadas redes sociales. Así, el término «artistas» a estos efectos difiere del significado usual del vocablo que abarcaría también, por ejemplo, a pintores, escultores o artistas plásticos. Es criterio unánimemente sostenido que los artistas plásticos cuyas obras se destinan normalmente a la venta no se incluyen en esta disposición, al no concurrir una actividad personal, prestada ante una audiencia, con una finalidad de entretenimiento y un elemento de espectáculo».

- Presentadores de eventos digitales en directo, como galas, lanzamientos o espectáculos: ejecutan de forma personal, directa y pública un rol con función de espectáculo (por ejemplo: persona que presenta en directo un evento virtual desde su domicilio).

- Ilustradores o artistas visuales que participan en eventos online en vivo: ejecutan una forma artística con interacción directa (por ejemplo: *live drawing* contratado por plataformas, en el que el artista dibuja en directo con interacción del público).

- *Performers* digitales en festivales o exposiciones virtuales: realizan un espectáculo en directo, aunque mediado por tecnologías digitales (por ejemplo: artista multimedia que realiza una danza digital durante un festival retransmitido).

- Actores o actrices en teatro o cine digital en *streaming*: actúan en directo, aunque el medio sea exclusivamente digital (por ejemplo: actor contratado por una compañía para representar una obra emitida virtualmente).

- Artistas visuales que hacen sesiones en vivo o tutoriales interactivos contratados por marcas: realizan un elemento escénico y de proyección personal ante el público (por ejemplo: ilustrador digital que realiza una «masterclass en vivo» promocionada por una empresa).

- Coreógrafos o bailarines que realizan actuaciones virtuales en directo: hacen una performance artística visible por el público en tiempo real (por ejemplo: bailarín contratado para un espectáculo transmitido desde su estudio).

- Artistas de *performance* digital o arte multimedia interactivo online: ejecutan un acto performativo emitido en directo con participación o exposición pública (por ejemplo: *performer* que hace instalaciones interactivas en vivo por encargo de una entidad cultural).

- Artistas de *spoken word*, poesía o narración oral en directo: interpretan en público con componente escénico y expresivo (por ejemplo: persona que hace lecturas o actuaciones literarias por *streaming* en eventos contratados).

- Artistas digitales interactivos de experiencias inmersivas en directo (holografía remota): creación artística en vivo y dirigida al público (por ejemplo: artista visual contratado por una empresa tecnológica para desarrollar y ejecutar en tiempo real performances holográficas inmersivas que se proyectan simultáneamente en eventos internacionales).

- Narradores digitales de realidad extendida en experiencias literarias inmersivas: actúan de forma escénica personalizada y en tiempo real mediante tecnologías inmersivas (por ejemplo: actriz contratada por una empresa cultural para prestar su voz, expresividad facial y gestualidad mediante captura remota, como narradora interactiva en experiencias de realidad virtual y mixta organizadas por festivales internacionales).

En todos estos casos, aunque el artista digital trabaje desde su país de residencia y no se desplace físicamente, a través del artículo 17.1, se permite gravar también al Estado contratante donde se ejercita la actividad personal, es decir, por ejemplo, donde se proyecta o recibe públicamente la actuación.

De esta manera, ante un artista holográfico residente en España, que trabaja físicamente en España, pero que su actuación se proyecta en un festival digital en otro país, esta Jurisdicción puede gravar la parte de la renta atribuible a la actividad personal desarrollada en su territorio.

La renta puede gravarse incluso si no se paga directamente al artista.

Si el artista está contratado por una empresa o agencia (por cuenta ajena), y la renta se canaliza a través de esta entidad, el artículo 17.2 permite igualmente gravar las rentas al Estado donde se realiza la actividad.

Por último, cuando un mismo artista digital realiza la actividad personal para varios países desde su lugar de residencia, se debe atribuir proporcionalmente la renta generada en cada Estado, en función del número de actuaciones, visualizaciones o contratos vinculados.

En definitiva, el artículo 17 del MC OCDE prevalece sobre el artículo 15 del mismo Modelo cuando haya actividad pública escénica digital.[11]

No obstante, el mismo artista digital puede diseñar estrategias para desvirtuar la aplicación del art. 17 del MC OCDE y que sea aplicable el artículo 15.2 del mismo Modelo (para no tributar en la Jurisdicción donde se realiza la actividad artística).

La clave está en eliminar la presencia de la actividad personal, creativa y remunerada como espectáculo en el entorno digital o la realidad virtual. En particular:

- Evitar el carácter público, escénico y personal de la actividad, limitándola a la producción de contenidos pregrabados, técnicos o sin interacción en directo con el público (por ejemplo, entregando animaciones o grabaciones editadas que se usarán posteriormente, pero sin intervenir en eventos en vivo).

- Evitar la ejecución personal directa en eventos públicos (por ejemplo, la actuación pública en un evento digital la realiza otra persona o equipo, mientras el artista realiza tareas de soporte desde su domicilio (diseño, postproducción, etc.). El artista actúa como técnico o creador sin presencia escénica (personal administrativo o de apoyo). Asimismo, eliminar o limitar la interacción de cualquier forma con el público.

- Estructurar la actividad como trabajo interno sin difusión inmediata. Actividad técnica creativa, no escénica ni dirigida directamente al público. Los contenidos del artista digital deben ser utilizados como parte de un producto mayor (por ejemplo, un videojuego o una película que no implique su presentación pública directa).

- No vincular las rentas a actuaciones públicas concretas. Estructurar el contrato de trabajo como un sueldo fijo, no asociado a eventos específicos o emisiones públicas (por ejemplo, el salario cubre tareas continuas de producción digital, sin existencia de remuneraciones por participación en directos).

Así, por ejemplo, un diseñador digital residente en España que trabaje como asalariado de una empresa residente en Argentina, diseñando trajes digitales para videojuegos, sin participar en eventos, podrá aplicar el artículo 15 del MC OCDE si demuestra que no hay espectáculo, no hay presencia física y es un trabajo técnico y continuo.

2.2. Aplicación del artículo 15 del Modelo de Convenio de la OCDE

2.2.1. Modelo de contratación directa trasnacional del artista digital por parte de un empleador operativo situado en otra Jurisdicción

El artista digital firma directamente con el empleador operativo, que está situado en una Jurisdicción distinta a la del teletrabajador, pero no hay intermediarios.

La relación laboral se establece directamente entre el empleador y el trabajador; el empleador es responsable de todas las obligaciones laborales, fiscales y de seguridad social, según la normativa del país de residencia del trabajador.

El artículo 15 del MC OCDE se aplica a la mayoría de los artistas digitales por cuenta ajena cuya actividad es interna o técnica, como un diseñador de videojuegos contratado por una empresa o un ilustrador que hace material para marketing sin aparecer públicamente.

El apartado 1 del artículo 15 del MC OCDE establece la regla general aplicable a la imposición de la renta del trabajo por cuenta ajena conforme a la que esta renta es gravable en el Estado donde se ejerza.

A este respecto, el párrafo 1 de los Comentarios al artículo 15 del MC OCDE, relativo a la imposición de la renta del trabajo dependiente, establece que: «El trabajo por cuenta ajena se ejerce en el lugar donde el empleado esté físicamente presente cuando realiza las actividades por las que se paga la renta correspondiente. Como consecuencia de ese principio, un residente de un Estado contratante que perciba una retribución, por razón de un trabajo por cuenta ajena, de fuentes situadas en el otro Estado, no puede estar sujeto a imposición en ese otro Estado respecto de dicha retribución por el mero hecho de que los resultados de su trabajo se exploten en ese otro Estado».

11. En la monografía de Toribio Bernández (2020), en el capítulo V, se tratan diferentes propuestas doctrinales sobre reforma (o supresión) del artículo 17 del Modelo de Convenio de la OCDE y la posición de dicho autor para la optimización de su aplicación en la práctica.

En consecuencia, las rentas percibidas por un residente de un Estado mediante el sistema de teletrabajo, sólo se pueden sujetar a gravamen en el Estado de residencia donde se ejerce el trabajo de forma remota, siendo irrelevante que los frutos de dicho trabajo se obtengan en otras jurisdicciones (en este sentido, las Consultas Vinculantes de la Subdirección General de Fiscalidad Internacional: V1451-14, de 30/5/2014; V0686-15, de 3/3/2015; V1305-15, de 28/4/2015; V1952-16, de 6/5/2016; V3794-16, de 9/9/2016; V2852-17, de 3/11/2017; V3286-17, de 27/12/2017; V0597-20, de 16/3/2020; V2960-21, de 22/11/2021; V0066-22, de 18/1/2022; V1162-22, de 26/5/2022; V2440-22, de 25/11/2022; V2614-22, de 23/12/2022; V2631-22, de 27/12/2022; V1277-23, de 16/5/2023; V2790-23, de 16/10/2023; V2883-23, de 26/10/2023; V3326-23, de 28/12/2023; V3328-23, de 28/12/2023; V0162-24, de 19/2/2024; y las Consultas Vinculantes de la Subdirección General de Impuestos sobre la Renta de las Personas Físicas: V3945-15, de 10/12/2015; V0906-17, de 11/4/2017; V1908-17, de 18/7/2017; V2621-20, de 3/8/2020; V194-21, de 8/2/2021; V1040-21, de 21/4/2021; V0355-22, de 24/2/2022; V1265-22, de 6/6/2022; V2223-22, de 25/10/2022; V0057-23, de 17/1/2023; V2334-24, de 11/11/2024).

En relación con el teletrabajo y la necesaria reforma del artículo 15 del MC OCDE, pueden verse los magníficos trabajos de Escribano (2024, págs. 405-414) y Rovira Ferrer (2024a, págs. 514-527, 2024b, págs. 457-474).

En cualquier caso, actualmente, las rentas obtenidas por un artista digital que realiza su actividad artística en modalidad de teletrabajo, sin estar vinculado al ámbito del espectáculo y con presencia física en un Estado determinado, solo podrán ser gravadas en dicho Estado.

2.2.2. Modelo *Employer of Record*: artista digital contratado por una empresa intermediaria situada en una tercera Jurisdicción

En el contexto de estructuras de empleo internacional, como el modelo denominado *Employer of Record* (EOR), es frecuente que el artista digital pueda estar formalmente contratado por una entidad situada en una tercera jurisdicción, distinta tanto del Estado de residencia del trabajador como del Estado del cliente o empleador operativo. No obstante, en la práctica, es este último –el cliente– quien asume las funciones sustantivas propias del empleador: determina las tareas a realizar, supervisa los resultados, proporciona los medios técnicos para la ejecución del trabajo digital e incluso integra funcionalmente al trabajador en su estructura organizativa.

En aquellos supuestos en los que el artista digital presta servicios a favor de una empresa ubicada en otra Jurisdicción, pero desarrolla su actividad íntegramente desde su Estado de residencia, sin desplazarse físicamente a la jurisdicción del cliente, la renta obtenida queda, en principio, sujeta exclusivamente a imposición en el Estado de residencia. Esta regla se deriva directamente del artículo 15.1 del MC OCDE, que atribuye al Estado de residencia del trabajador la potestad tributaria exclusiva sobre las rentas del trabajo dependiente, siempre que el empleo no se ejerza en el otro Estado contratante.

Por tanto, mientras la actividad laboral digital –aunque realizada por encargo de una entidad extranjera– se realice exclusivamente desde el territorio del trabajador, sin presencia física en el Estado del cliente, no se genera el nexo territorial necesario que justifique la intervención fiscal de la otra jurisdicción.

Sin embargo, esta situación se ve alterada cuando el artista digital se desplaza físicamente al Estado del cliente para ejercer su actividad profesional, aunque sea de forma temporal. En estos casos, el artículo 15.2 del MC OCDE introduce una excepción que habilita al Estado de la fuente para gravar la renta del trabajador, siempre que no se cumplan conjuntamente los tres requisitos que establece:

a) que la presencia física del artista digital en el Estado de la fuente no exceda los 183 días en un período de doce meses;

b) que el pagador, o aquel por cuenta de quien se paguen las retribuciones al artista digital, sea un empleador no residente del otro Estado; y

c) que las retribuciones no corran a cargo de un establecimiento permanente que el empleador tenga en el otro Estado.

La interpretación y aplicación del requisito b) ha dado lugar al desarrollo del concepto de «empleador económico», una figura no recogida explícitamente en el articulado del Modelo, pero ampliamente recogida en sus Comentarios como herramienta antiabuso.

Con esta figura se intenta evitar que estructuras contractuales artificiales, mediante el uso de entidades interpuestas sin sustancia económica real, conduzcan a una asignación incorrecta de la potestad tributaria. El objetivo es identificar a la entidad que, en términos sustanciales, se comporta como el verdadero empleador del artista digital desplazado.

En este sentido, es evidente que en este tipo de situaciones de obtención de rentas transnacionales debe atenderse a la figura del «empleador con enfoque económico», y no solo a la figura del empleador formal, para determinar la Jurisdicción a la que debe atribuirse la potestad tributaria (véase, al respecto, Aguas Alcalde, 2003, págs. 164-165; Álvarez Barbeito y Calderón Carrero, 2010, págs. 193-199; Calderón Carrero, 2014, págs. 495-499; Carmona Fernández, 2020, págs. 81-83; Jiménez-Valladolid y Vega Borrego, 2013, págs. 188-195; Lang, 2014, págs. 57-66; López López, 2015, págs. 75-80; o Vega Borrego, 2019, págs. 1011-1013).

Los párrafos 8 a 8.14 de los Comentarios al artículo 15 del MC OCDE proporcionan una guía detallada sobre cómo identificar al empleador económico.

El párrafo 8.1, en particular, ya advierte de la dificultad que puede surgir para distinguir si los servicios prestados por una persona física en un determinado Estado deben encuadrarse como trabajo dependiente (artículo 15) o como actividad empresarial independiente (artículo 7).

Asimismo, el párrafo 8.4 señala que muchos Estados aplican criterios normativos o jurisprudenciales –como la sustancia económica– para determinar si existe realmente una relación laboral, más allá del ropaje jurídico formal.

En este sentido, el principio de la «primacía del fondo sobre la forma» se utiliza para determinar quién es el empleador efectivo y la Jurisdicción tributaria real aplicable. De modo especial, los párrafos 8.13 y 8.14 enumeran los factores clave para identificar la existencia de una verdadera relación de dependencia laboral con la empresa beneficiaria de los servicios.[12]

Estos criterios permiten establecer que, en presencia de una entidad que actúa como cliente en el Estado de la fuente y que cumple las funciones propias del empleador, dicha entidad debe considerarse el empleador económico a efectos del artículo 15.2.b.

En consecuencia, cuando se constata que el cliente ubicado en el Estado de la fuente ejerce el control operativo, proporciona los medios, integra al trabajador en su organización y se beneficia del resultado del trabajo, se entiende que asume el papel de empleador económico, lo que implica el incumplimiento del requisito de residencia previsto en el artículo 15.2.b. Por tanto, el Estado de la fuente queda habilitado para gravar la remuneración correspondiente al período de actividad ejercida en su territorio, al haberse roto la cadena de requisitos que impediría su intervención tributaria.

La entidad que, con independencia de la existencia de una relación contractual formal, sea considerada como empleadora del artista digital a efectos tributarios, por ser quien en la práctica ejerce el control directo y efectivo sobre el trabajo del artista digital, asume los riesgos y responsabilidades vinculados a la ejecución de su trabajo, se beneficia económicamente del resultado de los servicios artísticos prestados, y soporta los costes derivados de su contratación, determinará la tributación real del artista digital.

Un ejemplo ilustrativo de esta situación es el de un artista digital residente en España que desarrolla tareas de diseño visual y animación interactiva para una empresa tecnológica con sede en Estados Unidos, especializada en videojuegos

12. En el párrafo 8.13 se resalta que «resultará clave dirimir qué empresa asume la responsabilidad o el riesgo respecto de los resultados generados por el trabajo de la persona física». A continuación, en el párrafo 8.14 se señala que cuando la comparación de la naturaleza de los servicios prestados por la persona física con la actividad económica ejercida por su empleador formal y por la empresa a la que se prestan los servicios revele una relación de trabajo por cuenta ajena que difiere de la relación contractual formal, los factores adicionales que siguen pueden ayudar a determinar si este es realmente el caso: quién está facultado para dar instrucciones a la persona física en relación con el modo en que debe realizarse el trabajo; quién controla el lugar en el que se lleva a cabo el trabajo y es responsable de él; el empleador formal factura la retribución percibida por la persona física directamente a la empresa a la que se prestan los servicios; quién pone a disposición del trabajador las herramientas y materiales necesarios; quién determina el número de personas que van a desarrollar el trabajo y su cualificación; quién está facultado para elegir a la persona física que ejecutará el trabajo y para poner fin a los acuerdos contractuales acordados con el trabajador a ese fin; quién está facultado para imponer medidas disciplinarias en relación con el trabajo efectuado por esa persona física; quién determina los períodos de vacaciones y el plan de trabajo de esa persona física.

y experiencias inmersivas. En este caso, el trabajador está formalmente contratado por una empresa EOR establecida en Irlanda, que actúa como empleador legal en nombre de la empresa estadounidense, facilitando la contratación de personal en jurisdicciones en las que esta última no dispone de estructura física ni presencia directa.

El artista digital desarrolla toda su actividad profesional desde su domicilio habitual en territorio español, empleando sus propios recursos informáticos y accediendo a las plataformas digitales proporcionadas por la empresa estadounidense. No ha viajado nunca a Estados Unidos ni ha prestado servicios de forma presencial en dicho país. Las instrucciones de trabajo, el seguimiento del desempeño, la revisión de entregables, el calendario de producción y el control de calidad proceden directamente de los responsables técnicos de la empresa americana. Si bien la remuneración mensual es abonada por la entidad EOR residente en Irlanda, los fondos utilizados provienen de la empresa estadounidense, que además deduce dichos importes como gasto operativo en su contabilidad empresarial.

Con base en el artículo 15.1 del MC OCDE, la renta derivada del trabajo dependiente del residente en España se encuentra sujeta exclusivamente a imposición en España, siempre que el empleo no se ejerza en el otro Estado contratante, en este caso Estados Unidos.

En este supuesto, el residente en España no se desplaza físicamente a EE.UU. en ningún momento, por lo que no existe ejercicio del empleo en el Estado de la fuente en los términos exigidos por el artículo 15.1. Por tanto, no procede activar la excepción prevista en el artículo 15.2, ya que no se da la premisa fáctica de presencia territorial en la jurisdicción del cliente.

No obstante, si se hipotetizara una situación futura de desplazamiento temporal del trabajador a Estados Unidos (por ejemplo, para participar en una feria sectorial, colaborar *in situ* en un proyecto o integrarse en un equipo local por un período determinado), la determinación del verdadero empleador se convertiría en un elemento clave para resolver la atribución de la potestad tributaria. A pesar de que el vínculo contractual formal se haya suscrito con una empresa irlandesa (la EOR), diversos indicios objetivos (como el control efectivo del trabajo, la dirección funcional, la integración operativa del trabajador, el beneficio económico directo y la asunción del coste salarial) apuntan inequívocamente a que la empresa estadounidense ostenta la condición de empleador económico.

De acuerdo con los párrafos 8 a 8.14 de los Comentarios al artículo 15 del MC OCDE, y especialmente con los criterios funcionales establecidos en el párrafo 8.13, esta empresa debe ser considerada el verdadero empleador del artista digital a efectos fiscales. Por tanto, si el trabajador viajara a Estados Unidos por un período superior a 183 días, o si la empresa estadounidense tuviera en España un establecimiento permanente que soportara los costes salariales, se incumplirían los requisitos del artículo 15.2, y el Estado de la fuente –en este caso, Estados Unidos– quedaría habilitado para gravar la renta correspondiente a la parte del empleo efectivamente ejercido en su territorio.

Este supuesto refleja cómo la aplicación del concepto de empleador económico y la atención a la realidad sustancial de la relación laboral resultan determinantes para asignar correctamente la potestad tributaria, evitando tanto la doble imposición como la erosión artificial de la base imponible.

En definitiva, la figura del empleador económico se revela, así, como un criterio sustantivo esencial para garantizar una distribución justa de la potestad tributaria entre jurisdicciones. En sectores especialmente propensos al uso de estructuras contractuales flexibles, como el del trabajo artístico digital, los servicios artísticos creativos o las tecnologías de la información aplicadas al proceso creativo, este enfoque resulta crucial para prevenir la erosión de bases imponibles mediante esquemas de planificación fiscal agresiva.

Conclusiones

La digitalización de la creación artística ha disuelto muchas de las fronteras que tradicionalmente separaban la actividad cultural local de la internacional, y también ha difuminado los límites jurídicos entre lo escénico y lo técnico, lo presencial y lo virtual, lo individual y lo colectivo. En este nuevo escenario, el artista digital no solo es un sujeto creativo, sino también un contribuyente transfronterizo complejo, cuya tributación exige una interpretación flexible y material de las normas convencionales vigentes.

La evolución de las prácticas artísticas y la digitalización de los entornos creativos obligan a adoptar una lectura

funcional, tecnológica y finalista del artículo 17 del MC OCDE. Esta norma, concebida en un contexto analógico, debe reinterpretarse conforme al principio de neutralidad tecnológica, extendiendo su ámbito de aplicación a aquellas manifestaciones contemporáneas del arte digital que, aunque desmaterializadas y remotas, mantienen los elementos esenciales que justifican su tributación en la fuente: actuación personal, componente escénico y proyección pública. La actividad artística ya no requiere un escenario físico, sino un entorno digital interactivo en el que el artista actúa, se relaciona con el público y genera valor económico en una jurisdicción distinta a aquella en la que se encuentra físicamente. Esta circunstancia permite aplicar legítimamente el artículo 17 incluso en ausencia de desplazamiento, reconociendo que la actividad escénica tiene lugar, tributariamente, allí donde se recibe y se remunera.

El despunte de perfiles como los *streamers* contratados por plataformas, los *performers* virtuales, los narradores en realidad aumentada o los artistas de experiencias inmersivas con intervención en tiempo real demuestra que el espectáculo digital transnacional es una realidad consolidada que encaja plenamente en la lógica del artículo 17. En estos casos, la renta derivada de tales actuaciones debe poder ser gravada por el Estado fuente, como contrapartida a la utilización de su mercado y a la captación de audiencia y rentabilidad dentro de su territorio. Esta línea interpretativa protege la soberanía fiscal del Estado donde el espectáculo se visualiza, evitando la erosión de su base imponible mediante estructuras artificiales de desconexión territorial.

Sin embargo, esta misma digitalización abre la puerta a estructuras laborales o contractuales que permiten, de forma lícita, desvirtuar la aplicación del artículo 17 y desplazar la calificación a la del artículo 15. Cuando la actividad desarrollada por el artista digital carece de un componente escénico, se limita a tareas técnicas de producción o diseño sin intervención pública y no hay interacción en directo ni vínculo entre la renta y una actuación visible, el marco de imposición debe ser el previsto para el trabajo por cuenta ajena. Este es el caso de diseñadores de videojuegos, compositores para entornos sonoros sin visibilidad personal, ilustradores técnicos o programadores de IA artística sin exposición escénica. La clave radica en demostrar que la actividad, aunque creativa, no es un espectáculo ni se presenta ante un público como tal.

En este sentido, la estructura contractual, el contenido efectivo de la prestación, la forma de retribución y la ausencia de proyección pública permiten construir estrategias sólidas para aplicar el artículo 15 y excluir la tributación en el Estado fuente, siempre que se respeten los requisitos materiales previstos en el MC OCDE. Estas estrategias son especialmente relevantes en contextos de teletrabajo transnacional, en los que el artista trabaja íntegramente desde su país de residencia y no existe presencia física ni relación con un establecimiento permanente en la jurisdicción del empleador. La delimitación entre ambos artículos, por tanto, no puede hacerse de forma abstracta, sino caso por caso, atendiendo a la sustancia de la relación y a la verdadera naturaleza de la actividad artística.

El auge del modelo *Employer of Record* ha introducido nuevos retos para la asignación de la potestad tributaria, ya que en estos esquemas el empleador formal puede diferir del empleador económico real. La aplicación del principio de sustancia sobre forma muestra que la verdadera residencia fiscal del empleador debe determinarse según quién controla, dirige y se beneficia del trabajo del artista. Esta interpretación es clave para evitar el abuso de estructuras interpuestas y garantizar una tributación coherente con la realidad económica. En los sectores creativos digitalizados, en los que la movilidad física es escasa, pero la movilidad de los efectos económicos es elevada, la figura del empleador económico se convierte en un instrumento esencial para preservar la integridad de los convenios tributarios bilaterales.

Todo lo anterior evidencia la necesidad de actualizar y armonizar los convenios de doble imposición para que reflejen adecuadamente la realidad del trabajo artístico digital. Resulta recomendable que las Jurisdicciones Parte incorporen cláusulas interpretativas o protocolos específicos que aclaren la aplicación del artículo 17 a actuaciones digitales sin presencia física, reconociendo expresamente que la actuación artística puede tener lugar, a efectos tributarios, en el territorio donde se recibe y visualiza públicamente, independientemente del lugar desde el que se ejecuta. Una cláusula modelo podría establecer que «a los efectos del artículo 17, se entenderá que la actividad artística se realiza en el territorio de un Estado contratante cuando, aun en ausencia de desplazamiento físico, la actuación personal del artista sea difundida en tiempo real al público situado en dicho Estado, mediante medios digitales o tecnológicos que permitan su recepción directa».

La clarificación normativa contribuiría a garantizar la seguridad jurídica de los artistas digitales, a prevenir la doble imposición y a ofrecer a las administraciones fiscales criterios uniformes para la calificación y distribución de rentas en escenarios de teletrabajo transnacional. Esta modernización del sistema fiscal internacional resulta urgente si se quiere responder con eficacia a la transformación estructural de las industrias culturales y creativas en la era digital, sin obstaculizar la movilidad artística ni la innovación tecnológica.

Referencias bibliográficas

AGUAS ALCALDE, E. (2003). *Tributación internacional de los rendimientos de trabajo*. Thomson Aranzadi.

ALMUDÍ CID, J. M.; SERRANO ANTÓN, F. (2005). «La fiscalidad internacional de los artistas y deportistas: especial referencia al artículo 17 del MCOCDE». *Revista Aranzadi de Derecho de Deporte y Entretenimiento*, n.º 13.

ÁLVAREZ BARBEITO, P.; CALDERÓN CARRERO, J. M. (2010). *La tributación en el IRPF de los trabajadores expatriados e impatriados*. Netbiblo. DOI: https://doi.org/10.4272/978-84-9745-448-3

CALDERÓN CARRERO, J. M. (2007). «La tributación de los artistas (y deportistas) no residentes en el marco de los convenios de doble imposición». *Fiscalidad del no residente: aspectos conflictivos*, págs. 137-161. CISS.

CALDERÓN CARRERO, J. M. (2014). «Trabajos dependientes». *Convenios Fiscales Internacionales y Fiscalidad de la Unión Europea*, págs. 483-508. Wolters Kluwer CISS.

CARMONA FERNÁNDEZ, N. (2020). *Medidas antiabuso y Convenios sobre doble imposición*. Francis Lefebvre.

ESCRIBANO, E. (2024). «A New Model Tax Convention for a World of Increasing Remote Work and Mobility of Individuals». *World Tax Journal*, vol. 16, n.º 2, págs. 379-416. DOI: https://doi.org/10.59403/3e87wy9

GONZÁLEZ-CUÉLLAR SERRANO, M. L. (2019). *El Estatuto fiscal del artista*. La cultivada.

JIMÉNEZ-VALLADOLID DE L´HOTELLERIE-FALLOIS, D. J.; VEGA BORREGO, F. A. (2013). «Algunos aspectos fiscales del desplazamiento internacional de trabajadores». *RJUAM*, n.º 28, págs. 177-195.

LANG, M. (2014). *Introducción al Derecho de los Convenios para evitar la doble imposición*. Editorial Temis, IBFD.

LÓPEZ LÓPEZ, H. (2015). *Régimen fiscal de los trabajadores desplazados al extranjero*. Thomson Reuters Aranzadi.

MAGRANER MORENO, F. J. (2019). *La imposición sobre las rentas obtenidas en España por artistas y deportistas*. Editorial Tirant Lo Blanch.

MATA SIERRA, M. T. (2024). «La incidencia del teletrabajo en el Impuesto sobre la Renta de las Personas Físicas». *Nuevos problemas y nuevas soluciones en teletrabajo transfronterizo*, págs. 391-419. Aranzadi.

MORA PÉREZ, J. (2023). «La tributación de artistas y deportistas en el MCOCDE». *Cuadernos de Formación IEF*, n.º 29.

MORIES JIMÉNEZ, M. T. (2023). *Fiscalidad del teletrabajo*. Editorial Tirant Lo Blanch.

OECD (2019). *Modelo de Convenio Tributario sobre la Renta y sobre el Patrimonio: Versión Abreviada 2017*.

ROVIRA FERRER, I. (2023). *La fiscalidad del trabajo a distancia*. Thomson Reuters Aranzadi.

ROVIRA FERRER, I. (2024a). «A New Scenario in International Tax Law: Two Proposals to Rethink the OECD Model in Response to the Generalization of Distance Work by Employees». *World Tax Journal*, vol. 15, n.º 3, págs. 509-541.

ROVIRA FERRER, I. (2024b). «La necesaria reformulación del art. 15 del MCOCDE ante el trabajo a distancia». *La atención a la juventud en el sistema tributario: Medidas fiscales de apoyo directo o indirecto al colectivo joven*, págs. 457-474. DOI: https://doi.org/10.59403/wh5spm

TORIBIO BERNÁNDEZ, L. (2020). *Tributación de futbolistas y clubes de fútbol en los convenios para evitar la doble imposición*. Aranzadi.

TRAPÉ VILADOMAT, M. (2014). «Rentas de artistas y deportistas». *Convenios Fiscales Internacionales y Fiscalidad de la Unión Europea*, págs. 519-539. Wolters Kluwer CISS.

VEGA BORREGO, F. A. (2019). *Rendimientos del trabajo y convenios para evitar la doble imposición. Fiscalidad Internacional (I)*, págs. 993-1094. CEF.

Cita recomendada

URQUIZU CAVALLÉ, Ángel (2026). «Los artistas digitales en régimen de teletrabajo transnacional: una reinterpretación tributaria a la luz de la transformación cultural digital». En: Irene Rovira Ferrer (coord.). «Sobre la consolidación del trabajo a distancia». *IDP. Revista de Internet, Derecho y Política*, núm. 44. UOC. [Fecha de consulta: dd/mm/aa]. DOI: http://dx.doi.org/10.7238/idp.v0i44.433199

Sobre el autor

Ángel Urquizu Cavallé
Universitat Rovira i Virgili
angel.urquizu@urv.cat
ORCID: https://orcid.org/0000-0003-3361-356X

Catedrático de Universidad del área de Derecho Financiero y Tributario. Director de la Cátedra Fundación Aduanera – URV de Estudios Aduaneros. Director del máster de Derecho Aduanero de la URV. Coordinador de la oferta formativa de negocios y lengua española de la URV, para universidades chinas. Investigador principal (1) del proyecto de I+D del Ministerio de Ciencia, Innovación y Universidades: «Descarbonización, energías renovables y ESG: El hidrogeno verde. Impulso de una agenda fiscal y económica sostenible» (PID2024-155367OB-I00). Autor de más de 120 publicaciones científicas. Impartición de docencia y realización de estancias de investigación en más de 30 universidades nacionales e internacionales.

IDP
REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Monográfico: «Sobre la consolidación del trabajo a distancia» (coord.: Irene Rovira Ferrer)

La atracción de teletrabajadores internacionales en el marco del régimen español de impatriados y sus posibles controversias jurídico-fiscales

Daniel Santiago Marcos
Universitat de Girona

Fecha de presentación: agosto 2025
Fecha de aceptación: octubre 2025
Fecha de publicación: marzo 2026

Resumen

El presente artículo analiza el régimen español de impatriados, regulado en el artículo 93 de la LIRPF y actualizado en 2022. Se trata de un régimen concebido para atraer talento internacional mediante un tratamiento fiscal preferencial. En este contexto, los teletrabajadores internacionales representan una oportunidad para dinamizar la economía y favorecer la retención de profesionales altamente cualificados. No obstante, las medidas adoptadas por el legislador español en esta materia también generan nuevos escenarios que ponen a prueba la competencia fiscal en un ámbito aún desconocido y poco considerado por las instituciones internacionales y europeas, como son las rentas obtenidas por las personas físicas en contextos digitales y el posible aprovechamiento indebido de ventajas fiscales. En paralelo, se evidenciará que la inclusión del teletrabajo internacional en el régimen español de impatriados podría desnaturalizar el concepto de residencia fiscal e incrementar las desigualdades frente al resto de residentes fiscales debido a las diferencias en su tributación.

Palabras clave

teletrabajo internacional; impatriados; competencia fiscal; residencia fiscal

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Attracting international teleworkers under the Spanish regime for impatriates and its potential legal and tax controversies

Abstract

This article analyses the Spanish expatriate regime, regulated in Article 93 of the Personal Income Tax Law (LIRPF) and updated in 2022. This regime is designed to attract international talent through preferential tax treatment. In this context, international teleworkers represent an opportunity to stimulate the economy and promote the retention of highly skilled professionals. However, the measures adopted by the Spanish legislator in this sphere also create new scenarios that challenge tax competition in a relatively unexplored and underconsidered area by international and European institutions: income earned by individuals in digital environments and the potential abuse of tax advantages. Additionally, it will be demonstrated that including international teleworking within the Spanish expatriate regime could distort the concept of tax residency and increase inequalities among tax residents due to disparities in their taxation.

Keywords

international teleworking, impatriates, tax competition, tax residence

1. Los desafíos del actual mercado de trabajo y la necesidad de teletrabajadores internacionales

El mercado de trabajo español se enfrenta a grandes cambios procedentes de la digitalización, la transición ecológica y los cambios demográficos. El futuro que nos aguarda plantea importantes retos, pero también abre oportunidades que países como España están aprovechando para mejorar su competitividad internacional. En este sentido, el *Informe sobre el futuro del empleo 2025*, elaborado por el World Economic Forum, subraya un importante crecimiento del empleo en sectores digitalizados. Sin embargo, al igual que señala el Banco de España, persiste un obstáculo significativo: el 45,8 % de las empresas perciben un problema de disponibilidad de mano de obra cualificada (Férnandez Cerezo e Izquierdo, 2025, pág. 8). En la misma línea, el Servicio Público de Empleo Estatal (SEPE) en su informe *El ajuste de la oferta y la demanda de empleo en el mercado de trabajo. 2025*, indica que las actividades profesionales, científicas y técnicas concentran un 11,30 % de las vacantes de difícil cobertura, debido fundamentalmente a la falta de cualificación y formación adecuada.

Ante esta realidad, el legislador español ha tratado de dar una respuesta a las necesidades expuestas a través de la Ley 28/2022, de 21 de diciembre, de fomento del ecosistema de las empresas emergentes (Ley 28/2022). Su preámbulo apuesta por un mercado laboral digitalizado y, en consecuencia, por el impulso del teletrabajo. Las empresas se benefician de esta modalidad, aunque es cierto que sin un marco normativo adecuado no es posible gestionar los avances. En este sentido, la Ley 28/2022 ha introducido modificaciones fiscales, entre ellas las relativas al régimen de impatriados, en el que el teletrabajo internacional es clave para la atracción de talento. De esta manera, el teletrabajo internacional queda reflejado como circunstancia en el artículo 93 de la Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas (LIRPF), que regula el actual régimen de impatriados.

La flexibilidad que ofrece el teletrabajo ha favorecido la aparición de los denominados *nómadas digitales*, trabajadores que, por el modelo de trabajo al que están acogidos, son capaces de prestar sus servicios –por cuenta propia o ajena– desde cualquier lugar. Diversos estudios sitúan a España entre los países mejor posicionados para ofrecer las mejores condiciones para los nómadas digitales y, por ende, para los teletrabajadores internacionales.[1]

1. Véase el estudio realizado por NordLayer sobre los mejores países para realizar teletrabajo https://nordlayer.com/global-remote-work-index/. [Fecha de consulta: 20 de agosto de 2025]. España se sitúa en la cuarta posición, por debajo de Dinamarca, Holanda y Alemania. Los criterios utilizados son variados: nivel de ciberseguridad, seguridad económica, infraestructura digital, entre otros.

Tras la entrada en vigor de la Ley 28/2022 no solo se han introducido mejoras en el ámbito fiscal –aunque algunas de ellas resultan criticables, como se analizará más adelante–, sino que también se ha tratado de consolidar un nuevo ecosistema de emprendimiento e innovación, cuyo punto de inflexión, como es sabido, se produjo a raíz de la pandemia de 2020.

Esta evolución ha dado lugar a un escenario internacional en el que muchos países compiten por diseñar regímenes adaptados a las nuevas dinámicas del mercado de trabajo, con el objeto de atraer a nuevos residentes fiscales. Prueba de ello es que el diario británico *The Guardian*, en una de sus portadas, se refirió al régimen español con el siguiente titular: «Trabajar al sol, disfrutar de un coste de la vida menor y menos impuestos». España, sin duda, reúne todas las cualidades para crear ese clima tan deseado para los teletrabajadores internacionales.

No obstante, desde la perspectiva fiscal, la competitividad internacional entre países, incluida España, exige una reflexión sobre las medidas introducidas para atraer a teletrabajadores internacionales. Como ya se ha señalado, en el marco del artículo 93 de la LIRPF, el legislador ha considerado oportuno incluir expresamente a esta modalidad de trabajadores entre las circunstancias que permiten acceder a un régimen tributario más favorable durante el proceso de adquisición de la residencia fiscal. Si bien estas disposiciones tienen una legitimidad evidente, no están exentas de controversias, pues surgen nuevos problemas jurídicos que se superponen a las históricas disputas relacionadas, en particular, con la definición del concepto de residencia fiscal, que constituye, o así debería, el objetivo central de los teletrabajadores internacionales.

2. La histórica problemática en materia de residencia fiscal de las personas físicas

La atracción de talento en los teletrabajadores internacionales se vincula directamente con la residencia fiscal, que constituye el nexo entre el elemento subjetivo del hecho imponible y el territorio. Este nexo se analiza en función de unas circunstancias fácticas, lo que reviste especial importancia en el régimen de impatriados del artículo 93 de la LIRPF, en un contexto marcado por la creciente competitividad fiscal entre sistemas impositivos.

En primer término, el artículo 8.1.a) de la Ley del IRPF establece que la condición de contribuyente se atribuye a la persona física residente habitual en territorio español. La consecuencia es la sujeción plena prevista en el artículo 2 de la LIRPF, esto es, la obligación personal de contribuir por la totalidad de las rentas, sin importar el lugar de su obtención ni el pagador.

El artículo 9 de la Ley del IRPF precisa qué se entiende por residencia habitual. No suponen una definición, pero sí una especificación a través de tres criterios alternos: el primero, en la letra a), según el cual se considerará residente fiscal en España a aquel que permanezca más de 183 días en el país durante el año natural. A continuación, en la letra b) del mismo apartado, se encuentra el segundo criterio, que establece que el núcleo principal o la base de las actividades o intereses económicos del sujeto radique en territorio español, ya sea de forma directa o indirecta. En tercer y último lugar, se encuentra el criterio familiar, configurado como una presunción *iuris tantum*, según la cual un sujeto será considerado residente en España si reside en el país su cónyuge no separado legalmente y sus hijos menores de edad que dependan de él. Estos criterios, concebidos para vincular jurídicamente al sujeto con el territorio, han generado controversias, que se intensifican en el marco del teletrabajo internacional.[2]

El criterio de permanencia (artículo 9.1.a) de la LIRPF) exige más de 183 días en España en un año natural. A efectos del cómputo, se incluyen las ausencias esporádicas, salvo que el contribuyente pruebe su residencia en otro país. La jurisprudencia ha tratado de delimitar su alcance. Así, en la sentencia del Tribunal Supremo (TS) de 28 de noviembre de 2017, subrayó, en el fundamento jurídico (FJ) tercero, que una ausencia esporádica no puede entenderse como un período dilatado en el tiempo y parece concretar, a nuestro juicio, que por dilatado será un período superior a los 183 días. La resolución del Tribunal Económico Administrativo Central de fecha 25 de abril de 2023 circunscribe bien el tema de las ausencias, pues expone qué días se computarán en el período total de los 183 días. Para ello establece una triple tipología de días: primero, los días de presencia real, sobre los que consta una prueba directa de presencia –una multa de tráfico, por

2. Sobre el impacto del teletrabajo vid. Rovira Ferrer (2023).

ejemplo–; segundo, los días presuntos, que son días que se encuentran entre días probados (días de presencia real) y, además, no hay ningún dato que refleje la presencia física en el extranjero. La suma de las dos tipologías anteriores da paso a los días de permanencia efectiva. Por último, la tercera tipología de días son las mencionadas ausencias esporádicas. Estas últimas únicamente deberían servir de refuerzo a las conclusiones de permanencia en España o en el extranjero. De modo que solo computan si no se ha rebasado el umbral de los 183 días.

Además, el cálculo de los días es objetivo, como afirmó el TS en la anterior sentencia en su FJ quinto, pues no se atiende a la intención (la voluntad) del sujeto, solo a la duración e intensidad. Un claro ejemplo, aunque criticable, es el considerado por la Dirección General de Tributos (DGT) en la Consulta vinculante (CV) de 12 de abril de 2021. Se trata de un conocido caso en que un residente en Tánger quedó atrapado en España debido a las restricciones de la COVID-19. La intención de este sujeto no era permanecer en España, pero, como el criterio no atiende a subjetividades, la DGT estimó que el tiempo transcurrido en nuestro territorio sirvió para iniciar el cómputo de permanencia.

La segunda circunstancia está prevista en el artículo 9.1.b) de la Ley del IRPF, esto es, que radique en el territorio español el núcleo principal o la base de sus actividades o intereses económicos, de forma directa o indirecta. Este núcleo puede determinarse según un criterio absoluto (se centra en el lugar donde haya la mayor parte de intereses económicos en comparación con el resto de los intereses que radiquen en otros Estados) o relativo (comparación únicamente con el Estado en conflicto). La resolución del TEAC de fecha 2 de noviembre de 2017 estableció que basta con que en España se concentren más bienes que en cualquier otro Estado (relativo), aunque no superen el conjunto global.

Hay que tener en cuenta que este segundo criterio atiende tanto a las rentas como al patrimonio, sin que uno sea más relevante que otro. La Audiencia Nacional y el Tribunal Supremo, en sentencias de 10 de noviembre de 2021 y 4 de julio de 2006, respectivamente, apostaron por igualar la importancia de ambos elementos. Otra cosa bien distinta será que en nuestro territorio únicamente haya uno de ellos o que sea más fácil probar uno que otro. Además, no se limita a la mera titularidad, sino también al lugar de gestión y administración de los bienes; el lugar donde se evidencia la capacidad económica en términos de ingresos y gastos; donde se lleva a cabo la actividad empresarial o profesional, y donde se concentra la mayor parte de las inversiones. Unos lugares también mencionados por el Libro Blanco para la reforma tributaria del año 2022.

El apartado b) in fine del artículo 9.1 de la LIRPF contiene la tercera circunstancia, el criterio familiar. Se indica que existirá una presunción *iuris tantum* de que el contribuyente es residente fiscal en territorio español cuando en este resida su cónyuge no separado legalmente junto con los hijos menores de edad que dependan de él. La doctrina debate qué debe entenderse por *dependencia*. Unos consideran que hace referencia a cuestiones económicas; otros, en cambio, a cuestiones civiles como sería la patria potestad. Sin embargo, a nuestro juicio, consideramos que la patria potestad podría acoger la posición económica de la otra mitad de la doctrina y que el significado de depender quedase clarificado.

Otra cuestión radica en conocer qué significado tiene la conjunción y, pues conviene conocer si la intención del legislador es tratar de forma acumulativa la residencia en España del cónyuge no separado legalmente junto con la dependencia de los hijos menores. Apostamos por lo siguiente: si existen ambos (cónyuge e hijos), deben aparecer de forma acumulativa; en caso de que no existan de forma simultánea, también sería aplicable la presunción. De lo contrario, no podría aplicarse a viudos, solteros o matrimonios sin hijos, lo cual sería un sinsentido, dado que en todos los casos anteriores también se incluyen en el concepto de familia.

Finalmente, la crítica a la presunción establecida en el vínculo familiar, pues la misma se consolida como *iuris tantum*. La norma no señala cómo podría destruirse la presunción. Además, deberán ser residentes fiscales conforme a los criterios del artículo 9.1 de la LIRPF, pues si no son residentes, no puede invocarse este criterio, lo cual es razonable. De ahí que algunos autores consideren que no se trata de una verdadera circunstancia para determinar la residencia fiscal.

Como hemos visto, los criterios de residencia previstos en el artículo 9 de la LIRPF, diseñados en un contexto previo a la irrupción del teletrabajo, plantean problemas de aplicación y requieren de una reinterpretación para poder sustentarse en nuevas situaciones como las que en el punto siguiente describiremos.

3. Nuevos problemas: la creciente competencia fiscal y el arraigo del teletrabajo

La Comisión Europea ha señalado que los países utilizan cada vez más sus sistemas tributarios como herramienta de competencia, en particular mediante normas sobre residencia fiscal que pueden favorecer prácticas perniciosas (Comisión Europea, 2020). En la misma línea, la OCDE ha advertido sobre los riesgos derivados de la adquisición de la ciudadanía y la residencia fiscal a través de las inversiones, ya que en algunos casos estos mecanismos evitan tributar en jurisdicciones con mayor presión fiscal.[3] Estos problemas, como aseguró la Comisión Europea, surgen en buena parte con la crisis financiera de 2007, lo que llevó a algunos Estados miembros a implantar regímenes de residencia para inversores[4] sin requerir, en algunos casos, una presencia física significativa, como exige el criterio de permanencia al que hemos aludido.

La adopción de estas prácticas puede llegar a considerarse perniciosa al desnaturalizar el concepto de residencia fiscal, que ya de por sí plantea múltiples dificultades interpretativas. La OCDE considera como perniciosas aquellas disposiciones fiscales que imponen bases imponibles que, por derecho, corresponderían a otros territorios, aprovechando la movilidad geográfica de ciertas actividades (OCDE, 1998, pág. 15). En este sentido, el informe final sobre la Acción 5 del Proyecto sobre la Erosión de la Base Imponible y el Traslado de Beneficios relativa a las prácticas fiscales perniciosas destaca el criterio de la actividad sustancial para plantear que un régimen resulta dañino cuando otorga beneficios con fines meramente fiscales, sin exigir una actividad económica real en el territorio (OCDE, 2016).

En un contexto digitalizado proliferan las actividades de fácil deslocalización. El mercado laboral se ha transformado con el auge del trabajo a distancia. Según los datos de EUJOBS, la población activa europea asciende a 259 millones de personas. De acuerdo con Eurostat, un 9 % de esta población adopta la filosofía *work from anywhere*. Ello supone un importante potencial de trabajadores interesados en acogerse a los regímenes preferenciales que varios Estados miembros, entre ellos España, han puesto en marcha.

Según el informe *Global Tax Evasion Report 2024* del Observatorio Fiscal de la UE, en 1995 tan solo existían 5 regímenes preferenciales, mientras que en 2024 la cifra alcanzó los 24. El mismo informe clasifica a los regímenes preferenciales en tres categorías: los regímenes que permiten una tributación menor sobre los ingresos mundiales o extranjeros en comparación con la tributación asumida por residentes ordinarios. En este grupo se sitúan España, Grecia, Francia, Luxemburgo o Italia. La segunda son aquellos aplicables sobre los ingresos obtenidos en el Estado que aplica el régimen a cambio de realizar una actividad económica específica, sobre cuyos ingresos se aplican una serie de reducciones fiscales (Chipre, Finlandia, Irlanda, etc.). Por último, aquellos regímenes que benefician a personas jubiladas, entre los que destacó el régimen portugués, derogado con efectos a partir del 1 de enero de 2024 a través de una ley de presupuestos. En cifras, al menos 260.000 personas se benefician de los regímenes, lo que supone un crecimiento, según el Observatorio, de 30.000 beneficiados con respecto a 2021. En España, el número de impatriados asciende a 11.078, con un coste en nuestras arcas públicas de 105,78 millones de euros.[5]

A nuestro juicio, el auge de este tipo de regímenes responde a diversos factores. Por un lado, la digitalización del trabajo ha hecho innecesaria la coincidencia física entre empleador y empleado, facilitando la movilidad. Por otro lado, los Estados actúan unilateralmente gracias a la soberanía fiscal de la que aún disponen en materia de tributación directa (OCDE, 2015). En el ámbito de la UE, pese a las exigencias de cooperación y armonización para mantener un mercado único, los Estados se muestran reacios a ceder competencias en materia de fiscalidad personal y

3. Para más información, véase: https://www.oecd.org/en/topics/sub-issues/international-standards-on-tax-transparency/residence-citizenship-by-investment.html. [Fecha de consulta: 19 de agosto de 2025].
4. COMISIÓN EUROPEA (2019). *Informe de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de Regiones sobre Regímenes de ciudadanía y residencia para inversiones en la Unión Europea*. COM (2019) 12 final. En 2019, unos 20 Estados miembros disponían de uno de ellos. España lo eliminó con efectos a partir del 3 de abril de 2025, por la disposición final 21.1 de la Ley Orgánica 1/2025, de 2 de enero, de medidas en materia de eficiencia del Servicio Público de Justicia.
5. En base a los datos establecidos en la Memoria de Beneficios Fiscales de los Presupuestos Generales del Estado del año 2023.

empresarial. El artículo 4.1 del Modelo de Convenio (MC) de la OCDE confirma lo que comentamos, al dejar a las legislaciones nacionales la definición de «residente». Así, el MC actúa solo como orientación, lo que, como arguye Serrano Antón, explica que los Convenios para evitar la Doble Imposición (CDI) no hayan tenido el efecto armonizador esperado (Serrano Antón, 2006, pág. 7).

Otro factor determinante ha sido la tendencia de las instituciones internacionales y europeas a prestar más atención a las actividades empresariales, relegando las realizadas por personas físicas a un segundo plano. Esta exclusión resulta evidente en el Código de Conducta sobre fiscalidad empresarial aprobado por la Comisión Europea en 1998 y reformado en 2022. Aunque el Código constituye un compromiso político y no vinculante, su finalidad es evitar que los Estados adopten medidas fiscales perniciosas que provoquen una competencia lesiva. Sin embargo, desde su creación se ha planteado, sin éxito, ampliar su alcance a regímenes preferenciales vinculados a rentas de personas físicas. En palabras de la Comisión Europea, «la definición del ámbito de aplicación debe modificarse para abarcar otro tipo de regímenes y aspectos generales de los sistemas nacionales de impuestos de sociedades, así como otros impuestos pertinentes». Posteriormente, señala que «el Código no cubre los regímenes o medidas especiales de ciudadanía para atraer a expatriados o personas adineradas, a pesar de que a menudo son una puerta trasera para atraer de forma desleal a empresas e inversiones de otros países». A pesar de este antecedente, la reforma del Código el 8 de noviembre de 2022 no ha contemplado estos aspectos, o al menos no de forma expresa. Esta demanda, en la actualidad, tiene mucho sentido, pues, como advierte Kostic (2019, pág. 201), la fuerza del trabajo ya no es un recurso sedentario e inamovible.

La urgencia de ampliar el ámbito de aplicación del Código se justifica por el elevado coste de estos regímenes: unos 7.500 millones de euros al año (AA. VV, 2023, pág. 58). Los regímenes de Holanda y Portugal son los que asumen mayores pérdidas, pues son más los sujetos que se acogen a ellos. El Observatorio Fiscal de la UE establece una puntuación del 1 al 10 para medir el perjuicio que pueden provocar. Los criterios para estimarlo son cuatro: la duración del régimen, las condiciones de ingreso, los requisitos de actividad profesional y el tamaño del beneficio fiscal. En esta escala, el régimen español de impatriados recibe una calificación de 5.

A la vista de lo anterior, resulta oportuno abordar en el siguiente apartado el análisis del régimen de impatriados dispuesto en el artículo 93 de la LIRPF, el cual contempla, entre sus diferentes supuestos, el teletrabajo internacional.

4. El régimen de impatriados como punto de controversia

4.1. Propósito y contenido: especial énfasis a los teletrabajadores internacionales

El régimen fiscal especial aplicable a los trabajadores, profesionales, emprendedores e inversores desplazados a territorio español –conocido como régimen de impatriados– fue introducido hace veinte años en el ordenamiento jurídico español y está regulado en el artículo 93 de la LIRPF. Tras varias reformas, la última a través de la Ley 28/2022, se introdujo como supuesto el teletrabajo internacional.

Su finalidad principal es atraer a personas altamente cualificadas o vinculadas a sectores emergentes. Quienes se acojan al régimen tributan por el impuesto sobre la renta de no residentes (IRNR), aunque conservan la condición de contribuyente del IRPF durante el ejercicio de su desplazamiento y los cinco siguientes. Para acceder, deben cumplirse tres requisitos: el primero, no haber sido residente en España durante los cinco períodos impositivos anteriores a aquel en el que se produce el desplazamiento a territorio español; el segundo, que el desplazamiento venga motivado por alguna de las situaciones dispuestas en el precepto (el inicio de una relación laboral, la adquisición de la condición de administrador, la realización de una actividad económica calificada como emprendedora o una actividad económica por parte de un profesional altamente cualificado que preste servicios a empresas emergentes); y, el tercero, no obtener rentas mediante un establecimiento permanente.

Una de las novedades de la reforma ha sido la posibilidad, cumpliendo una serie de requisitos, de que el régimen especial beneficie a los hijos del contribuyente menores de 25 años o con discapacidad, así como al cónyuge del contribuyente. Para ello, tendrán que cumplir con las exigencias marcadas en el artículo 93.3 de la LIRPF: que se desplacen a territorio español con el contribuyente o en un momento posterior (aunque el artículo 113.1 del RIRPF dispone que puede ser con anterioridad al desplazamiento

del contribuyente principal), siempre que no hubiera finalizado el primer periodo impositivo en el que el régimen resulte de aplicación; que se adquiera la residencia fiscal, pues otra de las exigencias es que el núcleo familiar del contribuyente principal no ha tenido ni que ser residente fiscal en España durante los cinco períodos impositivos anteriores al desplazamiento ni obtener rentas a través de establecimientos permanentes, salvo si son por las excepciones marcadas en el precepto. Así mismo, la suma de sus bases liquidables en cada periodo impositivo debe ser inferior a la base liquidable del contribuyente que solicita el régimen, el principal. Es interesante remarcar la importancia que tiene que el núcleo familiar mencionado del contribuyente principal no obtenga unas bases liquidables superiores, pues de ser así, quedarían excluidos del régimen, tal y como dispone el artículo 118.4 del RIRPF.

Señalado lo anterior, para que el desplazamiento de un teletrabajador internacional resulte efectivo en este régimen, será necesario que el trabajador se desplace a territorio español para prestar servicios a distancia para un empleador radicado en otro país. Dichos servicios deben realizarse, de manera exclusiva, a través de medios y sistemas informáticos, telemáticos y de telecomunicación. Conviene recordar, en este sentido, que la Ley 10/2021, de 9 de julio, de trabajo a distancia, precisa en su artículo 2.b) que el teletrabajo es aquel trabajo a distancia que se lleva a cabo mediante el uso exclusivo o prevalente de medios informáticos, telemáticos y de telecomunicación. Esta definición resulta clave, pues permite diferenciar el desplazamiento de un teletrabajador internacional de un desplazamiento laboral ordinario: en el primero, no se requiere que el empleador ordene o imponga el traslado, lo que otorga al trabajador plena flexibilidad para acogerse a esta modalidad. Ahora bien, dicha flexibilidad se encuentra matizada por la exigencia de un visado de teletrabajo internacional, previsto en la Ley 14/2013, de 27 de septiembre, de apoyo a los emprendedores y su internacionalización (Ley 14/2013).[6]

La exigencia de visado delimita el tipo de teletrabajador que España pretende atraer, pues entre Estados miembros no aparece este requisito dado que los ciudadanos europeos gozan de libertad de circulación en el espacio Schengen. El capítulo V bis de la Ley 14/2013 regula específicamente esta figura. En particular, el artículo 74 bis define el teletrabajo internacional como aquel desarrollado por nacionales de terceros Estados autorizados a permanecer en España para ejercer una actividad laboral o profesional a distancia para empresas radicadas fuera del territorio español, debiendo acreditarse que dicha actividad se presta en remoto, de conformidad con el artículo 74 ter, b) de la Ley 14/2013. Además, el apartado segundo del precepto indicado exige, para la concesión del visado, acreditar formación en universidades, escuelas de negocio o centros de formación profesional de reconocido prestigio.

En materia tributaria, los rendimientos obtenidos por los teletrabajadores internacionales acogidos al régimen que comentamos se califican como rendimientos del trabajo, conforme al artículo 17 de la LIRPF. Este tipo de rendimientos, según el artículo 93.2.b) de la LIRPF, se entenderán obtenidos en territorio español, con independencia del lugar de su obtención. Esto implica, a nuestro considerar, que pese a tributar bajo las reglas del IRNR –esto es, con obligación real–, el trabajador queda sujeto al principio de sujeción plena previsto en el artículo 2 de la LIRPF, que obliga a contribuir por la totalidad de sus rentas. Esta circunstancia podría llevar a considerar que el régimen resulta poco beneficioso;[7] sin embargo, como se verá, la aplicación de las reglas 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 (LIRNR), compensa en determinados aspectos.

En concreto, la cuota se determina aplicando un tipo proporcional: el 24 % para bases liquidables de hasta 600.000 euros y el 47 % para las que superen dicho importe. Comparado con la tributación ordinaria de los residentes, cuya escala progresiva (artículo 63 de la LIRPF) alcanza un tipo máximo del 47 % a partir de los 300.000 euros, el régimen de impatriados resulta ventajoso a partir de bases superiores a los 60.000 euros sobre las que recae un tipo aplicable del 22,5 %.

6. Respecto al visado, la exposición de motivos de la Ley 28/2022 indica que se añade una nueva categoría de visado con una validez máxima de un año para los teletrabajadores. Sin embargo, existe la posibilidad de continuar en nuestro país a través de la solicitud de una autorización por un período máximo de tres años que será renovable por un plazo de otros dos.
7. También habrá que tener en cuenta que los teletrabajadores internacionales no podrán aplicarse el mínimo personal y familiar ni algunas reducciones en sus rendimientos del trabajo como, en concepto de aportaciones a planes de pensiones, entre otros. Además, tendrán que tributar por cada devengo de renta que se somete a gravamen sin posibilidad de compensación al aplicarse las reglas del IRNR.

4.2. La experiencia comparada: el caso de Italia y Portugal

El régimen de impatriados ha sido utilizado en otros países de nuestro entorno para atraer talento. Italia y Portugal son un claro ejemplo de la evolución de estos regímenes, aunque la tendencia ha sido a favor de una restricción de las ventajas fiscales originarias y focalizadas en perfiles más vinculados a la innovación y la investigación.

En Italia, el régimen de *impatriati* fue introducido por el artículo 16 del *Decreto Internazionalizzazione* número 147 de 14 de septiembre de 2015,[8] con el objeto de ofrecer una tributación más favorable para contribuyentes que trasladaran su residencia fiscal a Italia y que se comprometieran a permanecer en el país al menos dos años, desarrollando actividades laborales para una empresa residente –o extranjera controlada por una residente–. En caso de incumplimiento, los beneficios debían ser reintegrados. El perfil de beneficiado era el de trabajador altamente cualificado y, adicionalmente, no podría haber residido en Italia durante los cinco ejercicios fiscales anteriores al año en que se ejerce el traslado. Inicialmente, el régimen disponía de una exención del 30 % de las rentas brutas de los trabajadores de origen italiano, aunque posteriormente se aumentó hasta el 50 % durante cinco ejercicios fiscales, incluyendo el ejercicio del desplazamiento.

En 2019, por medio del Decreto ley número 34 de fecha 30 de abril, se produjo una ampliación sustancial de los requisitos subjetivos y las ventajas. Entre las principales novedades figuraban la posibilidad de desarrollar actividades empresariales, la reducción del periodo de no residencia previa de cinco a dos años y la extensión del régimen de cinco a diez ejercicios fiscales si el contribuyente tenía un hijo menor de 18 años o adquiría una vivienda en los 12 meses previos al traslado o en el año en que este se produce. Bajo estas condiciones, la exención podía alcanzar el 70 % durante los primeros cinco años y descendía al 50 % en los cinco ejercicios restantes. Además, se establecieron incentivos adicionales en favor de quienes se trasladarán a regiones del sur de Italia, como Calabria o Sicilia, donde la exención podía alcanzar hasta el 90 %.

Sin embargo, el Gobierno italiano, mediante el Decreto legislativo 209/2023, de 19 de diciembre,[9] puso freno a las disposiciones anteriores para aquellos que trasladen su residencia fiscal a Italia a partir del 1 de enero de 2024. El nuevo régimen exige no haber sido residente en Italia durante los tres ejercicios fiscales anteriores, permanecer en el país al menos cuatro ejercicios y cumplir con requisitos de cualificación profesional. La exención se reduce del 70 % al 50 % de la base imponible, desaparecen los beneficios reforzados vinculados a determinadas regiones del sur y se fija un límite máximo de ingresos exentos de 600.000 euros anuales. Solo en caso de contribuyente con hijos menores de 18 años la reducción se incrementa del 50 % al 60 %. Un aspecto especialmente relevante es que ya no se exige interrumpir la relación laboral previa, lo que abre la puerta a la utilización del régimen a los teletrabajadores internacionales.

En palabras de Beretta y Cipolli, ha sido positiva la ampliación de la exigencia de tres ejercicios de no residencia, pues con los dos periodos impositivos anteriores, a fin de cuentas, el sujeto no pasaba más de un año natural fuera de Italia –del 30 de junio del año *X* y el retorno el 1 de julio del año *X* + 1, por ejemplo– (Beretta y Cipolli, 2024, pág. 176 y ss.). De esta forma, se evitan los posibles traslados meramente temporales para acogerse a una tributación más ventajosa. Además, estos mismos autores valoran favorablemente el mantenimiento de reducciones reforzadas para familias con hijos menores de edad, alineadas con la necesidad de responder al desafío demográfico del país.

Por su parte, Portugal ofrece un recorrido distinto, pero en la senda restrictiva. El régimen de residentes «no habituales», vigente desde 2009,[10] fue concebido no para beneficiar indiscriminadamente a los no residentes, sino para atraer a profesionales de alto valor añadido –arquitectos, investigadores, cineastas, profesores universitarios o

8. Publicado en la *Gazzetta Ufficiale* número 220 del 22 de septiembre de 2015.
9. Publicado en la *Gazzetta Ufficiale* número 301 en fecha 28 de diciembre de 2023.
10. En base al artículo 126 de la Ley 64-A/2008, de 31 de diciembre de 2008, y el Decreto-ley núm. 249/2009 de 23 de septiembre (en la parte III, artículos 23 a 25), el cual estableció el régimen especial de residentes «no habituales».

inversores–, así como pensionistas.[11] Los requisitos principales eran: no haber ostentado la condición de residente fiscal en los cinco ejercicios anteriores,[12] inscribirse como residente no habitual y acreditar la aportación de un valor añadido. Una vez concedida la inscripción, los beneficiarios disfrutaban de un tratamiento preferencial durante diez años consecutivos, con un tipo reducido del 20 % sobre los rendimientos del trabajo y actividades profesionales, frente a la escala progresiva de hasta el 48 % aplicable al resto de contribuyentes. Como apuntó Gil García con el cumplimiento de estos requisitos, inferiores a los exigidos en el artículo 93 de la LIRPF, muchos teletrabajadores podrían instalarse en Portugal para acceder a un régimen durante los diez años indicados, planteando la autora la posibilidad de que un teletrabajador español que opera para una empresa no residente (en España) se traslade a Portugal para beneficiarse del régimen luso (Gil García, 2022); aunque, si se diera el caso, no será tan fácil perder la residencia fiscal en España como bien se expuso en epígrafes anteriores.

Esta tributación privilegiada finalizó el 2 de octubre de 2023, cuando el por entonces primer ministro portugués, Antonio Costa, anunció el fin de los «no habituales».[13] La Ley 82/2023, de 29 de diciembre, de Presupuestos para 2024, en su artículo 263, confirmó su desaparición y, en su lugar, creó un régimen fiscal orientado a la investigación científica y la innovación con efectos a partir del 1 de enero de 2024. Este se desarrolla mediante la ordenanza 352/2024/1, de 23 de diciembre, y el artículo 58.A del Estatuto de beneficios fiscales.[14] El nuevo sistema mantiene una duración de diez años y el tipo reducido del 20 % sobre rendimientos del trabajo o actividades profesionales específicas, eximiendo rentas extranjeras, pero limita el acceso a perfiles profesionales concretos. Además, no podrán acogerse quienes ya hubieran optado anteriormente por el régimen de no habituales.

A diferencia de lo que sucede en España e Italia, en Portugal no parece contemplarse expresamente la posibilidad de compatibilizar este régimen con el teletrabajo internacional, pues no se prevé la posibilidad de mantener el empleador en el extranjero, lo que reduce su atractivo para este tipo de contribuyentes.

5. Reflexiones sobre los aspectos controvertidos del régimen español de impatriados

El régimen de impatriados, al igual que los existentes en países de nuestro entorno como Portugal e Italia, comparte un mismo propósito: atraer talento altamente cualificado. Estos regímenes identifican el mérito y la innovación como mecanismos para reforzar la competitividad internacional y, en particular, dentro de la UE. Si bien es cierto que la elevada presión fiscal puede actuar como freno para el desarrollo de determinados profesionales y favorecer la fuga de talento, consideremos que los incentivos tributarios, aunque relevantes, no son el único factor determinante a la hora de fijar la residencia fiscal en un país. Aspectos como la remuneración, el coste de la vida, el clima o la calidad de los servicios públicos también son decisivos.

11. Pablos Mateos, (2021). (Versión electrónica [BIB 2021/4862]). Esta tipología de personas, aunque no es el objeto del artículo, produjo grandes conflictos debido a que Portugal consideraba exentas de tributación las pensiones no obtenidas en territorio portugués, lo que incentivó a ciudadanos suecos y finlandeses a desplazarse y tributar estas rentas en el Estado de residencia del beneficiario, que en este caso sería Portugal. Al tributar en Portugal, no se gravarían en el Estado de origen (por ejemplo, Finlandia), evitando así la doble imposición. Esto llevó efectivamente a una situación de doble no imposición en la práctica. Ante esta situación, Finlandia denunció el CDI que tenía suscrito con Portugal desde 1971. Portugal tuvo que reaccionar y, por vía de la Ley 2/2020, de 31 de marzo de 2020, de Presupuestos del año 2020, introdujo el tipo porcentual del 10 por ciento para pensiones extranjeras.
12. La adquisición de la residencia fiscal portuguesa atiende a los requisitos indicados en el artículo 16.1 del Código do Imposto sobre o Rendimento das Pessoas Singulares, el cual señala que deben permanecer más de 183 días durante los últimos doce meses y, si se permanecen menos de dicho plazo, se debe disponer de una vivienda con la vocación de mantenerla y ocuparla en concepto de residencia habitual.
13. En palabras de Antonio Costa, «mantener esta medida para el futuro es prolongar una medida de injusticia fiscal que no está justificada, además de ser una forma sesgada de seguir inflando el mercado inmobiliario». Para más información, véase: https://cnnportugal.iol.pt/habitacao/vistos-gold/neste-momento-nao-faz-mais-sentido-costa-anuncia-fim-da-taxacao-especial-para-residentes-nao-habituais/20231002/651b2ac9d34e65afa2f5f4cf. [Fecha de consulta: 21 de agosto de 2025]. A pesar de ello, se mantiene una especie de régimen transitorio para aquellos que ya estaban acogidos al régimen, de modo que el tiempo que reste de esos 10 años seguirán siendo incentivados.
14. Para más información, véase: Botelho Moniz (2024).

La consolidación del teletrabajo ha intensificado la movilidad internacional, aunque no todos los Estados han decidido incluir esta modalidad en el ámbito subjetivo de sus regímenes. España es el único que lo contempla de forma expresa, con el fin de atraer a profesionales altamente cualificados. No obstante, este supuesto plantea riesgos que conviene analizar.

Un primer aspecto es la manera en que se configura la atracción de talento. Tras la Ley 28/2022, el artículo 93 de la LIRPF amplió los supuestos contemplados, poniendo de relieve la importancia del trabajo a distancia y la digitalización, pero también la necesidad de dinamizar la España vaciada. Sin embargo, a diferencia de lo previsto en Portugal o en la normativa italiana anterior a 2023, el legislador español no ha tenido en cuenta incentivos destinados a traslados en zonas despobladas, lo que podría ser interesante teniendo en cuenta los efectos que podrían tener estos trabajadores sobre estas zonas (mejora del patrimonio, creación de empleo por el aumento de la demanda, posibilidad de mejora de servicios públicos, etc.). Como vemos, uno de los primeros problemas que tiene el régimen español de impatriados es que, a pesar de la exposición de motivos de la Ley 28/2022, pone el foco en los centros urbanos donde se desarrolla más actividad económica, sin valorar que con el teletrabajo es posible establecerse en entornos con menor concentración demográfica y seguir prestando con la misma efectividad el servicio. Es por ello por lo que cobra sentido la opinión de Szudoczky y Rodríguez (2024, pág. 271) al precisar que este tipo de regímenes deberían diseñarse con flexibilidad para adaptarse a la situación socioeconómica del país donde se aplican.

El segundo de los problemas es la desigualdad que generan estos regímenes entre residentes fiscales ordinarios y beneficiarios del trato preferencial. En España, un residente, en tributación individual, con bases imponibles iguales o superiores a 60.000 euros tributa al 22,5 %, mientras que un impatriado disfruta de un tipo proporcional más ventajoso hasta los 600.000 euros, a partir de los cuales se tributa al 47 %. En Portugal la situación es incluso más evidente, donde el régimen especial permite aplicar un 20 % fijo durante diez años, frente al tipo progresivo del 48 % que recae sobre bases en torno a los 83.000 euros. Sobre estas diferencias es conveniente añadir dos cuestiones: la primera, desde la perspectiva constitucional, este régimen plantea cuestionarse una posible vulneración de la igualdad tributaria dispuesta en el artículo 31.1 de la CE, pues claramente la capacidad económica de los beneficiados no concuerda con los tipos aplicados. Si bien el Tribunal Constitucional en la sentencia 76/1990, de fecha 26 de abril, marcó unas pautas de razonabilidad y proporcionalidad que, a nuestro juicio, parecen complicar los argumentos sobre una posible vulneración del principio de igualdad tributaria. La segunda cuestión tiene que ver con otra diferencia, la territorial, pues en función de la comunidad autónoma en la que se someta a debate la posible desigualdad, será mayor o menor la diferencia en vista de las competencias normativas que tienen estas sobre los tipos del IRPF al ser un impuesto parcialmente cedido.

Aunque estas medidas buscan estimular las economías nacionales, también fomentan la deslocalización, especialmente en un contexto en que el teletrabajo internacional está cada vez más arraigado. En este sentido, y como tercera controversia, este tipo de beneficios puede producir una protección patrimonial de los trabajadores altamente y, todo sea dicho, con alta capacidad adquisitiva, que aprovechan el proceso transitorio de adquisición definitiva de la residencia fiscal para trasladarse entre países en busca de regímenes más favorables para sus intereses. De ahí que Portugal, con acierto, haya prohibido expresamente la posibilidad de volver a acogerse a su régimen especial tras haberlo disfrutado, previsión que no existe en España. En Italia, por su parte, el plazo de no residencia se amplió de dos a tres años, limitando así retornos apresurados. Más aún si tenemos en cuenta el funcionamiento de los períodos impositivos, pues, por ejemplo, del 30 de marzo del año *X* al 1 de abril del año *X* + 1 no representan más que un año natural, aunque nos encontremos ante dos períodos impositivos distintos. España y Portugal, al exigir cinco ejercicios de no residencia, garantizan una mayor desvinculación con el territorio anterior y, por tanto, más seguridad jurídica. Por tanto, habría que poner mayor énfasis en este posible abuso temporal, aunque estaría reñido con la finalidad de atracción de los regímenes de impatriados.

En cuarto lugar, el régimen español de impatriados no vincula la residencia fiscal con el criterio familiar ni con el criterio de los intereses económicos, sí con el de permanencia. Esta idea se confirma en el artículo 115 del RIRPF, que dispone: «este régimen especial se aplicará durante el período impositivo en el que el contribuyente adquiera su residencia fiscal en España (...) a estos efectos, se considerará como período impositivo en el que se adquiere la resi-

dencia el primer año natural en el que, una vez producido el desplazamiento, la permanencia en territorio español sea superior a 183 días».[15] A partir de esta previsión surge la duda de si un teletrabajador internacional que se traslada formalmente a España, cumpliendo con todos los requisitos para acogerse al régimen, puede seguir beneficiándose del mismo, aunque, en la práctica, preste sus servicios en remoto desde otro Estado, tributando de forma más ventajosa que cualquier otro residente fiscal.[16] Entonces, habría dos problemas: en primer lugar, el abuso de un régimen preferencial sin aportar el valor que la economía de dicho territorio requiere; y en segundo lugar, la utilización en otro Estado de sus servicios públicos, infraestructuras y recursos naturales sin contraprestación alguna, más allá de algunos impuestos indirectos derivados del consumo, como sería el caso del impuesto sobre el valor añadido. Pese a lo anterior, una interpretación sistemática de los artículos 93 de la LIRPF y 115 del RIRPF permitiría argüir que la permanencia requiere necesariamente una presencia física durante 183 días. No obstante, debería exigirse esta obligación, a la vista de los riesgos de deslocalización que acarrean estos regímenes.

El último de los problemas lo situamos en las ausencias esporádicas como parte del cómputo del periodo de permanencia. Bajo esta premisa, un teletrabajador internacional que se encuentre fuera de España, pero acogido al régimen de impatriados, seguiría considerándose, a nuestro juicio, como residente a efectos de permanencia y, por tanto, beneficiándose de los tipos proporcionales previstos en el régimen. En este punto, la rigidez con la que el legislador español configura el criterio de permanencia podría favorecer eventuales abusos en el marco del teletrabajo internacional de los impatriados.

Ahora bien, esta hipótesis no tendría cabida en el periodo inicial en que se produce el traslado por varios motivos. En primer lugar, porque el Tribunal Supremo, en la sentencia de 28 de noviembre de 2017, estableció que una ausencia esporádica no puede prolongarse de forma dilatada en el tiempo, ni superar la permanencia mínima de 183 días, ni absorber la totalidad del período impositivo. En segundo lugar, porque las ausencias esporádicas encuentran mayor justificación en los supuestos en que acaba de cumplirse el requisito de la permanencia, aplicándose entonces con mayor rigor, dado que aún no existen indicios claros de estabilidad (Cubero Truyo, 2019; García Carretero, 2013). De modo que, el posible abuso se podría enmarcar en el segundo período impositivo.

15. Véase, sobre este tema, la CV 3235-13 de fecha 4 de noviembre de 2013, un consultante que reside desde 2005 en Suiza y en el año 2014 decidió trasladarse a España, y quería optar al régimen de impatriados. La DGT respondió que «se considerará que la consultante adquiere su residencia fiscal en España en el período impositivo 2015 si, una vez producido el desplazamiento, su permanencia en territorio español a lo largo de dicho año es superior a 183 días».
16. Conviene precisar que la norma no es clara con la posibilidad que tiene el teletrabajador internacional de acudir al centro de trabajo de su empleador para tener reuniones o actividades corporativas esporádicas de forma presencial. Un hecho que parece ser un asunto menor si lo comparamos con la laguna respecto al criterio de permanencia comentado.

Referencias bibliográficas

AA. VV. (2023). *Global Tax Evasion - Report 2024*. EUTAX Observatory.

BERETTA, G.; CIPOLLI, C. (2024). «The New Italian Tax Regime for Inbound Workers: Has the "Bel Paese" Become Less Attractive for Inward Expatriates?». *European Taxation*, págs. 170-178. DOI: https://doi.org/10.59403/2gzsr89

BOTELHO MONIZ, R. (2024). «The new portuguese tax incentive regime for expatriates». *European Taxation*, págs. 230-232. DOI: https://doi.org/10.59403/1c4tzec

COMISIÓN EUROPEA (2019). *Informe de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de Regiones sobre Regímenes de ciudadanía y residencia para inversiones en la Unión Europea*. COM (2019) 12 final.

COMISIÓN EUROPEA (2020). *Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre la buena gobernanza fiscal en la UE y más allá de sus fronteras*. COM (2020) 313 final.

CUBERO TRUYO, A.; TORIBIO BERNÁRDEZ, L. (2019). «Propuestas para una reorientación del concepto de residencia en la Ley del IRPF, a la búsqueda de una mayor coherencia con los criterios de los Convenios de doble imposición». *Revista de Fiscalidad Internacional y Negocios Transnacionales*, n.º 12, (artículo en línea).

FÉRNANDEZ CEREZO, A.; IZQUIERDO, M. (2025). «Encuesta a las empresas españolas sobre la evolución de su actividad: primer trimestre de 2025». *Boletín económico*. Banco de España, págs. 1-10. DOI: https://doi.org/10.53479/39358

GARCÍA CARRETERO, B. (2013). «La residencia de las personas físicas en la legislación interna». En: CHICO DE LA CÁMARA, P. (dir.). Residencia fiscal y otros aspectos conflictivos. *La armonización de la imposición directa*. Navarra: Ed. Aranzadi-Thomson Reuters.

GIL GARCÍA, E. (2022). «La residencia fiscal de las personas físicas: indeterminación, ubicuidad y deslocalización». *Revista Española de Derecho Financiero*, n.º 193 (articulo en línia). Editorial Civitas

KOSTIC, S. (2019). «In search of the Digital Nomad – Rethinking the Taxation of Employment Income under Tax Treaties». *World Tax Journal*, vol. 11, n.º 2.

KOSTIC, S. (2019). «Rethinking Article 15 of the OECD Model in Light of Digitalization». *Kluwer International Tax Blog*. DOI: https://doi.org/10.59403/1g8jv1y

OCDE (1998). *Harmful tax Competition. An emerging global issue*. París: OCDE Publishing.

OCDE (2015). *Nota explicativa*, Proyecto OCDE/G20 de Erosión de Bases Imponibles y Traslado de Beneficios [en línea]. Disponible en: https://www.oecd.org/ctp/beps-nota-explicativa-2015.pdf. [Feha de consulta: 18 de agosto de 2025].

OCDE (2016). *Combatir las prácticas fiscales perniciosas, teniendo en cuenta la transparencia y la sustancia, Acción 5 – Informe final 2015, Proyecto de la OCDE y del G-20 sobre la Erosión de la Base Imponible y el Traslado de Beneficios*, París: Éditions OCDE. DOI: https://doi.org/10.1787/9789264162945-en

PABLOS MATEOS, F. (2021). «Los beneficios fiscales en el marco del reto demográfico: el caso de Portugal». *Quincena Fiscal*, n.º 17.

ROVIRA FERRER I. (2023). «A new scenario in international tax law: two proposals to rethink the OECD Model in response to the generalization of distance work by employees». *World Tax Journal*, vol. 15, n.º 3. DOI: https://doi.org/10.59403/wh5spm

SERRANO ANTÓN, F. (2006). «Hacia una reformulación de los principios de sujeción fiscal». *Documentos*, n.º 18, págs. 3-30.

SZUDOCZKY, R.; RODRÍGUEZ, C. (2024). «Preferential personal income tax regimes in the European Union: a new form of permitted (Harmful) tax competition?». *World Tax Journal*, págs. 245-288. DOI: https://doi.org/10.59403/g98bvq

Cita recomendada

SANTIAGO MARCOS, Daniel (2026). «La atracción de teletrabajadores internacionales en el marco del régimen español de impatriados y sus posibles controversias jurídico-fiscales». En: Irene Rovira Ferrer (coord.). «Sobre la consolidación del trabajo a distancia». *IDP. Revista de Internet, Derecho y Política*, núm. 44. UOC. [Fecha de consulta: dd/mm/aa]. DOI: http://dx.doi.org/10.7238/idp.v0i44.9800377

Sobre el autor

Daniel Santiago Marcos
Profesor lector de Derecho Financiero y Tributario de la Universitat de Girona
daniel.santiago@udg.edu

Es doctor en Derecho por la Universitat de Girona (2023) con la tesis doctoral «La fiscalidad del teletrabajo» (Premio Extraordinario de Doctorado de 2023). Sus principales líneas de investigación se han centrado en: la fiscalidad internacional sobre las rentas del trabajo, las haciendas locales, el acceso a la vivienda a través de políticas fiscales, los derechos digitales de los contribuyentes, etc. Cada uno de estos ámbitos de estudio aparece publicado en artículos de revista y capítulos de libro especializados. Además, han sido expuestos en múltiples seminarios y jornadas a escala nacional e internacional. Forma parte de proyectos de investigación competitivos, así como de contratos de investigación con diferentes administraciones públicas. Como docente, ha impartido diversas asignaturas de grados y másteres de la Facultad de Derecho de la Universitat de Girona.

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Monográfico: «Sobre la consolidación del trabajo a distancia» (coord.: Irene Rovira Ferrer)

Fiscalidad de las compensaciones retributivas percibidas por los trabajadores a distancia: cuestiones controvertidas y propuestas de regulación

Montserrat Casanellas Chuecos
Universidad de Barcelona

Fecha de presentación: julio 2025
Fecha de aceptación: septiembre 2025
Fecha de publicación: marzo 2026

Resumen

El trabajo a distancia plantea importantes desafíos fiscales, especialmente en lo que respecta al tratamiento tributario de las compensaciones retributivas que perciben quienes desempeñan su trabajo en remoto. Tras más de cuatro años de vigencia de la Ley de trabajo a distancia, aún persisten importantes controversias sobre si tales compensaciones están o no sujetas a tributación. En este contexto, en el artículo se analizan las deficiencias de la regulación actual, se revisan los criterios administrativos y jurisprudenciales más relevantes y se proponen mejoras normativas orientadas a dotar de mayor certeza y equidad a la fiscalidad de dichas compensaciones.

Palabras clave

compensaciones salariales; retribuciones en especie; teletrabajo; trabajo a distancia; rendimientos del trabajo

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Taxation of compensation payments received by remote workers: controversial issues and proposals for regulation

Abstract

Remote working poses significant tax challenges, especially regarding the tax treatment of compensation payments received by remote workers. More than four years after the Remote Working Act came into force, significant controversy persists over whether such compensation is taxable. In this context, this article analyses the shortcomings of the current regulation, reviews the most relevant administrative and jurisprudential criteria and proposes regulatory improvements aimed at providing greater certainty and fairness in the taxation of such compensation.

Keywords

compensation payments; payments in kind; telecommuting; remote work; earned income

Introducción

Tras la crisis sanitaria provocada por la COVID-19, el mercado laboral ha sufrido una importante transformación que se ha visto impulsada por el impacto de las TIC, la digitalización e internacionalización de las empresas y la globalización, circunstancias que, en mayor o menor medida, han contribuido a la generalización y consolidación del trabajo a distancia como modalidad laboral preferente o complementaria de los trabajadores por cuenta ajena en el último lustro.[1]

Esta evolución en la forma de prestación de servicios, esencialmente caracterizada por el desempeño regular de la actividad laboral fuera del centro de trabajo, bien en la vivienda habitual o en el lugar elegido, a tal efecto, por el trabajador,[2] ha generado nuevas dinámicas en el desarrollo de las relaciones laborales, particularmente en lo que respecta a las retribuciones y compensaciones que reciben los trabajadores a distancia. Así, pierden relevancia e, inclusive, pueden desaparecer, algunos complementos económicos estrechamente vinculados al trabajo presencial –como puede ser el plus de transporte–, a la vez que aparecen nuevas compensaciones requeridas por la ley encaminadas a sufragar gastos motivados por las singularidades del trabajo en remoto –tales como las destinadas a compensar los gastos de wifi, luz, calefacción o teléfono, o los que responden a los costes asumidos por el trabajador para adquirir los materiales o herramientas necesarios para el desempeño de su trabajo en condiciones adecuadas, como una silla ergonómica, una luz de sobremesa, un ordenador o una pantalla–.

En cualquier caso, resulta evidente que el trabajo a distancia requiere que el empleado disponga de los medios necesarios para desempeñar las tareas propias de su puesto de trabajo en equivalentes condiciones a las que gozaría de hacerlo presencialmente o, en su caso, de las que disponen quienes no optan por trabajar en remoto. En este sentido, el legislador deja claro que todos los trabajadores tienen los mismos derechos, al margen del modo en que desempeñen su trabajo, sea presencial o

1. Según el informe del Observatorio Nacional de Tecnología y Sociedad (2024), el teletrabajo ha cobrado fuerza en los últimos trimestres de 2024, situándolo en el punto más alto desde 2021. Los datos ponen de relieve que el 7,5 % de los empleados en España teletrabajan más de la mitad de los días laborables, mientras que el 7 % lo hace de manera ocasional. Así, prácticamente el 15 % de la población activa, esto es, más de 3 millones de personas, está desarrollando su trabajo en remoto, sea de forma habitual u ocasional, datos que duplican los porcentajes que, por los mismos conceptos, existían en 2019 y superan, en un punto porcentual, los correspondientes al mismo período del año 2023. Esta misma tendencia se ha producido a nivel global en la Unión Europea, según pone de relieve el Informe de Eurofound (2022).
2. El art. 2 de la Ley 10/2021, de 9 de julio, de trabajo a distancia (en adelante, LTD), define el trabajo a distancia como una «forma de organización del trabajo o de realización de la actividad laboral conforme a la cual esta se presta en el domicilio de la persona trabajadora o en un lugar elegido por esta, durante toda su jornada o parte de ella, con carácter regular», mientras que el teletrabajo se configura como una subespecie de aquel en cuanto «trabajo a distancia que se lleva a cabo mediante el uso exclusivo o prevalente de medios y sistemas informáticos, telemáticos y de telecomunicación».

a distancia, y prohíbe las diferencias injustificadas entre ambas formas de prestación de los respectivos servicios (art. 4 LTD). Ineludiblemente, este principio de igualdad de trato irradia sus efectos sobre el sistema retributivo. A este respecto, la LTD determina que la actividad laboral llevada a cabo bajo esta modalidad no puede suponer la asunción de ningún gasto por parte de la persona trabajadora relacionado con los medios utilizados para su desarrollo e impone al empleador la obligación de sufragar y compensar los gastos vinculados a la ejecución del trabajo a distancia y, de forma específica, a dotar al trabajador de los medios, equipamiento o herramientas que sean necesarios para el cumplimiento de su actividad laboral (art. 11 LTD), debiendo, también, compensarle por los gastos en que incurra en la realización a distancia de la misma (art. 12.1 LTD). El alcance concreto de este derecho y de la correlativa obligación del empresario se deja en manos de la negociación colectiva, de modo que será preciso atender a las disposiciones convencionales (art. 12.2 LTD), además de los correspondientes acuerdos individuales de trabajo a distancia (art. 7 LTD), para identificar los mecanismos concretos previstos para la determinación, compensación y abono de tales conceptos. El abanico de fórmulas que se pueden adoptar al efecto, acomodadas a las preferencias, necesidades o exigencias de las empresas o del correspondiente sector empresarial, es amplio y variado (Romero, 2024) y su concreta configuración tiene, como veremos, una directa incidencia en su tributación.

Sin lugar a dudas, la fiscalidad de dichas entregas y compensaciones retributivas presenta cierta complejidad jurídica, dado que la regulación tributaria vigente, diseñada en un marco laboral presencial, requiere de la oportuna adaptación a las particularidades del trabajo a distancia. La inexistencia, hasta el momento, de medidas concretas encaminadas a tal fin provoca que, en más ocasiones de las deseadas, existan dudas razonables sobre la sujeción a gravamen de las compensaciones recibidas por la prestación laboral en remoto. Resulta incuestionable que la correcta interpretación y aplicación de las obligaciones fiscales relacionadas con las retribuciones asociadas al trabajo a distancia son esenciales para garantizar el cumplimiento de la legalidad vigente y evitar, así, interpretaciones administrativas restrictivas que choquen con el derecho del trabajador a percibir tales retribuciones, a la vez que eludir la generación de compensaciones encubiertas que, bajo el paraguas del trabajo a distancia, no se sometan a gravamen a pesar de que, en puridad, deberían tributar como retribuciones dinerarias o, bien, en especie.

En el contexto descrito, el presente trabajo pretende identificar los principales desafíos y oportunidades que plantea la fiscalidad de las compensaciones retributivas del trabajo a distancia a la vez que aportar propuestas normativas que contribuyan a solucionar las principales carencias que la regulación actual de esta cuestión plantea. A tal efecto, el estudio se estructura en dos grandes apartados guiados por los derechos que los arts. 11, por un lado, y 7.b y 12 LTD, por otro, reconocen a favor del trabajador a distancia.

1. Provisión al trabajador de los medios, equipamiento o herramientas necesarias para el desarrollo de la actividad laboral a distancia

Por mor del art. 11 LTD, el trabajador a distancia tiene derecho a la dotación y mantenimiento adecuado, por parte de la empresa, de todos los medios, equipos y herramientas necesarios para el desarrollo de su actividad laboral. Para dar cumplimiento a esta obligación, el empleador puede hacer uso de fórmulas diversas: desde la entrega directa o cesión de uso de tales medios al trabajador, hasta el abono de una cuantía dineraria para que sea el trabajador quien los adquiera o bien para compensarlo por el uso de sus medios personales. En este contexto, en el presente apartado nos proponemos analizar la tributación de las principales fórmulas que las empresas pueden utilizar para proveer al trabajador de las herramientas, equipamiento y medios necesarios para el desempeño de su trabajo, tomando en consideración el uso de los mismos para fines exclusivamente laborales o, bien, por ser susceptibles de uso privado, también potencialmente dispuestos a favor del trabajador para su uso particular, al ser esta una circunstancia que, a la vista de la doctrina administrativa vigente, tiene una directa incidencia en la tributación de estas entregas.

1.1. Tributación de la entrega de medios, equipamientos o herramientas al trabajador a distancia para su exclusivo uso laboral

Con carácter general, cualquier prestación económica, ventaja o utilidad recibida en el contexto de la correspondiente relación laboral o estatutaria en pago o remune-

ración de los servicios prestados por cuenta ajena queda sujeta a tributación en el IRPF de su perceptor como rendimiento del trabajo personal. En este sentido, el art. 17.1 LIRPF señala que «se considerarán rendimientos íntegros del trabajo todas las contraprestaciones o utilidades, cualquiera que sea su denominación o naturaleza, dinerarias o en especie, que deriven, directa o indirectamente, del trabajo personal o de la relación laboral o estatutaria y no tengan el carácter de rendimientos de actividades económicas». Así, salvo exclusión expresa, la totalidad de las retribuciones, dinerarias o no, percibidas por el trabajador a distancia, dentro de la respectiva relación laboral de dependencia, deberán integrarse en su autoliquidación del IRPF como rendimientos del trabajo personal.

En este contexto, cuando la empresa entrega al trabajador equipos, medios o herramientas para el desempeño de sus tareas, la primera cuestión que surge es su posible calificación como retribución en especie del trabajo personal, puesto que dicha entrega constituye una utilidad o prestación a favor del empleado, satisfecha *in natura*, que percibe a causa de su condición de trabajador. Para abordar esta cuestión es preciso acudir a la definición y caracterización que de tales retribuciones efectúa el art. 42.1 LIRPF, de acuerdo con el cual «constituyen rentas en especie la utilización, consumo u obtención, para fines particulares, de bienes, derechos o servicios de forma gratuita o por precio inferior al normal de mercado, aun cuando no supongan un gasto real para quien las conceda». Una primera aproximación al precepto nos lleva a interpretar que la entrega de equipos, medios o herramientas al trabajador a distancia es susceptible de ser calificada como retribución en especie, aunque, en tal caso, deberán concurrir, simultáneamente, los elementos definitorios de tales rendimientos.

Así, en primer lugar, es preciso que exista una utilización, consumo u obtención de bienes, derechos o servicios por parte del trabajador. No cabe duda de que la provisión de los aperos necesarios para el desempeño de la correspondiente prestación laboral es una retribución no dineraria que comporta la «obtención» o «uso» de un bien por parte del trabajador al proceder la empresa a ponerlos a su disposición mediante la respectiva entrega o cesión de uso de los mismos. Por otro lado, la calificación de tal provisión como retribución en especie requiere que los bienes, derechos o servicios que constituyen el objeto de la retribución sean obtenidos de forma gratuita o a un precio inferior al normal del mercado. En este contexto, la entrega de los correspondientes medios podrá ser calificada de retribución en especie cuando el trabajador no haya abonado importe alguno para poder disponer de los mismos o, bien, en caso de haber asumido parte del coste de adquisición, cuando la cuantía satisfecha por este sea inferior a su valor de mercado. Asimismo, resulta irrelevante el gasto que la entrega de tales medios suponga para el empleador y, por tanto, es intrascendente que su satisfacción conlleve o no un gasto real para quien la concede. De este modo, solo cuando dicha entrega comporte un beneficio económico al trabajador, aunque sea un simple ahorro, será posible calificarla como retribución en especie, con independencia del coste que tal retribución pueda suponer para la empresa (Mories, 2023, pág. 87).

Finalmente, deberá conceptuarse como retribución en especie aquella que haya sido entregada al trabajador para su disfrute particular o, en los términos utilizados por el legislador, cuando el trabajador proceda a la utilización, consumo u obtención, «para fines particulares», de los bienes puestos a su disposición por el empleador.[3] De tal configuración cabe inferir que la entrega de medios, herramientas o instrumentos para ser utilizados en el exclusivo desempeño de las tareas propias del puesto de trabajo, sin que los mismos sean susceptibles de uso particular, implica, de forma automática, la ausencia de retribución en especie alguna. Parafraseando a Moreno Fernández (1994, pág. 176), podemos decir que, si tales medios son facilitados por el empresario como simple instrumento de trabajo en orden a facilitar el cumplimiento del mismo, no corresponde imputar una renta para el trabajador puesto que los mismos no reportan un beneficio al empleado, sino que son una concesión para una mejor consecución de los fines y objetivos de la empresa, a la vez que resultan indispensables para el correcto cumplimiento de la prestación laboral o para el mejor desempeño de la misma.[4]

3. Como señalan Rancaño y González (2002, pág. 781), «el concepto de renta en especie tiene como eje fundamental el fin al cual se destina la retribución satisfecha al contribuyente –un fin particular–, excluyendo, por tanto, aquellas otras formas de utilización, consumo u obtención de bienes, derechos o servicios cuyo fin no sea este; por ejemplo, tratándose de rendimientos del trabajo, en los casos en los que dicha retribución sirva al objeto de la actividad ajena y dependiente que suele regular la relación entre empleador y empleado».
4. *Vid*. al respecto la Consulta Vinculante V150-22, de 31 de enero de 2022.

De lo hasta aquí expuesto podemos concluir que la entrega al trabajador a distancia de máquinas, útiles o herramientas que tengan una indubitable conexión con el desempeño de la respectiva actividad laboral y no sean susceptibles de uso particular –bien por la naturaleza o características del utensilio u objeto entregado, bien por la restricción expresa impuesta por la empresa a tal efecto–, no constituyen retribución en especie alguna y, por tanto, su entrega al trabajador queda excluida del concepto de salario y, por ende, no sujeta al IRPF de aquel. Coincidimos con Sedeño (2022, pág. 122) al considerar que, en estos casos, la entrega o cesión de uso de tales aperos al trabajador a distancia resulta equivalente a la utilización que, de los mismos, efectúan los trabajadores que pueden acceder a dicho material en el respectivo centro de trabajo por desarrollar sus tareas presencialmente sin que su uso deba suponer una carga fiscal mayor o diferenciada para el empleado que opta por desempeñar su trabajo en remoto.

1.2. Tributación de la puesta a disposición del trabajador a distancia de medios, equipamientos o herramientas susceptibles de uso privado

Aunque facilitados con el fin primordial de destinarlos a un uso laboral, puede suceder que los medios entregados por la empresa al trabajador a distancia sean susceptibles de uso privado y queden a disposición de este para que, potencialmente, pueda hacer un uso personal de los mismos. El legislador no ha ignorado el eventual uso mixto de dichos bienes por parte del trabajador a distancia al prever la posibilidad de que los convenios o acuerdos colectivos especifiquen «los términos dentro de los cuales las personas trabajadoras pueden hacer uso por motivos personales de los equipos informáticos puestos a su disposición por parte de la empresa para el desarrollo del trabajo a distancia, teniendo en cuenta los usos sociales de dichos medios y las particularidades del trabajo a distancia» (art. 17.3 *in fine* LTD). Esta posibilidad, regulada desde un prisma exclusivamente laboral, debería tener el correlativo trato tributario, de modo que cualquier uso particular de los útiles o herramientas puestos a disposición del trabajador a distancia que se corresponda con los usos sociales de dichos medios en los términos establecidos, a tal efecto, en el correspondiente convenio o acuerdo colectivo, no se someta a tributación.

Sin embargo, el parecer de la doctrina administrativa dista de esta opción, al entender que la simple disponibilidad de un bien para su potencial uso personal por parte del trabajador ya implica la existencia de una retribución en especie, con independencia de que dicho uso sea real y efectivo. En este contexto, la entrega de medios, equipamientos y herramientas al trabajador a distancia es susceptible de ser calificada como una retribución en especie sujeta a tributación si la empresa no ha limitado su uso a fines exclusivamente laborales y existe la posibilidad, aunque solo sea eso, una posibilidad, de que el trabajador haga uso de los mismos en su esfera privada.[5]

En tal caso, se plantea una primera dificultad, de difícil solución en relación con nuestro objeto de estudio, consistente en determinar la valoración y cuantificación de la respectiva retribución en especie que deriva del uso particular de los medios, herramientas e instrumentos entregados al trabajador. Al no existir una regla de valoración específica prevista para tal supuesto, procede aplicar la regla general dispuesta en el art. 43.1 LIRPF y, por tanto, atender a «su valor normal de mercado», un valor de difícil, por no decir imposible, determinación[6] al referirse, no al bien entregado, sino al valor de mercado del uso particular del mismo. Esta circunstancia nos lleva a considerar, con Mories (2023, pág. 96), que esta regla de valoración no resulta válida para cuantificar la retribución en especie que venimos estudiando y aconsejar, si la voluntad del legislador es gravar tales supuestos, el establecimiento de una regla de valoración específica que permita una estimación justa y proporcionada del respectivo uso de los bienes entregados al trabajador a distancia, a la vez que otorgar mayor seguridad jurídica a las partes. Tal regla podría seguir el formato previsto para

5. Aunque con relación al uso particular de vehículos por parte de los trabajadores, la DGT ha entendido que «procederá imputar al contribuyente una retribución en especie en la medida en que este tenga la facultad de disponer del vehículo para usos particulares, con independencia de que exista o no una utilización efectiva para dichos fines» (entre otras, consultas V1503-18, de 4 de junio, V0939-20, de 17 de abril, V1387-20, de 13 de mayo, V1261-22, de 6 de junio y la más reciente V1670-24, de 10 de junio).
6. Con acierto, Rovira (2023b, pág. 105) destaca que esta tesitura «resulta difícilmente compatible con el principio de capacidad económica (en el sentido de que la riqueza que se grave depende de la exactitud y precisión de su concreción) y con el principio de reserva de ley tributaria», a la vez que también puede contravenir el principio de seguridad jurídica.

el uso de vehículos automóviles en el art. 43.1.1º.b) LIRPF, de modo que el uso se cuantificase mediante la aplicación de un porcentaje concreto sobre el valor de mercado del correspondiente bien. Adicionalmente, en caso de que el medio, herramienta o instrumento fuese posteriormente entregado en propiedad al trabajador, se podrían descontar las imputaciones realizadas con anterioridad por el uso del bien.

Una vez cuantificada, en su caso, la retribución en especie por aplicación de la correspondiente regla de valoración, se plantea un escollo adicional consistente en determinar el grado de utilización efectiva de los bienes que se encuentran a disposición del trabajador a distancia para su uso particular. A juicio de la Administración, tal determinación debe efectuarse en atención a las horas del día en las que, al margen de la jornada laboral, el bien está a disposición del trabajador para su uso privado y, por tanto, calculado sin descontar las horas de descanso, los fines de semana o los festivos,[7] de lo que resulta un porcentaje de uso privado cercano al 80 % sobre la base del cual se calculará la retribución en especie a imputar en la nómina del trabajador.[8] En cualquier caso, la fijación del criterio de reparto a utilizar en cada supuesto concreto deberá tomar en consideración el tipo de tareas desarrolladas y las funciones propias del puesto de trabajo puesto que, aunque «la validez del criterio de disponibilidad puede resultar operativa en multitud de casos, no puede homologarse como un criterio general aplicable a cualquier situación, pues habrá supuestos en los que las características y peculiaridades de la actividad desarrollada (...) en el puesto de trabajo y otras circunstancias comporten una disponibilidad diferente».[9]

Al margen de la polémica y alambicada fiscalidad de tales retribuciones por aplicación de la normativa y doctrina administrativa analizada, nos cuestionamos si las entregas que venimos estudiando ponen de manifiesto una capacidad económica susceptible de tributación o, contrariamente, no constituyen una verdadera manifestación de riqueza y, por tanto, no deberían quedar sujetas a tributación. Siguiendo a Durán Sindreu (2020), entendemos que el uso particular de los medios entregados al trabajador únicamente puede ser considerado una retribución en especie cuando se trate de una «contraprestación o utilidad que derive, directa o indirectamente, del trabajo personal o de la relación laboral», según prevé el art. 17.1 LIRPF, o bien se trate de percepciones por «la prestación profesional de servicios laborales por cuenta ajena, ya retribuyan el trabajo efectivo, cualquiera que sea la forma de remuneración, o los períodos de descanso computables como trabajo», según determina el art. 26.1 del Estatuto de los Trabajadores. Solo en tal caso cabría considerar que dicha entrega tiene naturaleza retributiva y, en consecuencia, quedar sujeta a tributación.

A nuestro juicio, la LTD deja claro que la dotación de medios al trabajador a distancia para que desempeñe sus tareas laborales es un derecho de aquel y, a su vez, una obligación de la empresa y, por tanto, queda al margen de cualquier pacto de naturaleza retributiva que pueda estipularse entre las partes. En este sentido, la entrega de tales medios tiene su razón de ser en la imperativa necesidad de disponer de los instrumentos necesarios para llevar a cabo las tareas propias del puesto de trabajo, sin que corresponda al empleado asumir ningún coste consustancial al desarrollo del mismo. En consecuencia, la plena disponibilidad de dichos medios no comporta beneficio alguno para el empleado que pueda ser considerado una contraprestación por el trabajo realizado, sino más bien una entrega cuyo fin no es otro que el de facilitar el cumplimiento de los objetivos definidos por la empresa, quien, en definitiva, es la que obtiene el beneficio principal por el citado uso (Mories, 2023, pág. 87). A mayor

7. En este sentido, la DGT entiende que no son aceptables como medios de valoración «las horas de utilización efectiva o kilometraje, pues el parámetro determinante debe ser la disponibilidad para fines particulares» (entre otras, consultas V0939-20, de 17 de abril, V1261-22, de 6 de junio y V1670-24, de 10 de junio). Este mismo criterio es adoptado por el TEAC, entre otras, en las resoluciones de 3 de diciembre de 2009, 17 de marzo de 2010 y 5 de octubre y 4 de diciembre de 2017. En el ámbito judicial se ha mantenido este mismo criterio (entre otras, SSAN de 22 de enero, 22 de julio y 30 de septiembre de 2020), aunque existen puntuales sentencias en las que se han aplicado criterios más flexibles, defendiendo la valoración de la retribución en especie en atención al «uso real» del bien para fines particulares y no a la «facultad de utilización del mismo» (en este sentido, SSAN de 13 de abril de 2009 y 8 de abril de 2012). Sobre la evolución de la doctrina administrativa en esta materia *vid*. Gutiérrez Abarquero (2020).
8. Frente a este criterio, algunos autores se han mostrado partidarios de aplicar una regla similar a la prevista en el art. 30.2.5º.b) RIRPF, de modo que se previese un grado de afectación laboral del bien del 30 % diario, lo que llevaría a presumir que el restante 70 % corresponde al potencial uso privado del bien. En este sentido, Chico de la Cámara (2021, pág. 3), Rovira (2021, pág. 28) y Gorospe (2022, pág. 283).
9. Consulta DGT V0228-2025, de 4 de marzo.

abundamiento, entendemos que el uso particular que el trabajador pueda realizar de tales medios resulta residual, accesorio e irrelevante respecto a otros de especial trascendencia, como lo es su uso esencialmente laboral, por lo que no cabe considerar que el potencial uso privado del bien suponga una contraprestación que deba someterse a gravamen.[10]

Por los motivos expuestos, creemos oportuno sugerir la incorporación de un supuesto de no sujeción en la normativa del IRPF que excluya de la consideración de retribución en especie la entrega de herramientas, instrumentos y medios a los trabajadores a distancia cuando resulten necesarios para el desempeño de la prestación laboral, en concordancia con lo establecido en el respectivo acuerdo de trabajo a distancia y, en su caso, en las disposiciones convencionales, por entender que no existe manifestación de riqueza alguna susceptible de imposición.[11] Con los mismos efectos excluyentes, aunque con distinta articulación técnica, también podría optarse por configurar un supuesto de exención. En tal caso, la medida partiría de la existencia de una renta gravable resultante de la cuantificación del potencial uso privado del bien entregado al trabajador y la exclusión de tributación encontraría su justificación en razones esencialmente extrafiscales en aras a incentivar las bondades de esta modalidad laboral –como podría ser la contribución del trabajo a distancia en la satisfacción de los grandes retos que plantean los Objetivos de Desarrollo Sostenible al impulsar la adopción de tecnologías digitales, conectividad y prácticas de trabajo en áreas con menos oportunidades, en la línea de los ODS 9 y 10, o bien promover la sostenibilidad medioambiental por la reducción de los desplazamientos y su impacto en la disminución de las emisiones de gases de efecto invernadero, en coherencia con los ODS 11 y 13, o bien favorecer el adecuado equilibrio entre la vida personal, familiar y laboral, la ergonomía y la reducción de las cargas laborales desiguales en el marco de los ODS 3 y 5,[12] por citar algunos ejemplos–.

La no tributación de la entrega de tales medios al trabajador a distancia, sea mediante el establecimiento de un supuesto de no sujeción o bien de exención, ha sido la alternativa adoptada en gran parte de los países de nuestro entorno. Así, por citar algunos ejemplos, Alemania, Reino Unido o Irlanda han optado por no someter a tributación la entrega del equipamiento de oficina destinado a uso profesional si la empresa mantiene su propiedad y, además, en el caso del Reino Unido e Irlanda, si su uso privado no es significativo. Por su parte, Bélgica excluye de gravamen la entrega de material de oficina que resulte necesario para la realización normal de las actividades profesionales y en los Países Bajos se prevé la exención total de los materiales y herramientas que la empresa suministre al empleado a distancia.[13] Asimismo, en este punto resulta oportuno referirnos a la reciente modificación introducida en las normas reguladoras del IRPF de los territorios forales de Vizcaya y Guipúzcoa para excluir de la consideración de retribución en especie «la entrega por parte del empleador o empleadora de los medios necesarios para el desarrollo de su actividad laboral, en la modalidad de teletrabajo, en las condiciones que se establezcan reglamentariamente».[14] Debemos congratularnos con esta iniciativa, aunque será preciso esperar al correspondiente desarrollo reglamentario para conocer los requisitos que resultaran exigibles para la exclusión de gravamen de tales entregas.

10. Sobre el particular, resulta de interés la posición mantenida por la DGT, entre otras, en la Consulta V0968-08, de 14 de mayo, al negar que el uso privado vinculado a la cesión gratuita de vivienda pueda tener la consideración de retribución en especie cuando dicho uso particular resulta irrelevante o accesorio respecto a otros de especial trascendencia, como sería el uso de la vivienda por motivos de seguridad. Asimismo, nos adherimos a la opinión de los autores que han abogado por la aplicación analógica del art. 22.4 RIRPF en aras a excluir de la consideración de retribución en especie el uso del respectivo bien, para fines privados, en días y horas inhábiles por entender que en tal caso dicho uso es accesorio y notoriamente irrelevante. Son de este parecer Durán Sindreu (2020), Chico de la Cámara (2021, nota núm. 4), Rovira (2021, pág. 19), Casanellas (2022, pág. 266), Gorospe (2022, pág. 283), Mories (2023, pág. 92), y Jabalera (2024, pág. 269).
11. En este mismo sentido, Rovira (2021, pág. 22), Mories (2021, pág. 44) y Sedeño (2022, págs. 125-126), así como por el Comité de personas expertas encargado de la elaboración del *Libro blanco para la reforma tributaria* (2022, págs. 607-608).
12. Para mayor detalle sobre el impacto del trabajo a distancia en la satisfacción de los ODS, vid. Millan (2023) y Otoya y Bolaños (2024).
13. Para una visión detallada del tratamiento tributario que la entrega de tales medios tiene en los principales países de nuestro entorno, nos remitimos al estudio de KPMG (2021).
14. *Cfr*, art. 1.Dos de la Norma Foral 2/2025, de 9 de abril, por la que se aprueban medidas para la revisión fiscal del sistema tributario del Territorio Histórico de Bizkaia y art. 1.Dos de la Norma Foral 1/2025, de 9 de mayo, por la que se aprueba la reforma del sistema tributario del Territorio Histórico de Guipúzcoa y otras modificaciones tributarias.

En cualquier caso, hasta que se aprueben medidas normativas específicas en la materia y en aras a limitar las nefastas consecuencias tributarias derivadas de la estricta interpretación administrativa vigente, creemos que es esencial que, en el acuerdo de trabajo a distancia firmado entre el trabajador y la empresa y, en su caso, en el correspondiente convenio o acuerdo colectivo, se proceda a una identificación precisa de los medios, herramientas y equipos entregados al trabajador, poniendo especial énfasis en su uso exclusivamente laboral y a la naturaleza no retributiva de su entrega.[15] A tal efecto, recomendamos que se expliciten las condiciones de uso de los útiles informáticos, así como las limitaciones y las facultades de control empresarial respecto al uso de dichos medios –tales como restricciones de acceso a contenidos de índole personal, a redes sociales o a direcciones de correo no corporativo, o bien protocolos de seguridad en el acceso a documentos compartidos– (Fragua y Rosanas, 2020).[16] Aunque deberá ser la Administración quien acredite, aunque sea mediante pruebas indiciarias, que los medios, herramientas o equipos se están usando, de forma efectiva, también para fines particulares (Chico de la Cámara, 2021), la concreción del uso exclusivamente laboral en el respectivo acuerdo de trabajo constituye una prueba relevante para rebatir el criterio administrativo. Entendemos que esta concreción permitiría acreditar, de forma indefectible, la singular vinculación de dichos bienes a la exclusiva prestación laboral del trabajador y excluir la cesión de uso de los mismos de la consideración de retribución en especie y, por tanto, de su tributación en el ámbito del IRPF del empleado en remoto. Asimismo, si en el acuerdo de trabajo a distancia también se admite un uso particular de los medios de trabajo entregados, es recomendable que se identifique, de la forma más clara posible, la jornada laboral del empleado y, en su caso, las características y particularidades del puesto de trabajo en aras a justificar los criterios utilizados por la empresa para efectuar la valoración de la retribución en especie y el criterio de reparto empleado para su integración en la nómina del trabajador.

1.3. Mecanismos alternativos para la dotación de las herramientas, medios o instrumentos necesarios al trabajador a distancia

Junto a los supuestos analizados en el apartado anterior, la empresa puede optar por otras fórmulas dirigidas, también, a dotar al trabajador a distancia de los recursos necesarios para desempeñar las tareas propias de su puesto de trabajo. Así, puede proceder a la entrega de una cuantía dineraria, a tanto alzado, sin requerir que el trabajador justifique el gasto. En el marco legal vigente, tales pagos deben ser considerados una retribución dineraria del trabajo personal en los términos establecidos en los arts. 17.1 y 42.1 *in fine* LIRPF, puesto que lo entregado al trabajador no son bienes, sino importes en metálico, a la vez que suponen una prestación económica de carácter general que, al no existir una identificación específica de su destino, podrán ser empleados en lo que el trabajador desee.[17] En este contexto, la imposibilidad de vincular el importe abonado por el empleador con la adquisición de las herramientas necesarias para el desempeño del trabajo a distancia comporta que tal abono quede sujeto a tributación, de modo que la empresa deberá adicionar tales cuantías a las respectivas retribuciones anuales y practicar e ingresar la correspondiente retención a cuenta. Aunque esta situación pueda considerarse penalizadora en los supuestos en los que el trabajador destina, realmente, los importes recibidos a la adquisición de algún equipamiento necesario para el desempeño de su trabajo (Mories, 2023, pág. 103), la falta de justificación documental imposibilita constatar la realidad y finalidad del gasto lo que nos lleva a considerar que, con la normativa vigente, corresponde sujetar a tributación el pago recibido.

Por otro lado, si quien adquiere los medios o herramientas es el propio trabajador y el empleador procede al posterior reembolso del gasto tras la justificación documental del mismo, el impacto fiscal de dicha operación deberá determinarse tomando en consideración el sujeto al que corresponde la titularidad del bien. Así, si el utensilio adquirido pasa a ser titularidad de la empresa, de modo que

15. Tal sugerencia resulta unánime por parte de la doctrina que ha estudiado esta problemática. Por todos, Chico de la Cámara (2021), Rovira (2021, pág. 26), Mories (2023, pág. 101) y Sedeño (2023, pág. 126).
16. A este respecto resulta ilustrativa la consulta de la DGT V0159-22, de 31 de enero, al considerar que la prohibición de uso privativo de los teléfonos de empresa en el código de conducta y en las cláusulas de los contratos individuales de los trabajadores, asevera que dichos terminales son una herramienta de trabajo cuya cesión no constituye retribución en especie.
17. Así lo ha entendido la DGT en las consultas V3986-15, de 15 de diciembre y V1039-18, de 24 de abril, en relación con las cuantías recibidas por los agentes de policía de paisano en concepto de indemnización sustitutoria del uniforme.

el trabajador actúa como un simple intermediario en la compra, nos hallaríamos, nuevamente, ante una cesión de uso de un bien propiedad del empleador, por lo que podría volver a surgir el problema del doble uso del bien y su posible consideración como retribución en especie.[18] En tal caso, resulta incuestionable que las cuantías abonadas por la empresa para compensar al trabajador por la adquisición de los correspondientes medios, herramientas o equipos no deben tributar en la parte que corresponde a su uso para fines laborales, puesto que no constituyen contraprestación alguna por la prestación de los respectivos servicios laborales, sino que, por imperativo legal, buscan compensarlo por los gastos incurridos en la adquisición de un bien necesario para el desempeño de la prestación laboral y directamente vinculado a la misma. En este contexto, cabe entender que el pago efectuado por la empresa en los términos descritos no constituye una verdadera manifestación de riqueza para el empleado, de modo que no puede apreciarse la existencia de una mínima capacidad económica susceptible de imposición puesto que el reintegro de tales cuantías no supone una mayor riqueza para aquel sino el resarcimiento de unos gastos que buscan dotar al trabajador de las herramientas requeridas para llevar a cabo las tareas propias del lugar de trabajo en equivalentes condiciones a quienes desempeñan su trabajo presencialmente, y que, como tales, deben ser asumidos por el empleador. De no ser así, el trabajador a distancia podría ver alteradas sus retribuciones por el simple hecho de acogerse a esta modalidad laboral, vulnerándose, en consecuencia, la igualdad de trato referida en el art. 4 LTD.[19]

Asimismo, si trasladamos aquí las consideraciones efectuadas en el epígrafe anterior, nos inclinamos a pensar que el uso privado que el trabajador pueda realizar de los bienes adquiridos es residual, accesorio y notoriamente irrelevante respecto al uso esencialmente laboral del bien, de modo que las cuantías abonadas por la empresa para compensar su adquisición no deberían tributar si quedan debidamente justificadas y acreditada su propiedad por parte de la empresa. Sin embargo, la aplicación de la regulación actual y la doctrina administrativa existente no permite llegar a esta conclusión de forma irrefutable, por lo que, como ya hemos puesto de relieve, nos parece necesaria la incorporación de una previsión normativa expresa en el sentido apuntado. De este modo, únicamente cuando la cuantía abonada resultase superior a la justificada en la correspondiente factura por la adquisición de los equipos, medios y herramientas requeridos al efecto, correspondería tributar por el exceso, puesto que el mismo sí supondría un beneficio económico para quien lo recibe.

Sin perjuicio de estas consideraciones, creemos que para reforzar la prueba relativa a la propiedad del bien por parte de la empresa sería conveniente que en los acuerdos individuales de trabajo a distancia y, en su caso, en los convenios o acuerdos colectivos, quedase constancia expresa de la obligación por parte del trabajador de devolver el material a la empresa en caso de cese de la relación laboral o bien en el supuesto de reversión de la modalidad de trabajo a la presencialidad total. Asimismo, sería conveniente que la factura emitida por el vendedor estuviese a nombre de la empresa, lo que constituiría un elemento de prueba adicional ante eventuales comprobaciones posteriores por parte de la Administración Tributaria (Mories Jiménez, 2021, pág. 21), además de ser un requisito necesario para la deducción de las cuotas de IVA si el empleador tiene derecho a ello.

Por su parte, si, tras el reembolso del gasto, la propiedad del bien pasa a ser del trabajador, nos hallaríamos ante una retribución dineraria del trabajo personal sujeta a tributación en el IRPF en virtud del art. 42.1 *in fine* de la LIRPF, lo mismo que sucedería si la empresa paga una cuantía que viene a compensar el uso de medios propios del trabajador. En este supuesto, la inexistencia de obligación de restitución alguna y su plena disponibilidad para el uso personal del trabajador contribuyen a dar argumentos a la Administración para entender que nos hallamos ante

18. Lo mismo cabe decir respecto a los supuestos en los que la empresa abona directamente al proveedor el importe del bien adquirido por el trabajador. En tales casos, la retribución en especie se articula mediante el pago directo del empleador al tercero en cumplimiento de los compromisos asumidos con los trabajadores en el respectivo contrato de trabajo o convenio colectivo. En este sentido, Consulta V1804-23 de 21 de junio.
19. A mayor abundamiento, como más elevados sean los gastos a compensar por la empresa mayor será la cuantía económica a recibir por el trabajador y, por tanto, mayor la base imponible y la cuota tributaria correspondiente a su tributación en el ámbito de la imposición personal del trabajador, lo que contravendría, además, las premisas del principio de progresividad (vertemos aquí las conclusiones planteadas por Rovira (2023a, pág. 170) en relación con la compensación al trabajador por el uso de sus propios medios personales).

una retribución del trabajo personal sujeta a tributación.[20] Sin embargo, también aquí resulta cuestionable esta posición, puesto que la finalidad del reembolso económico no es otra que compensar económicamente al empleado por la adquisición de elementos necesarios para el desempeño de su trabajo o bien por el uso de sus bienes personales con el mismo fin, aun cuando exista una utilización privada de los mismos que, como venimos argumentando, entendemos residual y accesoria, más aún si se tienen en cuenta las características y naturaleza de los bienes afectados (piénsese, por ejemplo, en un reposapiés, un flexo o una silla ergonómica).

Por todo ello, nos sumamos a la propuesta de Rovira (2021, pág. 26), quien aboga por eximir de tributación a las cuantías abonadas por los empleadores para cubrir el importe de adquisición de los medios, herramientas o instrumentos necesarios para el desempeño del trabajo a distancia «y es que, tanto si se suministran como si se compensa su coste, se trata de unos mismos elementos que, con un mismo coste, se destinan a una misma finalidad». En este contexto, entendemos que en todos los supuestos analizados el pago efectuado por la empresa busca compensar al empleado por unos gastos directamente vinculados a su trabajo, por lo que consideramos que tales cuantías no deberían someterse a tributación y deberían recibir el mismo tratamiento que el que propondremos, en el siguiente apartado, respecto a la compensación de gastos ocasionados por el desarrollo del trabajo a distancia. En aras de evitar reiteraciones innecesarias, nos remitimos al mismo.

2. Compensación de los gastos ocasionados por el desarrollo de la actividad laboral a distancia

En virtud de los arts. 7.b y 12 LTD, el trabajador en remoto debe ser compensado por los gastos que pudiera tener por la prestación de servicios a distancia,[21] siendo preciso que la cuantificación, forma y momento en que dicha compensación debe ser efectuada conste, de forma expresa, en el acuerdo de trabajo a distancia firmado entre la empresa y el empleado, atendiendo, en su caso, a las previsiones recogidas en el respectivo convenio o acuerdo colectivo de aplicación. Como ha destacado el Tribunal Supremo, nos hallamos ante una obligación legalmente impuesta al empresario en virtud de la cual debe compensar económicamente, de forma imperativa, los gastos en que pudiera incurrir el trabajador a distancia por la prestación de los correspondientes servicios, sin que quepa considerar que las ventajas que ofrece esta modalidad laboral son, por sí mismas, modos en que pueda materializarse la citada compensación (por todas, SSTS de 4 de marzo y 2 de abril de 2025).

Esta obligatoriedad nos lleva a considerar que las cuantías reembolsadas por la empresa en concepto de gastos ocasionados por el desarrollo de la actividad laboral a distancia no deben tributar, pues su objetivo no es retribuir al empleado en remoto por el trabajo efectuado, sino resarcirlo por el desembolso realizado respecto a unos gastos directamente vinculados al desempeño de la prestación laboral y que, como tales, deben ser soportados por el empleador. En tales circunstancias, entendemos que dichas cuantías tienen una naturaleza indemnizatoria,[22] y, por ende, no cabe considerar que su percepción suponga manifestación de riqueza o indicio de capacidad económica alguna susceptible de gravamen en el IRPF, constituyendo, en consecuencia, un supuesto de no sujeción. A tal conclusión podemos llegar si tomamos en consideración otros supuestos similares previstos en la LIRPF, como sería el caso de las dietas o gastos de manutención y estancia o del complemento de transporte abonado a modo de compensación de los gastos de desplazamiento, cuya naturaleza indemnizatoria ha sido expresamente reconocida por el Tribunal Supremo cuando el trabajador incurre en el respectivo gasto con motivo de su trabajo, determinando, sin embargo, su naturaleza

20. En este sentido se ha manifestado la DGT en la Consulta V0932-14, de 2 de abril, en relación con las cuantías abonadas por la empresa a los trabajadores para la adquisición de un terminal móvil utilizado, indistintamente, para fines laborales y personales.
21. Como indica Alzaga (2022, pág. 40), «la finalidad del art. 12 LTD es que la persona trabajadora no asuma ningún gasto por prestar servicios desde su domicilio: ni los gastos derivados de las herramientas, medios y equipos (art. 11 LTD), ni los gastos corrientes derivados de la prestación de servicios desde su vivienda o desde el lugar libremente elegido por la persona trabajadora, ni los denominados complementos extrasalariales, cuya naturaleza es resarcitoria y compensan a la persona trabajadora por otros gastos soportados».
22. En este mismo sentido, Durán Sindreu (2020), Rovira Ferrer (2021, pág. 27) y Mories (2023, pág. 112).

retributiva si la correspondiente compensación es abonada con independencia del trabajo realizado y de las circunstancias vinculadas al mismo.[23] En cualquier caso, la exclusión de tributación en los términos expuestos requiere la previa justificación del gasto, de modo que no pueda objetarse la realidad del mismo y su vinculación directa y principal con la labor profesional desempeñada por el trabajador. Asimismo, si la cuantía abonada fuese superior a la justificada, el exceso constituiría renta gravable en el IRPF en concepto de rendimiento del trabajo de carácter dinerario.[24]

No obstante, la intrínseca dificultad que entraña la delimitación de las cuantías vinculadas al uso laboral y personal de determinados consumos o suministros –piénsese, por ejemplo, en la factura de teléfono, la conexión a internet o el consumo de luz, agua o calefacción de la vivienda del trabajador a distancia–, así como el inconveniente que supone la individualización del gasto a compensar a cada empleado, han llevado a las empresas a utilizar mecanismos de compensación a tanto alzado. Así, la formulación convencional más habitual para proceder a la compensación de los gastos derivados del trabajo a distancia consiste en abonar al trabajador una cuantía fija –diaria, mensual o anual–, que en algunos supuestos se establece como cuantía mínima y en otros como límite máximo, a concretar en el respectivo acuerdo individual de trabajo a distancia, y que, con carácter general, no requiere justificación alguna (Romero, 2024, págs. 33-34). En el marco de la normativa vigente, la entrega de tal cantidad a tanto alzado constituye un complemento de carácter dinerario y naturaleza retributiva y, en consecuencia, íntegramente sujeto a tributación en el IRPF del trabajador perceptor de las mismas, dada la dificultad de probar la realidad del gasto y su exclusiva vinculación con la actividad laboral.

Nos inclinamos a pensar que el actual tratamiento tributario de las compensaciones por gastos vinculados al trabajo a distancia no se corresponde con la finalidad de tal medida, que no es otra que evitar que el trabajador en remoto asuma unos costes que, por corresponder a herramientas necesarias para el desempeño del trabajo, debe asumir la empresa y que, en caso de desempeñar sus labores presencialmente, no afrontaría.[25] Así y todo, vuelve a surgir aquí la dificultad, por no decir imposibilidad, de deslindar los gastos que corresponden a un uso personal o bien laboral de los correspondientes suministros o servicios y, por tanto, la inviabilidad de determinar la proporción del gasto compensado que, en su caso, no debería someterse a tributación por estar estrictamente vinculado al ámbito laboral. En este contexto, podría resultar adecuado establecer una norma de simplificación, de carácter objetivo, de acuerdo con la cual se previese que un porcentaje determinado del respectivo gasto efectuado en los conceptos que venimos estudiando se entendiese afectado al desarrollo de la actividad laboral, de modo que su importe no se sometiese a tributación si existe la correspondiente justificación documental.[26] Con un efecto similar, otra opción sería configurar una desgravación fiscal, a modo de gasto deducible para la determinación de los rendimientos netos del trabajo personal, que permitiese deducir un porcentaje de los gastos satisfechos por el trabajador a distancia en dichos conceptos.[27] O, más simple aún: prever la exención de las cuantías satisfechas en concepto de compensación por gastos vinculados al trabajo a distancia en los términos

23. *Vid*. a este respecto, SSTS de 3 de octubre de 2013 y 20 de marzo de 2024 en relación con los cheques comida y las SSTS de 1 de junio de 2022, 23 de octubre de 2024 y 11 de enero de 2024 respecto al plus de transporte. En este mismo sentido, la DGT ha puesto de relieve que, «si tal compensación se limita a reembolsar a los empleados por los gastos ocasionados por esa utilización en el desarrollo de su trabajo cabe afirmar que no comporta para ellos un supuesto de obtención de renta, es decir, no se entiende producido el hecho imponible del impuesto» (Consulta V0932-14, de 2 de abril).
24. *Vid*. al respecto, consulta de la DGT citada en la nota anterior.
25. En consonancia con esta idea, tales compensaciones no cotizan a la Seguridad Social, como ha puesto de relieve la TGSS en su Boletín de Noticias RED 3/2021, de 28 de mayo.
26. Esta fórmula ha sido adoptada en Alemania en relación con los gastos de telefonía, de modo que queda libre de tributación el 20 % de los gastos mensuales de telefonía debidamente justificados, con un máximo de 20 € (KPMG, 2021, pág. 4). Se trata de una fórmula similar a la establecida en el art. 30.2.5ºb) RIRPF comentada en la nota núm. 8.
27. Esta ha sido la solución adoptada en Irlanda, país que permite aplicar una desgravación atendiendo a los gastos efectivamente soportados por el trabajador a distancia, atendiendo al número de días en los que ha trabajado en remoto y al tipo marginal al que tributa. Esta alternativa únicamente está prevista para los supuestos en los que el empleador no abona al trabajador compensación alguna por dichos conceptos (página web del Revenue, fecha de consulta 22/07/2025).

establecidos en el respectivo Convenio Colectivo, de modo que, fuera cual fuese la fórmula adoptada por la empresa para realizar tal compensación, las cuantías abonadas no deberían adicionarse a los rendimientos del trabajo si se ajustan a las previsiones convencionales.[28]

Asimismo, otra opción podría ser disponer una exención similar a la prevista en el art. 17.1.d) LIRPF para las dietas y asignaciones por gastos de viaje, de modo que se fijaran unas cuantías a tanto alzado que quedasen excluidas de gravamen dentro de los límites reglamentariamente establecidos.[29] Esta ha sido la opción escogida por algunos países de nuestro entorno, como Francia[30] o Portugal,[31] que han establecido un sistema de compensación a tanto alzado por gastos relativos a equipos informáticos, conexiones y otros suministros necesarios para el correcto desarrollo del trabajo a distancia. En concreto, las cuantías exentas varían en función del número de días en que el empleado trabaja a distancia y de la existencia o no de convenio colectivo que regule la cuestión. Así, en Francia, se consideran exentos de tributación, sin necesidad de aportar justificación alguna, 3,25 €/día o 2,70 €/día, con un máximo de 71,50 € o 59,40 €, según exista o no convenio colectivo, respectivamente. Incluso si superan los citados límites, la cuantía recibida a modo de compensación estará exenta de tributación siempre que los gastos estén justificados. Por su parte, en Portugal, se entiende que no constituye rendimiento sujeto a tributación 1 € por día de trabajo en remoto –0,10 €/día en concepto de consumo eléctrico, 0,40 €/día por consumo de internet y 0,50 €/día en relación con el equipo informático correspondiente–, pudiendo incrementarse la cuantía exenta en un 50 % si dicho importe estuviese previsto en un instrumento de regulación colectiva.

Si bien es cierto que el empleo de cualquiera de las fórmulas objetivas indicadas no toma en consideración las particularidades propias de cada puesto de trabajo que, sin lugar a dudas, pueden variar sustancialmente de un supuesto a otro (Rovira, 2021, pág. 29), lo cierto es que las mismas proporcionan un tratamiento neutral, coherente con el principio de igualdad, entre el trabajo a distancia y el trabajo presencial, a la vez que contribuyen a proporcionar una mayor seguridad jurídica y facilitan la gestión y control de las correspondientes obligaciones tributarias de los agentes implicados, empresas y trabajadores.

Conclusiones

Tras el análisis efectuado, hemos podido constatar las inconsistencias de la tributación que, a tenor del ordenamiento vigente, corresponde atribuir a las compensaciones retributivas por el desarrollo del trabajo a distancia. A lo largo del estudio se han efectuado diversas propuestas que pueden resultar útiles para proporcionar coherencia al sistema y alinear el tratamiento tributario de tales compensaciones con la finalidad con la que, desde la perspectiva laboral, fueron concebidas por el legislador. Así, en la medida en que el trabajador a distancia tiene el derecho a ser dotado de los medios, herramientas o equipamiento preciso para el desarrollo de la respectiva prestación laboral y la empresa la correlativa obligación de suministrarlos, cabe entender que tal dotación no debe someterse a tributación, con independencia de que los elementos sean directamente entregados por el empleador o bien se proceda a la entrega de una cuantía dineraria para costear su adquisición o compensar el uso de los medios propios

28. Esta ha sido la opción adoptada en los territorios forales de Guipúzcoa, Vizcaya y Álava tras la reciente modificación del IRPF introducida mediante las Normas forales 1/2025, de 9 de mayo, 2/2025, de 9 de abril y 3/2025, de 9 de abril, respectivamente. Las tres normas coinciden en su redacción, declarando que tienen la consideración de rendimientos del trabajo sujetos a tributación «las cantidades puestas a disposición de la persona trabajadora en concepto de compensación por los gastos soportados por esta como consecuencia de su trabajo desarrollado en la modalidad de teletrabajo, excepto aquellas que no excedan de los importes establecidos en cada momento por Convenio Colectivo, hasta el límite del valor de mercado de los citados gastos». Se trata de un avance significativo en la regulación de la materia que venimos estudiando, aunque el inciso final puede seguir planteando dificultades prácticas puesto que no siempre será fácil determinar el valor de mercado del gasto compensado.
29. Se han manifestado partidarios de esta alternativa, entre otros, la Comisión de expertos que elaboraron el *Libro Blanco para la reforma tributaria* (2022, pág. 607), Sedeño (2022, pág. 130), Gorospe (2022, pág. 284), Díaz Calvarro (2022, pág. 449), Rovira (2023b, pág. 117), Mories (2023, pág. 112), y Jabalera (2024, pág. 272).
30. *Cfr*. *Formulaire nº2041-GP-Allocations pour frais d'emploi* (2024, pág. 5) e información disponible en la página web de la DGFiP (fecha de consulta 22/07/2025).
31. Art. 2 de la Orden nº292-A/2023, de 29 de septiembre.

del trabajador, y con independencia, también, de que los mismos sean o no susceptibles de uso privado.

De este modo, si el elemento o medio en cuestión no es susceptible de uso particular, bien por la naturaleza o características del mismo, bien por la restricción expresa impuesta por la empresa a tal efecto, su recepción no puede ser calificada como retribución en especie, como tampoco debe ser considerada retribución dineraria la cuantía monetaria entregada por la empresa para compensar su adquisición, pues su uso responde, en exclusiva, al fin de facilitar el cumplimiento de los objetivos de la empresa que es quien, en definitiva, resulta beneficiada por el citado uso.

De igual modo, aun existiendo un potencial uso particular del respectivo bien, nos inclinamos a pensar que el mismo carece de la necesaria relevancia tributaria para poder otorgarle naturaleza retributiva, resultando ser un uso que resulta residual, accesorio y notoriamente irrelevante respecto a su uso principal o esencial, que no es otro que el laboral. Dado que esta interpretación no resulta irrefutable a la vista de la doctrina administrativa existente, sería preciso que el legislador previese, de forma expresa, la no tributación de las diversas fórmulas empleadas para dotar al trabajador de los medios, herramientas y equipamiento necesario para el desempeño de la prestación laboral, se suministren directamente los bienes, se compense su adquisición mediante la entrega de una cuantía dineraria o bien el uso de los medios propios. A tal efecto, puede proceder a la articulación técnica de un supuesto de no sujeción o, en su caso, de exención, dos medidas que, aunque con un resultado económico equivalente, responden a fundamentos distintos. Así, si se entiende que el uso particular del bien constituye una manifestación de riqueza susceptible de imposición, el legislador debería optar por la configuración de una exención, mientras que, si se entiende que el mismo no supone riqueza alguna, deberá establecerse un supuesto de no sujeción, quedando al margen del hecho imponible gravado por el IRPF.

Por su parte, en caso de que la empresa abone una compensación económica al trabajador por los gastos ocasionados por el trabajo a distancia, entendemos que las cuantías entregadas por tal concepto no deben quedar sujetas a tributación, puesto que su objetivo no es retribuir al trabajador en remoto, sino resarcirlo por el desembolso de unos gastos directamente vinculados a su trabajo y sin la satisfacción de los cuales no habría podido desempeñar las tareas encomendadas por el empleador. Sin embargo, la intrínseca dificultad de individualizar estos gastos y deslindar con exactitud la parte que corresponde a la actividad laboral o bien privada, nos lleva a recomendar el establecimiento expreso de su no tributación. A tal efecto, podría adoptarse una fórmula equivalente a la prevista en el IRPF en relación con las dietas y asignaciones por gastos de viaje, de modo que las cuantías recibidas quedasen exentas si existe la correspondiente justificación documental. Asimismo, otra posibilidad que podría resultar adecuada a tal fin, sería exceptuar de gravamen la cuantía resultante de aplicar un porcentaje objetivamente determinado sobre el importe del gasto debidamente justificado, o bien, con un efecto similar, permitir la aplicación de una desgravación fiscal, a modo de gasto deducible, para la determinación de los rendimientos netos del trabajo personal sujetos a tributación.

En cualquier caso, mientras no se produzcan cambios normativos, resulta esencial el contenido del respectivo acuerdo de trabajo a distancia, siendo especialmente relevante que quede recogida la naturaleza no retributiva de la entrega de medios, herramientas e instrumentos al trabajador en remoto, su exclusivo uso para fines laborales y los mecanismos de control empresarial de los mismos, así como la necesidad de aportar justificación documental de cualquier gasto cuya compensación se efectúe por el empleador.

Reconocimientos

El presente trabajo se ha desarrollado en el marco del Proyecto de investigación «El estímulo a los empleadores y la mitigación de la inseguridad jurídica: dos factores clave en la consolidación del trabajo a distancia», con referencia PID2023-146204OB-C21 y financiado por MCIN/AEI /10.13039/501100011033 y por FEDER, UE.

Referencias bibliográficas

ALZAGA RUIZ, I. (2022). «El derecho al abono y compensación de gastos en la Ley 10/2021, de 9 de julio, de trabajo a distancia». *Revista Crítica de Relaciones de Trabajo. Laborum*, n.º 2, págs. 35-53.

CASANELLAS CHUECOS, M. (2022). «Incidencia del criterio de residencia fiscal en el ámbito de la imposición personal del teletrabajador». *Revista General de Derecho del trabajo y de la Seguridad Social*, n.º 63, págs. 246-283.

CHICO DE LA CÁMARA, P. (2021). «Aspectos tributarios controvertidos del teletrabajo». *El Notario del siglo XXI*, n.º 96.

COMITÉ DE PERSONAS EXPERTAS (2022). *Libro blanco para la reforma tributaria*. Madrid: IEF.

DÍAZ CALVARRO, J.M. (2022). «Fiscalidad y teletrabajo: análisis de algunas cuestiones de interés». En: MARÍN ALONSO, I., IGARTUA MIRÓ, M.T. y SOLÍS PRIETO, C. (dirs.). *Digitalización, desarrollo tecnológico y derecho del trabajo: nuevas perspectivas de sostenibilidad*, págs. 433-459. Navarra: Aranzadi.

DURAN SINDREU, A. (2020). «¿Preocupa de verdad la fiscalidad del teletrabajo?». *Taxlandia. Blog Fiscal y de Opinión Tributaria*. [Fecha de consulta: 30 de junio de 2025].

EUROFOUND (2022). *The rise in telework: Impact on working conditions and regulations*. Luxembourg: Publications Office of the European Union.

FRAGUA, S.; ROSANAS, C. (2020). «Impuestos: los grandes olvidados en la nueva regulación del teletrabajo». *Actualidad jurídica Aranzadi*, n.º 986.

GOROSPE OVIEDO, J.I. (2022). «Medidas fiscales para un modelo de transporte urbano sostenible: impuesto de circulación, trasporte colaborativo y teletrabajo». *Documentos de trabajo del Instituto de Estudios Fiscales*, n.º 8, págs. 274-287.

GUTIÉRREZ ABARQUERO, D. (2020). *Imputación fiscal y criterios de afectación de vehículos en IRPF: análisis y propuesta preliminar*. Documentos AEDAF: Sección Asesores internos.

JABALERA RODRÍGUEZ, A. (2024). «La dimensión fiscal del teletrabajo desde la perspectiva internacional e interna». En: CASTILLO, F. y MALDONADOL, J.A. (dirs.). *Régimen jurídico del teletrabajo en las Administraciones Públicas*. Madrid: Dykinson.

KPMG (2021). *Teletrabajo. Regulación en España y en países de nuestro entorno*. Versión electrónica.

MILLAN, S. (2023). «Teletrabajo en la agenda de los objetivos de desarrollo sostenible». En: PÉREZ MARTELL, R. (dir.). *La tecnología y los objetivos de desarrollo sostenible*. Barcelona: Bosch Editor.

MORENO FERNÁNDEZ, J.I. (1994). *Las retribuciones en especie del trabajo personal en la Ley del IRPF*. Valladolid: Lex Nova.

MORIES JIMÉNEZ, M.T. (2021). «Régimen fiscal de las compensaciones retributivas derivadas del teletrabajo: cuestiones sin resolver y propuestas de regulación en el IRPF». *Quincena Fiscal*, n.º 8.

MORIES JIMÉNEZ, M.T. (2023). *Fiscalidad del teletrabajo*. València: Tirant lo Blanch.

OBSERVATORIO NACIONAL DE TECNOLOGÍA Y SOCIEDAD (2024). *Teletrabajo 2024*. Secretaría de Estado de Digitalización e Inteligencia Artificial, Ministerio para la Trasformación Digital y de la Función Pública.

OTOYA CHAVARRIA, M.; BOLAÑOS HERRERA, I. (2024). «El Teletrabajo como un mecanismo para contribuir al Desarrollo Sostenible». *Política Económica y Desarrollo Sostenible*, vol. 10, n.º 1, págs.1-22. DOI: https://doi.org/10.15359/btkp7c39

RANCAÑO MARTÍN, M.A.; GONZÁLEZ SÁNCHEZ, G. (2002). «Las rentas en especie en el impuesto sobre la renta de las personas físicas». *Revista de Derecho Financiero y Hacienda Pública*, vol. 52, nº. 266, págs. 781-828.

ROMERO BURILLO, A.M. (2024). «La regulación del contenido económico del teletrabajo en la negociación colectiva». *Revista General de Derecho del Trabajo y de la Seguridad Social*, n.º 69, págs. 1-53.

ROVIRA FERRER, I. (2021). «Las entregas y compensaciones de gastos a causa del trabajo a distancia en el IRPF de los empleados». *Revista Jurídica de Castilla y León*, nº 55, págs. 7-34.

ROVIRA FERRER, I. (2023a). «Propuestas para adaptar y mejorar el IRPF, el IS y el IVA al trabajo a distancia y la realización de actividades económicas o profesionales desde el domicilio». *Crónica Tributaria*, n.º 188, págs. 149-181. DOI: https://doi.org/10.47092/CT.23.3.5

ROVIRA FERRER, I. (2023b). *La fiscalidad del trabajo a distancia*. Pamplona: Aranzadi.

SEDEÑO LÓPEZ, J.F. (2022). *Instrumentos financieros y tributarios frente a la despoblación: retos y oportunidades en el contexto del teletrabajo*. Barcelona: Atelier.

Cita recomendada

CASANELLAS CHUECOS, Montserrat (2026). «Fiscalidad de las compensaciones retributivas percibidas por los trabajadores a distancia: cuestiones controvertidas y propuestas de regulación». En: Irene Rovira Ferrer (coord.). «Sobre la consolidación del trabajo a distancia». *IDP. Revista de Internet, Derecho y Política*, núm. 44. UOC. [Fecha de consulta: dd/mm/aa]. DOI: http://dx.doi.org/10.7238/idp.v0i44.9800298

Sobre el autor

Montserrat Casanellas Chuecos
Profesora agregada del área de Derecho Financiero y Tributario (Departamento de Derecho Administrativo, Derecho Procesal y Derecho Financiero y Tributario), Facultad de Derecho. Universidad de Barcelona
montse_casanellas@ub.edu

Ha impartido docencia en los Grados en Derecho, Gestión y Administración Pública y Relaciones Laborales, y los másteres oficiales de Gestión Cultural, Derecho de la Empresa y los Negocios y Abogacía. Ha desarrollado diversos cargos y encargos de gestión académica. Entre otros, ha sido coordinadora del Máster oficial de Gestoría Administrativa, coordinadora del máster Oficial de la Abogacía, Directora de la Escuela de Másteres y Postgrados y vicedecana de Relaciones Institucionales, Patrocinio y Postgrados de la Facultad de Derecho de la Universidad de Barcelona.

Su actividad investigadora ha estado centrada en la tributación de las entidades sin ánimo de lucro y el mecenazgo, así como en las medidas de simplificación de la tributación de las rentas empresariales, ámbitos en los que he publicado diversos artículos científicos y monografías. Asimismo, ha sido miembro de varios proyectos de investigación financiados por el Ministerio de Economía y Competitividad, la Agencia Española de Cooperación y Desarrollo, el Institut d'Estudis d'Autogovern y el Instituto de Estudios Fiscales.

Ha sido profesora visitante de la Universidad de Verona (Italia) y ha realizado diversas estancias de investigación en Brasil, Venezuela e Italia. Asimismo, en el ámbito docente, es autora de varios manuales de Derecho Financiero y Tributario, parte general y especial, y artículos sobre competencias transversales y actividades de aprendizaje por competencias.

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Monográfico: «Sobre la consolidación del trabajo a distancia» (coord.: Irene Rovira Ferrer)

La tributación del teletrabajo y el impuesto municipal sobre actividades económicas

Benjamí Anglès Juanpere
Universitat Oberta de Catalunya (UOC)

Fecha de presentación: octubre 2025
Fecha de aceptación: diciembre 2025
Fecha de publicación: marzo 2026

Resumen

El teletrabajo se ha generalizado y consolidado a partir de la pandemia de coronavirus al convertirse en una solución óptima para mantener la actividad económica y los puestos de trabajo. Sin embargo, al tratarse de una modalidad de trabajo en remoto que implica el traslado del trabajador del lugar donde radica la empresa a su domicilio particular, ello puede comportar el cambio del ordenamiento jurídico aplicable en el supuesto de que dicho traslado implique trasladarse a otro país, región o municipio. Obviamente, este cambio también tiene implicaciones fiscales, ya que determinará el derecho tributario aplicable según el territorio de destino. En los Estados multinivel, como España, estos cambios pueden afectar tanto a tributos estatales, como a regionales y locales. En este trabajo se abordan precisamente los efectos del teletrabajo en el impuesto sobre actividades económicas, especialmente los supuestos de sujeción y la aplicación de beneficios fiscales en este impuesto local.

Palabras clave

trabajo a distancia; teletrabajo; municipio; hacienda local; impuesto local; IAE

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

The taxation of telework and the municipal tax on economic activities

Abstract

Telework has become widespread and consolidated since the coronavirus pandemic, as it proved to be an optimal solution for maintaining economic activity and employment. However, since this is a remote work modality that involves the employee's relocation from the place where the company is based to their private residence, it also entails a change in the applicable legal framework if such relocation involves moving to another country, region, or municipality. Obviously, this change also has tax implications, as it determines which tax laws will apply according to the new territory. In multi-level states, such as Spain, these changes can affect state, regional, and local taxes. This paper addresses the effects of teleworking on the municipal tax on economic activities, especially the conditions for its application and the tax benefits available under this local tax.

Keywords

remote work; telework; municipality; local treasury; local tax; IAE

Introducción

El teletrabajo, como modalidad de trabajo en remoto, existe desde hace décadas. Sin embargo, el incesante avance de la tecnología y la digitalización, así como las consecuencias de la crisis sanitaria del coronavirus, han ampliado y consolidado su implantación. Sin duda, la obligación de distanciamiento social durante la pandemia convirtió el teletrabajo en una solución óptima para mantener la actividad económica y los puestos de trabajo. Superada aquella etapa, lo cierto es que el teletrabajo persiste en no pocas empresas y ramas de actividad, habiéndose convertido en una opción de trabajo viable, aceptada tanto por trabajadores como por empleadores.

De acuerdo con el art. 2.b de la Ley 10/2021, de 9 de julio, de trabajo a distancia (en adelante, LTD), el teletrabajo se define como aquel trabajo a distancia que se realiza mediante el uso exclusivo o prevalente de medios y sistemas informáticos, telemáticos y de telecomunicación. Es decir, por una parte, el teletrabajo es una modalidad de trabajo a distancia, entendido como aquel trabajo que se presta en el domicilio de la persona trabajadora o en el lugar elegido por esta, a diferencia del trabajo presencial que se presta en el centro de trabajo o en el lugar determinado por el empleador.[1] Y, en segundo lugar, además de ser remoto, el teletrabajo se debe llevar a cabo fundamentalmente mediante el uso de las tecnologías de la información y la comunicación (en adelante, TIC).[2]

En todo caso, el teletrabajo se ha generalizado y consolidado como una modalidad de trabajo que no solo responde de forma eficaz a las necesidades de empleados y empleadores en determinadas circunstancias, sino que además genera beneficios para ambos. Los más citados serían el ahorro en los costes de transporte, la flexibilidad horaria, la conciliación familiar y una mayor autonomía para realizar las tareas. Por ejemplo, Agudo Moreno (2014, págs. 179-180) señala que el teletrabajo «es una práctica laboral que cada vez tiene más penetración en las organizaciones por los enormes beneficios que aporta tanto a la organización como a los empleados. La flexibilidad laboral es un factor primordial que afecta positivamente en los resultados empresariales y ayuda

1. Por tanto, una característica del teletrabajo según Andrade Rodríguez (2023, pág. 478) sería que normalmente «se realiza sin presencia del empresario, sin la supervisión directa de éste, sin el suministro detallado de instrucciones previstas (donde realmente existe un control posterior de la calidad del trabajo entregado) y sin que haya un horario controlado por la empresa».
2. De acuerdo con Sierra Benítez (2025, pág. 139), «hay que tener en cuenta que la tecnología ha sido capaz de unir dos ámbitos desconectados: mundo físico y mundo digital (4ª Revolución Industrial: fábrica inteligente), y que esta transformación afecta a las personas y a la nueva manera de trabajar en un mundo digital cuya principal materia prima son ahora los datos (y no los materiales ni los bienes producidos)».

a conciliar la vida laboral con la familiar». Igualmente, Martínez Sánchez *et al*. (2006, pág. 254) estiman que el teletrabajo «constituye una estrategia para acomodar la sobrecarga de trabajo de los empleados y liberarles de los horarios fijos de trabajo. Por tanto, el uso simultáneo del teletrabajo y otras prácticas flexibles de trabajo puede tener un mayor impacto sobre los resultados de la empresa». Por su parte, Rimbau Gilabert (2021, pág. 23) destaca que el teletrabajo «tiene también un potencial efecto positivo derivado, en general, de la mayor autonomía que la persona que teletrabaja tiene para organizar sus tareas, lugares y tiempos de trabajo».

Asimismo, la reciente Sentencia del Tribunal Supremo (en adelante, STS) núm. 164, de 4 de marzo de 2025, también reconoce el valor positivo del teletrabajo en el Fundamento Jurídico 4º (en adelante, FJ) al considerar que «puede ser una herramienta muy útil para conciliar la vida familiar y laboral porque el teletrabajador puede desarrollar su actividad laboral en su domicilio y, mientras tanto, puede acompañar a sus hijos menores u otras personas que, por su edad o discapacidad, necesiten supervisión. Si la empresa puede obligar al teletrabajador a acudir a su centro de trabajo en los días en los que está previsto teletrabajar, ello puede dificultar esa conciliación de la vida familiar y laboral».

Ello no quiere decir que el teletrabajo no pueda comportar también inconvenientes para los trabajadores, como el sedentarismo, la pérdida de contacto social y problemas de salud derivados de una mala gestión del tiempo de trabajo. García Calvente (2020, pág. 62) cita algunos como «la extensión de las jornadas laborales, la dificultad para conciliar por la convivencia en el mismo espacio de trabajo y vida personal, el aislamiento, el denominado presentismo virtual [por el que las personas optan por trabajar en casa incluso cuando se encuentran mal pero aún son capaces de realizar algunas tareas], y en ocasiones menores oportunidades de desarrollo profesional como consecuencia de la invisibilización». Mientras que Martín-Pozuelo (2020, pág. 33-34) destaca la reducción de las relaciones personales, el aumento de los costes asociados a la actividad laboral, el sentimiento de menores perspectivas de promoción, las menores garantías de seguridad y salud en el lugar de trabajo y el riesgo de no desvincular las actividades profesionales de las personales.

Por último, cabe señalar que el teletrabajo admite distintas modalidades, ya que los teletrabajadores pueden actuar por cuenta propia (en régimen de autónomos) o por cuenta ajena (como asalariados), pueden trabajar para una empresa situada en España o en cualquier otro país, y pueden llevar a cabo la actividad laboral de forma habitual en su domicilio o de forma itinerante desde diferentes lugares. De modo que la ubicación del teletrabajador será fundamental para determinar el ordenamiento jurídico aplicable, pudiendo incluso ser distintos ordenamientos jurídicos, ya sea a nivel internacional cuando afecte a más de un Estado, como también a nivel interno en Estados con un reparto competencial multinivel. Por ejemplo, en el caso de España, su ubicación determinará tanto la aplicación de la ley española, como de las normas autonómicas y locales que correspondan.

1. Consideraciones tributarias del teletrabajo

1.1. La residencia y la aplicación de los tributos

De igual forma que el cambio del lugar donde se realiza la actividad determina el ordenamiento jurídico aplicable, este desplazamiento también puede tener implicaciones tributarias, ya que el lugar donde se realiza el hecho imponible de un tributo es primordial para fijar el derecho tributario correspondiente, la sujeción al tributo en cuestión y, consiguientemente, la administración tributaria competente para su gestión. Precisamente, Martos (2002, pág. 170) considera que la posibilidad de trabajar en remoto «libera a un sector importante de trabajadores de la obligación de residir en el lugar donde se encuentre el establecimiento o centro de trabajo; donde sus servicios son requeridos, lo que les otorga mayor libertad para decidir donde fijar su residencia, cuestión que resulta capital para determinar las reacciones previstas en los sistemas tributarios». Mientras que Escribano López (2022, pág. 576) alerta sobre la «popularización del trabajo en remoto, que en casos extremos puede llevar al teletrabajador a emprender una vida nómada, puede llevar a la ruptura del vínculo territorial entre las oficinas de la empresa y el lugar donde prestan sus servicios los individuos vinculados a ella (trabajadores o directores) y, en consecuencia, al incremento potencial de las oportunidades de movilidad

de éstos últimos. Una realidad que no concilia bien con las actuales reglas de imposición sobre la renta y que genera multiplicidad de retos, oportunidades y riesgos».[3]

De acuerdo con el art. 11 de la Ley 58/2003, de 17 de diciembre (en adelante, LGT), los tributos se aplicarán conforme a los criterios de residencia o territorialidad que establezca la ley en cada caso. En su defecto, los tributos de carácter personal se exigirán conforme al criterio de residencia, mientras que los demás tributos se exigirán conforme al criterio de territorialidad que resulte más adecuado según la naturaleza del objeto gravado. En este sentido, en cuanto al criterio de residencia en el ámbito tributario, se hace referencia al domicilio fiscal del sujeto, siendo para las personas físicas el lugar donde tengan su residencia habitual, mientras que para las personas jurídicas será su domicilio social. No obstante, el domicilio fiscal no tiene por qué coincidir necesariamente con el domicilio o el lugar de residencia habitual del contribuyente. Ciertamente, entre otras, la STS núm. 632, de 15 de abril de 2024, declara en el FJ 3º que el concepto de residencia habitual «es una cuestión fáctica, existente con independencia del lugar en que el contribuyente tenga formalmente señalado como domicilio fiscal. La residencia habitual se refiere al lugar donde una persona vive de manera regular, es decir, donde se establece su residencia principal. Para su determinación se tienen en cuenta diversos factores, como la permanencia en el lugar, el tiempo que se pasa en él, la existencia de vínculos familiares, laborales o económicos, etc.».

Dado que el teletrabajador es una persona física, según el art. 9 de la Ley 35/2006, de 28 de noviembre, del Impuesto sobre la Renta de las Personas Físicas (en adelante, LIRPF), se entenderá que el contribuyente de este impuesto tendrá su residencia habitual en España cuando se dé cualquiera de las siguientes circunstancias:

a) Que permanezca más de 183 días, durante el año natural, en territorio español.

b) Que radique en España el núcleo principal o la base de sus actividades o intereses económicos, de forma directa o indirecta.

c) Cuando resida habitualmente en España el cónyuge no separado legalmente y los hijos menores de edad que dependan de aquel.

Lo resume muy bien Chico de la Cámara (2004, pág. 78), cuando dice: «A su vez, para determinar la residencia habitual, el legislador tributario emplea una serie de índices fácticos omnicomprensivos que tienen como finalidad atraer al ámbito de sujeción del Estado (*vis atrativa*) cualquier signo de riqueza que haya sido obtenida por el sujeto considerado residente. Así, en aras de sujetar al tributo toda la renta obtenida por el residente, la norma empleará tres tipos de índices: de carácter temporal o de índole administrativo –consistente en la permanencia en nuestro país más de medio año–, de carácter económico –intereses de índole material en nuestro país–, y por último, de carácter sociológico –al presumir salvo prueba en contrario que reside en nuestro país por la permanencia en nuestro país de la unidad familiar–».

Ahora bien, si una persona física obtiene rentas en territorio español y no se da ninguna de las circunstancias anteriores, se podrá considerar como persona no residente y, por tanto, sujeta al Impuesto sobre la Renta de no Residentes (en adelante, IRNR). Entre los criterios de sujeción a este impuesto, cabe destacar el de territorialidad, o de lugar de situación, de los bienes o de las explotaciones económicas generadoras de las rentas. Concretamente, según el art. 13, 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 (en adelante, LIRNR), pueden resultar contribuyentes de este impuesto aquellos no residentes que, no disponiendo de un establecimiento permanente (en adelante, EP), obtengan rendimientos que deriven, directa o indirectamente, de una actividad personal desarrollada en territorio español.

3. Esta posibilidad de buscar la jurisdicción más favorable puede ser aprovechada tanto por el empleador, al querer contratar teletrabajadores en países con bajos costes y garantías laborales, como por el trabajador, al buscar lugares de residencia con baja o incluso nula tributación como sería un paraíso fiscal. En este sentido, Mories Jiménez (2023, pág. 175) afirma que «podemos estar abonando el terreno no solo para la deslocalización de los trabajadores sino también para las empresas, que ubicarán su presencia física en territorios con una tributación que les resulte más favorable puesto que no van a necesitar de establecimientos o centros de trabajo en los territorios desde dónde operan sus trabajadores». Mientras que Toribio Bernárdez (2021, pág. 141) se pregunta «si es lícito que una persona organice su modo de vida y la forma en la que trabaja para poder esquivar la condición de residente fiscal en todos aquellos países con los que tenga algún tipo de relación personal o económica».

De igual forma, podrán resultar sujetos al impuesto los no residentes que obtengan rentas mediante un EP situado en España, o bien porque actúan por medio de un agente autorizado para contratar en nombre y por cuenta de la persona no residente, o bien por disponer, por cualquier título, de instalaciones o lugares de trabajo en los que se realice la actividad de forma habitual.

El lugar de residencia en España no sólo determinará el marco jurídico y los efectos tributarios en el ámbito estatal, sino que también decidirá las normas autonómicas y locales aplicables en cada caso. El art. 72 LIRPF establece que se considerará residente en una comunidad autónoma a los contribuyentes con residencia habitual en territorio español cuando permanezcan en su territorio un mayor número de días del período impositivo. Es decir, la residencia autonómica no la marcará la residencia fiscal, sino que será determinada por el lugar donde se resida el mayor número de días del año natural, comparando entre comunidades autónomas cuando sean más de una.[4] Por lo que respecta a la incidencia del trabajo a distancia en la fiscalidad autonómica, Mories Jiménez (2023, pág. 195) considera que es evidente que «ello tendrá consecuencias en relación con todos los impuestos cedidos así como respecto a los tributos propios exigidos por la Comunidad Autónoma de la que se considere residente (...) deberá aplicar los tipos impositivos y los beneficios fiscales en cualesquiera de sus variantes que la Comunidad Autónoma haya aprobado, lo que puede constituir un incentivo para que se incremente la movilidad de los trabajadores también en el territorio nacional». Además, según Rovira Ferré (2023, pág. 209): «las consecuencias más relevantes se circunscriben ante los criterios de sujeción que, aparte de poder influir en los tributos propios de las CCAA, operen como puntos de conexión en los tributos concertados de los territorios históricos forales del País Vasco (Álava, Vizcaya y Guipúzcoa) i la CCAA foral de Navarra». Dadas las diferencias tributarias entre comunidades autónomas, los efectos de cambiar de residencia dentro del territorio español son una cuestión a tener en cuenta.

En cuanto al ámbito local, tampoco el certificado de empadronamiento sería suficiente para determinar el municipio de residencia habitual. Así lo estima la Consulta vinculante de la Dirección General de Tributos (en adelante, DGT), núm. 132, de 16 de febrero de 2024, que dispone que «el simple empadronamiento no constituye, por sí mismo, elemento suficiente de acreditación de residencia y vivienda habitual en una determinada localidad, como tampoco lo es el hecho de trasladar el domicilio fiscal a lugar determinado». Igualmente, la STS núm. 401, de 7 de mayo de 2025, en el FJ 3º declara que «la referencia legal al certificado de empadronamiento no impide la utilización de otros medios de prueba, sino que el padrón municipal solamente es un medio de prueba privilegiado, que produce una presunción iuris tantum de que los datos resultantes del mismo corresponden a la realidad, si bien tal presunción puede ser desacreditada». Según Ramos Prieto (2001, pág. 711), esta confusión entre residencia y domicilio se produce porque el domicilio «es el lugar donde se materializa –de cara al cumplimiento de las obligaciones tributarias– la idea de permanencia o vinculación efectiva inherente a la residencia habitual», pero no se deben entender como equivalentes.

1.2. El cambio de residencia debido al teletrabajo y sus implicaciones tributarias, cuando el domicilio de destino está en España

Como se ha explicado, el teletrabajo implica el traslado del trabajador del lugar o establecimiento del empleador hacia su domicilio, o lugar que elija, para seguir desempeñando sus tareas de forma telemática, lo que puede suponer un cambio de municipio, región o incluso de país, lo cual también afectará al derecho tributario aplicable.[5] Cuando el domicilio de destino de este traslado se encuentre en España, se puede diferenciar entre: **a)** el teletrabajador que ya residía en España y **b)** el teletrabajador que no residía en España.

4. Según SANTIAGO MARCOS (2024, p. 279) en «el ámbito de las comunidades autónomas, existe una mayor posibilidad de circulación de trabajadores, lo que plantea un reto adicional en cuanto a la fijación de la residencia. Por lo tanto, el legislador ha optado por establecer una presunción basada en la vivienda habitual (...) De esta forma, la ley viene a exigir que se fije como primer criterio el lugar donde se halla sita la vivienda habitual a través de una circunstancia fáctica de permanencia».
5. El cambio de domicilio incluso puede afectar al fuero del teletrabajador. La reciente STS núm. 365, de 24 de abril de 2025, en el FJ 2º declara: «Cuando el empresario pacta con el actor que preste servicios teletrabajando desde su domicilio particular, ello significa que el lugar de prestación de servicios laborales será el domicilio del trabajador y que, por aplicación literal del 10.1 de la LRJS, el fuero territorial electivo incluirá el Juzgado de lo Social del domicilio del trabajador, donde presta sus servicios».

a) El teletrabajador que ya residía en España

El trabajador que adopte la modalidad de teletrabajo, siendo ya residente fiscal en España, mantendrá las mismas obligaciones tributarias a nivel estatal que tenía como trabajador presencial, ya sea por cuenta propia o por cuenta ajena, ya sea para un empleador residente en España o de fuera del territorio español. Básicamente, estará sujeto al Impuesto sobre la Renta de Personas Físicas (IRPF), tanto para los rendimientos del trabajo como para las rentas de actividades económicas, independientemente de su origen. De modo que, el cambio de domicilio dentro del territorio español debido al teletrabajo por parte de un trabajador ya residente fiscal en España, no implicaría cambios en sus obligaciones con la Administración tributaria del Estado. Otra cuestión sería si ese traslado supone un cambio de la comunidad autónoma o el municipio de residencia, dado que entonces sí que implicaría cambios en la tributación de acuerdo con las normas tributarias de los territorios de destino.

Entre otras, la Consulta vinculante de la DGT, núm. 57, de 17 de enero de 2023, sobre la tributación de un trabajador con residencia en España contratado por una empresa suiza sin sede en España para que realice labores de programación informática en remoto desde territorio español. Dice la respuesta a la consulta: «un residente de un Estado contratante que perciba una remuneración, en concepto de un trabajo dependiente, de fuentes situadas en el otro Estado, no puede estar sujeto a imposición en ese otro Estado respecto de dicha retribución por el mero hecho de que los resultados de su trabajo se exploten en ese otro Estado». Dado que este trabajador con residencia fiscal en territorio español trabajará desde España más de 183 días al año, las rentas que perciba del empleador situado fuera de España por el trabajo que realiza desde su domicilio privado mediante teletrabajo solamente tributarán por el IRPF español.

Como recuerda Rovira Ferré (2023, pág. 32): «la normativa interna que regula la residencia fiscal de las personas físicas viene a garantizar la potestad tributaria de España con independencia de la movilidad geográfica que puede permitir el trabajo a distancia, ya que, si un trabajador por cuenta ajena de un empleador extranjero decide desarrollar su prestación laboral desde el territorio español, podrá resultar residente por el criterio de permanencia». En este sentido, como ha puesto de manifiesto Gil García (2022, pág. 125), la residencia «no es solamente un criterio de sujeción, sino también un elemento de competencia fiscal». Es decir, estamos ante otra posible competición fiscal a la baja entre países, en este caso en relación con la imposición a las personas físicas, cuyas consecuencias en España serían más notorias dado que afectaría al IRPF, una de las figuras tributarias más importantes en términos de recaudación y redistribución de rentas.

b) El teletrabajador que no residía en España

Cuando un teletrabajador no residente en España decida trasladar su domicilio a nuestro país, será residente fiscal o no residente en función de las circunstancias y requisitos que determinen su residencia en territorio español.[6] Mientras que las personas físicas con residencia fiscal en España están sujetas al IRPF, de acuerdo con el art. 93 LIRPF, las personas físicas que adquieran su residencia fiscal en España como consecuencia de su desplazamiento a territorio español podrán optar por tributar por el IRNR, manteniendo la condición de contribuyentes por el IRPF, por las rentas obtenidas sin mediación de EP, durante el período impositivo en que se efectúe el cambio de residencia y durante los cinco períodos impositivos siguientes.[7] Entre los requisitos para elegir esta opción cabe destacar el supuesto de cuando, sin ser ordenado por el empleador, la actividad laboral se preste a distancia mediante el uso exclusivo de medios y sistemas informáticos, telemáticos y de telecomunicación, es decir, mediante teletrabajo.

En cambio, en el supuesto de los teletrabajadores desplazados no residentes (y por tanto sujetos al IRNR), que sean residentes en un Estado miembro de la Unión Europea (en adelante, UE) o del Espacio Económico Europeo (en adelante, EEE) con el que exista normativa sobre asistencia mutua en materia de intercambio de información tributaria, podrán solicitar tributar de forma efectiva en España por el IRPF, siempre y cuando cumplan alguna de las siguientes condiciones:

6. Según Santiago Marcos (2024, pág. 226): «En relación con la acreditación de la permanencia durante más de 183 días en territorio español, la Administración tributaria tendrá que probar la presencia de la persona que alega no ser residente».
7. Sobre la aplicación del régimen fiscal especial del art. 93 LIRPF, ver la Consulta vinculante de la DGT, núm. 275, de 13 de marzo de 2025.

- Que los rendimientos del trabajo y de las actividades económicas obtenidos en España hayan supuesto, como mínimo, el 75 % de sus rentas.

- Que la renta obtenida en España sea inferior al 90 % del mínimo personal y familiar que le hubiese correspondido si hubiese sido residente en España.

En todo caso, si el trabajador opta por este régimen por resultarle más beneficioso, en primer lugar tendrá que declarar y tributar por sus rentas por el IRNR y, posteriormente, declarar y tributar por el IRPF para instar el procedimiento de devolución de lo tributado por exceso, es decir, primero pagará el IRNR y luego ejercitará la opción del IRPF.[8] Por su parte, el resto de trabajadores desplazados no residentes que no opten por el régimen anterior o cuya residencia se encuentre en un Estado situado fuera de la UE o del EEE quedarán sujetos a doble imposición, la española y la del otro Estado, pudiendo aplicarse las disposiciones del respectivo convenio para evitar la doble imposición entre los dos países en el caso de que exista dicho convenio.[9]

Aclaran Puerta y Morales (2023, pág. 5) que, de considerarse residente en el Estado del empleador, «el teletrabajador también está obligado a tributar por sus rentas en el Estado extranjero, con el correspondiente riesgo de doble imposición si no se permite la deducción del impuesto soportado en el extranjero (...) El riesgo de doble residencia debería poder neutralizarse si resulta de aplicación un convenio para evitar la doble imposición suscrito por España y el país extranjero». En tal caso, si dicho convenio existe, según Martos (2002, pág. 187) se posibilita al teletrabajador «la planificación internacional, al utilizar el traslado de su residencia, ya que le puede resultar atractivo cambiarla a algún Estado, con el que se hubiese firmado un Convenio de Doble imposición, que tenga una tributación sobre la renta inferior a la de su Estado de origen».

Además de determinar la tributación de los teletrabajadores, la ubicación en territorio español del domicilio desde el cual trabajan también podría obligar a tributar a las empresas no residentes para las que trabajan. Cuando el teletrabajador actúe como agente dependiente de la empresa no residente, o cuando la empresa no residente realice actividades de forma habitual o sea titular directa del lugar donde el teletrabajador desarrolla su actividad para aquella, entonces dicho lugar se considerará un establecimiento permanente de la empresa no residente y tendrá que tributar en España por las actividades que allí realice,[10] no solo por los impuestos estatales sino también por los autonómicos y locales como el Impuesto sobre Actividades Económicas (IAE).

2. La tributación del teletrabajo en el impuesto sobre actividades económicas

2.1. La sujeción del teletrabajo al IAE

De acuerdo con lo previsto por la Ley Reguladora de Haciendas Locales (en adelante, TRLRHL), entre los sujetos pasivos exentos del IAE, se encuentran las personas físicas y los sujetos del Impuesto sobre Sociedades (IS) cuyo importe neto de la cifra de negocios (en adelante, INCN) sea

8. Hay que señalar que, a pesar de aplicar este régimen opcional, el contribuyente mantiene su condición de no residente, de modo que la opción de tributar por el IRPF es a los efectos de poder instar un procedimiento de devolución en caso de haber tributado de más por el IRNR (esta opción deriva de la Sentencia del Tribunal de Justicia de la Unión Europea, de 14 de febrero de 1995, caso Schumacker, para evitar la posible discriminación fiscal de los no residentes).
9. Martos (2002, pág. 177) señala que cuando los tratados para evitar la doble imposición se incorporan a los ordenamientos nacionales, «se superponen jerárquicamente a las normas con rango legal, lo que provocará que ante la presencia de un Tratado aplicable a un hecho que causa un conflicto de doble imposición internacional, debamos obviar los mandatos previstos en la norma tributaria interna que le puedan ser aplicables, y regular el supuesto atendiendo al contenido del Tratado. Esta razón, unida a que continuamente se incrementa el número de convenios de este tipo que firman los Estados, obliga a fijar la vista en los mismos en relación a los problemas fiscales que el teletrabajo presenta».
10. La STS núm. 1500, de 11 de noviembre de 2020, en el FJ 4º enumera los requisitos necesarios para que se pueda hablar de EP en territorio español de una sociedad situada en otro Estado a efectos tributarios: **i)** la existencia de un lugar fijo de negocio en España que determine la vinculación con el territorio de aplicación del impuesto; **ii)** una estructura adecuada en términos de medios humanos y técnicos con la finalidad de realizar operaciones sujetas al impuesto, y **iii)** salvo excepciones, no actuar a través de filiales, pues éstas tienen personalidad jurídica propia y serían sujetos pasivos del impuesto.

inferior a un millón de euros. También estarán exentos los contribuyentes del IRNR que operen en España mediante establecimiento permanente y tengan un INCN inferior a un millón de euros. Igualmente, quedan excluidas del ámbito de aplicación del IAE aquellas actividades que se ejerzan en régimen de dependencia laboral. Por consiguiente, los principales contribuyentes de este impuesto municipal serán los sujetos al IS y los sujetos al IRNR con establecimiento permanente, siempre que el INCN de cada uno sea igual o superior a un millón de euros.

Por ello, a la hora de analizar la posible sujeción del teletrabajo al IAE, se deberá centrar en alguno de los casos siguientes: **a)** cuando una empresa no residente tenga un empleado en España realizando algún trabajo para ella mediante teletrabajo; **b)** cuando una empresa ya sujeta al impuesto tenga un empleado realizando labores para ella mediante teletrabajo desde un domicilio distinto; y **c)** cuando los teletrabajadores realicen su actividad desde otros espacios o locales distintos a sus domicilios, como centros de *coworking* o telecentros.[11]

a) Empresa no residente con un empleado en España en modalidad de teletrabajo

Cuando una empresa no residente tenga un empleado en España realizando algún trabajo para ella mediante teletrabajo, lo primero que se debe tener en cuenta, como ya se ha señalado anteriormente, es que tanto los teletrabajadores en régimen de dependencia laboral como los autónomos personas físicas quedarán excluidos del ámbito de aplicación del IAE. Ahora bien, la empresa puede resultar sujeta al impuesto si se estima que el teletrabajador actúa como agente dependiente, o si la empresa realiza de forma efectiva alguna actividad de manera habitual en el domicilio del teletrabajador, o si se aprecia que dicho domicilio puede considerarse como EP de la empresa.[12] Si se dan tales circunstancias, la empresa no residente tendrá que darse de alta y tributar por el impuesto municipal. Sin embargo, tal y como recuerda Rovira Ferré (2023, pág. 221), «tales consideraciones procederán si no tiene lugar ninguna de las demás exenciones que contempla el art. 82 del TRLRHL, entre las que destaca la relativa a los sujetos pasivos que inicien el ejercicio de su actividad en el territorio español, durante los dos primeros períodos impositivos en los que esta se desarrolle; la prevista para los contribuyentes del IRNR que operen en España mediante EP y que tengan un importe neto de la cifra de negocios inferior a 1.000.000 de euros; y las que sean de aplicación a los sujetos pasivos en virtud de tratados o convenios internacionales». Es decir, la tributación en el impuesto local conlleva la lógica aplicación de todos sus preceptos.

Sobre esta cuestión, la Consulta vinculante de la DGT núm. 1, de 19 de enero de 2000, responde sobre si una oficina de una empresa no residente que utiliza para realizar actividades auxiliares para la propia empresa puede considerarse EP. Mientras que «respecto a la tributación por el Impuesto sobre Sociedades, que es al que es aplicable el Convenio en el caso consultado, no se considera que la oficina abierta en España por la entidad holandesa constituya un establecimiento permanente si cumple los requisitos de realizar las actividades auxiliares de dar información y hacer publicidad y que estas se realicen única y exclusivamente para la propia empresa». En cambio, este criterio «no es aplicable al Impuesto sobre Actividades Económicas, por lo que será de aplicación la legislación interna española. En virtud de la misma, la Oficina abierta en España deberá tributar por el IAE por las actividades realizadas en territorio español, aunque dichas actividades sean ejercidas para la propia empresa, por lo que deberá darse de alta en el epígrafe o epígrafes que correspondan a la actividad o actividades desarrolladas en España». Dejando claro que la existencia de un EP conlleva en todo caso la sujeción al impuesto municipal.

b) Empresa ya sujeta al IAE con un empleado en modalidad de teletrabajo

11. En todo caso, López Laborda et al. (2005, pág. 2) se muestran críticos con la tributación del teletrabajo en el IAE, dada la «Escasa actualización de los elementos tributarios ante los cambios de las organizaciones económicas. El Impuesto se ha desmarcado de la evolución de actividades vinculadas a lo que se ha dado en llamar "nueva economía", tales como el teletrabajo, o, en general, aquellas actividades que se desarrollan en un espacio virtual, sin sede física asentada en un territorio».
12. Según Martos (2002, pág. 173), «Junto a la Residencia, como criterio de sujeción personal por excelencia en los sistemas fiscales, se ha generalizado, en la mayor parte de los mismos, el Principio de personalización del establecimiento permanente, en virtud del cual se convierte a éstos en obligados tributarios similares a los residentes. En base a esta equivalencia, las rentas mundiales generadas por un establecimiento permanente no residente se someten a gravamen en la jurisdicción donde se localice el mismo».

Cuando una empresa ya sujeta al IAE tenga un empleado realizando labores para ella mediante teletrabajo desde un domicilio distinto, deberán tenerse en cuenta las mismas consideraciones vistas en los apartados anteriores. Es decir, en primer lugar, si el teletrabajador es un autónomo persona física o mantiene una relación de dependencia laboral con la empresa no estará sujeto al impuesto municipal. En cambio, la empresa sí podría tributar por el IAE en aquel domicilio si se estima que el teletrabajador actúa como agente dependiente, o si la empresa realiza de forma efectiva y habitual alguna actividad, o si se aprecia que puede considerarse como EP de la empresa,[13] lo que implicaría una nueva alta en el impuesto. De acuerdo con RovirA Ferré (2023, pág. 222): «cuando los sujetos pasivos dispongan de local, resultará irrelevante que toda o parte de la prestación laboral de sus empleados se realice desde su domicilio o lugar por ellos elegido sobre el que el empleador carezca de disponibilidad directa por cualquier título (propiedad, arrendamiento, cesión de uso, etc.), de modo que únicamente existirá la obligación de matricularse y tributar por el IAE en el municipio o provincia donde el sujeto pasivo disponga de local o establecimiento».

Sobre este particular, la DGT ya se ha pronunciado en varias ocasiones, tanto en relación con actividades de prestación de servicios como comerciales. Por ejemplo, en el supuesto de prestación de servicios, según la Consulta vinculante de la DGT, núm. 3293, de 6 de noviembre de 2020, deben considerarse como establecimientos los locales sobre los que el sujeto pasivo tenga, por cualquier título, disponibilidad directa. En consecuencia, el sujeto pasivo deberá de figurar dado de alta en el IAE por los servicios que preste y, en su caso, satisfacer la cuota correspondiente por cada una de las actividades que efectivamente ejerza en el municipio en el que esté situado el establecimiento. En cuanto a las actividades comerciales, la Consulta vinculante de la DGT, núm. 2586, de 21 de diciembre de 2022, analiza el supuesto de una actividad comercial realizada por una sociedad que no dispone de locales ni establecimientos permanentes. Resulta que las ventas son efectuadas por comerciales mediante visitas a los establecimientos de los potenciales clientes, a quienes ofrecen los productos y donde, en caso de llegar a un acuerdo, se formalizan las ventas. Asimismo, la sociedad no interviene en el transporte de los artículos vendidos, ya que, una vez celebrada la venta, se cursa pedido a la empresa mayorista y es ésta la que transporta e instala los artículos vendidos, no disponiendo la sociedad ni de almacenes, ni de centro administrativo, mientras que los trabajos administrativos son realizados por un empleado desde su domicilio en modo de teletrabajo, y el domicilio social y fiscal de la empresa está radicado en la vivienda del administrador de la sociedad. La consulta resuelve que, a pesar de no disponer la sociedad de un local o establecimiento permanente, el lugar de realización de sus actividades comerciales será el término municipal en el que se celebren las operaciones de venta.

c) Los empleados en modalidad de teletrabajo realizan su trabajo desde otros espacios o locales distintos a sus domicilios

Cuando los teletrabajadores, en lugar de hacerlo desde sus domicilios, trabajen en otros espacios o locales como centros de *coworking* o telecentros, tendrá que analizarse si son susceptibles de ser considerados establecimientos permanentes, como ya se ha explicado anteriormente. Por una parte, estos espacios no tendrán la consideración de EP cuando la empresa no tenga una disponibilidad directa sobre ellos, de modo que, a efectos del IAE, la empresa no estará sujeta al impuesto municipal. Según Martín-Pozuelo (2020, pág. 22), el telecentro «es un centro dispuesto por la empresa '*ad hoc*' para el desempeño del teletrabajo, centro que cuenta con recursos compartidos y con instalaciones informáticas y de telecomunicaciones imprescindibles para poder llevar a cabo el trabajo en

13. Para que exista un EP que habilite el cobro del IAE, la actividad de la empresa debería realizarse de forma habitual y no puntual. Como aclara la Consulta vinculante de la DGT, núm. 66, de 18 de enero de 2022, «habitual» significa que la presencia de la empresa en una jurisdicción debe ser de carácter no meramente transitorio para considerar que mantiene ahí un establecimiento permanente y, por tanto, que su presencia justifica la obligación de tributar.

cuestión».[14] En todo caso, tal y como manifiesta Andrade Rodríguez (2023, pág. 493), cuando los telecentros sean «lugares de trabajo con plena disposición de la empresa, donde los trabajadores se ubican usando los recursos de la empresa», estaremos ante una prestación equivalente «a la del trabajo presencial» y la empresa deberá darse de alta y tributar por el IAE.

La Consulta vinculante de la DGT núm. 3548, de 11 de diciembre de 2020, resuelve la consulta de una empresa que plantea si, a efectos del IAE, se consideran como centro de trabajo los emplazamientos donde sus trabajadores realizan sus funciones en modo de teletrabajo, ya sea el domicilio del propio trabajador o un centro de *coworking*. Dice la respuesta: «la sociedad consultante no está obligada a matricularse ni tributar en aquellos municipios en donde no disponga de local o establecimiento para el ejercicio de su actividad de prestación de servicios de asesoramiento laboral, contable y fiscal. En este sentido cabe indicar que no pueden tener tal consideración de establecimientos las superficies de los domicilios de sus empleados desde donde estos trabajan en modo de teletrabajo ni aquellas otras de las que la sociedad consultante no tenga por cualquier título (propiedad, arrendamiento, cesión de uso, etc.) una disponibilidad directa sobre ellas, ya que en dichas superficies no concurre, desde el punto de vista del sujeto pasivo prestador del servicio que se contempla, la circunstancia de disponibilidad directa sobre las mismas». Es decir, cuando el teletrabajo se realice en centros de *coworking* o en telecentros, habrá que analizar las circunstancias concretas del caso para determinar si, en realidad, se trata de un centro de trabajo de la empresa y, por consiguiente, si debería tributar por él.

2.2. Los beneficios fiscales del IAE para el teletrabajo

En el momento de establecer la exacción del IAE mediante ordenanza fiscal, los ayuntamientos también pueden acordar aplicar diversas bonificaciones potestativas previstas en el TRLRHL, pero ¿podrían aprobar alguna bonificación específica para la modalidad del teletrabajo? De entrada, todas las bonificaciones previstas no tienen en cuenta si las empresas disponen o no de empleados en régimen de teletrabajo, por lo que su aplicación no dependerá de esta circunstancia. Quizás la bonificación que pudiera aplicarse al teletrabajo sería la prevista para aquellas empresas que desarrollen actividades económicas declaradas por las respectivas corporaciones como de especial interés o utilidad municipal.[15] Para aplicar esta bonificación deben concurrir circunstancias sociales, culturales, histórico-artísticas o de fomento de la ocupación que justifiquen su declaración. Sin duda, lo impreciso de su definición podría permitir el reconocimiento del teletrabajo y su aplicación a empresas con teletrabajadores, si un municipio así lo considerase.

Sin embargo, dada la discrecionalidad con que puede aplicarse esta medida, la concesión de una bonificación a determinadas actividades amparadas por este precepto podría verse como una arbitrariedad y un ataque al principio de igualdad. Calvo Sales (2007, pág. 573) advierte sobre la potestad de los ayuntamientos para conceder beneficios fiscales sobre sus impuestos, la cual «puede llegar a permitir la concesión de beneficios fiscales 'a medida' a determinados sujetos pasivos, con infracción de los principios de igualdad tributaria e interdicción de la arbitrariedad». En todo caso, en opinión de Martín Rodríguez (2014, pág. 67): «la aprobación de la declaración de especial interés o utilidad municipal no es un acto discrecional del pleno, a pesar de que se exige su aprobación. Su signo

14. El art. 70.2 de la Ley 31/2022, de 23 de diciembre, de Presupuestos Generales del Estado para el año 2023, añadió a la sección primera de las Tarifas del IAE el grupo 848, que comprende los servicios prestados por las oficinas flexibles, *coworking* y centros de negocios. Según la nota de este grupo, las empresas titulares de centros *coworking* o telecentros ofrecen a sus clientes (empresas y profesionales) la infraestructura necesaria para desarrollar su actividad: espacios de trabajo, oficinas y salas de reuniones, de formación o de conferencias completamente equipadas, eventos, puestos de trabajo flexibles o fijos, servicio de comunicaciones, videoconferencia y conexión a Internet, oficinas virtuales, gestión de documentaciones y correspondencia, servicios de secretariado, catering, ofimática, etc.
15. Tal y como se reconoce en la Editorial Wolters Kluwer (2020, pág. 2): «nos encontramos con el problema de la expresión "especial utilidad o interés municipal". Estamos, como sabemos, ante conceptos jurídicos indeterminados que, por tanto, son de difícil acotación. Ahora bien, una cosa es que sea un concepto jurídico indeterminado y otra cosa es que se admita cualquier interpretación. Por utilidad pública se entiende las exigencias derivadas de la actuación administrativa en el marco de obras públicas, servicios, dotaciones y demás aspectos relacionados con el giro o tráfico administrativo, directa o indirectamente, de la Administración. (...) Y por interés general o social se entiende cualquier fin supraindividual que denota una necesidad colectiva prevalente».

únicamente debe depender de si el sujeto pasivo que solicita dicha declaración cumple objetivamente con los requisitos que dan acceso a dicha categoría conforme a la ordenanza correspondiente y, por ende, a la bonificación».

Para reconocer o fomentar el teletrabajo se podrían ampliar alguna de las actuales bonificaciones reconocidas en el IAE, como por ejemplo la vigente bonificación a favor de aquellas empresas que establezcan un plan de trasporte para sus trabajadores con el objetivo de reducir el consumo de energía y las emisiones causadas por el desplazamiento al lugar de trabajo. Visto este objetivo, se podría introducir una bonificación específica para empresas con teletrabajadores, dado que estos no contaminarían al no tener que desplazarse al lugar de trabajo. De igual modo, se podría modificar la actual bonificación a favor de aquellas empresas que incrementen la media de su plantilla de trabajadores con contratos indefinidos, haciendo una especial referencia a la modalidad del teletrabajo si se considerase que este incremento fuese beneficioso, por ejemplo, por motivos medioambientales. Incluso se podría introducir una bonificación *ex novo* en el IAE para fomentar la modalidad de teletrabajo, si se considera favorable para la conciliación laboral o la sostenibilidad. En cualquier caso, tendría que ser el legislador estatal y no los municipios quien estableciera nuevas bonificaciones en el IAE para fomentar el teletrabajo.[16] Sin duda, si tales beneficios se aplicaran a impuestos estatales como el IRPF o el IS, su impacto sería mucho mayor.[17]

Consideraciones finales

El teletrabajo, como modalidad de trabajo en remoto, permite a los trabajadores realizar las tareas desde sus domicilios, o lugares que ellos elijan, gracias al uso de herramientas telemáticas. Su generalización, especialmente tras la pandemia de coronavirus, obliga a analizar las consecuencias jurídicas de estos traslados, incluidas las tributarias, dado que conllevan un cambio de lugar de residencia. En el caso de España, al tratarse de un Estado multinivel, el cambio de residencia no solo puede afectar a la imposición estatal sino también a la autonómica y a local, según el lugar de destino.

El cambio de domicilio debido al teletrabajo puede tener consecuencias tributarias tanto para los trabajadores como para las empresas empleadoras. Por una parte, los teletrabajadores pueden estar sujetos al IRPF o al IRNR en función de si se consideran residentes o no residentes en territorio español, teniendo en cuenta que no siempre el domicilio fiscal y el lugar de residencia son coincidentes. Con carácter general, tributarán en España por sus rentas, aunque también podrían quedar sujetos a la tributación del país de la empleadora en determinadas circunstancias. En tal caso, de existir, deberá aplicarse el convenio entre ambos Estados para evitar la doble imposición.

En cuanto a las empresas con teletrabajadores, tributarán es España en todo caso si son residentes y se dan los criterios de sujeción de los correspondientes tributos, mientras que las no residentes estarán obligadas a tributar cuando se estime que el teletrabajador actúa como agente dependiente de la empresa, o si ésta realiza de forma efectiva y habitual alguna actividad en el domicilio del teletrabajador, o si se aprecia que dicho domicilio puede considerarse como establecimiento permanente de la misma.

Sobre la tributación del teletrabajo en el IAE, resultan claros los supuestos que quedan excluidos del ámbito de aplicación del impuesto: las personas físicas, los sujetos del IS cuyo importen neto de la cifra de negocios sea inferior al millón de euros, los contribuyentes del IRNR que operen en España mediante EP cuyo importe neto de la cifra de negocios sea inferior a un millón de euros, y todas aquellas personas que ejerzan su actividad en régimen de dependencia laboral. Por consiguiente, los principales contribuyentes al impuesto municipal serán los sujetos al IS y al IRNR con EP, siempre que el importe neto de la cifra de negocios en ambos casos sea igual o superior al millón de euros.

Se entenderá que la empresa actúa en España mediante EP cuando el teletrabajador actúe como agente de-

16. Recuerda Anglès Juanpere (2020, pág. 21) que «en el ámbito local, el art. 9 TRLRHL establece que no podrán reconocerse otros beneficios fiscales en los tributos locales que los expresamente previstos en las normas con rango de ley y en los tratados internacionales. Es decir, aunque no se tenga una concepción precisa del concepto de beneficio fiscal, está claro que su establecimiento siempre tendrá que obedecer al principio de legalidad».
17. Sobre incentivos fiscales para promocionar el teletrabajo en España, ver a AEDAF (2020) y Sedeño López (2022).

pendiente de la misma, o cuando esta realice de forma efectiva y habitual alguna actividad en el domicilio del teletrabajador, o cuando disponga de algún título sobre las instalaciones o el lugar de trabajo. En tal caso, ya sea una empresa con residencia fiscal en España o no residente, tendrá que darse de alta y tributar por el IAE siempre que cumpla con el resto de los requisitos establecidos para ello. En cuanto a la posibilidad de aplicar una bonificación en el impuesto municipal por razón del teletrabajo, deberá ser el legislador estatal quien la incorpore para que los municipios que lo deseen puedan incentivar esta modalidad de trabajo en remoto.

Referencias bibliográficas

AEDAF (2020). «Propuesta de enmienda normativa en materia de gastos vinculados al teletrabajo, a efectos del Impuesto sobre Sociedades e Impuesto sobre la Renta de las Personas Físicas e Impuesto sobre el Valor Añadido». *Propuestas de medidas tributarias*, pág. 53-58.

AGUDO MORENO, M.J. (2014). «El teletrabajo en las organizaciones: análisis de sus beneficios y barreras en las empresas españolas». *Cuadernos de Gestión de Información*, n.º 4, págs. 172-187.

ANDRADE RODRÍGUEZ, B. (2023). «Una visión transversal de la definición del teletrabajo y el nexo para la tributación de los teletrabajadores internacionales: perspectiva laboral, tributaria y de seguridad social». En: Oliver Cuello, R. (dir.). *El Derecho, la Empresa y la Comunicación en la sociedad de la información*, págs. 471-502. Barcelona: Bosch Editor. DOI: https://doi.org/10.2307/jj.11786266.23

ANGLÈS JUANPERE, B. (2020). «Medidas fiscales locales para ayudar a la economía y el empleo, también en tiempos de Covid-19». *Crónica Tributaria*, n.º 4, págs. 11-38. DOI: https://doi.org/10.47092/CT.20.4.1

CALVO SALES, T. (2007). *El impuesto sobre construcciones, instalaciones y obras: la mayoría de edad del ICIO*. Madrid: El Consultor.

CHICO De La CÁMARA, P. (2004). «¿Crisis del criterio de la residencia habitual? una propuesta de revisión para someter los tributos de naturaleza personal exclusivamente en el estado de la fuente». *Revista de Contabilidad y Tributación CEF*, n.º 257-258, págs. 65-132. DOI: https://doi.org/10.51302/rcyt.2004.16113

EDITORIAL WOLTERS KLUWER (2020). «Bonificaciones en los impuestos locales para teletrabajadores o empresas con teletrabajo». *El consultor de los ayuntamientos y de los juzgados*, n.º 11, págs. 1-3.

ESCRIBANO LÓPEZ, E. (2022). «La fiscalidad de las rentas del teletrabajador y de las empresas que los emplean en escenarios transfronterizos». En: Merino Jara, I. (dir.). *Cuestiones actuales y conflictivas de la fiscalidad internacional*, pág. 573-608. Madrid: Wolters Kluwer.

GARCÍA CALVENTE, Y. (2020). «Avances y desafíos en la regulación del teletrabajo: reflexiones desde el ingreso y el gasto público en un contexto de pandemia». *Nueva Fiscalidad*, núm. 3, págs. 53-80.

GIL GARCÍA, E. (2022). «La residencia fiscal de las personas físicas: indeterminación, ubicuidad y deslocalización». *Civitas, Revista Española de Derecho Financiero*, n.º 193, págs. 123-158.

GUTIÉRREZ BENGOECHEA, M. (2022). «Algunas notas sobre la fiscalidad del establecimiento permanente». *Revista Técnica Tributaria*, n.º 138, págs. 91-120. DOI: https://doi.org/10.48297/rtt.v3i138.2311

LOPEZ LABORDA, J.; TRUEBA CORTÉS, C.; ZÁRATE MARCO, A. (2005). «La reforma del Impuesto sobre Actividades Económicas». *XII Encuentro de Economía Pública. Evaluación de las Políticas Públicas*, págs. 1-40.

MARTÍN RODRÍGUEZ, J.M. (2014). «Las nuevas bonificaciones potestativas por especial interés o utilidad municipal en IBI, IAE e IIVTNU. Análisis crítico a través del antecedente en el ICIO». *Tributos Locales*, n.º 116, págs. 55-84.

MARTÍN-POZUELO LÓPEZ, A. (2020). «Una aproximación al concepto, modalidades y principales ventajas e inconvenientes del teletrabajo». En: Sala Franco, T. (dir.). *El teletrabajo*. València: Tirant lo Blanch.

MARTÍNEZ SÁNCHEZ, A.; PÉREZ PÉREZ, M.; DE LUIS CARNICER, P.; VELA JIMÉNEZ, M.J. (2006). «Teletrabajo y flexibilidad: efecto moderador sobre los resultados de la empresa». *Cuadernos de Economía y Dirección de Empresa*, n.º 29, págs. 229-262.

MARTOS, J.J. (2002). «Criterios de sujeción de las rentas del teletrabajo internacional. Residencia fiscal y doble imposición internacional». *Trabajo*, n.º 11, págs. 169-188. DOI: https://doi.org/10.33776/trabajo.v11i0.174

MORIES JIMÉNEZ, M.T. (2023). *Fiscalidad del teletrabajo*. València: Tirant lo Blanch.

PUERTA RUIZ DE AZÚA, C.; MORALES GIL, T. (2023). «Tributación en España del teletrabajo transfronterizo». *Unión Europea Aranzadi*, n,º 2, pág. 1-14.

RAMOS PRIETO, J. (2001). *La cesión de impuestos del Estado a las Comunidades Autónomas. Concepto, régimen jurídico y articulación constitucional*. Sevilla: Editorial Comares.

RIMBAU GILABERT, E. (2021). «El complejo impacto del teletrabajo sobre el bienestar individual». *Dossieres EsF*, n.º 42, págs. 22-26.

ROVIRA FERRÉ, I. (2023). *La fiscalidad del trabajo a distancia*. Navarra: Aranzadi.

SANTIAGO MARCOS, D. (2024). *La tributación de las actividades laborales prestadas a distancia*. València: Tirant lo Blanch.

SEDEÑO LÓPEZ, J.F. (2022). *Instrumentos financieros y tributarios frente a la despoblación: Retos y oportunidades en el contexto del teletrabajo*. Barcelona: Atelier.

SIERRA BENÍTEZ, E.M. (2025). «Nómadas digitales: una perspectiva jurídico-laboral». En: Ludovico y Nahas (dirs.). *Diritti fundamentali, lavoro e nuove tecnologie*, págs. 125-146. Milán: Milano University Press.

TORIBIO BERNÁRDEZ, L. (2021). *La dimensión internacional del deporte desde la perspectiva del derecho tributario: reexaminando el concepto de residencia fiscal y el principio de imposición en la fuente*. Granada: Editorial Comares.

Cita recomendada

ANGLÈS JUANPERE, Benjamí (2026). «La tributación del teletrabajo y el impuesto municipal sobre actividades económicas». En: Irene Rovira Ferrer (coord.). «Sobre la consolidación del trabajo a distancia». *IDP. Revista de Internet, Derecho y Política*, núm. 44. UOC. [Fecha de consulta: dd/mm/aa]. DOI: http://dx.doi.org/10.7238/idp.v0i44.9800605

Sobre el autor

Benjamí Anglès Juanpere
Profesor agregado de Derecho Financiero y Tributario en la Universitat Oberta de Catalunya (UOC)
bangles@uoc.edu
ORCID: https://orcid.org/0000-0002-7635-8151
Dialnet: https://dialnet.unirioja.es/servlet/autor?codigo=4031628

Licenciado en Derecho (UOC) y doctor en Derecho (URV), también máster en Fiscalidad (UDIMA), máster en Derecho público (URV) y máster en Educación y TIC (UOC). Además de las labores como docente en el máster de Fiscalidad y el Grado de Gestión y Administración Pública de la UOC, también realiza labores de investigación sobre los ámbitos de los ingresos públicos, la tributación local y autonómica, los procedimientos tributarios y la fiscalidad de las nuevas tecnologías. En este sentido, ha participado en múltiples congresos nacionales e internacionales, y también ha publicado numerosos trabajos académicos sobre los ámbitos señalados.

IDP
REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Monográfico: «Sobre la consolidación del trabajo a distancia» (coord.: Irene Rovira Ferrer)

El derecho a la desconexión desde una perspectiva europea: propuestas sobre su regulación y su ejercicio y primeros efectos en el régimen vigente en España

Ferran Camas Roda
Universitat de Girona

Fecha de presentación: agosto 2025
Fecha de aceptación: febrero 2026
Fecha de publicación: marzo 2026

Resumen

El artículo analiza el derecho a la desconexión digital, especialmente respecto de las personas que realizan un trabajo a distancia, con una perspectiva europea. En este sentido, se aportan las propuestas que instituciones políticas europeas, agentes sociales y entidades académicas del ámbito de la Unión Europea están lanzando sobre si hay que regular o no en el ámbito europeo el teletrabajo y, en particular, el derecho a la desconexión digital, y en caso afirmativo, cómo se debería llevar a cabo su ejercicio e implementación. Para ello, se incluye también una perspectiva jurídica comparada sobre las regulaciones de los Estados miembros que han regulado el trabajo a distancia y el derecho a la desconexión. Finalmente, se habla del régimen vigente en España sobre la desconexión y cómo recientes sentencias judiciales la están moldeando, en algunos puntos con respecto a los vientos provenientes del ámbito europeo.

Palabras clave

teletrabajo; derecho a la desconexión

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

The right to digital disconnection from a European perspective: proposals for its regulation, practice, and initial effects on the existing regime in Spain

Abstract

The article explores the right to digital disconnection, particularly in the context of telework, from a European perspective. It examines proposals launched by European political institutions, social agents, and academic entities within the European Union regarding whether remote work should be regulated in Europe and, in particular, the right to digital disconnection. It also considers how such rights might be exercised and implemented. Additionally, the article offers a comparative legal review of the regulations enacted by Member States concerning remote working and the right to disconnection. Finally, it discusses the current legal framework in Spain concerning disconnection and how recent judicial decisions are influencing it, partly influenced by developments within the European Union.

Keywords

telework; right to disconnection

Introducción

La convocatoria de artículos que tengan por objeto la consolidación del trabajo a distancia para ser publicados en *IDP: Revista de Internet, Derecho y Política* que ha promovido la Universitat Oberta de Catalunya (UOC), con la coordinación de su profesora Irene Rovira, es una iniciativa encomiable para poder aportar conocimientos e ideas que contribuyan a la promoción del teletrabajo como una modalidad de trabajo útil para empresas y personas trabajadoras.

Para enfocar el objeto de este artículo, considero necesario localizarlo bajo tres premisas básicas: en primer lugar, asumir que la consolidación del trabajo a distancia no debe afectar al bienestar de las personas trabajadoras que lo ejecutan; en segundo término, que, detectado un problema que pueda afectarlo, la legislación y su efectiva puesta en práctica deben ser fundamentales para solucionarlo. En función de ello, este artículo parte de considerar que uno de los problemas que coadyuvan mayormente a obstaculizar el bienestar de las personas trabajadoras, y en particular de las que teletrabajan, es la situación de conectividad permanente a la que pueden verse sometidas. Por esa razón, en el siguiente apartado se ofrecerán aquellas claves que evitan la mencionada hiperconectividad, entre las que emerge como un instrumento clave el «derecho a la desconexión».

Así, el objeto de este trabajo es realizar un análisis desarrollado del derecho a la desconexión, principalmente en el ámbito del «teletrabajo» y en todo caso desde una perspectiva principalmente europea. Para ello, se van a aportar las líneas maestras del debate que, para armar dicho derecho, se está llevando a cabo en la Unión Europea (UE) en el ámbito político-institucional, jurídico e incluso de prestigio académico,[1] para finalmente dar a conocer la evolución en el reconocimiento de dicho derecho en el ámbito español, por parte de sentencias judiciales y su amoldamiento a los vientos que soplan desde la UE.

1. En este sentido, va a ser de interés aportar el informe del EUROPEAN LAW INSTITUTE (Instituto de Derecho Europeo) de 2023, relativo a los «Principios rectores para la aplicación del derecho de los trabajadores a la desconexión», en traducción, conforme a la traducción al español realizada por el profesor Ferran Camas Roda, Catedrático en Derecho del Trabajo y de la Seguridad Social en la Universitat de Girona, en colaboración con Andrea Cano Redondo, técnica de investigación en la Universitat de Girona (2024): https://europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Principios_rectores_para_la_aplicacio__n_del_derecho_de_los_trabajadores_a_la_desconexio__n__ESP_.pdf. [Fecha de consulta: diciembre de 2025].

1. Sobre la cultura de la conectividad permanente y las claves para evitarla

El punto de partida de este apartado es el estudio que la Comisión Europea publicó en inglés en el año 2024 (con traducción propia al español) titulado *Estudio explorador del contexto social, económico y jurídico, y las tendencias del teletrabajo y del derecho a la desconexión, en el marco de la digitalización y el futuro del trabajo, durante y después de la pandemia de COVID-19* (Comisión Europea, 2024a). En este informe se señala que el teletrabajo ha llegado para quedarse, lo que se prueba con proyecciones que indican que en 2030 se prevé que entre un 12 % y un 22 % de los empleados en la UE-27 trabajarán desde casa de forma ocasional o habitual, con una estimación base del 17 %. Esa afirmación es objeto de valoración positiva por el propio informe, ya que, a su juicio, el incremento futuro de la prevalencia del teletrabajo puede conllevar ahorros de costes, así como fomentar la innovación y digitalización en el entorno laboral, mayores niveles de empleo (incluidos los correspondientes a colectivos desfavorecidos en el mercado de trabajo, como, por ejemplo, pueden ser las mujeres trabajadoras), mejor conciliación y una inclusión laboral más amplia.

Frente a esos datos, el informe que se está reseñando señala una serie de retos que deben superarse en relación con el teletrabajo, por ejemplo, en materia de seguridad y salud en el trabajo. Según la Comisión Europea, los teletrabajadores se enfrentan a realidades de aislamiento, así como a nuevos riesgos psicosociales, como puede ser una sobrecarga informativa, asociados al uso intensivo de herramientas de comunicación virtual. Además, pueden estar más expuestos a riesgos ergonómicos, dada la dificultad de empleadores, representantes de trabajadores e inspecciones laborales para efectuar evaluaciones de riesgos de los puestos de trabajo en el domicilio e imponer el cumplimiento de las obligaciones preventivas. En este sentido, el informe propone que la prevención de riesgos laborales en el ámbito del teletrabajo se oriente a evitar la intensificación del trabajo, el aislamiento, el exceso de jornada y los riesgos emergentes vinculados a la comunicación digital y la ergonomía, y también, añadiría yo, a la protección frente a los riesgos de ansiedad que el uso constante de dispositivos digitales puede ocasionar a la persona trabajadora, y en especial a la teletrabajadora.

En todo caso, lo que más llama la atención es una de sus conclusiones, en la que se exige garantizar la conciliación en el contexto del teletrabajo y mitigar los riesgos que conlleva la flexibilidad horaria, evitando la realización de horas extraordinarias y las solicitudes laborales fuera del tiempo de trabajo. El informe señala en este sentido que «es fundamental proteger a los trabajadores frente a los riesgos de conectividad permanente y jornadas prolongadas, asegurando el derecho al descanso».

La problemática de la conectividad permanente, también conocida como trabajo «always-on» o «trabajo sin fin», de forma que ya está adquiriendo tintes de «cultura laboral de estar siempre conectado», está siendo ya objeto de atención preferente por instituciones especializadas en materia de condiciones de trabajo por las implicaciones que su seguimiento puede tener referente a los derechos laborales de las personas trabajadoras, entre los que se encuentra su salud. El mencionado informe de la Comisión Europea se hace eco de una encuesta realizada por Eurofound en 2022 en cuatro países (Bélgica, Francia, Italia y España), en la que más del 80 % de los encuestados refirieron haber sido contactados por motivos laborales fuera de su horario contractual, respondiendo a dichos contactos nueve de cada diez personas; las principales razones aducidas para ello fueron el sentimiento de responsabilidad respecto a las propias tareas (82 %); el deseo de mantenerse informados (75 %); la percepción de que se esperaba tal disponibilidad (75 %); el temor a consecuencias negativas en caso de no responder (61 %) o la expectativa de una mejor progresión profesional (50 %).

En todo caso, donde más se está cebando la cultura de la conexión permanente es en las personas que prestan sus servicios en régimen de trabajo a distancia, de hecho, el trabajo sin fin o con conectividad permanente dispone de una potencial afectación en las prestaciones laborales realizadas bajo régimen de teletrabajo, o de trabajo móvil con uso de tecnologías (Eurofound-Organización Internacional del Trabajo, 2019), dicho de otra manera, si bien factores estresantes como la intensidad del trabajo, la interferencia entre la vida laboral y personal y la realización de trabajo en el tiempo libre, que implica la conectividad permanente, afectan a todos los trabajadores, su impacto es más acusado en aquellos que teletrabajan respecto de quienes prestan servicios en los locales de la empresa (Comisión Europea, 2025).

El estar siempre conectado, principalmente cuando afecta a personas que teletrabajan, impacta plenamente en el incremento de la jornada laboral, la disminución de los periodos de descanso y vacaciones anuales, lo que impacta directamente en derechos de conciliación de la vida laboral y personal o familiar, así como también en el padecimiento de las personas trabajadoras de estrés y agotamiento laboral, lo que a su vez deriva en alteraciones de la salud de estas personas. Para atajar la extensión de esta cultura de la disponibilidad permanente, en especial en el marco de la prestación de un trabajo a distancia, el derecho a la desconexión aparece como un instrumento clave.

De hecho, se ha considerado que las dificultades que enfrentan las personas trabajadoras para desconectar derivan de la ausencia de una cultura de desconexión en el ámbito empresarial, en el sentido de que entre los representantes empresariales prevalezca un pensamiento que considere que la mayoría de los empleados deban estar disponibles para atender cuestiones laborales durante su tiempo libre, y más aún si se trata de directivos (Eurofound, 2022). De hecho, las investigaciones realizadas hasta la fecha han detectado que los grupos con más exposición a tener dificultades para desconectar son, en general, los directivos y las personas trabajadoras que ostentan posiciones jerárquicas elevadas en las empresas (Eurofound, 2020), y, de forma específica, la personas teletrabajadoras, que desde la pandemia del Covid-19, en el año 2020, empezaron a afrontar importantes dificultades para desconectar del trabajo, extendiendo su jornada laboral más allá de lo deseable.

Para mitigar los riesgos inherentes a una cultura de «conexión permanente», es el «derecho a la desconexión» el que puede contribuir a delimitar con mayor claridad las fronteras entre la vida profesional y la privada, favoreciendo con ello la salud, la seguridad y el equilibrio entre la vida laboral y personal de las personas trabajadoras (Comisión Europea, 2025, págs. 9 y 75). De hecho, según la Comisión Europea, los datos de que dispone indican que, en el ámbito empresarial, existe una asociación positiva entre la implantación efectiva del derecho a la desconexión y la mejora del equilibrio vida-trabajo, la salud, el bienestar y la satisfacción global en el empleo (Comisión Europea, 2025, págs. 9 y 75).

Así, se está reconociendo por autoridades públicas europeas que, justamente ante el auge de la realidad del teletrabajo en sus diversas variables de realización, se plantean la adopción de medidas regulatorias, siendo el «derecho a la desconexión» el eje central de sus debates y esfuerzos normativos, tanto en el ámbito nacional como en la Unión Europea (European Labour Authority, 2023).

En conclusión, la necesidad de reconocer un derecho a la desconexión, que sea de aplicación efectiva, se convierte en una medida clave para combatir la cultura de la conectividad permanente, pero también, en lo referente al ámbito del teletrabajo, para establecer al máximo nivel jurídico la diferencia entre periodos de trabajo y periodos de descanso o de tiempo libre.

No obstante, en la Unión Europea no existe un acto normativo específico sobre el teletrabajo o el derecho a la desconexión (Comisión Europea, 2024a), sin perjuicio de que lo que sí está vigente, lo que ya de por sí no es poco, es un acervo jurídico comunitario de carácter laboral, entre la que resalta la *Directiva 2003/88/CE del Parlamento Europeo y del Consejo, de 4 de noviembre de 2003, relativa a determinados aspectos de la ordenación del tiempo de trabajo,* cuyas disposiciones sobre el tiempo de trabajo así como sobre lo que no lo es, el tiempo de descanso, debe ser respetada para el conjunto de las personas trabajadoras.

2. Estado del debate en el ámbito europeo del derecho a la desconexión

Ante esta realidad de falta de instrumentos legales sobre trabajo a distancia, el 30 de abril de 2024 la Comisión Europea presentó una iniciativa muy interesante: se trata de la primera fase de la consulta a los interlocutores sociales sobre una posible acción de la Unión Europea en el ámbito del teletrabajo y del derecho de las personas trabajadoras a la desconexión (Comisión Europea, 2024c).

Esta iniciativa política de consulta a los agentes sociales busca recabar la opinión de los agentes sociales europeos sobre la posible orientación de una actuación de la UE destinada a introducir un derecho a la desconexión y a garantizar condiciones de trabajo adecuadas en el teletrabajo. En lo que interesa a este trabajo, la Comisión Europea expresa que «la introducción de un derecho a la desconexión puede constituir un avance positivo para los trabajadores, especialmente para aquellos cuya actividad profesional se realiza principalmente a través de herra-

mientas digitales». Es decir, la Comisión Europea apuesta por adoptar una regulación específica sobre el derecho a la desconexión, lo que a su vez justifica, en el marco de su propuesta de consulta, por cuánto dicho derecho puede contribuir a garantizar la protección de la salud y la seguridad de las personas trabajadoras, así como unas condiciones de trabajo adecuadas, y a facilitar un mejor equilibrio entre la vida laboral y personal; a su vez, y desde la perspectiva empresarial, la Comisión manifiesta que las empresas también podrían beneficiarse de una reducción de los riesgos para la salud física y psicosocial de las personas trabajadoras, una mayor satisfacción laboral y una plantilla más eficiente y productiva.

Ante estas disquisiciones, es de interés aportar la respuesta que la Confederación Europea de Sindicatos (CES) realizó el 25 de junio de 2024 (Confederación Europea de Sindicatos, 2024) a la iniciativa de la Comisión. En primer lugar, la CES expresa su disconformidad con el hecho de que deba introducirse un derecho a la desconexión, porque el derecho a la desconexión como tal ya existe y debería describirse con más detalle y aplicarse en forma de directiva de la UE. Con esa expresión, la CES hace referencia a aquellas normativas sobre tiempo de trabajo aplicables en general al conjunto de personas trabajadoras, condensadas principalmente en la *Directiva 2003/88/CE*, ya mencionada anteriormente, y en la *Directiva 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 de la salud de los trabajadores en el trabajo*, bajo cuyos parámetros se encuentran regulaciones sobre el tiempo en el que las personas trabajadoras están a disposición del empleador. La CES recuerda en su respuesta que, más allá de lo que marcan, el empleador no tiene derecho a reclamar más tiempo del trabajador, es decir, el derecho de las personas trabajadoras a no ser contactadas por su empleador durante su tiempo libre. Por lo tanto, la CES concluye que lo que se debería llevar a cabo es un ejercicio de «aclarar y hacer respetar» este derecho a la desconexión. En mi opinión, sin poner en duda que la normativa europea en materia de tiempo de trabajo y de seguridad y salud dispone medidas para garantizar que no se contacte a una persona trabajadora o se le requiera para trabajar en su tiempo libre, también considero que la presencia prominente de los dispositivos de comunicación o tecnológicos bajo uso de cualquier tipo de trabajador, pero sobre todo respecto de los que trabajan a distancia, sí debieran requerir de una normativa específica, al amparo de las competencias de la Unión Europea, que estableciese el régimen de su uso en dicho marco.

En este sentido, del conjunto de países que conforman la Unión Europea, trece han pasado a regular de forma específica el régimen del teletrabajo y, en este ámbito, han implementado medidas específicas sobre el derecho a la desconexión, si bien con diferencias respecto a su alcance, definición, implementación y mecanismos de control. En este marco, se ha de destacar que España está entre los primeros países en adoptar legislación nacional sobre el derecho a la desconexión (Comisión Europea, 2025), país que, a su vez, ha merecido una atención especial de la Agencia Europea de Seguridad y Salud en el Trabajo por el régimen de sanciones arbitrado en el caso de que la empresa no se dote de una política de desconexión en el trabajo (European Agency for Safety and Health at Work, 2021).

No obstante, en lo que se detecta cierto consenso en los informes, las posturas y los trabajos de investigación en relación al derecho a la desconexión en aquellos países en los que este derecho ha sido reconocido normativamente es que el principal reto reside en su efectiva implementación (Comisión Europea, 2024b) –por cierto, vale la pena aportar en este punto como la Comisión Europea se ha hecho eco de lo establecido en la Universitat Oberta de Catalunya sobre el derecho a la desconexión (Universitat Oberta de Catalunya, s.f.)–, por ejemplo, sobre el establecimiento de franjas horarias de disponibilidad y para la celebración de reuniones, la supresión de reuniones los viernes, así como la determinación de los canales de comunicación apropiados para cada equipo, con el objetivo de mitigar el estrés derivado del uso simultáneo de múltiples canales digitales o la implantación de un sistema de alertas mediante el cual los empleados pueden canalizar reclamaciones por posibles vulneraciones de su derecho a desconectar, aunque en el informe de la Comisión también se señala que ni la representación empresarial ni la social han facilitado información sobre los resultados de dichos mecanismos (Comisión Europea, 2024b).

En este contexto, aunque no exista una directiva o normativa vinculante específica europea que regule el derecho a la desconexión, sí está aprobada la *Resolución del Parlamento Europeo, de 21 de enero de 2021, con recomendaciones destinadas a la Comisión sobre el derecho a la desconexión (2019/218 [INL])*. En sus considerandos, hace referencias de calado sobre el derecho a la desconexión, como las relativas a que «el derecho a desconectarse es un derecho fundamental», lo que entroncaría, a mi parecer, con la inclusión de ese derecho dentro del relativo al respeto al descanso de las personas trabajadoras y, por

tanto, de protección de su salud, así como posteriormente, en la parte dispositiva de la resolución, del reconocimiento de que el derecho a la desconexión «permite a los trabajadores abstenerse de realizar tareas, actividades y comunicaciones electrónicas relacionadas con el trabajo, como llamadas telefónicas, mensajes electrónicos y otro tipo de mensajes, fuera de su horario laboral, también durante los períodos de descanso, las vacaciones oficiales y anuales, las bajas por maternidad, paternidad y el permiso parental, así como otros tipos de permisos, sin tener que afrontar posibles consecuencias negativas».

En todo caso, en el anexo de la Resolución, que incluye una «Propuesta de Directiva sobre el Derecho a la desconexión», se encuentran sus claves. En primer lugar, lo que se debería entender por derecho a la desconexión, que haría referencia «al derecho de los trabajadores a no participar en actividades o comunicaciones laborales fuera de su tiempo de trabajo, a través de herramientas digitales, como llamadas telefónicas, mensajes electrónicos u otro tipo de mensajes»; en segundo lugar, y no menos importante, la advertencia de que dicho derecho debe aplicarse a todas las personas trabajadoras y a todos los sectores, tanto públicos como privados, y debe cumplirse de forma efectiva. En tercer lugar, *last but not least*, el objetivo del derecho a la desconexión; para el Parlamento Europeo, esa finalidad se centraría en «garantizar la protección de la salud y la seguridad de los trabajadores, y unas condiciones de trabajo justas, incluido el equilibrio entre la vida profesional y la vida privada» (véase el apartado 11 del anexo de la Resolución).

Como se puede observar, tres cuestiones relucen de este apartado: en primer lugar, la aplicación universal del derecho a la desconexión; en segundo término, la necesidad de que se cumpla de forma efectiva, cuestión en la que considero que se estarían produciendo serios quebrantos; y, en tercer lugar, que el objetivo esencial del derecho a la desconexión es asegurar la protección de la salud y la seguridad de las personas trabajadoras, así como favorecer unas condiciones de trabajo justas, que incluyan el equilibrio entre la vida personal y laboral.

Este doble objetivo, intrínsecamente entrelazado, de que el derecho a la desconexión digital persigue garantizar la seguridad y salud de la persona trabajadora y favorecer unas condiciones de trabajo justas, entre las que expresamente se incluye el equilibro de la vida personal y laboral, ha sido desarrollado por instituciones académicas como el Instituto de Derecho Europeo (European Law Institut-ELI), que publicó el documento *Guiding Principles on Implementing Workers' Right to Disconnect* en el año 2023 (European Law Institut, 2023).

En este documento de principios se asigna al derecho a la desconexión un objeto específico estructurado en dos ejes: por una parte, proteger la salud física y mental de todas las personas trabajadoras, garantizándoles efectivamente el tiempo de descanso al que tengan derecho; y, por otra, promover la igualdad de género y el equilibrio entre la vida laboral y personal y garantizar la previsibilidad de los horarios de trabajo. Como se observa, el primero de los principios subraya la conexión entre el derecho a la desconexión y la protección de la seguridad y salud de las personas trabajadoras, de tal manera que pueda incluirse como un derecho perteneciente al grupo de normas sobre prevención de riesgos laborales en relación especial con el tiempo de trabajo y el respeto al descanso. Junto a ello, el derecho a la desconexión también se vincula a una dimensión de igualdad de género, en especial en lo referente a derechos de conciliación.

Al primero de los principios rectores del derecho a la desconexión que el ELI enumera, que es justamente el que se ha mencionado como objetivo del derecho a la desconexión, le siguen otros nueve de calado, entre los que quisiera centrarme brevemente en varios que considero muy relevantes. En primer lugar, el principio tercero consistente en el reconocimiento que la «implementación efectiva del derecho a la desconexión requiere acciones preventivas con el fin de evitar una cultura "siempre activa" en las entidades empleadoras». Así, se revalida científicamente cómo el derecho a la desconexión es una pieza clave para luchar contra la cultura laboral de la sobreconectividad o *always-on*, y que su configuración debiera incluirse dentro del ámbito de la prevención de riesgos laborales. De hecho, frente a la cultura de la conectividad permanente, se debería erigir otra cultura de raíz preventiva, en concreto la de la cultura de que, fuera del tiempo de trabajo, no se debe exigir conectividad a la persona trabajadora. En este marco, conviene traer a colación el *Acuerdo Marco de los Interlocutores Sociales Europeos sobre Digitaliza-*

ción de 2020,[2] que tiene un apartado sobre modalidades de conexión y desconexión, en el que se expresa que el cumplimiento de los objetivos de una organización empresarial no debería requerir una conexión fuera de horario. Se añade que, con pleno respeto de la legislación sobre la jornada laboral y de las disposiciones sobre la jornada laboral de los convenios colectivos y los acuerdos contractuales, el trabajador no está obligado a estar localizable fuera de su horario para ningún contacto adicional por parte de las personas empleadoras.

En segundo lugar, es necesario subrayar el principio que el ELI destaca como el «deber de reconectar durante un periodo de desconexión», conforme al cual se reconoce la posibilidad de que una persona trabajadora deba conectarse mientras disfruta de su derecho a la desconexión, aunque ello solo podría producirse en situaciones absolutamente extraordinarias, y siempre que se le compensase de forma proporcional al hecho producido. En este punto, conviene traer a colación, en España, el Convenio colectivo para los establecimientos financieros de crédito de 2024.[3] En su artículo 35, sobre derecho a la desconexión digital, se reconoce el derecho de las personas trabajadoras a no atender dispositivos digitales fuera de su jornada de trabajo ni durante los tiempos de descanso, permisos, licencias o vacaciones, salvo que se den las causas de urgencia justificada; y, en este sentido, las define como aquellos «supuestos que puedan suponer un grave riesgo hacia las personas o un potencial perjuicio empresarial hacia el negocio, sus clientes y/o a sus accionistas, así como cualquier otro de carácter legal y/o regulatorio cuya urgencia requiera de la adopción de medidas especiales o respuestas inmediatas».

En tercer y último lugar, debe tenerse en cuenta el principio rector 5 del ELI, conforme al cual el derecho a la desconexión debe ser reconocido por la ley como un derecho individual de las personas trabajadoras, de manera que la implementación específica y sus modalidades sean determinadas por convenios colectivos, de cualquier tipo, adaptados a cada situación de trabajo. En este punto es donde deben encontrarse las mejores soluciones para los problemas de aplicación e implementación del derecho a la desconexión: como a tal efecto se expresa en la posición de la CES sobre el derecho a la desconexión adoptado en el Comité Ejecutivo del 22-23 de marzo de 2021 (Confederación Europea de Sindicatos, 2021), las modalidades prácticas de ejercicio y aplicación del derecho a la desconexión deben ser acordadas por los interlocutores sociales mediante convenio colectivo en los ámbitos adecuados (nacional, sectorial o de empresa); deben prohibirse las modalidades establecidas unilateralmente por la persona empresaria o basadas en acuerdos individuales con las personas trabajadoras afectadas.

3. El derecho a la desconexión digital en España: tendencias sobre su ejercicio impulsadas por resoluciones judiciales

Algunas de las consideraciones que derivan de las nuevas tendencias que en materia de derecho a la desconexión cruzan Europa estarían dejando ya su impronta en el ámbito español, y, como se va a ver, mediante la labor efectuada por los tribunales del orden social.

Antes de valorar el alcance que la legislación de protección de datos y garantía de derechos digitales tiene sobre el derecho a la desconexión, conviene precisar que, en el marco de la legislación española, el derecho a la desconexión queda unido a los derechos a la intimidad. En este sentido, recuérdese que en el ámbito laboral el propio artículo 20 bis del *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* (en adelante LET) tiene un epígrafe explícito de ese vínculo entre ambos derechos: «Derechos de los trabajadores a la intimidad en relación con el entorno digital y a la desconexión». No obstante, la interpretación de que el derecho a la desconexión solo deba moverse en el marco del derecho a la intimidad de la persona trabajadora se estaría resquebrajando, pero en todo caso las presiones para su autodeterminación lo estaría haciendo ante los primeros embates de la doctrina

2. Véase en: https://www.ceoe.es/sites/ceoe-corporativo/files/content/file/2020/12/22/110/acuerdo_marco_interlocutores_sociales_europeos_digitalizacion_2020.pdf
3. Resolución de 3 de julio de 2024, de la Dirección General de Trabajo, por la que se registra y publica el Convenio colectivo para los establecimientos financieros de crédito. Véase en el «BOE» núm. 172, de 17 de julio de 2024. https://www.boe.es/buscar/doc.php?id=BOE-A-2024-14717

judicial, por ejemplo, como se va a ver a continuación, llevando el derecho a la desconexión hacia el campo del derecho fundamental a la integridad moral, previsto en el artículo15 de la Constitución Española.

En este punto, se ha de traer a colación la Sentencia del Tribunal Superior de Justicia-TSJ de Galicia 3558/2025, de 25 de abril de 2025, en la que se valora el hecho de que una trabajadora (según los hechos probados, su trabajo era de carácter presencial, no a distancia, aunque gozaba de gran flexibilidad horaria), estando en situación de incapacidad temporal informada por ansiedad y estrés por motivos laborales, recibió correos electrónicos, desde el primer día de su baja laboral, como parte de un hilo de comunicación previamente creado cuyo contenido estaba dirigido a otras personas (la sentencia reconoce, en todo caso, que en esos correos no se le pedía que respondiera inmediatamente a los correos electrónicos). Ante la reclamación de la trabajadora por haber recibido correos estando en situación de incapacidad temporal, la resolución judicial resuelve que, en el caso planteado, el derecho a la desconexión digital está vinculado al derecho fundamental a la integridad moral, «mediante el cual se protege la inviolabilidad de la persona, no solo contra ataques dirigidos a lesionar su cuerpo o espíritu, sino también contra cualquier tipo de intervención en dichos bienes sin el consentimiento de su titular» (SSTC n.º 120/1990 y n.º 207/1996, y art. 15 CE), el cual se habría vulnerado por no haber garantizado la empresa el derecho a la desconexión digital de la trabajadora cuando se encontraba fuera de su jornada laboral, dado que el contrato estaba suspendido por incapacidad temporal. Además, la sentencia refuerza su argumento al constatar que la actuación de la empresa, realizada sabiendo que la trabajadora sufría un trastorno de ansiedad que la imposibilitaba para trabajar, muestra a las claras su ideario de que la persona trabajadora está a su disposición en cualquier momento de su vida para atender o al menos recibir comunicaciones de la empresa, lo que infringe su derecho a la integridad moral, porque cosifica a la persona trabajador y atenta contra su dignidad. La sentencia añade que esa conducta empresarial impide el libre desarrollo de la personalidad sin injerencias injustificadas fuera de los límites estrictos del tiempo de trabajo y dificulta el ejercicio de la intimidad inherente a la vida personal y familiar y los derechos de conciliación contemplados en el artículo 88 de la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales* (en adelante, LOPDGDD). Como se observa, en relación al derecho a la desconexión, la sentencia pone en juego dos derechos fundamentales: uno referente al derecho a la integridad moral, que en el supuesto litigioso se habría vulnerado al haber enviado la empresa correos electrónicos estando la trabajadora en situación de incapacidad temporal, pero también el derecho fundamental a la intimidad vinculado a la vida privada de la persona trabajadora, que se habría infringido al no haberse abstenido la empresa de ponerse en contacto con esta fuera del horario laboral.[4]

Aportado este marco legal e interpretativo por la sentencia, conviene analizar las referencias jurídicas que expresa. Para empezar por el ámbito legal, se ha de partir de la base de que el artículo 88 LOPDGDD (al que se reenvía el artículo 20 bis de la LET en relación con los derechos de las personas trabajadoras a la intimidad en relación con el entorno digital y a la desconexión) tiene por epígrafe el siguiente: «Derecho a la desconexión digital en el ámbito laboral», y regula que dicho derecho se desenvuelve «fuera del tiempo de trabajo legal o convencionalmente establecido», aunque no concreta más, dejando a la empresa la obligación de elaborar una política interna, previa audiencia de los representantes obreros (por tanto, se exige audiencia, pero no necesariamente acuerdo con la representación laboral) (Pérez Campos, 2025, pág. 709), en la que se definan las modalidades de ejercicio del derecho a la desconexión. Esta regulación supone reconocer a las políticas empresariales porque, entre otras razones de calado, se establecen en términos obligacionales para el empresario sin contemplarse excepciones subjetivas u objetivas (Pérez Campos, 2025, pág. 709).

En relación con cómo se debería concretar el derecho a la desconexión, cabe recordar que la resolución del Parlamento Europeo, que se ha tratado anteriormente, establece que el derecho a la desconexión supone el derecho de las personas trabajadoras «a no participar» en actividades o comunicaciones laborales fuera de su tiempo de trabajo, a través de herramientas digitales, como llamadas telefónicas, mensajes electrónicos u otro tipo de mensajes. En la sentencia del TSJ de Galicia, de 25 de abril de 2025, se

4. Según Álvarez Cortés (2025), el incumplimiento del deber de abstención del empleador a no ponerse en contacto con el trabajador durante su periodo de descanso sería una vulneración del derecho a la intimidad de su vida privada.

expresa, remitiéndose a una resolución previa del mismo tribunal de 4 de marzo de 2024 (rec. 5647/2023), que el derecho a la desconexión «está vinculado no solo al derecho del trabajador a no responder a las comunicaciones del empleador o de terceros, sino también al deber de la empresa de abstenerse de contactar con el trabajador». En este sentido, prosigue diciendo la STJS de Galicia, 25 de abril de 2025, que el derecho a la desconexión digital exige que no se reciban comunicaciones de la empresa fuera del horario laboral y concluye que este derecho no se cumple por el hecho de que la persona trabajadora no tenga la obligación de responder a las comunicaciones recibidas fuera del horario laboral de manera prácticamente inmediata. Para la resolución, el derecho a la desconexión digital lleva consigo, por regla general, un deber por parte de la persona empleadora y de las personas dependientes o vinculadas de abstención en las comunicaciones de orden laboral o vinculadas a la prestación de servicios fuera del tiempo de trabajo.

En este sentido, considero que ese deber de abstención, que estaría vinculado al derecho fundamental a la intimidad personal y familiar (reconocido directamente en el artículo 88 LOPDGDD), no puede tener carácter absoluto hasta el punto de impedir a la empresa enviar cualquier tipo de correo electrónico a la persona trabajadora en periodo de desconexión. A mi modo de ver, en el punto en el que se haya la actual evolución del derecho a la desconexión tendería a proteger el derecho de las personas trabajadoras a no acceder a sus dispositivos digitales, o en el supuesto de hacerlo, el derecho a no involucrarse con los mensajes o comunicaciones transmitidos desde la empresa, o dicho de otro modo, a que la empresa no le envíe mensajes fuera de su jornada laboral que le afecten hasta el punto de que deba responder so pena de poner en cuestión sus propios intereses laborales. En otras palabras, el derecho a la desconexión se erige en un derecho a no molestar a la persona trabajadora, de manera que este se vea obligado a activarse fuera de su tiempo de trabajo, pero dicho ello, tampoco considero que, respetando lo anterior, la empresa deba bloquear, silenciar o no mantener ningún tipo de comunicación en el buzón del trabajador (por ejemplo, información sobre actividades que puedan realizarse en la empresa o noticias de interés). No considero el derecho a la desconexión desde un punto de vista de bloqueo de comunicaciones de la empresa en cualquier asunto, sino como una garantía para la persona trabajadora de que no deba activarse fuera del tiempo de trabajo ante una comunicación empresarial. Visto desde una perspectiva opuesta, el derecho a la desconexión no implica, a mi juicio, una prohibición para las personas trabajadoras de conectarse desde sus domicilios:[5] *de facto*, el derecho a la desconexión no debería implicar, *per se*, una prohibición a la empresa de bloquear digitalmente la posibilidad de cualquier comunicación fuera de su tiempo de trabajo en los dispositivos utilizados por la plantilla, ya sea entre esta, ya sea de la empresa con aquella.

Regresando a la Sentencia del Tribunal Superior de Justicia de Galicia, de 25 de abril de 2025, que valida el deber de la empresa de abstenerse de contactar con la persona trabajadora de forma íntegra; no es solo que la persona trabajadora no tenga obligación alguna de leer mensajes, es que es el empresario el que tiene la obligación de facilitar su cumplimiento mediante un deber de abstención en contactar a través de cualesquiera dispositivos en cualquier periodo de descanso (Sánchez Trigueros, 2025, pág. 752). Es decir, entendiendo contactar como el envío de cualquier correo electrónico, ya sea a diversos trabajadores (entre los que se incluyese en copia a uno de ellos que está en periodo de descanso) como individualmente al propio trabajador en descanso, pero que no le supusiese intervenir tras la comunicación adoptada por la empresa (de hecho, que la empresa enviase un correo informativo, con copia a personas trabajadoras fuera del tiempo de trabajo, atestiguaría también el celo empresarial en mantener informado al trabajador de cualquier asunto por el que pudiera tener interés aunque no le afectase directamente). En este sentido, considero que ese deber de abstención intenso extralimita el derecho fundamental a la intimidad de la persona trabajadora, o no es una actuación que se encuentre bajo la órbita de dicho derecho constitucional. En todo caso, esa actuación debería ser objeto de la política interna de la empresa, conforme a los términos de la legislación sobre protección de datos y garantías de derechos digitales, asumiendo que dicho

5. Véase el comentario del libro *Deep Work*, de Newport (2016), quién considera anacrónico que una empresa prohíba a sus trabajadores conectarse desde sus casas (Little, Brown, 2016). Véase la reseña del libro en el Blog de Ferran Camas: https://www.ferrancamas.com/para-desconectar/deepwork-coment/ia430

derecho aún no tenga pleno arraigo interno en su integración en el día a día de las empresas o en la negociación colectiva (Rincón Sanchez, 2025, pág. 723). Ahora bien, otro aspecto a valorar es la vinculación del derecho a la desconexión con el derecho fundamental a la vida e integridad física (art. 15 CE), que podría verse vulnerado por actuaciones empresariales a través de comunicaciones digitales que desconociesen de modo grosero, por su intensidad, su contenido o por el estado en el que se encontrase la persona trabajadora, el disfrute por esta de su descanso o del periodo de desconexión digital que disfrutase. La Sentencia del Tribunal de Justicia de Galicia, de 25 de abril de 2025, habla de una actuación de la empresa que habría afectado a la inviolabilidad de la persona y, por tanto, su integridad moral, aunque también podría pensarse que si los mensajes enviados pudiesen ser reiterados, solicitando la actuación de la trabajadora de forma inmediata mientras se encuentra en un periodo de incapacidad temporal, la emergencia de un ataque a su salud, vía la infracción del derecho fundamental a su integridad física o moral, podría ponerse de manifiesto. En este caso, el enlace entre el derecho a la desconexión digital y la seguridad y salud en el trabajo sería oportuno, más cuando a nivel legislativo falta una vinculación entre el derecho a la desconexión digital y el sistema de protección de los derechos de seguridad y salud de la persona trabajadora, especialmente en cuanto a la prevención de los riesgos psicosociales (Igartua Miró, 2025, pág. 704).

Siguiendo esa estela, ya focalizando el análisis en el teletrabajo, el artículo 18 de la *Ley 10/2021, de 9 de julio, de trabajo a distancia* (en adelante LTD), que tiene por epígrafe el «Derecho a la desconexión digital», establece que las personas que trabajan a distancia, particularmente en teletrabajo, tienen derecho a la desconexión digital «fuera de su horario de trabajo» en los términos establecidos en el artículo 88 LOPDGDD. Asimismo, en el apartado 2 del artículo 18 LTD, que sigue la estela del artículo 88 LOPDGDD, se señala que la empresa, previa audiencia de la representación legal de las personas trabajadoras, elaborará una política interna dirigida a las personas trabajadoras, incluidas las que ocupen puestos directivos, en la que se definirán las modalidades de ejercicio del derecho a la desconexión. Esta regulación ha sido objeto de aplicación por la Sentencia de la Audiencia Nacional (Sala de lo Social), núm. 44/2022, de 22 de marzo de 2022 (Rec. n.º 33/2022), que conoce de un conflicto colectivo cuyo supuesto fáctico es el acuerdo sobre trabajo a distancia que una empresa firma con cada uno de sus trabajadores (mediante la estrategia de «acuerdos masa», es decir, acuerdos del mismo tenor firmados individualmente con cada persona trabajadora). En lo que a este análisis interesa, en una de las cláusulas acordadas se establecía el derecho de la persona trabajadora a no atender dispositivos digitales cuando su jornada laboral hubiese finalizado, salvo que concurran las circunstancias de urgencia justificada señaladas en esta cláusula», y, en otra, se delimitaba lo que debía entenderse por dichas «circunstancias», al entenderse que aquellas podían suponer un perjuicio empresarial o del negocio cuya urgencia temporal requiera una respuesta o atención inmediata por parte de la persona trabajadora. Respecto a ambas cláusulas, la Sentencia de la Audiencia Nacional núm. 44/2022 dictamina que «obvio es, que ningún derecho presenta perfiles absolutos desde el momento en que su ejercicio convive con otros derechos que ocasionalmente pueden contraponerse, pero los límites al derecho a la desconexión digital en el teletrabajo no los puede establecer unilateralmente el empresario, sino que, como indica el art. 88 LOPDGDD, se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y los representantes de los trabajadores», por lo que el tribunal declara la nulidad de las cláusulas mencionadas (a mi modo de ver, la referencia al artículo 88 LOPDGDD podría haberse hecho igualmente por la sentencia al artículo 18 LTD).

De hecho, esta resolución judicial ha sido validada en estos aspectos reseñados anteriormente por la Sentencia del Tribunal Supremo (Sala de lo Social), de 2 de abril de 2025 (Núm. de resolución 267/2025). En su resolución, el TS establece que la legislación española no solo permite, sino que obliga, a la empresa a elaborar una «política interna» sobre el derecho a la desconexión digital; ahora bien, esa política interna debe elaborarse «previa audiencia» de los representantes de las personas trabajadoras. Por cierto, cuando eso no se realiza, la resolución mencionada, tomando como fundamento también la STS 225/2024, de 6 de febrero (rec. 263/2022), declara la nulidad de las correspondientes decisiones empresariales adaptadas sin la preceptiva intervención de los representantes de las personas trabajadoras. Partiendo del acierto de esta resolución, la doctrina también ha mantenido que, al anular esas cláusulas que, recuérdese, formaban parte de unos denominados acuerdos masa, se crea un vacío regulativo en esta situación y, por tanto, una inseguridad jurídica sobre las obligaciones de las personas trabajadoras con-

cernidas de conectar o no para atender las situaciones de urgencia de la empresa sin atender a la desconexión digital (Cruz Villalón, 2025, pág. 480).

Conclusiones

Este trabajo ha empezado por poner de manifiesto la emergencia del problema que supone para muchas personas trabajadoras la conectividad permanente, también conocida como trabajo «always-on» o «trabajo sin fin», particularmente para aquellas que prestan sus servicios en régimen de teletrabajo en sentido amplio. Frente a esa cultura de disponibilidad permanente, la garantía jurídica que se erige como fundamental y que está atrayendo la mayor intensidad investigadora es el derecho a la desconexión digital, que en el ámbito europeo no está regulado, aunque cuenta con un importante punto de referencia en la Resolución del Parlamento Europeo, de 21 de enero de 2021, con recomendaciones destinadas a la Comisión sobre el derecho a la desconexión. La labor iniciada por la Comisión Europea en 2024, sobre una posible acción de la Unión Europea (UE) en el ámbito del teletrabajo y del derecho de las personas trabajadoras a la desconexión, debe ser objeto de desarrollo con la perspectiva puesta, como al efecto he pretendido defender, en la regulación de un derecho a la desconexión anclado en dos objetivos específicos y uno transversal: la protección de la salud física y mental de todas las personas trabajadoras; el equilibrio entre la vida laboral y personal y garantiza la previsibilidad de los horarios de trabajo; y de forma común a ambos, que el derecho a la desconexión promueva la igualdad de género.

En este trabajo se ha pretendido articular esa referencia con lo establecido en el artículo 88 LOPDGDD y el artículo 18 LTD, que regulan el derecho a la desconexión digital en nuestro país, poniéndose de manifiesto que debe aún profundizarse en lo que implica dicho derecho tanto para la empresa como para la persona trabajadora o teletrabajadora, así como también conseguir hacerlo más efectivo.

Referencias bibliográficas

ÁLVAREZ CORTÉS, J. C. (2025). «La desconexión digital como límite al poder de dirección del empresario». En: Antonio V. Sempere Navarro y José Luis Monereo Pérez (dirs.). *El poder de dirección del empresario: problemas y manifestaciones actuales. Libro Homenaje a Alfredo Montoya Melgar*, p. 696. Ediciones Laborum [en línea]. Disponible en: https://accesoabierto.laborum.es/index.php/oa/catalog/view/65/979-13-88025-22-8/157?fbclid=IwY2xjawPV7x9leHRuA2FlbQIxMABzcnRjBmFwcF9pZBAyMjIwMzkxNzg4MjAwODkyAAEeWxq4Zy0__mYQjOGEPT330morLOpgadJaiUYwluLboQCz179ib0x8ydQM3Ao_aem_IERaqqxVBcBeDwRMo-9wPQ

Comisión EUROPEA (2024a). *Study exploring the social, economic and legal context and trend of telework and the right to disconnect, in the context of digitalisation and the future of work, during and beyond the COVID-19 pandemic*. Publications Office of the European Union [en línea]. Disponible en: https://employment-social-affairs.ec.europa.eu/study-social-economic-and-legal-context-and-trends-telework-and-right-disconnect-context_en

Comisión EUROPEA (2024b). *Study exploring the social, economic and legal context and trends of telework and the right to disconnect, in the context of digitalisation and the future of work, during and beyond the COVID-19 pandemic- Annex 4 Synopsis report covering all stakeholder consultations*. Publications Office of the European Union [en línea]. Disponible en: https://op.europa.eu/en/publication-detail/-/publication/4a685add-fc75-11ee-a251-01aa75ed71a1/language-en

Comisión EUROPEA (2025). *Joint Employment Report 2025* [en línea]. Disponible en: https://employment-social-affairs.ec.europa.eu/joint-employment-report-2025-0_en

Comisión EUROPEA (2024c). *Consultation Document: First-phase consultation of social partners under Article 154 TFEU on possible EU action in the area of telework and workers' right to disconnect - Brussels, 30.4.2024 - C(2024) 2990 final* [en línea]. Disponible en: https://ec.europa.eu/social/BlobServlet?docId=27565&langId=en

CONFEDERACIÓN EUROPEA DE SINDICATOS (2024). «Respuesta de la CES a la primera fase de consulta de la Comisión a los interlocutores sociales europeos sobre posibles acciones en el ámbito del teletrabajo y el derecho de las personas trabajadoras a la desconexión Adoptada en la reunión del Comité Ejecutivo de la CES de 25 de junio de 2024». *UGT* (en línea). Disponible en: https://www.ugt.es/sites/default/files/20240624-25_CE_CES_12_Respuesta_CES_a_Consulta_Teletrabajo_final.pdf

CONFEDERACIÓN EUROPEA DE SINDICATOS (2021). «Posición de la CES sobre el derecho a la desconexión Adoptado en el Comité Ejecutivo del 22-23 de marzo de 2021». *UGT* (en línea). Disponible en: https://www.ugt.es/sites/default/files/210322_ce_ces_16_derechodesconexion_final.pdf

Cruz Villalón, J. «Los poderes empresariales en el trabajo a distancia». En: Antonio V. Sempere Navarro y José Luis Monereo Pérez (dirs.). *El poder de dirección del empresario: problemas y manifestaciones actuales. Libro Homenaje a Alfredo Montoya Melgar*, p. 480 (Dir.: Antonio V. Sempere Navarro y José Luis Monereo Pérez). Ediciones Laborum, 2025, p. 480. Ediciones Laborum [en línea]. Disponible en: https://accesoabierto.laborum.es/index.php/oa/catalog/view/65/979-13-88025-22-8/157?fbclid=IwY2xjawPV7x9leHRuA2FlbQIxMABzcnRjBmFwcF9pZBAyMjIwMzkxNzg4MjAwODkyAAEeWxq4Zy0__mYQjOGEPT330morLOpgadJaiUYwluLboQCz179ib0x8ydQM3Ao_aem_IERaqqxVBcBeDwRMo-9wPQ

EUROFOUND (2022). En: VARGAS LLAVE, O.; HURLEY, J.; PERUFFO, E.; RODRÍGUEZ CONTRERAS, R.; ADASCALITEI, D.; BOTEY GAUDE, L.; STAFFA, E.; VACAS SORIANO, C. (auts.). *The rise in telework: Impact on working conditions and regulations*. Luxemburgo: Publications Office of the European Union [en línea]. Disponible en: https://www.eurofound.europa.eu/system/files/2023-01/ef22005en.pdf

EUROFOUND (2020). En: ISUSI, I.; DURÁN, J.; CORRAL, A. (IKEI Research & Consultancy) (auts.). *Working conditions in telework during the pandemic and future challenges* [en línea]. Disponible en: https://a.storyblok.com/f/279033/0518187026/wpef22032.pdf

EUROFOUND; ORGANIZACIÓN INTERNACIONAL DEL TRABAJO (2019). *Trabajar en cualquier momento y en cualquier lugar: consecuencias en el ámbito laboral*. Luxemburgo: Oficina de Publicaciones de la Unión Europea y Santiago: Santiago [en línea]. Disponible en: https://www.ilo.org/es/media/406516/download

European Agency for Safety and Health at Work (2023). *Regulating telework in a post-COVID-19 Europe: recent developments* [en línea]. Disponible en: https://op.europa.eu/en/publication-detail/-/publication/a279d374-8435-11ee-99ba-01aa75ed71a1/language-en

European Labour Authority (2023). *The rise of teleworking: improvements in legislation and challenges for tackling undeclared work*. Publications Office of the European Union [en línea]. Disponible en: https://www.ela.europa.eu/sites/default/files/2023-12/output-paper-teleworking-March-2023-Plenary.pdf

European Law InstitutE (2023). *Guiding Principles on Implementing Workers' Right to Disconnect*. Puede consultarse en español (traducción realizada por Ferran Camas Roda y Andrea Cano Redondo) [en línea]. Disponible en: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/Principios_rectores_para_la_aplicacio__n_del_derecho_de_los_trabajadores_a_la_desconexio__n__ESP_.pdf

IGARTUA MIRÓ, T. (2025). «El derecho a la desconexión digital como límite al poder de dirección del empresario (art. 20 bis ET)». En: Antonio V. Sempere Navarro y José Luis Monereo Pérez (dirs.). *El poder de dirección del empresario: problemas y manifestaciones actuales. Libro Homenaje a Alfredo Montoya Melgar*. Ediciones Laborum [en línea]. Disponible en: https://accesoabierto.laborum.es/index.php/oa/catalog/view/65/979-13-88025-22-8/157?fbclid=IwY2xjawPV7x9leHRuA2FlbQIxMABzcnRjBmFwcF9pZBAyMjIwMzkxNzg4MjAwODkyAAEeWxq4Zy0__mYQjOGEPT330morLOpgadJaiUYwluLboQCz179ib0x8ydQM3Ao_aem_IERaqqxVBcBeDwRMo-9wPQ

NEWPORT, C. (2016). *Deep Work* (Little, Brown, 2016). Véase la reseña del libro en el blog de Ferran Camas. *El Diario de Ferran Camas* [en línea]. Disponible en: https://www.ferrancamas.com/para-desconectar/deepwork-coment/ia430

PÉREZ CAMPOS, A. I. (2025). «Poder de dirección, intimidad digital y desconexión: reflexiones a propósito de la STS 225/2024, de 6 de febrero (rec. 263/2022)». En: Antonio V. Sempere Navarro y José Luis Monereo Pérez (dirs.). *El poder de dirección del empresario: problemas y manifestaciones actuales. Libro Homenaje a Alfredo Montoya Melgar*. Ediciones Laborum [en línea]. Disponible en: https://accesoabierto.laborum.es/index.php/oa/catalog/view/65/979-13-88025-22-8/157?fbclid=IwY2xjawPV7x9leHRuA2FlbQIxMABzcnRjBmFwcF9pZBAyMjIwMzkxNzg4MjAwODkyAAEeWxq4Zy0__mYQjOGEPT330morLOpgadJaiUYwluLboQCz179ib0x8ydQM3Ao_aem_IERaqqxVBcBeDwRMo-9wPQ

RINCÓN SANCHEZ, C. (2025). «El poder de dirección de la empresa y sus implicaciones en el derecho de desconexión digital». En: Antonio V. Sempere Navarro y José Luis Monereo Pérez (dirs.). *El poder de dirección del empresario: problemas y manifestaciones actuales. Libro Homenaje a Alfredo Montoya Melgar*. Ediciones Laborum [en línea]. Disponible en: https://accesoabierto.laborum.es/index.php/oa/catalog/view/65/979-13-88025-22-8/157?fbclid=IwY2xjawPV7x9leHRuA2FlbQIxMABzcnRjBmFwcF9pZBAyMjIwMzkxNzg4MjAwODkyAAEeWxq4Zy0__mYQjOGEPT330morLOpgadJaiUYwluLboQCz179ib0x8ydQM3Ao_aem_IERaqqxVBcBeDwRMo-9wPQ

RUIZ GONZÁLEZ, C. (2025). «El derecho a la desconexión digital como límite al poder de dirección y control del empresario». En: Antonio V. Sempere Navarro y José Luis Monereo Pérez (dirs.). *El poder de dirección del empresario: problemas y manifestaciones actuales. Libro Homenaje a Alfredo Montoya Melgar*. Ediciones Laborum [en línea]. Disponible en: https://accesoabierto.laborum.es/index.php/oa/catalog/view/65/979-13-88025-22-8/157?fbclid=IwY2xjawPV7x9leHRuA2FlbQIxMABzcnRjBmFwcF9pZBAyMjIwMzkxNzg4MjAwODkyAAEeWxq4Zy0__mYQjOGEPT330morLOpgadJaiUYwIuLboQCz179ib0x8ydQM3Ao_aem_IERaqqxVBcBeDwRMo-9wPQ

SÁNCHEZ TRIGUEROS, C. (2025). «Doctrina judicial sobre desconexión digital». En: Antonio V. Sempere Navarro y José Luis Monereo Pérez (dirs.). *El poder de dirección del empresario: problemas y manifestaciones actuales. Libro Homenaje a Alfredo Montoya Melgar*. Ediciones Laborum [en línea]. Disponible en: https://accesoabierto.laborum.es/index.php/oa/catalog/view/65/979-13-88025-22-8/157?fbclid=IwY2xjawPV7x9leHRuA2FlbQIxMABzcnRjBmFwcF9pZBAyMjIwMzkxNzg4MjAwODkyAAEeWxq4Zy0__mYQjOGEPT330morLOpgadJaiUYwIuLboQCz179ib0x8ydQM3Ao_aem_IERaqqxVBcBeDwRMo-9wPQ

Universitat Oberta de Catalunya (s.f.). *Protocolo para el cumplimiento del derecho a la desconexión digital*. UOC [en línea]. Disponible en: https://campus.uoc.edu/webapps/intrauoc2/documents/733548/0/20211203_Protocol_desconnexio_digital_ES.pdf

Cita recomendada

CAMAS RODA, Ferran (2026). «El derecho a la desconexión desde una perspectiva europea: propuestas sobre su regulación y su ejercicio y primeros efectos en el régimen vigente en España». En: Irene Rovira Ferrer (coord.). «Sobre la consolidación del trabajo a distancia». *IDP. Revista de Internet, Derecho y Política*, núm. 44. UOC [Fecha de consulta: dd/mm/aa]. DOI: http://dx.doi.org/10.7238/idp.v0i44.98003877

Sobre el autor

Ferran Camas Roda
Universitat de Girona
fernando.camas@udg.edu

Catedrático de Derecho del Trabajo y de la Seguridad Social en la Universitat de Girona, donde además dirige la Cátedra de Inmigración, Derechos y Ciudadanía. También es miembro de la Red Europea de Expertos en Derecho de Igualdad de Género y No Discriminación en representación de España. Actualmente, dirige un proyecto de investigación concedido por el Ministerio de Ciencia, Innovación y Universidades sobre el tema «No discriminación, bienestar laboral y teletrabajo de personal extranjero: tres elementos clave para la consolidación del trabajo a distancia». Dispone de un blog sobre sus investigaciones de carácter jurídico y sus inquietudes culturales: https://www.ferrancamas.com.

IDP
REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Monográfico: «Sobre la consolidación del trabajo a distancia» (coord.: Irene Rovira Ferrer)

Teletrabajo y su afectación a los derechos de las personas trabajadoras desde una perspectiva de género

Ana María Castro Franco
Universidad de León

Fecha de presentación: septiembre 2025
Fecha de aceptación: enero 2026
Fecha de publicación: marzo 2026

Resumen

Entre los principales desafíos que suscita el teletrabajo en el contexto de la digitalización empresarial se encuentra la necesidad de compatibilizar su configuración como mecanismo idóneo para el ejercicio de los derechos de conciliación con la exigencia paralela de asegurar el pleno respeto a un derecho al descanso real y de calidad. El presente ensayo constata cómo la falsa ilusión de la libertad para autoorganizarse, la flexibilidad horaria y la autoexigencia laboral, en conjunción con las labores domésticas y de cuidado, suponen para las mujeres una sobrecarga de trabajo.

A partir de esta premisa, se analiza el modo en el que el teletrabajo, lejos de configurar un escenario neutro, reproduce y acentúa las desigualdades de género, tanto en la esfera laboral como en la de prevención de riesgos.

Además, procede examinar los riesgos ergonómicos y psicosociales específicos que afectan a las trabajadoras en este modelo organizativo. Este enfoque resulta esencial, pues los riesgos ergonómicos, derivados de un mobiliario o equipos diseñados sin tener en cuenta las especificidades antropométricas de las mujeres, se suman a los riesgos psicosociales, cuya complejidad se acrecienta en los entornos digitales. En el ámbito de la salud, los costes físicos, emocionales y laborales para las mujeres son mayores, en gran medida por la difícil gestión de los tiempos de trabajo.

Igualmente, no puede soslayarse en esta investigación la emergencia de nuevas formas de violencia laboral mediadas por la tecnología, entre las que ocupa un lugar central el ciberacoso, pues se erige como un riesgo psicosocial de especial complejidad en el marco del trabajo a distancia.

Por ende, el objetivo del presente trabajo es analizar el impacto del teletrabajo sobre los derechos de las personas trabajadoras desde una perspectiva de género, poniendo el foco en los ámbitos de la conciliación, la prevención de riesgos laborales –especialmente ergonómicos y psicosociales–, el acoso laboral mediado por las tecnologías y el derecho a la desconexión digital.

Palabras clave
teletrabajo; perspectiva de género; conciliación; desconexión digital; riesgos para la seguridad y salud; ciberacoso

Teleworking and its impact on the rights of workers from a gender perspective

Abstract
Among the main challenges posed by remote work in the context of enterprise digitization is the need to reconcile its role as a suitable mechanism for exercising reconciliation rights with the parallel requirement to ensure full respect for the right to genuine and quality rest. This essay explains how the false illusion of freedom to self-organize, time flexibility, and self-imposed work demands, alongside domestic and caregiving tasks, create a labour overload for women.

From this premise, it analyses how telework, far from constituting a neutral scenario, reproduces and accentuates gender inequalities, both in the work and risk-prevention spheres.

Furthermore, it is important to assess the specific ergonomic and psychosocial risks affecting workers within this organizational model. This is crucial because ergonomic risks from furniture or equipment that do not consider women's anthropometric specifics compound the psychosocial risks, which become more complex in digital environments. In healthcare, the physical, emotional, and labour-related costs for women are higher, mainly due to the challenging management of work hours.

Likewise, the emergence of new forms of technology-mediated workplace violence cannot be overlooked in this investigation, with cyberbullying occupying a central role since it represents a psychosocial risk of particular complexity within the context of remote work.

Therefore, the aim of this paper is to analyse the impact of remote work on workers' rights from a gender perspective, focusing on aspects such as work-life balance, prevention of occupational risks – particularly ergonomic and psychosocial – workplace harassment mediated by technologies and the right to digital disconnection.

Keywords
teleworking; gender perspective; reconciliation; digital disconnection; safety and health risks; cyberbullying

Introducción

El presente estudio realiza un análisis de la doctrina sustentado en la normativa aplicable y en el examen de la jurisprudencia más relevante en materia de teletrabajo, prevención de riesgos laborales y derechos digitales. La finalidad es valorar críticamente la suficiencia del marco regulador vigente y visibilizar sus principales déficits desde la óptica de la igualdad efectiva entre mujeres y hombres, así como formular propuestas de mejora, tanto en el plano normativo como en el preventivo.

La hermenéutica seguida es predominantemente deductiva, en la medida en que parte del análisis del marco normativo y la doctrina científica generalista para analizar su proyección concreta sobre el teletrabajo desde una perspectiva de género, sin perjuicio de la incorporación puntual de elementos inductivos derivados del análisis de los riesgos y las problemáticas específicas.

Por otra parte, el enfoque metodológico no es meramente descriptivo, sino que adopta una perspectiva valorativa orientada a la identificación de lagunas regulatorias, disfunciones prácticas y riesgos de reproducción de desigualdades de género en la aplicación del teletrabajo.

1. Las sombras del trabajo remoto y flexible

Las nuevas tecnologías impactan en la digitalización de las relaciones laborales y la automatización de las funciones, reforzando el poder empresarial incluso en contextos de deslocalización física del trabajo. En ausencia de límites claros en el ejercicio de las facultades de dirección y control, esta transformación puede intensificar la asimetría estructural de la relación laboral y derivar en la vulneración de derechos laborales, como el derecho al trabajo y a la ocupación efectiva, el derecho al descanso, la seguridad y salud laboral, la formación profesional, la conciliación, la intimidad personal o la protección de datos (Giraldo Restrepo, 2023).

A resultas de la crisis sanitaria provocada por el COVID-19, la normativa concedió un papel preferente al teletrabajo, ante otras medidas en relación con el empleo, a fin de mantener la actividad productiva ante la casi total ausencia de regulación específica previa. La extensión y normalización del trabajo remoto y flexible frente al paradigma corporativo tradicional ha evidenciado notables ventajas, pero también ha visibilizado y agravado algunos efectos negativos, entre los que destacan el tecnoestrés, el horario continuo, la fatiga informática, la hiperconectividad, la pérdida de la identidad corporativa, las deficiencias en las comunicaciones, las brechas digitales o el traslado de costes de la actividad productiva a la persona teletrabajadora.

El teletrabajo puro acaba por individualizar a quienes llevan a cabo esta modalidad, en la medida en que limita su interacción cotidiana con el resto de la plantilla, menoscabando los lazos de solidaridad y cohesión colectiva de la fuerza de trabajo (Álvarez Cuesta, 2023). Esta fragmentación no solo afecta al plano social, también puede repercutir en el ámbito jurídico-laboral, al dificultar la articulación de la acción sindical y la participación en órganos de representación colectiva. A su vez, las tecnologías pueden ahondar en las desigualdades existentes y servir de herramienta mediante la cual surgen nuevas formas de discriminación y acoso.

Conviene subrayar que una de las principales ventajas del teletrabajo consiste en su potencial para favorecer la conciliación de las esferas laboral y personal; sin embargo, el problema surge cuando esta premisa sirve para reforzar el estereotipo de que la crianza de los hijos, el cuidado de mayores o personas dependientes y los quehaceres domésticos le corresponden a la mujer. A mayores, son las teletrabajadoras quienes sufren, en mayor medida, el desgaste en la salud derivado de esta modalidad de trabajo.

2. Retos que plantea el teletrabajo en relación con el derecho de conciliación

El teletrabajo ha incidido especialmente sobre las trabajadoras, habida cuenta de que las mujeres están cuantitativamente más presentes en sectores con opción de realizar las tareas a distancia, mientras los hombres están sobrerrepresentados en ramas de actividad que no admiten dicha alternativa (De la Puebla Pinilla, 2020). Si bien el trabajo a distancia puede tener consecuencias positivas para la conciliación de la vida personal y laboral, debido al ahorro de costes y tiempos de desplazamiento y a la mayor flexibilidad en la gestión de los horarios, no es menos cierto que entraña riesgos relevantes desde una perspectiva de igualdad de género.

En particular, existe el peligro de que esta modalidad, lejos de favorecer un reparto equilibrado de responsabilidades, termine por reproducir o incluso acentuar patrones tradicionales de asignación de las tareas domésticas y de cuidado de menores y/o mayores o dependientes, en un momento en el que dicho esquema parecía estar en proceso de superación. En efecto, si las mujeres predominan en las actividades que permiten el teletrabajo y este se erige como una medida encaminada a favorecer la conciliación, es previsible que sean ellas quienes recurran con mayor frecuencia al trabajo a distancia.

La percepción errónea, según la cual el teletrabajo constituye, por sí mismo, la respuesta definitiva a los problemas de conciliación de la vida personal, familiar y laboral, puede desincentivar el desarrollo de políticas y medidas que promuevan un reparto corresponsable de las tareas domésticas y de cuidado entre mujeres y hombres. Una visión simplista del teletrabajo como mecanismo de conciliación, unida a la persistencia de los roles de género en este ámbito, puede derivar en una asimilación de esta modalidad laboral con actividades de menor responsabilidad, debilitando la vinculación con la empresa.

Como es sabido, un riesgo vinculado al teletrabajo es la dificultad para establecer una separación clara entre el espacio laboral y el familiar, pues dos esferas diferenciadas –el lugar de trabajo, asociado a la competitividad y el esfuerzo, frente al hogar, ligado al descanso, al ocio y a la vida privada– tienden a converger en un mismo entorno físico. Esta difuminación de límites, estrechamente condicionada por la disponibilidad horaria y la flexibilidad de la jornada, puede dar lugar a un solapamiento de tiempos y funciones que impacta negativamente tanto en la calidad del trabajo como en el bienestar personal.

De este modo, la desconexión digital se configura como una herramienta imprescindible para prevenir los riesgos psicosociales emergentes del teletrabajo y para mitigar los efectos adversos que tiene una disponibilidad horaria continua sobre la conciliación y la corresponsabilidad. La eficacia de este deber no puede depender únicamente de la buena voluntad de las empresas; por lo tanto, es necesaria su incorporación en los instrumentos de negociación colectiva, mediante cláusulas que regulen de manera clara los límites de disponibilidad y la responsabilidad de quien proporciona empleo en materia de supervisión digital.

Las personas que realizan su trabajo a distancia tienen reconocidos los mismos derechos que quienes acuden presencialmente al centro de trabajo en materia de conciliación y corresponsabilidad, incluyendo el derecho de adaptación de la jornada. Asimismo, las medidas para la protección de las víctimas de violencia de género deben observar las posibles consecuencias y singularidades de esta forma de prestación de servicios.

La Ley 10/2021, de 9 de julio, de trabajo a distancia, traslada a los convenios o acuerdos colectivos la responsabilidad de diseñar los mecanismos y criterios por los que la persona que desarrolla un trabajo presencial puede pasar al trabajo a distancia o viceversa, así como preferencias vinculadas a determinadas circunstancias, evitando la perpetuación de roles y estereotipos de género y considerando el fomento de la corresponsabilidad entre mujeres y hombres, debiendo ser objeto de diagnóstico y tratamiento por parte del plan de igualdad.

Por esta razón, resulta preocupante el escaso protagonismo que la reciente negociación colectiva otorga a la conciliación cuando regula el trabajo, mientras los derechos colectivos de las personas teletrabajadoras o la prevención de riesgos laborales reciben una atención prioritaria (Gala Durán, 2025). Las partes negociadoras no parecen ser conscientes del riesgo que el teletrabajo puede suponer para perpetuar el rol social de cuidadoras.

En la mayoría de los casos, los agentes sociales reconocen el derecho a la conciliación, los derechos digitales de la plantilla y la protección frente al acoso en el entorno laboral digital. Sin embargo, omiten la incorporación de un conjunto de medidas específicas orientadas a asegurar la implementación del teletrabajo desde una perspectiva de género. Las acciones a valorar consisten, entre otras, en garantizar que la mano de obra teletrabajadora esté integrada de forma equilibrada; fomentar un modelo híbrido de teletrabajo, si resulta oportuno; suspender o revocar el acuerdo individual de teletrabajo de una víctima de violencia de género, cuando las circunstancias así lo aconsejen, y aprobar un protocolo de actuación contra el ciberacoso laboral, en cumplimiento con el Convenio sobre la violencia y el acoso, 2019, núm. 190 (Melián Chinea, 2022).

3. Los riesgos ergonómicos en el teletrabajo

Los riesgos físicos y ergonómicos asociados al teletrabajo están relacionados directamente con las condiciones ma-

teriales y organizativas propias de esta modalidad laboral. Los riesgos se ven incrementados cuando el entorno no ofrece las condiciones adecuadas de iluminación, humedad, temperatura, ventilación o aislamiento acústico, lo que puede generar fatiga generalizada, estrés y una menor capacidad de concentración.

El espacio físico en el que se lleva a cabo la actividad suele carecer de las condiciones ergonómicas óptimas, especialmente cuando se utilizan mesas, sillas o dispositivos no diseñados para un uso profesional prolongado. Ello incrementa la probabilidad de desarrollar trastornos musculoesqueléticos, tales como lumbalgias, cervicalgias o dorsalgias asociados a posturas inadecuadas o movimientos repetitivos. En la misma línea, el uso intensivo de pantallas expone a las personas teletrabajadoras a la llamada fatiga ocular o astenopia (González-Menéndez *et al*., 2019).

Igualmente, las características personales y profesionales de cada persona teletrabajadora –como la edad, el estado de salud, el nivel de competencias digitales o la capacidad de autogestión del tiempo– interactúan con el contexto físico y organizativo, modulando la magnitud de los riesgos. En cualquier caso, la doble carga de trabajo –que combina las responsabilidades profesionales remuneradas con las labores domésticas y de cuidado no remuneradas–, junto con las condiciones laborales y de empleo generalmente más precarias a las que se enfrentan las mujeres, repercute de manera significativa en su salud.

En cualquier entorno laboral, en el diseño de un puesto de trabajo es fundamental tener en cuenta las diferencias antropométricas entre mujeres y hombres, pues ignorar estos parámetros puede incrementar la incidencia de lesiones y afectar de manera desproporcionada a quienes presentan dimensiones corporales atípicas respecto al estándar, tradicionalmente centrado en el modelo masculino. Las diferencias biológicas mueven a adoptar posturas forzadas y realizar sobreesfuerzos, debido a la falta de adaptación ergonómica de los puestos y equipos (Ferreras Remesal, 2019).

4. El auge de los riesgos psicosociales en las mujeres teletrabajadoras

Los riesgos psicosociales vinculados al teletrabajo vienen conformados por las elevadas cargas y ritmos de trabajo, la prolongación de la jornada laboral más allá de los límites formales, la percepción de tener que estar disponible en todo momento y en todo lugar, la falta de oportunidades de desarrollo profesional, la excesiva fragmentación de las tareas asignadas, la escasa autonomía y control sobre la propia actividad, una pobre cultura organizativa y las conductas de ciberacoso (Giuzio y Cancela, 2021).

El aumento del teletrabajo, en el que está sobrerrepresentado el colectivo femenino, puede derivar en estrés y conflictos de rol debido a la necesidad de llevar a cabo un intercambio justo entre la vida personal y laboral. Desde una perspectiva de género, teletrabajar puede resultar más estresante para las mujeres, pues no hay una división equitativa de las responsabilidades domésticas y de las tareas de cuidados (Montes Adalid, 2023).

De igual modo, la reducción de los intercambios interpersonales y las interacciones cara a cara crea una sensación de aislamiento, lo que aumenta la tensión y fatiga y provoca sentimientos de frustración, falta de pertenencia a la organización y soledad (Herrera, 2021). Con la finalidad de mitigar este creciente problema, quien proporciona empleo debe adoptar medidas para prevenir el aislamiento de la persona teletrabajadora en relación con la mano de obra presencial de la empresa, tales como propiciar los reencuentros regulares con los compañeros y otorgar acceso a las informaciones de la empresa.

El trabajo a distancia constituye una forma de facilitar el acceso al empleo de las víctimas de violencia de género o un medio de protección. Ahora bien, preocupa especialmente el riesgo de aislamiento en estos casos, al reducir la interacción presencial con compañeros y redes de apoyo formales e informales. Este aislamiento también puede dificultar la denuncia de situaciones de violencia y la búsqueda de asistencia externa. Por consiguiente, el teletrabajo debe ir acompañado de protocolos para las víctimas de violencia de género, canales de comunicación, orientación psicológica y programas de mentoría. Estas medidas buscan reducir el aislamiento, garantizar la protección de la víctima y asegurar que la modalidad de teletrabajo no se convierta en un factor que aumente su vulnerabilidad.

Indiscutiblemente, el aislamiento, el estrés laboral o el tecnoestrés (en sus múltiples variables), la sobrecarga de trabajo y las dificultades para conciliar, favorecen la aparición de trastornos emocionales y psicológicos como ansiedad, irritabilidad, estados depresivos, *burnout*, afectación de

los ritmos biológicos ante la falta de rutinas para teletrabajar, trastornos del sueño o sedentarismo. Algunos riesgos, como el aislamiento, la ansiedad o el estrés laboral, podrían neutralizarse al otorgar prioridad a la modalidad mixta de teletrabajo sobre la fórmula a jornada completa.

Las intervenciones preventivas deben partir de una evaluación de riesgos minuciosa y de la mejora de las condiciones de trabajo, pues todas aquellas características del trabajo, incluidas las relativas a su organización y ordenación, son susceptibles de producir daños. En cumplimiento del artículo 15 de la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos Laborales, se han de combatir los riesgos psicosociales, en primer término, en el origen, modificando los aspectos nocivos de la organización del trabajo. Asimismo, se debe adaptar el trabajo a la persona, atenuando las tareas monótonas y repetitivas, mediante cambios en la concepción de los puestos de trabajo, en la elección de los equipos y en los métodos de trabajo y producción.

A efectos de la prevención de riesgos, la persona teletrabajadora debe ser considerada, en todo momento, como un integrante más de la organización, con independencia de que la prestación de servicios se desarrolle total o parcialmente fuera del centro de trabajo.

En cualquier caso, se han de abordar todos los factores que configuran el teletrabajo, incorporando de forma transversal la perspectiva de género, tanto en los planes de prevención de riesgos laborales como en los procesos de evaluación, seguimiento y, en su caso, adaptación del puesto de trabajo. En relación con la prevención de los riesgos psicosociales asociados al teletrabajo, resulta deseable incorporar de manera sistemática la variable sexo en los procesos de recogida y análisis de datos, así como en los estudios e investigaciones en materia de prevención de riesgos laborales. Solo mediante esta perspectiva diferenciada es posible identificar patrones de desigualdad y visibilizar situaciones en las que los daños derivados de la actividad laboral puedan estar vinculados directa o indirectamente al sexo de las personas trabajadoras.

5. El acoso laboral a las mujeres en el teletrabajo

Las conductas hostiles propias del acoso presencial tienden a trasladarse al ámbito del teletrabajo, logrando el aislamiento digital y ambiental de la persona afectada. Como ejemplos de ciberacoso laboral, procede citar el sometimiento a la persona teletrabajadora a una falta de ocupación efectiva, asignarle tareas inútiles o repetitivas, dar órdenes imposibles de cumplir con los recursos o el tiempo disponible, provocar la incomunicación con terceras personas, no invitarla a las reuniones o videoconferencias, ignorar su participación en estos actos, eliminarla de grupos de WhatsApp laborales o crear un grupo paralelo en el que no esté (González, 2024).

La rapidez con la que la información se difunde en el entorno digital, la posibilidad de acceder a ella mediante motores de búsqueda y las dificultades para su eliminación generan nuevas formas de exposición y vulnerabilidad. La facilidad para viralizar contenidos, el anonimato y la perdurabilidad de la información en línea introducen situaciones de riesgo inéditas, que pueden afectar tanto a la reputación como a la seguridad y privacidad de las personas. Sin duda, las nuevas tecnologías se convierten en una herramienta sumamente peligrosa para el acoso sexual, pues permiten difundir determinadas imágenes, rumores o vídeos con mucha rapidez sin el consentimiento de la víctima.

Las teletrabajadoras pueden ser víctimas de acoso sexual a través de medios digitales, mediante el envío de mensajes humillantes, intimidatorios o amenazantes, que buscan coaccionarlas para satisfacer exigencias de carácter sexual bajo la amenaza de sufrir repercusiones negativas en su trayectoria laboral. Estas prácticas suelen derivar en una menor productividad y un clima laboral tóxico. Las redes sociales, mal utilizadas, pueden dar carta blanca a la *sextorsión* (coacción sexual mediante amenazas o chantaje en el ámbito digital), el *ciberstalking* (persecución a través de medios electrónicos traducida en hostigamiento) o el *doxing* (difusión, manipulación de datos, suplantación de identidad o uso indebido de datos personales con fines intimidatorios o maliciosos).

Las mujeres se ven especialmente afectadas por estos fenómenos de violencia en línea, sufriendo como consecuencia daños físicos, psicológicos y económicos. Sus efectos se traducen en ansiedad, aislamiento, soledad, miedo, baja autoestima, apatía, trastornos del sueño, trastornos de la conducta alimentaria, bajas laborales y, en los casos más extremos, suicidio. La separación física respecto al resto de la plantilla puede aumentar la vulnerabilidad de la persona teletrabajadora frente al ciberacoso,

al limitar la supervisión directa, reducir las oportunidades de apoyo entre compañeros y favorecer una sensación de aislamiento.

Como ha señalado la mejor doctrina, el acoso laboral requería la concurrencia de intencionalidad, producción de un daño y reiteración sistemática de la conducta. No obstante, los dos primeros elementos han perdido peso y han sido prácticamente desterrados, por cuanto el Tribunal Constitucional tiene en cuenta si: (i) la conducta enjuiciada es deliberada o está adecuadamente conectada al resultado lesivo; (ii) ha causado a la víctima un padecimiento físico, psíquico o moral, o poseía la potencialidad de hacerlo; y la conducta tenía como fin vejar, humillar o envilecer a la víctima, o era objetivamente idónea para producir o produjo efectivamente dicho resultado (Altés Tárrega y Aradilla Marqués, 2023).

En el ciberacoso, estas características tradicionales tienden a desdibujarse aún más debido al medio digital en el que se producen las conductas, al igual que ocurre con otras dimensiones propias del acoso, como el elemento de poder, la reiteración de la conducta y la liquidez de las fronteras espaciotemporales. El daño no depende exclusivamente de la proximidad física ni de una relación vertical, sino que emerge de complejas dinámicas mediadas por la tecnología, como la difusión, viralización y permanencia de los contenidos en la red.

A su vez, el ciberacoso, como manifestación de violencia de carácter psicológico y/o sexual, puede producirse tanto dentro como fuera del lugar físico de trabajo y durante la jornada laboral o fuera de esta (Ramos Quintana, 2018). De esta manera, se genera incertidumbre y dificultad para determinar con claridad si los comportamientos están vinculados directamente con el ámbito laboral, lo que complica su identificación y la aplicación de las correspondientes medidas de prevención y protección.

Con todo, no resulta obstáculo para apreciar la existencia de un comportamiento constitutivo de ciberacoso que los hechos tengan lugar fuera de la jornada laboral y del espacio físico de la empresa o incluso con la intervención de terceros ajenos a la relación laboral. De igual modo, carece de relevancia que los dispositivos o medios tecnológicos utilizados sean de titularidad privada o que los contenidos transmitidos aludan a cuestiones de la esfera personal no directamente vinculadas con la actividad profesional, siempre y cuando las conductas desplegadas incidan de manera negativa en el desarrollo de la relación de trabajo; por ejemplo, creando un entorno de trabajo hostil o haciendo que la convivencia en el ámbito laboral se torne insostenible (Altés Tárrega y Aradilla Marqués, 2023).

El Convenio sobre la violencia y el acoso, 2019 (núm. 190), requiere mejorar la protección frente a tales prácticas en el mundo del trabajo, particularmente cuando son facilitadas por las TIC. De este modo, resulta oportuno sensibilizar sobre el ciberacoso como un riesgo psicosocial emergente y comprender el espacio virtual en el que estos actos tienen lugar, con el propósito de delimitarlos y aplicar estrategias preventivas orientadas a su erradicación.

Todas las empresas, con independencia de su tamaño, tienen la obligación legal de llevar a cabo una evaluación de los riesgos psicosociales que puedan afectar a su plantilla, así como articular protocolos eficaces frente al acoso moral, el acoso sexual y las distintas formas de discriminación en el ámbito laboral. Las entidades deben dar cauce a las denuncias o reclamaciones que puedan formular quienes hayan sido víctimas de ciberacoso. La prevención del acoso sexual y por razón de sexo es una de las materias que deben figurar en el diagnóstico del plan de igualdad y el procedimiento de actuación formará parte de su negociación.

La implantación de sistemas de teletrabajo no constituye, en modo alguno, una excepción a estas exigencias, sino que, por el contrario, plantea la necesidad de reforzar dichas medidas mediante la adaptación de los instrumentos preventivos a las particularidades propias del trabajo a distancia.

A este respecto, una de las medidas estrella de los convenios colectivos viene dada por la tipificación como infracción laboral de la utilización indebida de los dispositivos digitales, incluidas las redes sociales (Fernández Fernández, 2020). En el grado máximo, por su naturaleza especialmente ofensiva, se han calificado como infracciones muy graves el acoso sexual y moral realizado por cualquier medio, incluidos los telemáticos.

Paralelamente, el Protocolo para la prevención y actuación frente al acoso sexual, el acoso por razón de sexo y otras conductas contrarias a la libertad sexual y la integridad moral en el ámbito laboral indica que la Estrategia Estatal para combatir las violencias machistas 2022-2025 dispone que han de tenerse en cuenta tres dimensiones

de la violencia digital, a saber: el acoso en línea y facilitado por la tecnología, el acoso sexual en línea y la dimensión digital de la violencia psicológica.

El primero hace referencia a la amenaza sexual, económica, física o psicológica; el daño reputacional; el *spyware* (seguimiento y recopilación de información privada); la suplantación de identidad; la solicitud de sexo, y el acoso con cómplices para aislar a la trabajadora. El segundo alude a la amenaza o difusión no consentida de imágenes o vídeos; la toma, producción o captación no consentida de imágenes o vídeos íntimos; las prácticas de *sexting*, *sextorsión*, amenaza de violación, *doxing* (revelar la identidad o información personal de la afectada) y *outing* (desvelar la orientación sexual); el *bullying* sexualizado, y el *ciberflashing* (enviar imágenes sexuales no solicitadas). En tercer lugar, se incluyen los actos individuales no tipificados como delito que adquieren especial gravedad al combinarse con la mentalidad de masa y la repetición; los discursos de odio sexistas; la intimidación o amenaza a las víctimas o a su familia, los insultos, la vergüenza y la difamación; la incitación al suicidio o a la autolesión, y el abuso económico.

El terrible caso Iveco, en el que una trabajadora de la empresa se suicidó tras la difusión entre sus compañeros de un vídeo sexual, puso de relieve el gran impacto de este tipo de conductas. Lamentablemente, en la vía jurisdiccional penal se archivó la causa por falta de prueba de la autoría, mientras la ITSS entendió que era un asunto privado, no estrictamente laboral. La dificultad en estos casos radica en demostrar la existencia de la relación directa entre el suicidio y las condiciones laborales de la persona trabajadora (De la Casa Quesada, 2021).

La recomendación para una persona afectada por estas situaciones es activar el protocolo de acoso en contextos de teletrabajo de la empresa y utilizar la propia tecnología como herramienta de defensa. A diferencia del acoso presencial –en el que gran parte de las conductas se manifiestan de forma verbal, sin testigos ni registros tangibles–, en los entornos digitales asociados al trabajo a distancia las interacciones dejan huella (González, 2024). Correos electrónicos, mensajes a través de aplicaciones de mensajería instantánea como WhatsApp, órdenes transmitidas mediante intranet o sistemas corporativos, así como grabaciones de reuniones virtuales o videoconferencias, pueden constituir evidencias relevantes. Estas pruebas permiten acreditar la existencia de las conductas hostiles y son clave en eventuales denuncias ante la Inspección de Trabajo o en procesos judiciales.

6. La desconexión digital en tiempos de hiperconectividad y nomofobia

Dada la creciente dificultad para delimitar las fronteras entre el tiempo profesional y el ámbito privado, lo que genera riesgos psicosociales vinculados directamente con una gestión inadecuada de las TIC, resulta crucial garantizar la protección de la seguridad y la salud de las personas teletrabajadoras. Ello requiere el estricto cumplimiento de la normativa relativa a los tiempos máximos de trabajo y a los periodos mínimos de descanso, así como una adecuada organización de los recursos tecnológicos para la prestación laboral.

Las *apps* de registro telemático permiten a la empresa monitorizar de una manera ágil y sencilla el cómputo diario, semanal y mensual de cada persona trabajadora (Llorens Espada, 2022). Asimismo, la ITSS puede verificar la información relativa a las jornadas y descansos desde cualquier lugar, mientras el personal cuenta con un instrumento adecuado para comprobar los tiempos de trabajo realizados, que redunda en una mejor conciliación. Ahora bien, la empresa ha de conocer el marco legal y adoptar las debidas cautelas para evitar el menoscabo de los derechos y libertades de la mano de obra o el uso ilícito de datos personales.

Pues bien, la introducción de nuevas formas de trabajo más flexibles y tecnológicas permite el desarrollo de las tareas profesionales en cualquier momento y desde cualquier emplazamiento. La persona trabajadora se ve frecuentemente compelida a mantenerse en un estado de alerta constante, en un contexto en el que las fronteras entre el tiempo de trabajo y los espacios de ocio y descanso se tornan difusas. Si bien, en teoría, esta modalidad puede otorgar una mayor libertad, autonomía y capacidad de gestión sobre el propio horario, en la práctica conlleva el riesgo de normalizar la disponibilidad permanente.

En efecto, las comunicaciones con clientes, superiores y compañeros de trabajo a través de correos electrónicos, SMS, mensajes de WhatsApp u otras plataformas digitales se han integrado de manera habitual a la dinámica laboral cotidiana, lo que, en numerosos casos, implica la extensión

de la jornada ordinaria o, al menos, la ampliación de los tiempos de disponibilidad. Esta situación, lejos de demostrar un mayor compromiso con la organización, como se suele pensar, termina por volverse en contra de la persona trabajadora, al favorecer la sobrecarga y el agotamiento, que termina incidiendo en su desempeño.

No resulta extraño que, a falta de un uso adecuado de las nuevas tecnologías, aparezcan fenómenos como el *workaholism*, la tecnoadicción, la nomofobia o el fenómeno FOMO (CC. OO., 2020).

Para enfrentar el problema de la hiperconectividad, el legislador español reconoce el derecho de las personas trabajadoras a la desconexión digital, *ex* artículo 88 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. El precepto refleja que las modalidades de ejercicio de este derecho se sujetarán a lo establecido en la negociación colectiva o, en su defecto, a lo acordado entre la empresa y la representación legal de las personas trabajadoras, atendiendo a la naturaleza y objeto de la relación laboral y potenciado el derecho a la conciliación. El tercer epígrafe contempla las obligaciones en materia de prevención de riesgos y hace mención expresa al derecho a la desconexión digital en la modalidad del teletrabajo.

Las empresas tienen el deber, previa audiencia de los representantes de los trabajadores, de elaborar políticas internas dirigidas al personal, incluidos quienes ocupen puestos directivos, para el ejercicio del derecho a la desconexión. Además, quien proporciona empleo ha de realizar acciones de formación y sensibilización del personal sobre un uso razonable de las herramientas tecnológicas para evitar el riesgo de fatiga informática. La organización debe asumir una posición proactiva e incorporar todas las medidas técnicas y organizativas necesarias para dar cumplimiento efectivo a la desconexión digital.

La Ley 10/2021 afirma que quienes desarrollan su trabajo a distancia se beneficiarán de los mismos derechos aplicables a las personas comparables que desempeñan sus funciones de manera presencial. No obstante, determinadas condiciones laborales requieren una regulación particular para asegurar un nivel de protección equivalente al del trabajo presencial, como sucede con la organización del tiempo de trabajo, incluidas la flexibilidad horaria, los periodos de disponibilidad y el adecuado registro de la jornada laboral, así como la correcta aplicación de las medidas de seguridad y salud laboral. Ahora bien, esto no implica que el teletrabajo cuente con un régimen normativo diferenciado respecto al aplicable de manera general en materia de jornada, registro de la misma, horario o descansos (Rodríguez Santos, 2022).

El artículo 18 del texto legal reconoce una protección específica para quienes desempeñan su actividad a distancia, estableciendo que el deber empresarial de garantizar la desconexión digital permite limitar de manera razonable el uso de los medios tecnológicos.

Resulta oportuno traer a colación la jurisprudencia más relevante en la materia y, en primer lugar, la sentencia de la Audiencia Nacional de 6 de mayo de 2024, núm. 53/2024, que aborda la solicitud de un sindicato de declarar la nulidad de la política de desconexión digital adoptada por la empresa, alegando que no había sido objeto de negociación previa. La empresa había implementado un sistema de teletrabajo, previa consulta con la representación unitaria, pero sin negociación con la misma, incorporando de igual forma una política de desconexión digital. El fallo indica que no se puede compartir con la organización sindical actora que los acuerdos individuales de teletrabajo deban ser objeto de negociación colectiva.

La Sala de lo Social confirma la facultad de las compañías para elaborar y aprobar unilateralmente sus políticas de desconexión, siempre y cuando respeten el derecho de audiencia de la representación legal de las personas trabajadoras. De este modo, la LOPDGDD distingue entre la creación de políticas internas y la regulación del ejercicio de los derechos de desconexión digital. La regulación del ejercicio de tales derechos se encomienda a la negociación colectiva o al acuerdo de empresa, mientras la elaboración del protocolo es responsabilidad de la entidad, previa audiencia de la representación legal de la plantilla, y puede aprobarse unilateralmente.

Esta conclusión viene a matizar el criterio defendido en su sentencia de 22 de marzo de 2022, núm. 44/2022, en la que argumentaba que los límites al derecho a la desconexión digital en el teletrabajo no los podía establecer unilateralmente quien proporciona empleo. En aquel caso, estimó la nulidad de la excepción genérica de una política de desconexión que permitía la obligación de las personas trabajadoras de estar conectadas digitalmente

en «circunstancias de urgencia justificada» que pudieran suponer un perjuicio empresarial o del negocio.

En segundo lugar, el Tribunal Supremo, en su sentencia de 2 de abril de 2025, núm. 1514/2025, analiza unas previsiones contenidas en una cláusula del contrato tipo de trabajo a distancia redactado por la empresa al que se adhieren las personas trabajadoras. Precisamente en esa redacción se encuentra la política interna sobre el derecho a la desconexión digital. En el supuesto enjuiciado, esta política se ha realizado sin la audiencia previa a la representación legal de las personas trabajadoras. Cuando la nulidad de una cláusula contenida en un contrato tipo se declara por razones formales ajenas al fondo material, resulta evidente que dicho contenido podría incorporarse legítimamente tanto en el acuerdo como en los pactos individuales (Lousada Arochena, 2025). La nulidad de la cláusula relativa a la desconexión digital obedeció exclusivamente a la ausencia de negociación con la representación legal de las personas trabajadoras y, por consiguiente, de haber cumplido con dicha exigencia, el contenido habría resultado plenamente válido.

Tercero, en cuanto a la posibilidad de establecer límites a la desconexión digital, resulta esclarecedora la sentencia del Tribunal Superior de Justicia de Madrid de 17 de julio de 2023, núm. 453/2023. El pronunciamiento valida la práctica empresarial consistente en comunicar a las personas trabajadoras el inicio de su jornada o turno de trabajo durante el tiempo de descanso, cuando se cobra un plus de disponibilidad. Si el convenio colectivo o el contrato laboral contempla la remuneración de la disponibilidad fuera del horario laboral, el descanso puede quedar interrumpido y las personas trabajadoras deben tener encendidos sus dispositivos corporativos.

En el presente caso, no cabe apreciar la vulneración del derecho a la desconexión digital de quienes recibieron una comunicación durante su periodo de descanso y percibían un plus de disponibilidad, destinado precisamente a retribuir la eventualidad de que la prestación laboral pudiera iniciarse fuera del horario inicialmente programado, con un preaviso mínimo de doce horas.

Procede mencionar, además, que en el marco de la negociación colectiva se han de incluir cláusulas de desconexión digital para abordar el tecnoestrés y el incremento de enfermedades de carácter psicosocial derivadas del uso excesivo de las TIC en el trabajo. Algunas buenas prácticas detectadas en los convenios colectivos implican establecer la obligación de no enviar comunicaciones en lugar de no contestar; la imposibilidad técnica de recibir mensajes de trabajo una vez finalizada la jornada, y la retirada del dispositivo facilitado por la empresa o la desconexión automática de las herramientas digitales corporativas (Álvarez Cuesta, 2020).

Asimismo, se contemplan fórmulas como la fijación de «periodos de siesta digital», «toques de queda digitales» o la restricción del uso de los canales de comunicación en determinadas franjas horarias, permitiendo que el contacto con la persona trabajadora solo sea posible en intervalos específicos posteriores a la jornada laboral.

Aun cuando estos mecanismos podrían considerarse coherentes con los principios que sustentan la regulación preventiva –que imponen a la empresa la obligación de proteger a la persona trabajadora incluso frente a su propia imprudencia–, resulta recomendable priorizar estrategias de capacitación dirigidas al personal. De esta manera, se deben reservar las medidas más restrictivas únicamente para los casos en los que tales iniciativas resulten insuficientes o hayan fracasado (Igartua Miró, 2019). El teletrabajo merece un tratamiento específico, pues incluso si se pretendiera invocar el artículo 29 LPRL para fundamentar un deber de la persona teletrabajadora de respetar la desconexión, las facultades de quien proporciona empleo para exigir su cumplimiento efectivo resultan limitadas.

Conclusiones

A diferencia de cuanto ocurre con los hombres que teletrabajan, el análisis realizado en el presente estudio ha permitido colegir cómo sobre las mujeres persiste la expectativa social implícita de que integren de manera natural las tareas domésticas y el cuidado de los hijos, mayores y dependientes dentro de su jornada laboral en el hogar. En el imaginario colectivo, y desde una visión reduccionista profundamente marcada por los estereotipos de género, el teletrabajo suele ser presentado como la «panacea» para las mujeres, bajo el argumento de que esta modalidad facilitaría la conciliación (Giuzio y Cancela, 2021). Sin embargo, al conjugar en femenino las labores domésticas y de cuidado, se olvida, una vez más, que el

teletrabajo no constituye un alivio automático de la carga de trabajo, sino más bien una intensificación de la doble jornada –la laboral y la no remunerada–, así como una superposición de tiempos y espacios.

La experiencia del trabajo a distancia muestra que, en ciertas ocasiones, las expectativas de las mujeres en torno a la compatibilidad de la vida laboral y familiar no resultan satisfechas por las condiciones laborales que ofrece la empresa (Moreno Colom *et al*., 2023a), mientras los hombres han incrementado su autonomía en la prestación de sus servicios, aun cuando ello no responda necesariamente a sus necesidades reales de conciliación (Rodríguez Rodríguez, 2021). Las mujeres no conciben el ahorro de tiempo resultante del teletrabajo para ellas mismas, sino como un facilitador para atender las necesidades de cuidado de otras personas.

La doble presencia femenina exige acciones exógenas para remediar este problema y lograr la corresponsabilidad, por ejemplo: ampliar y mejorar las políticas de permisos de cuidado para hijos y personas dependientes, de manera que hombres y mujeres puedan utilizarlos de forma efectiva; inversión en servicios públicos que reduzcan la carga del trabajo no remunerado, como guarderías y centros de cuidado; fomentar la participación de los hombres en el ámbito familiar y doméstico; articular el seguimiento del teletrabajo mediante el plan de igualdad y de la comisión paritaria, o establecer indicadores específicos de diagnóstico, evaluación y vigilancia del teletrabajo corresponsable, tales como, entre otros, la distribución de mujeres y hombres en el acceso y uso de esta modalidad de prestación de servicios, así como su impacto en los procesos de promoción profesional y en la formación (Romero Pedraz y Varela Ferrio, 2024).

Igualmente, el teletrabajo podría reforzar la división sexual del trabajo en el mercado laboral y dentro del hogar, empeorar las condiciones laborales con jornadas más intensas en horarios atípicos y provocar problemas de salud (Moreno Colom *et al*., 2023b). A falta de políticas empresariales adecuadas, esta situación debe encontrar acomodo en la evaluación de los riesgos psicosociales.

A este respecto, la Ley 10/2021 trata de cohonestar, de un lado, la plena garantía de los derechos de las personas trabajadoras y la adecuada prevención y protección frente a los riesgos derivados del uso de medios informáticos en el teletrabajo y, de otro, los legítimos intereses empresariales en el control de la actividad laboral y en la gestión de los riesgos digitales que les son propios (Valverde Asencio, 2025).

Así, detectado el desgaste emocional de la teletrabajadora (signos de ansiedad, estrés o similares), quien proporciona empleo habrá de asumir la responsabilidad de articular las adaptaciones necesarias, permitiendo una transición entre teletrabajo y presencialidad, configurando un sistema de «vasos comunicantes» (Igartua Miró, 2021). En consecuencia, deberá establecer todas las medidas correctoras necesarias para evitar que se produzca un riesgo para la salud del personal. Por ello, tener protocolos claros, sencillos, ágiles y detallados para luchar contra las situaciones de estrés en la unidad productiva sin duda alguna coadyuvará a mejorar la salud mental de los empleados, ya desarrollen su quehacer productivo de manera presencial o a distancia.

Además, las diferencias por razón de género en el desarrollo de la actividad productiva mediante herramientas tecnológicas comportan que la exposición a los riesgos laborales sea desigual. Las consecuencias de la doble carga de trabajo y las peores condiciones laborales y de trabajo a las que, con frecuencia, están sometidas las mujeres hacen que su estado de salud sea peor. Los factores de riesgo ergonómicos a los que están expuestas muchas teletrabajadoras se ven potenciados por el inadecuado diseño de los puestos de trabajo a sus características antropométricas. Para mitigar este problema, se recomienda basar el diseño de equipos y puestos de trabajo en mediciones representativas, considerando las diferencias corporales entre mujeres y hombres, y realizar evaluaciones ergonómicas periódicas.

En este sentido, la ergonomía de género procura integrar las diferencias físicas, fisiológicas y psicosociales de hombres y mujeres a fin de diseñar entornos laborales inclusivos y seguros. Un elemento clave de este enfoque es la disponibilidad de datos e indicadores desagregados por sexo o género. La recopilación y el análisis de estos datos permiten identificar patrones diferenciados de riesgo laboral para una posterior adaptación de los puestos de trabajo. La implementación de sistemas de monitoreo que registren variables como las posturas o las incidencias según el género, junto con el desarrollo de interfaces y dispositivos con criterios de diseño inclusivo, fortalece

significativamente la prevención. Procede recordar que la normativa en materia de prevención de riesgos establece que el trabajo debe adaptarse a la persona, no al revés.

Por tanto, las necesidades de estas mujeres deben ser incluidas en las evaluaciones de riesgos, incorporando la perspectiva de género de forma transversal en las actuaciones preventivas empresariales y asegurando la formación de todos los niveles jerárquicos para su efectiva implementación.

Dicho principio de transversalidad de género se ha incorporado al ámbito de la salud laboral, en virtud de lo dispuesto en el artículo 27 y en la disposición adicional duodécima de la Ley Orgánica 3/2007. A la par, bajo el amparo del artículo 8.3 de la Ley 10/2021, la determinación de las condiciones de acceso y retorno al trabajo presencial queda supeditada a una obligatoria consideración de la perspectiva de género, vinculando así la autonomía colectiva con el objetivo de neutralizar las desigualdades estructurales en el entorno digital. En cualquier caso, la integración de la perspectiva de género en la prevención de riesgos laborales debe ajustarse a la naturaleza de la actividad desarrollada, lo que exige un conocimiento exhaustivo de la legislación y de la normativa técnica aplicable.

Sin duda, las medidas preventivas deben ir encaminadas a reducir la exposición a los diferentes tipos de factores de riesgo, adaptar el puesto de trabajo a cada persona y realizar una correcta organización de las tareas, tomando en consideración las particulares del teletrabajo.

Ahora bien, la mención a los riesgos surgidos de la digitalización de las relaciones laborales –riesgos psicosociales, ergonómicos y organizativos– en el artículo 16 de la Ley 10/2021 resulta positiva, pero insuficiente al no prever posibles mecanismos dirigidos efectivamente a evitar su aparición. Aun cuando algunos están recogidos en otros preceptos del texto legal –por ejemplo, el derecho a la desconexión digital o la dotación de medios–, tampoco permiten superar los desafíos (López Vico, 2025).

A la hora de diseñar los objetivos y el contenido de la vigilancia de la salud, se han de tener en cuenta las exposiciones mayoritarias en las mujeres, las diferencias biológicas y las desigualdades sociales, poniendo énfasis en las enfermedades relacionadas o agravadas por el trabajo a distancia.

En paralelo, no obstante, la prolongación de la jornada laboral más allá de los límites pactados, a resultas de las tendencias propias de la revolución tecnológica, reaviva el debate en torno a la ordenación del tiempo de trabajo y a cómo evitar que las TIC continúen propiciando un aumento de los tiempos de trabajo (Martínez Barroso, 2025). En este escenario, las medidas empresariales para garantizar el derecho a la desconexión digital pueden concretarse en la implantación de sistemas de alerta o bloqueo automático de los dispositivos tecnológicos puestos a disposición de las personas trabajadoras cuando se exceda el tiempo de trabajo o en la adopción de algoritmos que impidan de manera automática la comunicación con los trabajadores cuando se encuentren en sus periodos de descanso, ya sea diario, semanal o anual. Así, se evita trasladar a la persona trabajadora la difícil decisión sobre si atender o no a un cliente en dichos momentos de asueto. Urge la consolidación de una cultura corporativa orientada a promover un uso responsable de las tecnologías, tanto en las relaciones profesionales como en las personales.

Lógicamente, el contenido de las políticas internas de desconexión digital debe adecuarse a las exigencias normativas y a las pautas ofrecidas por la doctrina judicial. En el marco de su revisión y actualización, resulta esencial precisar aspectos como las modalidades concretas de ejercicio del derecho a la desconexión, la delimitación de lo que debe entenderse por un uso razonable de las herramientas tecnológicas, así como la identificación de aquellas circunstancias que puedan permitir limitar o modular dicho derecho.

Por último, las empresas tienen la obligación de considerar las particularidades propias del teletrabajo en el momento de diseñar e implementar las medidas de prevención y actuación frente al acoso. Si bien las características específicas del trabajo remoto han de mover a establecer una protección reforzada frente al ciberacoso, en la práctica, los convenios colectivos no suelen ofrecer un tratamiento amplio y detallado sobre esta cuestión. En algunos supuestos minoritarios se ha optado por incorporar una regulación más amplia del ciberacoso, incluyendo una definición precisa y la delimitación de las conductas constitutivas. Dichas cláusulas suelen ir acompañadas de la adopción de un compromiso de «tolerancia cero», de la atención diferenciada a la situación de las personas teletrabajadoras y de la previsión de que los casos detectados se tramiten mediante el procedimiento para el acoso laboral (Agra Viforcos, 2025).

De hecho, en opinión de quien suscribe, utilizadas de manera adecuada, las TIC permiten una mayor difusión y accesibilidad de los protocolos internos frente al ciberacoso, simplifican la implantación de canales de denuncia confidenciales y eficaces y contribuyen a garantizar la trazabilidad y el seguimiento de las actuaciones emprendidas. La digitalización del trabajo, por tanto, abre una ventana ambivalente: si bien facilita nuevas modalidades de acoso, también provee a las víctimas de instrumentos de registro que pueden fortalecer su protección jurídica y laboral.

Referencias bibliográficas

AGRA VIFORCOS, B. (2025). «Perspectiva de género en el trabajo a distancia». En: ÁLVAREZ CUESTA, H. (dir.). *Digitalización y teletrabajo en la negociación colectiva: resumen ejecutivo*, págs. 183-188. Madrid: Ministerio de Trabajo y Economía Social.

ALTÉS TÁRREGA, J.; ARADILLA MARQUÉS, M.ª J. (2023). «Teletrabajo, violencia y acoso y Convenio 190 OIT». *Temas Laborales*, n.º 166, págs. 65-91.

ÁLVAREZ CUESTA, H. (2020). «Del recurso al teletrabajo como medida de emergencia al futuro del trabajo a distancia». *Lan Harremanak*, n.º 43, págs. 175-201. DOI: https://doi.org/10.1387/lan-harremanak.21722

ÁLVAREZ CUESTA, H. (2023). «El impacto de la tecnología en las relaciones laborales: retos presentes y desafíos futuros». *Revista Justicia & Trabajo*, n.º 2, págs. 39-59. DOI: https://doi.org/10.69592/2952-1955-N2-JUNIO-2023-ART-2

CC. OO. (2020). *El teletrabajo desde la perspectiva de género y salud laboral*. 2ª. ed. Madrid: Secretaría de Salud Laboral y Secretaría de las Mujeres de la Federación de Servicios a la Ciudadanía de CCOO.

DE LA CASA QUESADA, S. (2021). «Teletrabajo, género, riesgos psicosociales: una tríada a integrar en las políticas preventivas 4.0.». *Revista de Trabajo y Seguridad Social. CEF*, n.º 459, págs. 83-112. DOI: https://doi.org/10.51302/rtss.2021.2412

de la PUEBLA PINILLA, A. (2020). «Trabajo a distancia y teletrabajo: una perspectiva de género». *Labos*, vol. 1, págs. 4-11. DOI: https://doi.org/10.20318/labos.2020.5547

FERNÁNDEZ FERNÁNDEZ, R. (2020). *Redes sociales y Derecho del Trabajo. El lento tránsito desde la indiferencia legislativa a la necesaria regulación legal o convencional*. 1.ª ed. Navarra: Thomson Reuters Aranzadi.

FERRERAS REMESAL, A. (2019). «Ergonomía y género. Criterios de evaluación y recomendaciones». *Instituto de biomecánica de Valencia* [en línea]. Disponible en: https://goo.su/Nf02EvR.

GALA DURÁN, C. (2025). «El impacto del teletrabajo en la conciliación de la vida laboral y familiar: ¿avance u obstáculo?» En: SÁNCHEZ HUETE, M.A. (dir.). *Conectadas y desiguales: la brecha de género en la era digital,* págs. 101-121. Madrid: Reus.

GIRALDO RESTREPO, Y. (2023). «El impacto de la tecnología en los derechos laborales de las mujeres: desafíos y oportunidades». *Estudios Latinoamericanos de Relaciones Laborales y Protección Social*, n.º 16, págs. 73-85. DOI: https://doi.org/10.69592/2952-1955-N2-JUNIO-2023-ART-2

GIUZIO, G.; CANCELA. M. (2021). «Teletrabajo e inequidades de género». *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, vol. 9, págs. 410-426.

GONZÁLEZ, B. (2024). «Acoso laboral en el teletrabajo, el nuevo *mobbing*». *Universitat Oberta de Catalunya* [en línea]. Disponible en: https://goo.su/6UaQPPH.

GONZÁLEZ-MENÉNDEZ, E. *et al*. (2019). «Principales consecuencias para la salud derivadas del uso continuado de nuevos dispositivos electrónicos con PVD». *Revista española de salud pública*, n.º 93, págs. 1-11.

HERRERA, J. (2021). «El impacto del teletrabajo en el entorno laboral y familiar y los efectos en el trabajador». *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, vol. 9, págs. 250-271.

IGARTUA MIRÓ, M.ª T. (2019). «El derecho a la desconexión en la Ley orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales». *Revista de Trabajo y Seguridad Social, CEF*, n.º 432, págs. 61-87. DOI: https://doi.org/10.51302/rtss.2019.1350

IGARTUA MIRÓ, Mª.T. (2021). «Teletrabajo y riesgos psicosociales: la imperiosa necesidad de reforzar la tutela preventiva». *Trabajo, Persona, Derecho, Mercado: Revista de Estudios sobre Ciencias del Trabajo y Protección Social*, n.º 3, págs. 175-212. DOI: https://doi.org/10.12795/TPDM.2021.i3.10

LLORENS ESPADA, J. (2022). «Aplicaciones informáticas (*app*) para el registro diario de la jornada laboral. Condiciones de licitud». *Labos*, vol. 3, págs. 70-94. DOI: https://doi.org/10.20318/labos.2022.6853

LÓPEZ VICO, S. (2025): «Desafíos en la prevención de riesgos laborales en el teletrabajo: una reflexión crítica». *Revista de Derecho de la Seguridad Social, Laborum*, n.º 42, págs. 117-138.

LOUSADA AROCHENA, J.F. (2025). «¿Qué se puede poner, y qué no, en un acuerdo de teletrabajo?». *Revista de Jurisprudencia Laboral*, n.º 4, págs. 1-9. DOI: https://doi.org/10.55104/RJL_00637

MARTÍNEZ BARROSO, M.ª R. (2025). «Flexibilidad horaria y registro horario en entornos digitales». En: ÁLVAREZ CUESTA, H. (dir.). *Digitalización y teletrabajo en la negociación colectiva: resumen ejecutivo,* págs. 63-70. Madrid: Ministerio de Trabajo y Economía Social.

MELIÁN CHINEA, L. M.ª (2022). «Teletrabajo y negociación colectiva: una perspectiva de género». *Revista Derecho Social y Empresa*, n.º 16, págs. 87-109. DOI: https://doi.org/10.18172/redsye.6232

MONTES ADALID, G. M.ª (2023). «Empleo digital, conciliación y salud psicosocial de la mujer trabajadora». *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, vol. 11, págs. 186-213.

MORENO COLOM, S. *et al*. (2023a). «Desmontando el mito del teletrabajo desde la perspectiva de género: experiencias y expectativas durante la pandemia». *Cuadernos de Relaciones Laborales*, vol. 41, págs. 95-117. DOI: https://doi.org/10.5209/crla.80979

MORENO COLOM, S. *et al*. (2023b). «La experiencia del trabajo a distancia durante el confinamiento en Cataluña: una aproximación desde la perspectiva de género». *Revista Española de Investigaciones Sociológicas*, n.º 183, págs. 77-100. DOI: https://doi.org/10.5477/cis/reis.183.77

RAMOS QUINTANA, M.I. (2018). «Enfrentar la violencia y el acoso en el mundo del trabajo: la discusión normativa de la OIT». *Revista del Ministerio de Trabajo, Migraciones y Seguridad Social*, n.º 138, págs. 91-114.

RODRÍGUEZ RODRÍGUEZ, E. (2021). «De la conciliación a la corresponsabilidad en el tiempo de trabajo: un cambio de paradigma imprescindible para conseguir el trabajo decente». *Lex Social: Revista de Derechos Sociales*, vol. 11, págs. 40-78. DOI: https://doi.org/10.46661/lexsocial.5470

RODRÍGUEZ SANTOS, E. (2022). «Revisión de los conceptos de tiempo de trabajo y de descanso: el tiempo de disponibilidad en los tradicionales y en los nuevos escenarios laborales». En: Barcelón Cobedo, S.; Carrero Domínguez, C. y de Soto Rioja, S. (coords.). *Estudios de Derecho del Trabajo y de la Seguridad Social: homenaje al profesor Santiago González Ortega,* págs. 241-254. Sevilla: Consejo Andaluz de Relaciones Laborales.

ROMERO PEDRAZ, S.; VARELA FERRIO, J. (2024). «Teletrabajo y corresponsabilidad». *Estudios UGT* [en línea]. Disponible en: https://n9.cl/5vq63.

VALVERDE ASENCIO, A.J. (2025). «Implantación de nuevos Sistemas Tecnológicos y Derechos digitales. Guía de recomendaciones y buenas prácticas para la negociación colectiva andaluza». *Consejo Andaluz de Relaciones Laborales* [en línea]. Disponible en: https://n9.cl/kmio5.

Cita recomendada

CASTRO FRANCO, Ana María (2026). «Teletrabajo y su afectación a los derechos de las personas trabajadoras desde una perspectiva de género». En: Irene Rovira Ferrer (coord.). «Sobre la consolidación del trabajo a distancia». *IDP. Revista de Internet, Derecho y Política*, núm. 44. UOC [Fecha de consulta: dd/mm/aa]. DOI: http://dx.doi.org/10.7238/idp.v0i44.9800396

Sobre el autor

Ana María Castro Franco
Universidad de León
acasf@unileon.es

Profesora Ayudante Doctora en Derecho del Trabajo y de la Seguridad Social en la Universidad de León (España). Acreditada como Profesora Contratada Doctora por la ANECA.

Graduada en Derecho por la Universidad de León, con Máster Universitario en Abogacía. Doctora con calificación de sobresaliente *cum laude* por la tesis titulada «La reordenación del despido colectivo: entre las directrices europeas y el contexto de la industria 4.0».

Tal itinerario formativo se ha visto completado con el Curso Superior en Ciberseguridad (Universidad de Deusto), el Programa Executive en Ciberseguridad, Riesgos y Seguridad Digital (Centro de Estudios Garrigues), el Curso Experto en Derecho de Inteligencia Artificial (Aranzadi) y el Curso Experto en Derecho Concursal-Laboral (Tirant lo Blanch).

IDP
REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Algoritmos en el proceso civil: oportunidad de modernización o riesgo de desnaturalización. Creación de un algoritmo para la identificación de cláusulas abusivas

Federico Adan Domènech
Universidad Rovira i Virgili

Fecha de presentación: septiembre 2025
Fecha de aceptación: octubre 2025
Fecha de publicación: diciembre 2025

Resumen

El estudio examina el potencial de la inteligencia artificial, en adelante IA, en el proceso civil, destacando su valor como instrumento de apoyo judicial y no como sustituto de la decisión humana. Se analiza un modelo algorítmico capaz de identificar cláusulas abusivas en contratos mediante módulos. Esta propuesta pretende reducir dilaciones, homogeneizar criterios y aportar mayor seguridad jurídica. No obstante, se advierte sobre limitaciones estructurales: la motivación judicial no puede circunscribirse a la información algorítmica; la inmediación procesal debe garantizarse; y el principio dispositivo restringe la actuación *ultra petita*. El trabajo subraya la necesidad de expedientes electrónicos completos, protocolos de indexación y mecanismos de transparencia en el acceso a metadatos y racionales. Finalmente, se propone considerar el dictamen algorítmico como prueba documental sometida a contradicción, favoreciendo la celeridad y la economía procesal.

Palabras clave

algoritmo; juez; cláusula abusiva; inteligencia artificial

Algorithms in the civil process: opportunity for modernization or risk of denaturalization. Creating an algorithm for the identification of abusive clauses

Abstract

The study explores the potential of artificial intelligence, hereafter referred to as AI, in civil proceedings, emphasising its role as a tool for judicial support rather than a replacement for human decision-making. An algorithmic model designed to identify abusive clauses in contracts using modules is analysed. This proposal aims to reduce delays, standardize criteria, and enhance legal certainty. However, certain structural limitations are noted: judicial reasoning cannot rely solely on algorithmic information; procedural immediacy must be maintained; and the applied principle limits ultra petita *actions. The work highlights the importance of complete electronic records, indexing protocols, and transparency mechanisms for accessing metadata and reasoning. Finally, it is suggested that algorithmic judgments be regarded as documentary evidence subject to challenge, promoting procedural speed and efficiency.*

Keywords

algorithm; judge; abusive clause; artificial intelligence

Introducción

La denuncia de las cláusulas abusivas en contratos de consumo constituye uno de los principales ámbitos de litigiosidad en el ordenamiento jurídico tanto español como europeo en las últimas décadas.[1] Desde la crisis hipotecaria, se ha producido una proliferación de procedimientos judiciales relacionados con las condiciones generales de la contratación que generan un desequilibrio en perjuicio del consumidor, contraviniendo la Directiva 93/13/CEE y el Texto refundido Ley General Defensa Consumidores y Usuarios, en adelante, TRLGDCyU.[2] Expedientes que han puesto de manifiesto la dificultad de los órganos judiciales para dar respuesta rápida a un volumen masivo de litigios de naturaleza similar.

En este contexto, la IA y las técnicas de procesamiento de lenguaje natural, se presentan como alternativa para el análisis de cláusulas abusivas en contratos. A diferencia de los métodos tradicionales de revisión documental, lentos y costosos, los sistemas de IA permiten identificar patrones lingüísticos y semánticos con una capacidad de procesamiento masivo en tiempo reducido (Calero, 2024, pág. 184).

La relevancia del estudio se sostiene en la urgencia de reducir la sobrecarga judicial derivada de litigios masivos sobre cláusulas abusivas; y, en la necesidad de garantizar que la introducción de tecnologías de IA se realice bajo criterios de respeto de los derechos fundamentales y de los principios del proceso. El resultado esperado es avanzar hacia un modelo en el que la IA se configure como un instrumento de apoyo, optimizando los recursos judiciales sin menoscabar la función interpretativa que corresponde a los jueces (Velasco, 2024, pág. 175).

1. Escenario idóneo: digitalización del proceso y foliado de la documentación

La irrupción de la IA en el ámbito jurídico constituye uno de los fenómenos de mayor trascendencia en el derecho

1. Hecho que se erigió como motivo de la creación de Juzgados especializados. Acuerdo de 25/5/17 de la Comisión Permanente del CGPJ. BOE (27/5/17) pág. 2172.
2. La CE, en su artículo 51.1, configura *la protección de los legítimos intereses económicos y sociales de los consumidores en un principio esencial del ordenamiento jurídico* STS 22/4/15, Id Cendoj: 28079119912015100021.

procesal. Mientras que la digitalización de la justicia ha avanzado en las últimas décadas en aspectos instrumentales, como el expediente judicial electrónico[3] o la celebración de vistas telemáticas,[4] la introducción de algoritmos capaces de aprender de datos para asistir en la toma de decisiones abre un horizonte nuevo.

Hoy, el proceso no se limita a digitalizar documentos en formato imagen, sino que se articula sobre un expediente electrónico dinámico, compuesto por documentos digitales o copias auténticas electrónicas, dotados de metadatos, firma y sellado temporal. En este contexto, el foliado e indexado obligatorio de escritos y anexos deja de ser un requisito burocrático para transformarse en una oportunidad que permite a un algoritmo procesar y clasificar la información.

En este marco, el procurador debe garantizar que la presentación electrónica sea íntegra, que los documentos estén correctamente foliados e indexados, que sean legibles y que la versión aportada corresponda al contrato formalizado. Estas obligaciones se convierten en condición necesaria para que las herramientas de *legaltech* puedan operar, pues si el expediente está completo y ordenado, el algoritmo detectará con fiabilidad zonas de riesgo, cláusulas limitativas de responsabilidad, modificaciones unilaterales, etc., si, por el contrario, llega incompleto o caótico, ningún sistema podrá suplir esa carencia.

2. Paso previo: la creación de algoritmo

La posibilidad de crear un algoritmo capaz de detectar cláusulas abusivas en contratos no es una quimera tecnológica, es una hipótesis de trabajo ya respaldada por pruebas en otros ordenamientos.[5] La cuestión relevante no es tanto si puede hacerse, que sí se puede (Luna, 2022, págs. 243 y 246), sino cómo debe hacerse para que la herramienta sea útil en la práctica forense. De forma resumida y poco técnica, explicaremos el proceso de creación de un algoritmo que cumpla la finalidad de identificar «parámetros» en los contratos.[6]

El diseño del algoritmo para identificar cláusulas abusivas en contratos comienza con la recopilación de un *corpus* de documentos contractuales analizados por jueces, asociaciones de consumo u organismos reguladores, pues los mismos se erigen como ejemplo de actuación. Es decir, contratos donde se haya declarado expresamente qué disposiciones fueron consideradas abusivas y cuáles no. Esa etapa es crucial, porque el algoritmo no puede «inventar» qué es abusivo, necesita aprenderlo de la práctica jurídica consolidada (Fernández, 2023, págs. 239-240).

La siguiente fase consiste en convertir el lenguaje jurídico, denso y complejo, en datos que un modelo pueda procesar. La información contenida en los contratos se organiza en patrones que permiten al sistema informático identificar y extraer los datos pertinentes. Así, el algoritmo debería poder reconocer que, expresiones como «renuncia anticipada a acciones legales» o «limitación absoluta de responsabilidad» apuntan a un tipo de restricción, esto es, construye una taxonomía (Solar, 2018, pág. 83).

A continuación, se inicia la fase de entrenamiento, el algoritmo se expone a ejemplos de cláusulas ya clasificadas como abusivas o válidas. El sistema aprende de patrones, detecta términos recurrentes, estructuras sintácticas y combinaciones de conceptos que coinciden con abusos contractuales (Rivero, 2024, pág. 4), correlacionando los contratos con la jurisprudencia y normativa introducida (Franco, 2023, pág. 14). Para que sea aplicable en la labor de jueces y abogados, debe incorporar también un marco explicativo, debe mostrar por qué, esto es, cuáles son los elementos que la hacen potencialmente abusiva (Berenguer, 2024, pág. 113).

3. El punto de partida de la regulación del expediente electrónico fue la Ley 18/2011, de 5 de julio *BOE* (6/7/11), pág. 71320. La consolidación definitiva llegó con el Real decreto ley 6/2023, de 19 de diciembre, BOE (20/12/23), pág. 167808 que, impulsa un modelo de justicia digital.
4. La Ley 18/2011, de 5 de julio, BOE (6/7/11), pág. 71320, anticipó el uso de medios electrónicos sin una regulación específica de las vistas a distancia. El impulso normativo se produjo con el Real decreto ley 16/2020, de 28 de abril, *BOE* (29/4/20), pág. 30623, dictado en el contexto de la pandemia de la COVID-19. La medida excepcional ha pasado a consolidarse con carácter estructural en el Real Decreto-ley 6/2023, de 19 de diciembre, BOE (20/11/23), pág. 167808.
5. Por ejemplo, el predictive coding, desarrollado en el derecho anglosajón en el marco del *e-discovery*. DE LUCCHI, Y. (2023). «Eficiencia en el acceso a la información y fuentes de prueba en el proceso civil: tibias líneas convergentes EE. UU./Europa». *Revista Ítalo-Española de Derecho Procesal*, n.º 1, págs. 29-40.
6. Define algoritmo, De La Sierra, S. (2021). «¿Cuál es el papel hoy de la inteligencia artificial y los algoritmos en el sector público? Control judicial de los algoritmos: robots, administración y estado de derecho». *El Derecho.Com.* [Fecha de consulta: 1 de septiembre de 2025].

Con posterioridad, se procede a la etapa de prueba en casos reales. Se somete a contratos nuevos, y se evalúa su rendimiento. Aquí se mide no solo la precisión, sino también la tasa de falsos positivos, porque en justicia un error de exceso, marcar como abusiva una cláusula válida, puede ser tan problemático como no detectar un verdadero abuso. El algoritmo nunca se concibe como definitivo, el derecho evoluciona, los contratos cambian de redacción y las prácticas de mercado se transforman (Pacheco, 2024, págs. 140-171). El sistema debe actualizarse con nuevas resoluciones judiciales, nuevas leyes y ejemplos de contratos recientes.

Introducida la correspondiente información y parámetros, podremos establecer las preguntas que deben ser objeto de identificación por el algoritmo. El sistema operativo no funciona como una lista rígida de casillas a marcar, sino como una secuencia de módulos que se van activando según el tipo de problema jurídico que se plantea. Todo comienza en el módulo de entrada, donde el contrato se transforma en un conjunto de datos estructurados: fecha de firma, tipo de producto, cláusulas relevantes, y cualquier otro elemento contextual, pero a partir de este se pueden crear módulos específicos. Veamos ejemplos.

a) Ejemplo temporal: podemos demandar al algoritmo que identifique el cumplimiento de los presupuestos de transparencia, y para ello habremos de haber informado de los textos legales vigentes en cada momento histórico. Una vez hecho, entra en acción el módulo de contextualización temporal. El sistema vincula la fecha del contrato con el marco normativo vigente en ese momento. El sistema consulta una base de datos de leyes y jurisprudencia clasificadas por fecha. En definitiva, el módulo actúa como un instrumento de contextualización histórica que garantiza que el análisis de cada cláusula se ajuste a su marco jurídico originario.

Ejemplo 1: contrato firmado en 2016, antes de la entrada en vigor de la Ley 5/2019, de 15 de marzo,

- En las condiciones generales se identifica una cláusula que permite al banco dar por vencido anticipadamente el préstamo por el impago de una cuota.
- El sistema activa el módulo de contextualización temporal y se sitúa en el marco normativo de aquel año.
- Consulta la jurisprudencia vigente: el TS ya había empezado a declarar abusivas las cláusulas que permitían la ejecución por impagos mínimos.
- El algoritmo marca la cláusula como sospechosa de abusividad: un solo retraso en el pago no puede justificar la pérdida de la vivienda.[7]
- En su informe, se cita la doctrina jurisprudencial previa al 2019 que apuntaba a esta calificación.

Ejemplo 2: contrato firmado en 2020, después de la entrada en vigor de la Ley 5/2019, de 15 de marzo,

- En el clausulado se detecta cláusula de vencimiento anticipado que prevé la posibilidad de ejecución si el prestatario incumple el pago de doce mensualidades o bien quince mensualidades en la segunda mitad.
- El sistema se ubica en su línea de tiempo normativa y reconoce que en 2020 ya estaba en vigor la Ley 5/2019.
- Esa norma estableció parámetros concretos para que las cláusulas de vencimiento anticipado pudieran ser válidas. El algoritmo comprueba la redacción y constata que reproduce literalmente la Ley de Contratos de Crédito Inmobiliario, en adelante LCCI.
- En consecuencia, marca la cláusula como ajustada al marco normativo, sin activar alerta de abusividad.[8]

b) Ejemplo económico: el algoritmo debe activar el módulo de comparación económica, destinado a verificar la conformidad de determinados parámetros cuantitativos, tipos de interés u otros porcentajes, con los estándares de mercado y con los criterios establecidos por la jurisprudencia y normativa en materia de usura.

Este módulo opera mediante la conexión con parámetros oficiales del Banco de España. A partir de dichos datos se establecen criterios de normalidad estadística para el producto financiero correspondiente y en el momento

7. SSTS 18/2/16, Id Cendoj: 28079110012016100087, 23/12/15, Id Cendoj: 28079119912015100044, y STJUE 14/3/13, C 415/11.
8. STS 3/2/25, Id Cendoj: 28079110012025100202.

temporal concreto de suscripción del contrato. El valor consignado en la cláusula se contrasta con este patrón de referencia. Ante una tarjeta *revolving* con un interés remuneratorio del 27 % TAE, el sistema no se limita a identificar el dato numérico, sino que calcula la diferencia respecto de la media de mercado registrada ese año para operaciones análogas.

Ejemplo 1: contrato de tarjeta *revolving* firmado en 2018 con un TAE del 27 %

- El sistema recibe las condiciones generales de la tarjeta contratada. Entre las estipulaciones detecta el tipo de interés remuneratorio: un 27 % TAE.
- El sistema activa el módulo de comparación económica. El algoritmo localiza la fecha de contratación, y accede a las series históricas del Banco de España correspondientes a ese año. Se comprueba que la media de intereses aplicados en tarjetas *revolving* se situaba en torno al 20 % TAE.
- Se calcula la desviación: el 27 % supera en 7 puntos porcentuales la media del mercado. El sistema consulta la jurisprudencia aplicable en la época, que establecía que la diferencia sustancial respecto a los tipos medios podía constituir usura.[9]
- El sistema emite una alerta de riesgo de usura.

Ejemplo 2: contrato de tarjeta *revolving* firmado en los años 90 con un TAE del 27 %

- El sistema recibe las condiciones generales de una tarjeta contratada en 1995. Entre las estipulaciones identifica el tipo de interés remuneratorio: 27 % TAE.
- Se activa el módulo de comparación económica. El algoritmo reconoce la fecha de contratación y consulta los índices oficiales del Banco de España de ese año. En su base de datos localiza que la media de intereses aplicados en tarjetas *revolving* se situaba en torno al 24 % TAE.
- Con esos datos calcula la desviación: el 27 % supera en 3 puntos porcentuales la media de mercado. El sistema consulta la jurisprudencia aplicable en aquel momento y constata que, aunque ya existía la Ley de Represión de la Usura, la doctrina del TS todavía no había fijado criterios tan estrictos sobre lo que constituye un «interés notablemente superior al normal del dinero» en el ámbito del crédito al consumo.
- El sistema genera alarma con un nivel de riesgo reducido, y recomienda la revisión judicial teniendo en el contexto económico e histórico.[10]

3. La actuación de las partes como condicionante del éxito del algoritmo

3.1. Obligación de aportar prueba documental

El control de cláusulas abusivas, judicial o asistido por tecnología, solo es posible cuando se aporta la documentación contractual completa, que constituye la base del proceso. Así, la actuación de las partes en el proceso puede condicionar la eficacia de la implementación del algoritmo. La omisión de la aportación documental restringe tanto la eficacia procesal como la modernización tecnológica de la justicia. La Ley de Enjuiciamiento Civil, en adelante LEC regula diversos momentos para la aportación documental.

En primer lugar, la LEC, en su regla 265.1, obliga a las partes a acompañar la documentación en que funden sus pretensiones en sus escritos iniciales. De este modo, la obligación de acompañar los documentos relevantes con la demanda o la contestación no es un formalismo, sino una garantía de transparencia y lealtad procesal, que permite al juez y a la contraparte conocer desde el inicio la base jurídica y fáctica de la controversia.[11] En segundo lugar, el texto procesal contempla, en el artículo 270, situaciones en las que la parte actora no dispone materialmente de los documentos en el momento de interponer

9. STS 25/11/15, Id Cendoj: 28079119912015100038.
10. S 18/6/12, Id Cendoj: 28079110012012100507.
11. SAP Tarragona, 3.ª, 11/11/21, Id Cendoj: 43148370032021100521 y SAP Alicante, 4/2/25, Id Cendoj: 03014370052025100035 y PICÓ, J. (2013). *El principio de la buena fe procesal*, 2.ª ed., Barcelona: J. M. Bosch, págs. 182-183.

la demanda. En estos supuestos, se permite a las partes aportarlos después de la demanda o contestación, siempre que se justifique que no le fue posible acompañarlos antes, ya sea por causas no imputables a ellas o porque el documento no estaba en su poder.[12]

La aportación íntegra de los contratos garantiza no solo el derecho de defensa de las partes, sino también la efectividad de la tutela judicial reconocida en el artículo 24 Constitución Española, en adelante CE, al permitir al juez, y, en su caso, a herramientas tecnológicas de apoyo, realizar un examen completo y contextualizado de las cláusulas. El incumplimiento de este deber contravendría las reglas de la buena fe reguladas en los artículos 11 Ley Orgánica Poder Judicial, en adelante LOPJ y 247.1 LEC, estableciéndose en la Ley procesal dos efectos ante la actuación maliciosa de una de las partes. El primero de carácter económico, y el segundo de consecuencias de naturaleza jurídica.[13]

En el plano económico, la norma 247.3 LEC faculta a los tribunales a imponer multas pecuniarias a quienes litigan con mala fe o temeridad (Picó, 2013, pág. 182). La ocultación deliberada de un contrato, o el retraso injustificado en su aportación, se ajustan a ese supuesto. Esta medida tiene una doble finalidad, en primer lugar, disuasoria, al prevenir conductas dilatorias y, en segundo lugar, sancionadora, castigando pecuniariamente la deslealtad procesal.

El régimen sancionador del artículo 247.3 LEC plantea un problema en la práctica, la falta de concreción del montante de la multa, el legislador fija reglas de concreción que oscilan entre 180 y 6.000 euros, con el límite de no superar la tercera parte de la cuantía del litigio. La aplicación de la multa queda en manos de la discrecionalidad judicial. La ley ofrece parámetros orientativos, gravedad del hecho, perjuicios causados, capacidad económica del infractor y reiteración, pero no fórmulas de ponderación ni criterios de aplicación. Esta indeterminación puede tener un valor positivo, pues otorga al juez flexibilidad para adaptarse al caso concreto, pero también genera un riesgo, la falta de uniformidad judicial. Así, la gravedad de la conducta debe analizarse en relación con su potencial para alterar el equilibrio procesal; los perjuicios han de medirse no solo en términos económicos, sino también en términos de tiempo procesal y desgaste de recursos públicos; la capacidad económica debe ponderarse de manera realista, diferenciando entre un consumidor y una entidad bancaria multinacional; y la reiteración en la conducta regular en la actuación en los juicios en masa.

En el plano procesal, la LEC prevé, en el artículo 329, una consecuencia específica para la negativa injustificada a la exhibición documental. Cuando una parte incumple el mandato de aportar un documento, el tribunal puede otorgar valor probatorio a este conforme a lo sostenido por la parte que solicitó su aportación. Se reconoce a esa negativa efectos semejantes a los de la incomparecencia al interrogatorio de parte, es decir, la admisión ficticia de los hechos alegados por quien se ve privado de la prueba documental.[14] Sin embargo, cabe señalar que esta presunción, la *ficta admissio*, no opera de forma automática, requiere que el tribunal valore las circunstancias del caso, que la negativa del requerido sea infundada, y que el documento resulte relevante, e identificado. Debe existir una conducta procesal objetivamente obstruccionista que impida el acceso a medios de prueba esenciales para la parte solicitante.

3.2. Supuestos de actuación contraria a la buena fe procesal

Con independencia de los escenarios de falta de aportación documental, la casuística genera otras hipótesis caracterizadas por la voluntad obstruccionista de una de las partes, que deben ser analizadas para evitar que queden sin sanción económica o procesal y desvirtúen la utilidad práctica de la inteligencia artificial.

a) Destrucción del documento. Con frecuencia, las entidades financieras alegan que no están obligadas a conservarlos más allá de los cuatro años que fija el artículo 66 LGT para fines tributarios, o seis años sobre la base de las reglas empresariales del precepto 30 Código comercio.[15] ¿Se puede admitir la no presentación de los documentos sobre la base de estos argumentos? La respuesta debe ser negativa, y, como hemos dicho anteriormente, aplicar

12. SAP Valencia, 6ª, 2/2/18, Id Cendoj: 46250370062018100520.
13. STC 23/7/07, n.º 177/07.
14. SAP Madrid, 25ª, 17/9/24, Id Cendoj: 28079370252024101006 y ABEL, X. (2012). «La prueba documental». *Derecho probatorio,* pág. 845. Barcelona: J.M. Bosch.
15. STS 12/05/08, Id Cendoj: 28079110012008100372.

la *ficta admissio*, pero, asimismo, debe plantearse un refuerzo legislativo que imponga la obligación de conservar los contratos durante todo el plazo de prescripción de las acciones civiles, y no por un límite fiscal o empresarial que carece de relación con el derecho procesal (Sánchez, 2025).

b) El problema de la «remisión a modelos vacíos». La práctica de algunas entidades financieras de sustituir el contrato concreto por modelos genéricos no cumplimentados plantea un problema que trasciende lo estrictamente procesal. Así, desde la perspectiva del Código Civil, en adelante CC, la remisión a modelos estandarizados es sancionable por obstaculizar la actuación de la justicia. Los artículos 1281 a 1289 CC imponen reglas de interpretación contractual basadas en la literalidad, la intención de las partes y la realidad de lo pactado. Un formulario vacío carece de esos elementos esenciales: no expresa el consentimiento concreto, no acredita la prestación pactada y no refleja la voluntad contractual. Admitirlo como prueba sería tanto como aceptar un contrato sin objeto ni causa.[16]

c) La no correlación de la integridad formal con la integridad material. El expediente electrónico ha traído consigo un riesgo: la posibilidad de confundir la integridad formal de los documentos electrónicos con su veracidad material. La firma electrónica, los metadatos o el sello de tiempo acreditan que un fichero no ha sido alterado desde su presentación, pero nada dicen sobre si ese documento reproduce fielmente el contrato original, si es completo en todos sus extremos o si corresponde a la versión firmada entre las partes. Basta pensar en contratos escaneados con anexos omitidos, defectuosos o versiones contractuales desactualizadas para comprender que un documento «intacto» digitalmente puede ofrecer una verdad contractual mutilada, vulnerando la regla 9.3 CE que consagra la seguridad jurídica, pues esta se vacía de contenido si los documentos aportados garantizan integridad técnica pero no material, y la actividad valorativa del juez, pues se condiciona indebidamente la convicción judicial, que podría apoyarse en una prueba formalmente correcta pero materialmente sesgada.

El momento procesal para cuestionar la fiabilidad de la documental aportada por la contraparte es la fase de proposición y práctica de prueba. Ante la incertidumbre de la realidad documental y su correlación con el documento íntegro, la prueba pericial informática, prevista en los arts. 335 y ss. LEC, cobra un papel central, pues se rige como el instrumento idóneo para auditar la veracidad material de la prueba documental.[17]

d) Las excusas digitales. Para los supuestos en que los contratos se encuentren digitalizados, la parte incumplidora puede entregar PDF escaneados en baja calidad o incluso ilegibles, neutralizando la posibilidad de que la tecnología sea utilizada eficazmente por el juez o por la contraparte. La solución pasa por establecer estándares procesales mínimos de formato documental: exigencia de copia digital completa, legible y en soporte electrónico normalizado (p. ej. XML, PDF, etc.).

4. Instituciones procesales afectadas por el uso de la inteligencia artificial: problemas y ventajas

El empleo de algoritmos de cribado documental no altera la estructura ni tramitación del proceso, pero incide en derechos fundamentales y principios de este.[18] Incidencia que vamos a analizar.

4.1. Naturaleza de la prueba y valoración probatoria

Las partes incorporan el contrato que será objeto de análisis por el algoritmo como prueba documental de sus alegaciones, bien como documental privada, art. 299.1. 3.ª LEC, si se trata de un contrato *revolving*, por ejemplo, bien como documental pública, art. 317 LEC, si es una escritura pública donde consta formalizada la hipoteca. En ambos supuestos, el formato electrónico, previsto en la norma 299.2 LEC, como soporte de introducción al proceso no

16. Devienen aplicables, las argumentaciones contenidas en la SAP Madrid, 28ª, 18/7/22, Id Cendoj 28079370282022101691, en las que la falta de aportación al proceso del contrato supone su nulidad.
17. Resultan de aplicación, las reflexiones contenidas en BARRIOS, G. (2017). «La integridad y/o autenticidad de los medios de prueba digital en el proceso laboral: una aproximación al tema a propósito de los correos electrónicos». *Revista de Trabajo y Seguridad Social CEF*, n.º. 415, octubre, págs. 44-46.
18. STC 4/6/18, n.º 58/18.

debe alterar su naturaleza. La duda surge cuando el tribunal utiliza un programa para «buscar» cláusulas abusivas, ¿el resultado de la aplicación del algoritmo es una prueba documental o es una prueba pericial? La dicotomía nos la podríamos plantear por los siguientes razonamientos:

A) Si el sistema se emplea como un simple buscador para localizar datos del contrato y traerlos a la motivación, la fuente probatoria sigue siendo el documento aportado por las partes. El resultado de la aplicación del programa no es una «prueba autónoma», sino una actuación de auxilio para leer mejor lo ya incorporado. **B)** Si el objeto de prueba ya no es solo el documento, sino el método que lo procesa, esto es, métricas de error, alcance de los datos procesados, reglas de exclusión, etc., entonces el «cómo funciona» pasa a ser objeto de prueba. En ese escenario, podría defenderse que la aplicación del algoritmo convierte la prueba en pericial. El algoritmo no es el perito: es la herramienta cuyo uso y límites explica el perito, sometido a contradicción.

A nuestro entender, el resultado de la aplicación del algoritmo debe seguir manteniendo la categoría de prueba documental, pues la naturaleza del medio de prueba viene dada por la fuente que lo sustenta, no por la herramienta empleada para leerla. Si el tribunal utiliza un programa para localizar datos del contrato que obra en autos, la fuente probatoria sigue siendo la documental (Barona, 2023, pág. 37) aportada por las partes, el listado informático no crea un medio de prueba distinto ni lo desnaturaliza, convirtiéndolo en pericial por el mero hecho de intervenir tecnología. Esta conclusión se alinea con la clasificación de medios de prueba regulada en el artículo 299 LEC, que distingue entre prueba documental y pericial, pero incluyendo los formatos electrónicos como vehículos de reproducción, no como categorías probatorias autónomas.

La categorización que se conceda al informe derivado de la aplicación del algoritmo incide en la valoración probatoria. La documental tiene un régimen legal específico de valoración judicial en las normas 326 y 319 LEC, para documentos privados o públicos, porque la prueba es el propio documento. Por eso, la LEC prevé reglas de valoración predeterminadas. En contrapartida, la pericial se rige por la «sana crítica», sin valor tasado. En la prueba pericial no hay tasación legal del resultado ni una regla que le imponga dar «plena prueba» al dictamen. Es por ello, que transformar una prueba documental en una prueba pericial por el uso de un algoritmo también modificaría la valoración judicial, vulnerando las reglas probatorias reguladas en la ley procesal.

4.2. La motivación judicial frente al uso de la inteligencia artificial

La exigencia constitucional de motivación de las resoluciones judiciales, recogida en el artículo 120.3 CE, constituye una de las garantías del derecho fundamental a la tutela judicial efectiva y uno de los principios del proceso civil, como se postula en la norma 218.2 de la Ley ritual procesal.[19] No es un requisito formal, sino un pilar de control de la actividad jurisdiccional, pues solo a través de motivación puede la ciudadanía conocer las razones de una decisión y las partes procesales articular los recursos oportunos.[20]

En este marco, la irrupción de herramientas LegalTech plantea un desafío evidente. No es jurídicamente aceptable que un juez se limite a reproducir el resultado de un algoritmo, según una fórmula tan escueta e inadmisible como: el sistema señala que la cláusula es abusiva. Esa simple afirmación es insuficiente para cumplir la exigencia constitucional, pues se produciría un déficit de motivación propia, según el hecho de que el juez sustituiría su razonamiento por el de un sistema que no forma parte del ordenamiento jurídico. La justicia algorítmica en caso alguno debe sustituir la justicia humana (Comoglio, 2022, pág. 62).

Ante esta problemática, la solución no pasa por rechazar el uso de la IA, sino por integrar sus aportaciones dentro de una motivación reforzada. Los sistemas de cribado algorítmico pueden convertirse en instrumentos valiosos si se emplean como apoyo a la argumentación judicial y no como sustituto de esta. Los datos elaborados por parte de los algoritmos facilitan que el juez pueda identificar patrones o cláusulas problemáticas, pero resulta imprescindible que la decisión final se presente siempre como resultado de la aplicación del Derecho al caso concreto,[21] con referencia a las normas materiales: el artículo 82 TRLGDCU

19. ATS 22/7/25, Id Cendoj: 28079110012025202011.
20. STC 24/4/06, n.º 118/06 y STS 25/9/15, Id Cendoj: 28079110012015100509.
21. ALISTE, T.J. (2018). *La motivación de las resoluciones judiciales*. Madrid: Marcial Pons, págs. 138 y ss. y STC 4/8/99, n.º 147/99.

sobre cláusulas abusivas, el precepto 1255 CC en relación con la autonomía de la voluntad, o la norma 10 de la Ley de Condiciones Generales de Contratación, en adelante LCGC, sobre condiciones generales.

Desde la perspectiva de control *ex post*, el incumplimiento de estas exigencias no es neutro. Una sentencia basada exclusivamente en un algoritmo podría ser recurrida por vulneración del derecho a la tutela judicial efectiva y por incumplimiento del deber de motivación e incluso solicitar su nulidad.[22]

4.3. Inmediación judicial: riesgos de desplazamiento y vías de reconducción

La inmediación judicial (Berzosa, 2021, pág. 225), entendida como la exigencia de que el juez entre en contacto directo con la prueba es una garantía estructural del proceso.[23] Su reconocimiento normativo se desprende del artículo 229 LOPJ, que impone la presencia judicial en las actuaciones probatorias, y se conecta con el derecho fundamental a un proceso con todas las garantías.

La irrupción de sistemas algorítmicos de cribado documental amenaza con diluir esta función (Barona, 2023, págs. 35-36). Cuando el contrato llega segmentado y priorizado por una herramienta LegalTech, el juez corre el riesgo de sustituir la lectura completa del contrato por una mera verificación parcial de las alertas señaladas por la máquina, con los siguientes peligros: **a)** se produce un desplazamiento del centro de la valoración probatoria, el algoritmo actúa como filtro que selecciona qué merece atención y qué no; **b)** puede incurrirse en una modalidad de subjetivismo judicial, pues si el juez solo se concentra en las cláusulas sospechosas marcadas por el sistema, su percepción del resto del contrato puede resultar condicionada; **c)** se desnaturaliza uno de los principios básicos del proceso civil: la inmediación judicial. Ahora bien, la cuestión no exige rechazar sin más la tecnología, sino reencauzarla normativamente o reinterpretar los principios del proceso conforme a una justicia digital del siglo XXI. Con base en ello, varias soluciones son posibles:

En primer lugar, consideramos que la inmediación no se ve sustituida, sino reforzada por la posibilidad de contraste directo. El informe puede servir como guía, pero el juez conserva el acceso al texto completo del contrato y la potestad de acudir a él para verificar las alarmas o aspectos no resaltados. Lo relevante no es que el juez lea palabra por palabra, sino que la decisión final se funde en la valoración del documento íntegro y en la posibilidad de consultar el documento en toda su extensión.

En segundo lugar, con base en la exigencia de acreditación «del contacto directo con la prueba», la valoración de la prueba documental debería comprender: **a)** la identificación del documento algorítmico, número, fecha, versión, dejando claro que se trata de un instrumento auxiliar y no de una fuente normativa; **b)** la integración crítica del resultado del algoritmo, el órgano judicial debe confirmar, descartar o matizar la alerta, explicando los motivos jurídicos concretos de su decisión; y, **c)** justificar el peso probatorio otorgado al informe en relación con el resto de material probatorio.

4.4. Compatibilidad de la IA con el principio dispositivo

El papel del juez frente a las cláusulas abusivas no es idéntico en todos los procesos civiles. La clave está en diferenciar entre aquellos procedimientos donde la ley y la jurisprudencia imponen un control de oficio, y aquellos otros en los que, por respeto al principio dispositivo el examen judicial debe ceñirse a lo que las partes aleguen.

En los procesos de ejecución de títulos extrajudiciales, de ejecución hipotecaria y monitorio, el juez tiene obligación de examinar de oficio todas las cláusulas del contrato que puedan ser abusivas, aunque el consumidor no las haya denunciado. En estos supuestos, el uso de algoritmos resulta plenamente compatible con el rol judicial, un sistema que detecta todas las posibles cláusulas abusivas refuerza el deber de control oficioso, facilita que ninguna escape a la revisión judicial y actúa como garantía de los derechos del consumidor.

22. STC 8/5/23, n.º 39/23.
23. Partimos de un concepto amplio de inmediación judicial, en el sentido de no limitarse a estar presente el juez en la prueba, por ser un documento, sino que tenga contacto directo con ella.

En los procesos declarativos en los que se solicite en la demanda, la nulidad de alguna cláusula, esto es, los supuestos regulados en la norma 250.1.14 LEC, la situación es distinta. En estos rige el principio dispositivo, pues, conforme al artículo 261 LEC, son las partes quienes delimitan el objeto del proceso, realidad reforzada por la norma 218.1 LEC, al exigir que la sentencia sea congruente con las pretensiones deducidas oportunamente en el pleito.

Así, el juez solo puede pronunciarse sobre lo que ha sido pedido en la demanda. Si el algoritmo identifica cláusulas adicionales que no han sido invocadas, el juez no debe extender de oficio el control a ellas, porque implicaría vulnerar el principio dispositivo, ampliando artificialmente el objeto procesal, poniendo en riesgo su imparcialidad objetiva, al dejar de ser tercero para convertirse en promotor de pretensiones no ejercitadas. Asimismo, de pronunciarse sobre estas nuevas cláusulas abusivas, tal cuestión tendría una incidencia directa en la sentencia, pues esta podría ser objeto de impugnación por incongruencia *ultra petita*, por decidir más allá de lo realmente solicitado.[24]

4.5. Derecho a la transparencia

La introducción de algoritmos en el proceso exige una serie de cautelas para que su uso no erosione las garantías constitucionales. En este marco, adquiere relevancia el problema de la transparencia. El derecho de defensa exige que las partes puedan conocer y rebatir los elementos que sustentan la decisión judicial. No basta con que el juez «confíe» en un sistema, el proceso debe permitir que las partes contrasten su funcionamiento y sus resultados.

El acceso de la ciudadanía a los algoritmos utilizados por las administraciones públicas plantea un conflicto normativo, por un lado, el derecho de acceso a la información pública, reconocido en el artículo 12 de la Ley 19/2013, de transparencia, acceso a la información pública y buen gobierno, y, por otro, la protección de los secretos empresariales y de la propiedad intelectual, regulada en la Ley 1/2019, de Secretos Empresariales que concede cierta «opacidad» a los algoritmos (Cancio, 2023, págs. 184 y 186). Desde la perspectiva constitucional, el artículo 105.b CE garantiza el acceso de los ciudadanos a los archivos y registros administrativos, mientras que el artículo 24 CE ampara la tutela judicial efectiva y el artículo 120.3 CE impone a los jueces la obligación de motivar sus resoluciones. De ahí, que los algoritmos que influyen en decisiones administrativas o judiciales no puedan quedar al margen del conocimiento público, por incidir directamente en la vigencia de derechos fundamentales.

En el plano europeo, el Reglamento 2024/1689 sobre IA refuerza esta exigencia, imponiendo a los sistemas algorítmicos aplicados en la justicia y en la actividad administrativa, estándares de transparencia, documentación y explicabilidad. Ahora bien, estas exigencias deben coexistir con la necesidad de preservar el valor competitivo de los desarrollos tecnológicos. La normativa sobre secretos empresariales legitima que no se difunda íntegramente el código fuente de los programas, para proteger la innovación, la competencia y la seguridad de los sistemas.

La solución no reside en otorgar prioridad absoluta a uno de los intereses en juego, sino en aplicar un criterio de proporcionalidad, estableciendo diferentes grados de protección y confidencialidad (de la Cueva, 2018, págs. 24-27): la ciudadanía debe conocer los criterios y parámetros de decisión de los algoritmos en la medida imprescindible para garantizar sus derechos y permitir un control democrático; al mismo tiempo, los elementos técnicos que constituyan secreto empresarial pueden quedar resguardados mediante fórmulas de acceso limitado bajo confidencialidad. Así, consideramos que no es necesario revelar el código fuente ni la totalidad de las bases de datos de entrenamiento, pero sí debe garantizarse el acceso a los *rationales*, fragmentos textuales que activaron la alerta, a los metadatos relevantes, versión, fecha de ejecución, parámetros y corpus de referencia. De este modo, se asegura un nivel adecuado de transparencia conforme a los principios constitucionales y europeos, sin menoscabar los intereses legítimos de quienes desarrollan los algoritmos. Asimismo, el legislador ofrece un referente útil en el art. 283 bis a) LEC, que prevé formas de acceso bajo confidencialidad en procedimientos sobre competencia desleal: ese modelo puede inspirar un régimen *ad hoc* para la prueba algorítmica, equilibrando secreto industrial y derecho de defensa (Álvarez, 2025).

24. STC 3/7/24, n.º 95/24.

5. Ventajas procesales consecuencia de la aplicación de la inteligencia artificial

5.1. Derecho a no sufrir dilaciones indebidas

El artículo 24.2 CE reconoce el derecho a un proceso sin dilaciones indebidas, que la jurisprudencia constitucional ha caracterizado como garantía autónoma y exigible, y que el TEDH, en aplicación del art. 6.1 CEDH, vincula a la efectividad de la tutela judicial. No es un derecho programático ni abstracto, sino una condición de legitimidad de la jurisdicción.

Sin embargo, la realidad procesal muestra un desfase entre el mandato normativo y la práctica cotidiana. En litigios civiles, particularmente en materia bancaria y de consumo, el volumen documental es de tal envergadura que convierte este mandato constitucional en un ideal inalcanzable. Contratos con decenas de anexos, múltiples comunicaciones electrónicas y condiciones generales estandarizadas generan auténticos cuellos de botella. El juez, ante una masa de documentos difícilmente manejable, se ve obligado a dedicar largas horas a búsquedas manuales y relecturas, lo que retrasa la aproximación sustantiva al caso y la decisión final. El mal endémico estructural es la normalización de las dilaciones indebidas, que afectan al justiciable y socavan la credibilidad del sistema judicial.

En este escenario, la introducción de sistemas de cribado algorítmico puede ofrecer un instrumento en aras de la mejora de la eficiencia de la Justicia, quimera anhelada y a la que se encuentra orientada la mayoría de las reformas procesales (Alcoceba, 2024, págs. 79-80). El algoritmo opera como un filtro experto que, *ex ante*, reordena tiempos y tareas. De este modo, la primera revisión judicial no se retrasa hasta una lectura completa y dispersa, sino que se produce antes. La consecuencia práctica es acelerar la respuesta judicial a plazos razonables en procesos documentalmente densos.

Ahora bien, el potencial de la LegalTech debe respetar los siguientes extremos: **a)** el algoritmo no puede condicionar la admisión ni la práctica de la prueba, su función es auxiliar, nunca restrictiva; **b)** los informes deben ser objeto de motivación judicial; y **c)** debe dejarse constancia de que la herramienta se empleó únicamente como instrumento de gestión del tiempo procesal, y que la decisión judicial se adoptó tras una valoración autónoma y crítica de las pruebas. Solo bajo estas condiciones, la contribución de la IA a la reducción de dilaciones indebidas puede considerarse legítima constitucionalmente. Solo así, la celeridad se alcanzará sin erosionar la tutela judicial efectiva y sin relegar al juez a un papel subordinado frente a la máquina.

5.2. Seguridad jurídica como coherencia y uniformidad de las resoluciones

El principio de seguridad jurídica, consignado en la norma 9.3 CE, no se limita a la estabilidad normativa, implica también que las decisiones judiciales sean coherentes y uniformes.[25] En este marco, el uso de algoritmos en el proceso puede contribuir a reforzar la uniformidad (Franco, 2023, págs. 10-11). En la modalidad procedimental donde la litigiosidad es masiva: materia de cláusulas bancarias o contratos de adhesión, los sistemas de cribado pueden proporcionar al juez una clasificación de alertas y riesgos homogénea señalando cláusulas con base en patrones jurisprudenciales y criterios normativos consolidados. Esta función preventiva tiende a reducir la dispersión de criterios entre órganos de instancia y, con ello, favorece la coherencia de las resoluciones.

Ahora bien, el respeto a la seguridad jurídica no impide dos extremos: la modificación de los criterios base del algoritmo, conforme a la nueva doctrina judicial y normativa, y respetar la casuística en la valoración y motivación judicial, pues, la uniformidad algorítmica, si no se acompaña de control judicial crítico, puede desembocar en rigidez interpretativa, impidiendo que el juez valore matices contextuales o adapte la solución al caso concreto.

5.3. Economía procesal orientada a valor probatorio

La economía procesal no puede confundirse con un ideal de simplificación cuantitativa, hacer menos, sino que debe concebirse como un criterio de optimización cualitativa de los recursos jurisdiccionales, dedicar tiempo y esfuerzo

25. STC 4/6/12, n.º 120/2012.

a lo verdaderamente relevante para la decisión judicial. En este sentido, la introducción de sistemas de cribado algorítmico tiene la potencialidad de orientar la labor procesal hacia lo probatoriamente significativo, desplazando la atención desde cláusulas inocuas hacia aquellas que, conforme a categorías jurídicas contrastadas, generan un riesgo plausible de nulidad o abusividad, extremo que implicaría una colaboración digital en la reducción del tiempo que requiere el órgano judicial para la clasificación e identificación de cláusulas, hecho que directamente influiría en la agilización en la respuesta judicial (Miranda, 2022, págs. 388-389).

La contribución de la LegalTech a la economía procesal no es acelerar el trámite a costa de garantías, sino racionalizar el valor probatorio. La clasificación algorítmica por categorías jurídicas, limitación de responsabilidad, modificación unilateral, sumisión a fuero no imperativo, etc., permite ordenar las prioridades procesales.

Sin embargo, la promesa de economía procesal también plantea problemas jurídicos que no deben subestimarse. En primer lugar, si el algoritmo prioriza unas cláusulas y omite otras, puede inducir al juez y a las partes a descuidar elementos que sí tendrán relevancia, comprometiendo el principio de exhaustividad exigido en la norma 218 LEC, y, en segundo lugar, si la clasificación algorítmica se percibe como cerrada o determinante, las partes pueden ver constreñida su iniciativa probatoria, arts. 282 y ss. LEC, a los elementos identificados por el algoritmo.

En relación con el primero de los problemas planteados, la solución debe pasar necesariamente por reafirmar el carácter auxiliar y no vinculante del cribado algorítmico (Luna, 2022, pág. 252). El informe tecnológico solo puede entenderse como prueba documental, puesto a disposición del juez y de las partes, sin que por ello limite el deber de revisión integral del contrato. Solo de este modo, puede cumplirse el mandato del artículo 218 LEC y evitar que las partes no identificadas por el algoritmo equivalgan a exclusión de análisis.

En cuanto al segundo de los problemas, los artículos 282 y ss. LEC reconocen que corresponde a los litigantes proponer la prueba que estimen pertinente, en tanto la misma sea adecuada para acreditar hechos relevantes. Si la clasificación algorítmica se percibiera como cerrada, se correría el peligro de que las partes quedaran constreñidas a discutir únicamente lo que la máquina señaló. Para prevenir este efecto, resulta imprescindible recalcar que todo hallazgo algorítmico es impugnable y que las partes conservan plena libertad para proponer prueba sobre cualquier cláusula contractual, aun cuando no haya sido marcada.

6. Reflexión final

De lo desarrollado en los distintos apartados del trabajo se desprende una conclusión nítida: sí es posible la creación de un algoritmo eficaz para identificar cláusulas abusivas, modelo aplicable a otras modalidades procesales, y, de hecho, ya existen técnicas sólidas de procesamiento del lenguaje natural, aprendizaje supervisado y módulos de contextualización temporal y económica que permiten entrenar sistemas con resultados fiables.

Ahora bien, su eficacia no debe medirse solo en términos de precisión estadística, sino también en términos de compatibilidad con el proceso civil: transparencia, contradicción, posibilidad de impugnación y subordinación al juicio humano.

De esta forma, podemos defender que la implantación de un sistema LegalTech en el proceso es al mismo tiempo una oportunidad y una amenaza controlable. Oportunidad, porque en un sistema judicial aquejado de dilaciones indebidas crónicas, saturación y dispersión de criterios, los algoritmos pueden facilitar la organización del caso, homogeneizar la identificación de cláusulas abusivas y concentrar la actividad probatoria relevante. Amenaza, porque sin límites claros, la tecnología correría el riesgo de erosionar garantías constitucionales y principios básicos del proceso civil: la motivación, art. 120.3 CE, la inmediación, art. 229 LOPJ, la congruencia, art. 218 LEC, la libertad de prueba, arts. 282 y ss. LEC, y, la tutela judicial efectiva, art. 24 CE. Sin embargo, todos estos riesgos resultan controlables. De acuerdo con ello, para una correcta implementación de estos sistemas tecnológicos y en aras a garantizar la vigencia y correcta aplicación de las instituciones procesales informadoras del proceso civil es preciso:

En primer lugar, garantizar una exigencia de motivación reforzada. El juez no puede convertirse en portavoz de un sistema que «señala» cláusulas, sino que debe integrar críticamente esos hallazgos en su razonamiento jurídico. Un informe algorítmico no motivado es un mero acto

técnico, por lo que, el uso de tecnología solo es legítimo cuando potencia, y no sustituye, la capacidad de deliberación del juez.

En segundo lugar, la inmediación judicial no puede ceder ante la mediación tecnológica. El juez no tiene que releer exhaustivamente cada contrato de cientos de páginas, pero sí debe conservar el acceso integral al documento, con posibilidad de consultarlo y verificar lo señalado por el algoritmo. Solo así la inmediación mantiene su sentido como garantía de imparcialidad y contacto directo con la prueba. Un proceso en el que la mirada judicial queda reducida a lo que destaca una herramienta pierde profundidad deliberativa y corre el riesgo de convertirse en una justicia automatizada de mínimos.

En tercer lugar, es clave su compatibilidad con el principio dispositivo. En los procesos declarativos, el juez ha de ceñirse estrictamente a lo que las partes solicitan; si extendiera su pronunciamiento a cláusulas no invocadas, incurriría en incongruencia *ultra petita*, vulnerando así el art. 24 CE

La necesaria correlación y respeto entre inteligencia e instituciones procesales permite concluir que el uso de LegalTech en la justicia civil no es neutro, ni mucho menos inocuo; es una opción política y jurídica que exige una regulación clara, cultura procesal garantista y control judicial estricto, pero que puede aportar ventajas inestimables como la seguridad jurídica, la economía procesal y, lo que es más importante, favorecer la celeridad en la respuesta judicial. Su uso puede reforzar la eficiencia del proceso, pero también puede vaciarlo de garantías si se adoptan como sustituto de la deliberación judicial. La clave está en la subordinación estricta al marco normativo, los informes algorítmicos deben tratarse como prueba documental sujeta a contradicción, con transparencia suficiente para permitir impugnación y control, y con la obligación de que el juez motive expresamente su peso en la decisión.

El derecho a un proceso sin dilaciones indebidas no puede convertirse en excusa para automatizar la justicia, pero sí, debe servir como criterio para adoptar tecnologías que racionalicen tiempos sin degradar derechos. La seguridad jurídica tampoco puede confundirse con rigidez algorítmica, sino con uniformidad razonada de las resoluciones. Y la economía procesal, lejos de significar atajos, debe entenderse como orientación al valor probatorio, visible y discutible.

La instauración de la IA será compatible con el proceso civil si se integra como instrumento auxiliar, nunca como decisor. El juez debe seguir siendo el centro de la función jurisdiccional, y la tecnología, una herramienta transparente y discutible que le permita ejercer mejor su tarea. De lo contrario, la eficiencia se convertiría en una posible vulneración de la función jurisdiccional reconocida constitucionalmente.

Referencias bibliográficas

ABEL, X. (2012). «La prueba documental». *Derecho probatorio*, págs. 777-899. Barcelona: J.M. Bosch.

ALCOCEBA, J. M. (2024). «Aproximación a la litigación civil». *Justicia en redefinición: inteligencia artificial en los métodos adecuados de resolución de conflictos*, págs. 79-101. Madrid: Dykinson.

ALISTE, T. J. (2018). «La motivación judicial entendida como garantía constitucional y obligación legal: en torno a la configuración, función, alcance y extensión de la motivación en nuestro ordenamiento jurídico». *La motivación de las resoluciones judiciales*, págs. 138 y ss. Madrid: Marcial Pons.

ÁLVAREZ, V. J. (2025). «El derecho de acceso libre y gratuito a los algoritmos empleados por los poderes públicos». *Revista General de Derecho Administrativo*, artículo en línea. [Fecha de consulta: 3 de septiembre de 2025].

BARONA, S. (2023). «Datalización de la justicia, algoritmos, inteligencia artificial y justicia, ¿el comienzo de una gran amistad?». *Revista Boliviana de Derecho*, n.º 36, págs. 14-45.

BARRIOS, G. (2017). «La integridad y/o autenticidad de los medios de prueba digital en el proceso laboral: una aproximación al tema a propósito de los correos electrónicos». *Revista de Trabajo y Seguridad Social*, n.º 415, octubre, págs. 23-52. DOI: https://doi.org/10.51302/rtss.2017.1780

BERENGUER, M. C. (2024). «Transparencia y explicabilidad para prevenir la discriminación de los sistemas de inteligencia artificial: la interacción entre el RGPD y el RIA». *Inteligencia Artificial y Derecho de Daños: cuestiones actuales*, págs. 49-118. Madrid: Dykinson.

BERZOSA, V. (2021). «Principios del proceso». *La Evolución del Derecho procesal a la luz de la Justicia*, págs. 161-233. Barcelona: J.M. Bosch. DOI: https://doi.org/10.2307/j.ctv2k0582h.9

CALERO, M. (2024). «El Procesamiento de Lenguaje Natural en la revisión de literatura científica». *Revista Española de Urgencias y Emergencias*, n.º 3, págs. 184-195.

CANCIO, R. (2023). «Inteligencia Artificial y Administración de Justicia: una disrupción relativa». *Inteligencia artificial: los derechos humanos en el centro*, págs. 181-202. Madrid: Dykinson. DOI: https://doi.org/10.2307/jj.11102895.15

COMOGLIO, P. (2022). «Inteligencia artificial y selección de pruebas en el proceso civil: ¿hacia un proceso más inteligente o hacia un proceso más artificial?». *Revista Ítalo-Española de Derecho Procesal*, págs. 55-85. DOI: https://doi.org/10.37417/rivitsproc/840

DE LA SIERRA, S. (2021). «¿Cuál es el papel hoy de la inteligencia artificial y los algoritmos en el sector público? Control judicial de los algoritmos: robots, administración y estado de derecho». *El Derecho.Com* [en linea]. Disponible en: https://elderecho.com/control-judicial-de-los-algoritmos-robots-administracion-y-estado-de-derecho. [Fecha de consulta: 1 de septiembre de 2025].

DE LUCCHI, Y. (2023). «Eficiencia en el acceso a la información y fuentes de prueba en el proceso civil: tibias líneas convergentes EEUU/Europa». *Revista Ítalo-Española de Derecho Procesal*, n.º 1, págs. 23-52. DOI: https://doi.org/10.37417/rivitsproc/1255

FERNÁNDEZ, J. M. (2023). «Inteligencia artificial y abogacía. Herramientas legaltech basadas en inteligencia artificial». *Inteligencia artificial: los derechos humanos en el centro*, págs. 237-247. Madrid: Dykinson. DOI: https://doi.org/10.2307/jj.11102895.18

FRANCO, P.E. (2023). «Justicia algorítmica y predictibilidad constitucional». *Revista Iberoamericana de Derecho, Cultura y Ambiente*, n. º 4, diciembre.

LUNA, F. (2022). «Impacto y límites de la inteligencia artificial en la práctica jurídica». *Via Inveniendi et Iudicandi*, Tomo 17, n.º 2, págs. 234-254. DOI: https://doi.org/10.15332/19090528.8773

NIEVA, J. (2022). «Inteligencia artificial y proceso judicial: perspectivas tras un alto tecnológico en el camino». *Revista General de Derecho Procesal*, n.º 57, págs. 1-21.

PICÓ, J. (2013). *El principio de la buena fe procesal*, 2ª ed. Barcelona: J. M. Bosch.

RIVERO, S. (2024). «Inteligencia artificial y judicatura: sobre la dicotomía entre la asistencia y la sustitución. Aspectos técnicos y medioambientales». *IDP. Revista de los Estudios de Derecho y Ciencia Política*, n.º 41, octubre, págs. 1-12. DOI: https://doi.org/10.7238/idp.v0i41.426865

SÁNCHEZ, J. (2025). «Comentarios a la sentencia del TS de 19 de julio de 2021, sobre la obligación de conservar y entregar documentos bancarios». Artículo en línea, *Abogacía española*, 8/9/21. [Fecha de consulta: 3 de septiembre de 2025].

SOLAR, J. I. (2018). «La codificación predictiva: inteligencia artificial en la averiguación procesal de los hechos relevantes». *Anuario de la Facultad de Derecho de la Universidad de Alcalá*, n.º XI, enero, págs. 75-105. DOI: https://doi.org/10.2307/j.ctvq4bzpb.5

VELASCO, E. (2024). «Inteligencia artificial: aspectos penales y procesales». *Desafíos del derecho procesal del siglo XXI: prueba prohibida, inteligencia artificial y digitalización de la administración de justicia*, págs. 171 a 217. Madrid: Dykinson. DOI: https://doi.org/10.2307/jj.13286085.11

Cita recomendada

ADAN DOMÈNECH, Federico (2025). «Algoritmos en el proceso civil: oportunidad de modernización o riesgo de desnaturalización. Creación de un algoritmo para la identificación de cláusulas abusivas». *IDP. Revista de Internet, Derecho y Política*, núm. 44. UOC. [Fecha de consulta: dd/mm/aa]. DOI: http://dx.doi.org/10.7238/idp.v0i44.9800399

Sobre el autor

Federico Adan Domènech
Universidad Rovira i Virgili
federico.adan@urv.cat

Catedrático de Derecho Procesal de la Universidad Rovira i Virgili. Licenciado en Derecho por la Universidad de Navarra. Doctor en Derecho por la Universidad Rovira i Virgili. Fue nombrado magistrado suplente de la Audiencia Provincial de Tarragona por el CGPJ. Director de la Escuela de Práctica Jurídica del Ilustre Colegio de Abogados de Tarragona hasta el año 2024. Exdecano de la Facultad de Ciencias Jurídicas de la Universidad Rovira i Virgili, 13/11/2009 a 14/11/2011. Director del Máster de acceso a la abogacía (2012-13, 2011-12, 2010-11 y 2009-10) organizado por la Universidad Rovira Virgili y los Ilustres Colegios de Abogados de Tarragona, Reus y Tortosa, siendo en la actualidad su coordinador. Autor de más de noventa artículos jurídicos publicados en revistas especializadas.

IDP
REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Algunas consideraciones sobre los sistemas informáticos de facturación

Rafael Oliver Cuello
Universitat Internacional de Catalunya

Fecha de presentación: agosto 2025
Fecha de aceptación: octubre 2025
Fecha de publicación: marzo 2026

Resumen

La normativa sobre los sistemas informáticos de facturación establece los requisitos que estos deben cumplir, así como sus reglas de funcionamiento, al objeto de garantizar la integridad, conservación, accesibilidad, legibilidad, trazabilidad e inalterabilidad de los registros de facturación. Su principal objetivo es la lucha contra el fraude fiscal y el reforzamiento del control tributario, permitiendo acceder a una información que posibilite las labores administrativas de comprobación tributaria. Asimismo, con esta normativa se pretende facilitar el cumplimiento voluntario mediante la automatización del suministro de información tributaria, lo cual supone una mejora en la transparencia de la aplicación de los tributos. La aplicación de esta normativa también provocará un avance en la digitalización de la actividad empresarial y profesional, que es especialmente necesario en las pequeñas y medianas empresas, repercutiendo en una mejor gestión de la información contable y facilitando una modernización de las empresas y profesionales afectados. Sin embargo, no hay que olvidar los posibles inconvenientes derivados de la denominada brecha digital y la eventual afectación a los derechos y garantías de los obligados tributarios, por lo que es importante destacar el papel que debe desempeñar en este ámbito la información y asistencia al obligado tributario, así como la colaboración social en la gestión tributaria.

Palabras clave

sistemas informáticos; Verifactu; facturación; fraude fiscal; digitalización empresarial; información y asistencia

Some considerations about billing computer systems

Abstract

must meet and their operating rules to ensure the integrity, preservation, accessibility, legibility, traceability, and unalterability of billing records. Its main goal is to combat tax fraud and strengthen tax control by enabling access to information that supports administrative tax verification tasks. Additionally, this regulation aims to promote voluntary compliance by automating the provision of tax information, thereby increasing transparency in tax enforcement. Implementing this regulation will also drive the digitization of business and professional activities, which is particularly important for small and medium-sized enterprises, leading to better management of accounting information and supporting the modernization of affected companies and professionals. Nevertheless, it is crucial not to overlook potential issues stemming from the so-called digital divide and the possible impact on taxpayers' rights and guarantees. Therefore, highlighting the importance of providing information and assistance to taxpayers, along with social cooperation in tax management, remains essential.

Keywords

computer systems; Verifactu; billing; tax fraud; enterprise digitization; information and support

Introducción

Una de las reformas llevadas a cabo en 2021 en la Ley 58/2003, de 17 de diciembre, General Tributaria (LGT) por medio de la Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal, es la incorporación de una nueva obligación tributaria formal en su art. 29.2.j LGT. Se trata de «la obligación, por parte de los productores, comercializadores y usuarios, de que los sistemas y programas informáticos o electrónicos que soporten los procesos contables, de facturación o de gestión de quienes desarrollen actividades económicas garanticen la integridad, conservación, accesibilidad, legibilidad, trazabilidad e inalterabilidad de los registros, sin interpolaciones, omisiones o alteraciones de las que no quede la debida anotación en los sistemas mismos». En esta reforma legal, se introduce también una nueva infracción tributaria, el art. 201 bis LGT, que tiene por objeto asegurar el cumplimiento de la referida obligación tributaria formal (Sánchez Pedroche, 2021, págs. 190-191; Gómez Jiménez, 2021, págs. 1-18; Serrano Antón, 2022, págs. 63-95).

En desarrollo de la citada previsión legal, se aprueba el Real decreto 1007/2023, de 5 de diciembre, por el que se aprueba el Reglamento que establece los requisitos que deben adoptar los sistemas y programas informáticos o electrónicos que soporten los procesos de facturación de empresarios y profesionales, y la estandarización de formatos de los registros de facturación (RRSIF). Asimismo, se dicta la Orden HAC/1177/2024, de 17 de octubre, por la que se desarrollan las especificaciones técnicas, funcionales y de contenido referidas en esta norma reglamentaria.

A continuación, se realizan algunos comentarios sobre los principales objetivos de esta normativa, esto es, la lucha contra el fraude fiscal, el cumplimiento voluntario, la digitalización empresarial y la información y asistencia al obligado tributario.

1. El control tributario y la lucha contra el fraude fiscal

1.1. Concepto de SIF y sujetos obligados

Con la introducción de sistemas informáticos de facturación (SIF) certificados y la prohibición expresa del *software* de doble uso, es decir, aquellos programas que permiten modificar o eliminar registros contables sin dejar rastro, el margen de maniobra para prácticas fraudulentas se reduce considerablemente. Otro aspecto fundamental es la dificultad de ocultar ingresos mediante la no declaración de facturas. Con la exigencia de utilizar SIF certificados y la posibilidad de que la Agencia Estatal de Administración Tributaria (AEAT) acceda a los registros en tiempo real se reduce la capacidad de algunos negocios para declarar solo una parte de sus ventas.

Todos estos objetivos de control tributario y lucha contra el fraude fiscal se desarrollan en el RRSIF. Las disposiciones de esta norma reglamentaria entran en vigor de forma escalonada: por un lado, los productores y comercializadores de los SIF a los que les sea de aplicación el reglamento, el 29 de julio de 2025; por otro lado, los contribuyentes del impuesto sobre sociedades (IS) deberán tener sus SIF adaptados a los requisitos del RRSIF antes del 1 de enero de 2027; y, finalmente, el resto de emisores de facturas obligados al cumplimiento del RRSIF, es decir, los contribuyentes del impuesto sobre la renta de las personas físicas (IRPF), el impuesto sobre la renta de no residentes (IRNR) que operen en España por medio de establecimiento permanente y las entidades en atribución de rentas, el 1 de julio de 2027.

Quizá una de las novedades del RRSIF más conocidas por el público en general sea la incorporación de un código QR en el contenido de las facturas. Efectivamente, las facturas expedidas mediante SIF deben contener una información adicional: por un lado, la representación gráfica del contenido parcial de la factura mediante un código QR;[1] y, por otro lado, la frase «Factura verificable en la sede electrónica de la AEAT» o «Verifactu» cuando el SIF remita los registros de facturación a la Agencia Tributaria. Esta información ha de incluirse tanto en facturas completas como en facturas simplificadas. Además, hay que tener en cuenta que esta obligación de inclusión de contenido adicional en las facturas solo se exige a los obligados sujetos al RRSIF, no al resto de obligados a la emisión de facturas (como son las empresas que apliquen el SII o quienes no desarrollen actividades económicas).

Es importante destacar que en el RRSIF se regulan dos modalidades de funcionamiento de los SIF. Por un lado, los sistemas de emisión de facturas no verificables, que no remiten los registros de facturación a la AEAT, sino que únicamente los almacenan y los tienen disponibles por si se los requiere la administración.[2] Y, por otro lado, los sistemas de emisión de facturas verificables, que son los que, de forma voluntaria, remiten en línea los registros de facturación correspondientes a las facturas expedidas por ellos a la AEAT.[3]

Antes de analizar los requisitos de los SIF que permiten el control tributario y la lucha contra el fraude fiscal, es preciso delimitar qué se entiende por sistema informático de facturación. Según el art. 1.2 RRSIF, se considera SIF el conjunto de *hardware* y *software* utilizado para expedir facturas que admita la entrada de información de facturación por cualquier vía, conserve esta información y la procese para generar otros productos derivados, con independencia de dónde se realice este proceso. Por lo tanto, hay que considerar como SIF a los equipos informáticos que incorporan programas de gestión que tienen las funciones citadas y que normalmente se usan en las áreas de administración o contabilidad por las empresas o los profesionales.

Ahora bien, se plantea la cuestión de la posible consideración como SIF de las hojas de cálculo o los procesadores de texto existentes en el mercado. A este respecto, conviene destacar que el RRSIF no es exigible si estos programas informáticos se utilizan exclusivamente para introducir los datos de las facturas, expedir e imprimir las facturas y conservar la información de facturación. Pero si, además, se utilizan para procesar la información de facturación al objeto de generar directamente los libros registros del impuesto sobre el valor añadido (IVA) o del IRPF, la contabilidad o cualquier otro resultado que se utilice para el cumplimiento voluntario de obligaciones tributarias, tendrán la consideración de SIF, resultando exigibles los requisitos que establece el reglamento.[4]

También es importante delimitar quiénes son los sujetos obligados a cumplir con el RRSIF.[5] A esta cuestión se

1. Si bien, en caso de que la factura sea electrónica, la representación gráfica puede ser sustituida por el contenido que representa el código QR.
2. Para cumplir con los requisitos del reglamento, los sistemas de emisión de facturas no verificables deben incorporar adicionalmente determinadas medidas de control, como son el registro de eventos, la firma electrónica de los registros de facturación y de evento, permitir la posibilidad de exportación de los registros de facturación y de eventos, ofrecer la comprobación de varios requisitos (huella, firma, encadenamiento...) de los registros de facturación y de evento, gestionar alarmas, etc.
3. La remisión voluntaria de los registros de facturación es una forma de cumplir con los requisitos establecidos en el reglamento que hace innecesaria la adopción de otras medidas de control adicionales, a la vez que exime de responsabilidades de conservación y custodia de los registros a los usuarios de los SIF.
4. Véanse, al respecto, las consultas vinculantes de la Dirección General de Tributos V2653-24, de 27 de diciembre de 2024 y V0073-25, de 3 de febrero de 2025.
5. Hay que tener en cuenta que, de acuerdo con el art. 1.3 RRSIF, el reglamento únicamente es aplicable a los obligados tributarios que tengan su domicilio fiscal en territorio común. Por tanto, no es aplicable a quienes estén domiciliados en el territorio del País Vasco o Navarra.

refiere el art. 3 RRSIF, que establece la aplicación del reglamento a los obligados tributarios que utilicen SIF, aunque solo los usen para una parte de su actividad, que sean contribuyentes del IS (excluidas las entidades total o parcialmente exentas); o bien contribuyentes del IRPF que desarrollen actividades económicas; o bien contribuyentes del IRNR que obtengan rentas mediante establecimiento permanente; o bien sean entidades en régimen de atribución de rentas que desarrollen actividades económicas (sin perjuicio de que dichos rendimientos se atribuyan a sus miembros o partícipes). Es importante, pues, que el sujeto obligado realice actividades económicas, tal como establece el art. 29.2.j LGT y desarrolla el art. 3.1 RRSIF.

El RRSIF también resulta de aplicación, según el art. 3.2 RRSIF, a los productores y comercializadores de los SSIF en las cuestiones relativas a sus respectivas actividades de producción y comercialización de los sistemas puestos a disposición de los obligados tributarios. En particular, los desarrolladores de SIF deben afrontar las exigencias reglamentarias para hacer posible asegurar que, durante el periodo de conservación de los registros, no se han producido interacciones indebidas sobre aquellos que los hayan alterado, modificado, interpolado, suprimido o regenerado. Además, deben cumplir con las obligaciones de certificación de los SIF.[6]

Por otra parte, hay que tener en cuenta que, tal como establece el art. 3.3 RRSIF, las disposiciones de este reglamento no son aplicables a los sujetos que utilicen el suministro inmediato de información (SII) en el IVA, ya sea de forma obligatoria o bien voluntaria.

Asimismo, es importante destacar que, según el art. 6 RRSIF, el cumplimiento de lo dispuesto por el reglamento se puede encomendar a los destinatarios de las operaciones o a terceros, siempre que se cumplan los requisitos establecidos por el art. 5 del Reglamento por el que se regulan las obligaciones de facturación, con las facultades otorgadas para llevar a cabo el cumplimiento de la obligación de emisión de factura.

En el supuesto de que se delegue la emisión de factura en el cliente, es este quien, además de expedir materialmente la factura, deberá generar y, en su caso, remitir el registro de facturación de alta que exige el reglamento. Y en el caso de delegación del cumplimiento en terceros, es especialmente relevante el supuesto de los asesores fiscales o gestores administrativos. A este respecto, conviene tener presente que esta posibilidad se prevé expresamente por el art. 7 RRSIF, cuando señala que puede utilizarse un mismo SIF para su cumplimiento por parte de diversos obligados tributarios en el ejercicio de su actividad económica siempre que los registros de facturación de cada obligado tributario se encuentren diferenciados y se cumplan los requisitos exigidos en el reglamento por separado para cada uno de los obligados tributarios.

1.2. Requisitos de los SIF

Una vez analizados los obligados al cumplimiento del RRSIF, conviene detenerse en los requisitos de los SIF, que es una cuestión central de esta normativa, que se desarrolla en el art. 8 RRSIF, así como en los arts. 6 a 9 de la Orden HAC/1177/2024. En este sentido, hay que hacer referencia a la integridad e inalterabilidad de los registros de facturación, la trazabilidad de registros, su conservación, accesibilidad y legibilidad, el registro de eventos, la capacidad de remisión y la disociación de la información (Sánchez Gallardo, 2025, págs. 119-143).

En relación con el primero de los requisitos mencionados, hay que subrayar que los SIF deben garantizar la integridad e inalterabilidad de los registros de facturación de forma que, una vez generados y registrados, no puedan ser alterados sin que el sistema lo detecte y avise de ello. En consecuencia, cualquier necesidad de corrección o anulación de los datos registrados debe ser realizada mediante al menos un registro de facturación adicional posterior, de forma que se conserven inalterables los datos originalmente registrados. La integridad e inalterabilidad de los datos registrados se ha de asegurar utilizando cualquier proceso técnico fiable que garantice el carácter fidedigno y completo de los registros de facturación desde que hayan sido grabados en el sistema informático.

Respecto al requisito de la trazabilidad de los registros, lo que se pretende es garantizar que no haya saltos en la

6. Corresponde a la persona o entidad productora del sistema informático certificar, mediante una declaración responsable, que el sistema informático cumple con lo dispuesto en la normativa (art. 13 RRSIF). La certificación es el medio por el que el usuario puede utilizar el producto con la tranquilidad de que cumple los requisitos establecidos al respecto, los cuales, de otro modo, no serían fáciles de constatar.

secuencia de generación de los registros de facturación, así como que dicha secuencia se corresponda con la de la fecha y hora de generación empleadas. Es decir, se trata de asegurar que se cuenta con todos los registros de facturación generados y que estos están en el mismo orden en que fueron generados.

Los registros generados han de conservarse adecuadamente, es decir, el SIF debe almacenar bajo su control los registros que genere. Para ello, se permite que los registros de facturación generados se almacenen remotamente, incluso en la nube, a condición de que se cumpla la normativa que les sea de aplicación. Adicionalmente, los SIF deben ofrecer un procedimiento de descarga, volcado y archivo seguro de los registros de facturación generados, que deben poder ser exportados a un almacenamiento externo en formato electrónico legible.[7] El plazo para la conservación es el mismo que se establece en el art. 19.1 del Reglamento por el que se regulan las obligaciones de facturación, conforme al cual las facturas deben conservarse durante el plazo de prescripción del IVA, que, con carácter general, es de cuatro años.[8]

El registro de eventos consiste en que el SIF detecte y recoja automáticamente, en el momento en que se produzcan, determinadas interacciones con dicho sistema informático, operaciones realizadas con él o sucesos ocurridos durante su uso, guardando los datos correspondientes a cada uno de ellos, que deben poder ser consultados desde el propio SIF. Se deben firmar electrónicamente todos los registros de eventos que se generen, cumpliendo de forma análoga las especificaciones dadas al respecto para el caso de los registros de facturación.[9]

Por otra parte, los SIF deben tener capacidad de remitir por medios electrónicos a la AEAT de forma continuada, segura, correcta, íntegra, automática, consecutiva, instantánea y fehaciente, todos los registros de facturación generados. Esta capacidad ha de poder utilizarse, por ejemplo, ante un requerimiento de la Agencia Tributaria para comunicar directamente los registros que le sean requeridos, o también para adoptar en cualquier momento la modalidad de sistema de emisión de facturas verificables, con remisión inmediata en línea a la AEAT.

El último de los requisitos de los SIF es el relativo a la disociación de la información. En el art. 8.4 RRSIF se dispone que en los SIF deberá encontrarse debidamente disociado el acceso a la información con trascendencia tributaria del acceso a la posible información confidencial de carácter no patrimonial, de forma que la administración tributaria pueda acceder directamente a la consulta y al resto de funcionalidades exigidas sobre la información de los registros de facturación y de eventos. De esta forma, queda preservada la confidencialidad de otros datos distintos contenidos en el sistema informático, no pudiendo acceder indebidamente a ellos por esta vía.

1.3. Los registros de facturación

Siguiendo con el análisis de las obligaciones que impone el RRSIF, hay que referirse a los registros de facturación, tema regulado en los arts. 9 a 12 RRSIF y en los arts. 10 a 14 de la Orden HAC/1177/2024. A este respecto, conviene destacar que los SIF que sean utilizados por los obligados tributarios deben generar automáticamente un registro de facturación de alta de forma simultánea o inmediatamente anterior a la expedición de cada factura. En función de la forma en que funcione el SIF correspondiente, el registro de facturación así generado se enviará a la Agencia Tributaria o será debidamente conservado.

Hay que tener en cuenta que, una vez producido un registro de facturación de alta, si es necesario cambiar algún dato, debe generarse otro registro que complete, modifique o anule el contenido del anterior, pero no puede alterarse o manipularse el primer registro de facturación. Procede

7. Los SIF que remitan a la AEAT los registros de facturación no están obligados a conservar los registros generados, por cuanto estos ya obran en poder de la administración.
8. De acuerdo con lo que se dispone en el art. 8 de la Orden HAC/1177/2024, por accesibilidad debe entenderse el proporcionar acceso rápido, fácil e intuitivo a las funcionalidades exigidas al SIF por la normativa correspondiente, así como a los registros de facturación generados por el SIF, bien para consultarlos o para descargarlos de forma segura y fidedigna, independientemente de dónde y cómo se encuentren almacenados y conservados. Por su parte, la legibilidad consiste en que los registros de facturación generados tengan la estructura, contenido y formato exigidos, de forma que, mediante procesos electrónicos automáticos, puedan ser leídos y entendidos.
9. Este registro de eventos solo es obligatorio en el caso de los sistemas de emisión de facturas no verificables, no siendo necesario en los casos de sistemas de emisión de facturas verificables (es decir, los SIF que remiten a la AEAT los registros de facturación).

la generación de un registro de facturación de anulación cuando se haya emitido erróneamente una factura y sea por lo tanto necesario anular su correspondiente registro de facturación de alta. En cualquier caso, es importante el mantenimiento o conservación en el SIF de las facturas emitidas, aunque sean erróneas, con su correspondiente numeración, y sin perjuicio de que se anulen posteriormente y se sustituyan por nuevas facturas correctas.

Todos los SIF deben añadir una huella o *hash* a los registros de facturación de alta y de anulación que generen. Se trata del resultado de aplicar una función o algoritmo de cálculo de huella a una determinada información (en este caso, a unos datos del registro). La huella o *hash* de un registro juega un papel fundamental para saber si se ha mantenido la integridad e inalterabilidad de ciertos datos relevantes del registro. Es obligatoria para todos los registros que genere el SIF, tanto los de facturación (alta y anulación) como, en su caso, los registros de evento. Y se debe emplear por todos los SIF, independientemente del modo de funcionamiento (emisión de facturas verificables o no verificables).

Finalmente, hay que señalar que los registros de facturación de alta y de anulación deben ser firmados electrónicamente, cuando se trate de sistemas de emisión de facturas no verificables. En cambio, los sistemas de emisión de facturas verificables no tienen la obligación de firmar electrónicamente los registros de facturación.[10]

Conviene destacar, a nuestro juicio, que toda esta regulación de los requisitos de los SIF y de los registros de facturación debe necesariamente enmarcarse en el ámbito de la armonización fiscal europea. Como ha puesto de relieve la doctrina, aunque el ordenamiento jurídico tributario europeo aún no esté plenamente unificado desde el punto de vista material, sí se está consolidando una infraestructura digital homogénea, donde los Estados miembros interactúan bajo protocolos, formatos y garantías legales compartidas (Sanz Castaño, 2025, págs. 1-16). En este ámbito de la facturación electrónica, en particular, y de la administración electrónica, en general, a nivel europeo, se debería evolucionar hacia un marco de principios comunes, garantías constitucionales para el contribuyente europeo y competencias claramente delimitadas entre los Estados miembros y la Unión Europea. En caso contrario, gran parte de los objetivos de la normativa española de los SIF serán de muy difícil consecución.

1.4. Régimen sancionador

La Ley 11/2021, de 9 de julio, de medidas de prevención y lucha contra el fraude fiscal, introduce una nueva infracción tributaria, en el art. 201 bis LGT, que tiene por objeto asegurar el cumplimiento de la obligación tributaria formal incorporada en el art. 29.2.j LGT. El nuevo art. 201 bis LGT regula la infracción tributaria grave por fabricación, producción, comercialización y tenencia de sistemas informáticos que no cumplan las especificaciones exigidas por la normativa aplicable.

En este precepto legal se establece que constituye infracción tributaria la fabricación, producción y comercialización de sistemas informáticos cuando concurra cualquiera de las siguientes circunstancias: **a)** permitan llevar contabilidades distintas en los términos del art. 200.1.d LGT; **b)** permitan no reflejar, total o parcialmente, la anotación de transacciones realizadas; **c)** permitan registrar transacciones distintas a las anotaciones realizadas; **d)** permitan alterar transacciones ya registradas incumpliendo la normativa aplicable; **e)** no cumplan con las especificaciones técnicas que garanticen la integridad, conservación, accesibilidad, legibilidad, trazabilidad e inalterabilidad de los registros; **f)** no se certifiquen, estando obligado a ello por disposición reglamentaria, los sistemas fabricados, producidos o comercializados. Esta infracción se sanciona con multa de 150.000 euros por cada ejercicio en el que se hayan producido ventas y por cada tipo distinto de sistema informático que sea objeto de la infracción. No obstante, las infracciones por falta de certificación de los SIF se sancionan con multa pecuniaria fija de 1.000 euros por cada sistema comercializado en el que se produzca la falta del certificado.

Asimismo, se dispone que constituye infracción tributaria la tenencia de los sistemas o programas informáticos o electrónicos que no se ajusten a lo establecido en el art. 29.2.j LGT, cuando estos no estén debidamente certifica-

10. La justificación de esta diversa exigencia de firma electrónica es que los sistemas de emisión de facturas verificables remiten automáticamente a la AEAT los registros de facturación generados y este proceso de remisión ya incluye la autenticación del remitente mediante certificado electrónico cualificado, así como medios de transmisión seguros.

dos. Esta infracción se sanciona con multa fija de 50.000 euros por cada ejercicio, cuando se trate de la infracción por la tenencia de sistemas informáticos que no estén debidamente certificados, teniendo que estarlo por disposición reglamentaria, o se hayan alterado o modificado los dispositivos certificados.

Este régimen sancionador ha sido criticado doctrinalmente por considerar que la configuración de esta nueva infracción presenta elementos de colisión con algunos principios fundamentales del derecho sancionador tributario (García Novoa, 2021, págs. 5-6). Así, desde la exigencia de tipicidad, se puede entender afectado este principio, en tanto las especificaciones técnicas, que serán la base de la certificación, son objeto de regulación vía reglamento, siendo, por lo tanto, una norma reglamentaria la que complementa el tipo infractor, lo cual puede producir una quiebra a las exigencias de seguridad jurídica.

Por otra parte, en relación con la culpabilidad, se considera según esta opinión doctrinal que, en tanto se sanciona la mera tenencia del *software*, no necesariamente ligada a su producción o comercialización, estamos ante un tipo infractor semejante a lo que en el ámbito penal son los delitos de mero peligro. Se sanciona un hecho de simple riesgo, sin requerirse una consumación. Por lo que, en este tipo de infracciones, igual que ha exigido la jurisprudencia respecto a los delitos, es necesario asegurar la culpabilidad, verificando la concurrencia de una especie de dolo de peligro. Si se está sancionando por una conducta de mero peligro como es la simple tenencia del software, con independencia de su utilización, la necesaria concurrencia de culpabilidad requiere dolo de peligro, que implica un elemento cognitivo (conocer que el *software* que se tiene es de doble uso, susceptible de ocultar información) y un elemento volitivo.

Asimismo, hay que señalar que el bien jurídico protegido inmediato en el art. 201 bis LGT es el interés público en que los instrumentos informáticos y electrónicos que se utilizan en la confección de los asientos contables y registrales y en la emisión de facturas no estén diseñados para lesionar la corrección de la información tributaria y, más allá, el crédito tributario. Una crítica que puede realizarse es que se trata de un bien jurídico difuso, no se exige lesión o ataque concretos a los bienes jurídicos mediatos, pues el peligro ha sido apreciado ex ante en el objeto material de la acción, por lo cual el juicio de antijuridicidad material en las conductas tipificadas se difumina (Pérez Tena, 2021, págs. 5-46). Por otra parte, también se critica que el art. 201 bis.1.f LGT no protege dicho bien jurídico, sino que tipifica como ilícito un incumplimiento formal insustancial, la no solicitud de certificación de un *software* seguro y fiable. Se protege, pues, un mero interés administrativo formal sin bien jurídico relevante y, por ello, su desatención no constituye una omisión materialmente antijurídica.

Finalmente, también puede criticarse que la previsión legal de sanciones reiteradas cada ejercicio por comercialización o tenencia de software de doble uso, además de no ser respetuosa con el principio de proporcionalidad, genera, en tanto no se haya producido la ruptura jurídica de la acción, un bis in idem prohibido, por sancionarse al mismo sujeto por una única acción y con el mismo fundamento, por lo cual las sanciones subsiguientes previstas legalmente vulneran el art. 25.1 de la Constitución Española.

2. El fomento del cumplimiento voluntario

Además del principal objetivo de control tributario y lucha contra el fraude fiscal, la normativa sobre los SIF tiene también el objetivo del fomento del cumplimiento voluntario por parte del obligado tributario, mediante la automatización del suministro de información. Se trata de una mejora en la transparencia de la aplicación de los tributos, que, sin duda, tendrá como consecuencia la correspondiente mejora en el cumplimiento de las obligaciones tributarias por parte de los titulares de las actividades económicas (Gómez Requena, 2025, pág. 79-82).

Todo ello tiene que ver con las previsiones en el RRSIF sobre los sistemas de emisión de facturas verificables. Como ya se ha comentado, en el reglamento se regulan dos modalidades de funcionamiento de los SIF: por un lado, los sistemas de emisión de facturas no verificables, que no remiten los registros de facturación a la AEAT, sino que únicamente los almacenan y los tienen disponibles por si se los requiere la administración; y, por otro lado, los sistemas de emisión de facturas verificables, que son los que, de forma voluntaria, remiten en línea los registros de facturación correspondientes a las facturas expedidas por ellos a la AEAT.

Los sistemas de emisión de facturas no verificables deben incorporar adicionalmente determinadas medidas de con-

trol, como son el registro de eventos, la firma electrónica de los registros de facturación y de evento, permitir la posibilidad de exportación de los registros de facturación y de eventos, ofrecer la comprobación de varios requisitos (huella, firma, encadenamiento...) de los registros de facturación y de evento, gestionar alarmas, etc. Mientras que en los sistemas de emisión de facturas verificables no es necesaria la adopción de estas medidas de control adicionales, y se exime de responsabilidades de conservación y custodia de los registros a los usuarios de los SIF.

Los sistemas de emisión de facturas verificables se encuentran regulados en los arts. 15 y 16 RRSIF y en los arts. 16 y 17 de la Orden HAC/1177/2024. Así, se dispone por el reglamento que los obligados tributarios que utilicen SIF para el cumplimiento de la obligación de facturación pueden remitir voluntariamente a la AEAT, de forma automática y segura por medios electrónicos, todos los registros de facturación generados por dichos sistemas informáticos, de acuerdo con las especificaciones técnicas que se establezcan para la remisión.

Se presume que los sistemas de emisión de facturas verificables cumplen por diseño con los requisitos establecidos en el RRSIF, garantizando, pues, la integridad, conservación, accesibilidad, legibilidad, trazabilidad e inalterabilidad de los registros de facturación generados por ellos. Además, se dispone expresamente que no se les aplica lo dispuesto en el art. 14.2 RRSIF, es decir, la posibilidad de que la AEAT requiera una copia de los registros de facturación conservados. Tampoco tendrán la obligación de realizar la firma electrónica de los registros de facturación a la que se refiere el art. 12 RRSIF, siendo suficiente con que calculen la huella o *hash* de dichos registros.[11]

Cabe plantearse cuáles son las ventajas que tiene la emisión de facturas verificables, desde el punto de vista del usuario. En primer lugar, los usuarios de los SIF no están obligados a almacenar y exportar, así como conservar accesibles y legibles los registros de facturación y los registros de evento. En segundo lugar, no han de recibir requerimientos de la AEAT para que remitan posteriormente los registros de facturación de sus facturas expedidas (pues esta información ya está a disposición de la administración), con el consiguiente ahorro de recursos que ello supone. En tercer lugar, no están obligados a asegurar que, en todo momento, el reloj empleado por el SIF para datar los registros de facturación y de evento tiene la hora exacta (con un margen de error de un minuto). En cuarto lugar, permite a sus clientes comprobar que las facturas emitidas han quedado registradas en la AEAT por medio de los códigos QR que se incorporan a las facturas,[12] con todo lo que ello supone en cuanto a transparencia y calidad en el cumplimiento tributario. En quinto lugar, permiten disponer de servicios electrónicos de la AEAT que les faciliten la presentación de los libros registros de facturas expedidas, completándolos a partir de la información que ya se suministró al remitir los registros de facturación, así como ayudas en la confección de sus autoliquidaciones. Y, finalmente, está previsto que la AEAT ponga operativo un servicio que permita la descarga de la totalidad de los registros de facturación emitidos y comunicados por cada obligado tributario, así como la descarga de los registros emitidos por los proveedores de ese mismo obligado tributario, en la medida que también utilicen la emisión de facturas verificables (Sánchez Gallardo, 2025, págs. 146-147).

Sin embargo, la remisión de los registros de facturación a la AEAT no exime de la obligación de confeccionar el libro registro de facturas emitidas ni de presentar la declaración anual de operaciones con terceras personas (modelo 347) ni de presentar la declaración recapitulativa de operaciones intracomunitarias (modelo 349).

Asimismo, es importante tener en cuenta la posibilidad de remisión de información de la factura por parte de los destinatarios, cuestión regulada en el art. 17 RRSIF. El receptor de la factura puede proporcionar de forma voluntaria determinada información de esta a la AEAT, facilitando

11. No debe confundirse la emisión de facturas verificables con el cumplimiento del deber de envío de las facturas a los clientes. Esta obligación de envío de las facturas emitidas, cuando se efectúa por un SIF que cumple las especificaciones del reglamento, no tiene ninguna diferencia respecto a las facturas emitidas por otros sistemas. Por lo tanto, la forma en que se expida y reciba la factura depende de que sea facturación en papel o electrónica y, en este segundo caso, de si es estructurada o no.
12. En dichas facturas, además, también ha de aparecer la frase «Factura verificable en la sede electrónica de la AEAT» o «Verifactu».

los datos contenidos en el código QR de la factura.[13] En aquellos casos en los que en la factura figure la frase «Factura verificable en la sede electrónica de la AEAT» o «Verifactu», esta remisión por parte del receptor le permite verificar que la factura recibida ha sido remitida a la AEAT por su emisor. Esta posibilidad está abierta a cualquier destinatario de facturas, sea empresario o profesional, o bien sea consumidor final. La remisión de información no tiene la consideración de denuncia pública. Es importante destacar que esta información puede ser utilizada por la AEAT para el ejercicio de sus competencias para la aplicación de los tributos y, en particular, en sus funciones de control tributario.

3. La digitalización de la actividad empresarial y profesional

La normativa sobre los SIF, sin duda, provocará un avance en la digitalización de la actividad empresarial y profesional, especialmente en las pequeñas y medianas empresas. El efecto de la utilización de sistemas informáticos de facturación que cumplan con una serie de requisitos que los hacen más sólidos y transparentes incidirá en una modernización de la gestión empresarial.

La digitalización de la actividad empresarial y profesional ha sido y es uno de los objetivos de la normativa tributaria que, desde hace algunos años, ha apostado claramente por el empleo de las tecnologías de la información y la comunicación en las relaciones de la administración con los obligados tributarios. Algunos de los hitos más importantes en este proceso de digitalización y fomento de la administración electrónica son la generalización de las declaraciones tributarias electrónicas, el empleo de las notificaciones electrónicas, la facturación electrónica en el sector público, el suministro inmediato de información en el IVA, el suministro inmediato de libros contables en los impuestos especiales y la futura facturación electrónica obligatoria entre empresarios y profesionales.[14]

Destacan dos de los ámbitos de digitalización señalados, por su proximidad con la normativa de los SIF: el suministro inmediato de información en el IVA y la facturación electrónica obligatoria entre empresarios y profesionales.

El SII comporta la llevanza de los libros registro (los libros registro de facturas expedidas, de facturas recibidas, de bienes de inversión y de determinadas operaciones intracomunitarias) a través de la sede electrónica de la AEAT, mediante el suministro prácticamente inmediato de los registros de facturación. Los contribuyentes deben remitir a la administración tributaria de forma continuada los detalles sobre la facturación por vía electrónica, y con esta información actualizada se van configurando, casi en tiempo real, los libros registro del tributo. En consecuencia, se trata de uno de los cambios más significativos que se han introducido en la gestión del IVA desde la creación de este impuesto (Delgado García, 2017, págs. 101-124; Longás Lafuente, 2017, pág. 50; Ruiz Zapatero, 2017, pág. 2).

Conviene aclarar que mediante este sistema de gestión del IVA no se está estableciendo la obligación de enviar las facturas a la AEAT, pues lo que se debe remitir son los campos de los registros de facturación que se concretan en la Orden HFP/417/2017, de 12 de mayo, por la que se regulan las especificaciones normativas y técnicas que desarrollan la llevanza de los libros registro del IVA a través de la sede electrónica de la AEAT.

El SII presenta un doble ámbito de aplicación subjetivo, pues en algunos casos resulta de aplicación obligatoria, mientras que en otros supuestos el contribuyente puede optar por acogerse al mismo. El SII, según disponen los arts. 62.6 y 71.3.5.º del Reglamento del IVA, es obligatorio para los empresarios y profesionales y otros sujetos pasivos cuyo periodo de liquidación coincida con el mes natural: grandes empresas (facturación superior a 6.010.121,04 euros en el año anterior), grupos de IVA e inscritos en el registro de devolución mensual del IVA. Por otro lado, podrán utilizar de forma voluntaria el SII quienes ejerzan la opción a través de la correspondiente declaración censal, en cuyo caso, su período de declaración será mensual y la

13. A tal efecto, la Agencia Tributaria ha de facilitar una ruta específica en su sede electrónica o a través de la aplicación que al efecto ponga a su disposición para recibir dicha información. El acceso a la sede electrónica o a la aplicación ha de mostrar los datos del código QR en formato legible.
14. La normativa sobre los SIF se enmarca, pues, en el proceso de potenciación de la administración digital. Véase al respecto Delgado García (2023, págs. 405-421).

opción se entenderá prorrogada para los años siguientes en tanto no se produzca la renuncia a la misma.

Un paso más en el proceso de digitalización de la gestión empresarial es la facturación electrónica obligatoria entre empresarios y profesionales, que se incluye como una de las medidas normativas de la Ley 18/2022, de 28 de septiembre, de Creación y Crecimiento de Empresas (LCCE). El art. 12 LCCE establece que todos los empresarios y profesionales deberán expedir, remitir y recibir facturas electrónicas en sus relaciones comerciales con otros empresarios y profesionales.

En cuanto a la entrada en vigor de este régimen de facturación electrónica obligatoria, hay que tener en cuenta los períodos transitorios que se establecen en la norma legal, atendiendo al tamaño de los sujetos afectados, puesto que la incidencia de estas nuevas obligaciones formales no es idéntica en los profesionales y empresas de menor tamaño que en las grandes empresas, con una mayor capacidad de acceso a las tecnologías de la información y la comunicación.

Así, las previsiones legales contenidas en el art. 12 LCCE producirán efectos, para los empresarios y profesionales cuya facturación anual sea superior a ocho millones de euros, al año de aprobarse el desarrollo reglamentario (que actualmente todavía no ha sido aprobado). Para el resto de los empresarios y profesionales, este artículo producirá efectos a los dos años de aprobarse el desarrollo reglamentario.[15]

4. La información y asistencia al obligado tributario

A pesar de las indudables ventajas que aporta una mayor digitalización de la actividad empresarial y profesional, hay que tener en cuenta los posibles inconvenientes derivados de la denominada brecha digital y la eventual afectación a los derechos y garantías de los obligados tributarios. Por ello, es importante destacar el papel que debe desempeñar la información y asistencia al obligado tributario, al objeto de facilitar un mejor cumplimiento de la normativa en este ámbito (Delgado García, 2022, págs. 73-99).

Por lo que se refiere a la asistencia tributaria, la normativa de los SIF, cuando se emplean sistemas de emisión de facturas verificables, prevé algunas actuaciones de asistencia destacables. Así, hay que señalar que está previsto el desarrollo de la posibilidad de integrar los registros de facturación generados y remitidos a la AEAT por medio de los sistemas de emisión de facturas verificables en el contenido del libro registro de facturas expedidas del IVA, así como en los libros registros de ventas e ingresos del IRPF.[16] También se prevé que los destinatarios de las facturas cuya información haya sido remitida por sistemas de emisión de facturas verificables, además de poder verificar en línea la información de esas facturas recibidas, puedan descargarla para integrarla en sus libros registros.

En relación con la información al obligado tributario en este campo, destaca la existencia del informador verifactu, que la Agencia Tributaria ha puesto a disposición de los obligados tributarios en su sede electrónica. Se trata de una herramienta que ofrece información tributaria sobre los requisitos que deben cumplir los sistemas y programas informáticos o electrónicos de facturación a empresarios y profesionales y los registros de facturación. El usuario debe seleccionar las opciones que correspondan en los desplegables que se le van mostrando. Una vez seleccionados, los resultados se muestran al final, pudiendo obtener una copia del resultado de la consulta introduciendo la dirección de correo electrónico donde se envía la información en formato PDF.

Respecto a la colaboración social en la gestión de los tributos, conviene resaltar la posibilidad de que las empresas desarrolladoras de software puedan remitir los registros de facturación de los obligados tributarios en el marco de lo dispuesto en el RRSIF. Como terceros que actúen en representación del obligado tributario, tales empresas

15. Es importante destacar, asimismo, que la entrada en vigor de la facturación electrónica obligatoria entre empresarios y profesionales está supeditada a la obtención de la excepción comunitaria a los arts. 218 y 232 de la Directiva 2006/112/CE, de 28 de noviembre de 2006, relativa al sistema común del IVA, que establece como requisito el consentimiento del destinatario de la factura electrónica.
16. A estos efectos, la AEAT pondrá a disposición de los usuarios de estos SIF la información que le sea remitida de las facturas expedidas y facilitará las herramientas necesarias que permitan completar en la sede electrónica la llevanza de los libros registros mencionados.

desarrolladoras de *software* pueden suscribir el acuerdo de colaboración social en la aplicación de los tributos (tipo 17. Empresas de sistemas informáticos de facturación).

En definitiva, ante la imposición de la relación electrónica, tanto con la administración como en el ámbito empresarial y profesional, hay que apostar, además de la potenciación de los servicios de información y asistencia, por una normativa clara y unas garantías específicas que acrediten o aseguren que los obligados a la concreta relación electrónica tienen acceso efectivo a los medios electrónicos.[17] De lo contrario, podría provocar la existencia de discriminaciones o indefensiones en la relación administrativa, así como distorsiones indeseadas en las actividades económicas llevadas a cabo por empresarios y profesionales.

Conclusiones

La normativa sobre los SIF tiene un claro objetivo de lucha contra el fraude fiscal. En el momento de emisión de cualquier factura, el SIF deberá generar y guardar o remitir a la AEAT un resumen de la factura que incorpore algunas medidas de seguridad que garanticen el cumplimiento de los requisitos a los que se refiere la norma legal: integridad, conservación, accesibilidad, legibilidad, trazabilidad e inalterabilidad de los registros. Además, se establece la obligación de utilizar sistemas informáticos de facturación certificados, así como la obligación de que los SIF incluyan un código QR en las facturas expedidas, cuya lectura permita a quien las reciba remitir algunos de sus datos a la Agencia Tributaria para su verificación. Todo ello, pues, en la línea de reforzar el control tributario, permitiendo acceder a una información que posibilite las labores administrativas de comprobación tributaria.

Ahora bien, además de este principal objetivo de control tributario y lucha contra el fraude fiscal, la normativa sobre los SIF tiene también otras metas que merecen ser objeto de análisis. Así, hay que hacer referencia al fomento del cumplimiento voluntario por parte del obligado tributario. En efecto, con esta normativa, se pretende también facilitar el cumplimiento voluntario mediante la automatización del suministro de información. Se prevé que el destinatario de la factura capture un resumen de la información contenida en esta y la envíe a la Agencia Tributaria, que responderá indicando si dicha información consta ya en su sistema o no y, en su caso, si coincide con los datos que suministra el destinatario. De esta forma, se incrementa la transparencia del sistema tributario, ya que, con independencia de que el emisor de la factura suministre o no los registros de facturación a la AEAT, el destinatario siempre tendrá la posibilidad de realizar dicho suministro. Esta mejora en la transparencia de la aplicación de los tributos, sin duda, tendrá como consecuencia la correspondiente mejora en el cumplimiento de las obligaciones tributarias por parte de los titulares de las actividades económicas.

También es importante tener en cuenta que la aplicación de la normativa sobre los SIF, sin duda, provocará un avance en la digitalización de la actividad empresarial y profesional. Es especialmente necesaria esta transformación digital de la gestión en las pequeñas y medianas empresas. El empleo de SIF certificados repercutirá en una mejor gestión de la información contable, lo que, a su vez, ha de provocar una modernización de las empresas y profesionales afectados. Se trata de un paso más en el fortalecimiento de la administración electrónica tributaria y la digitalización empresarial, que ya comenzó hace unos años con la generalización de las declaraciones tributarias electrónicas, el empleo de las notificaciones electrónicas, la facturación electrónica en el sector público, el suministro inmediato de información en el IVA, el suministro inmediato de libros contables en los impuestos especiales y la futura facturación electrónica obligatoria entre empresarios y profesionales.

No obstante, a pesar de las indudables ventajas que aporta una mayor digitalización de la actividad empresarial y profesional, no hay que olvidar los posibles inconvenientes derivados de la denominada brecha digital y la eventual afectación a los derechos y garantías de los obligados tributarios. En este sentido, es importante destacar el papel

17. Uno de los aspectos que hay que tener en consideración a la hora de establecer soluciones es huir de las uniformidades, teniendo presente la variedad de circunstancias y necesidades de la ciudadanía, de forma que, dentro del grupo de empresarios y profesionales, hay que tener en cuenta que existen muchas diferencias en cuanto al acceso a las tecnologías de la información. Véase Díaz Calvarro (2021, pág.7). En el mismo sentido, véase Gil Rodríguez (2023, págs. 105-147).

que debe desempeñar en este ámbito la información y asistencia al obligado tributario, así como la colaboración social que puede producirse por parte de determinadas entidades, especialmente, los proveedores de sistemas informáticos, al objeto de facilitar un mejor cumplimiento de la normativa en este ámbito.

Referencias bibliográficas

DELGADO GARCÍA, A.M. (2017). «La regulación del suministro inmediato de información». *Revista Quincena Fiscal*, n.º 20. DOI: https://doi.org/10.7238/idp.v0i26.3130

DELGADO GARCÍA, A.M. (2022). «Información y asistencia tributaria para las empresas a través de Internet». En: OLIVER CUELLO, R. (dir.). *Las tecnologías de la información en la actividad empresarial: aspectos legales y fiscales*. Pamplona: Aranzadi.

DELGADO GARCÍA, A.M. (2023). «Los servicios de ayuda de la administración tributaria para el cumplimiento de las obligaciones fiscales». En: OLIVER CUELLO, R. (dir.). *El derecho, la empresa y la comunicación en la sociedad de la información*. Bosch Editor: Barcelona. DOI: https://doi.org/10.2307/jj.11786266.20

DÍAZ CALVARRO, J.M. (2021). «La brecha digital y su repercusión en los derechos y garantías de los contribuyentes: análisis crítico». *Revista Quincena Fiscal*, n.º 10.

GARCÍA NOVOA, C. (2021). «Algunas novedades de la Ley de Medidas de Prevención y Lucha contra el Fraude Fiscal. Software de doble uso, lista de morosos y prohibición de amnistías fiscales». *Revista Quincena Fiscal*, n.º 17.

GIL RODRÍGUEZ, I. (2023). «La brecha digital, un reto pendiente para la administración tributaria». *Revista Nueva Fiscalidad*, n.º 2. DOI: https://doi.org/10.14679/2086

GÓMEZ JIMÉNEZ, C. (2021). «La modificación de la Ley General Tributaria efectuada por la Ley 11/2021, de medidas de prevención y lucha contra el fraude fiscal». *Carta Tributaria*, n.º 79.

GÓMEZ REQUENA, J.A. (2025). *La digitalización de las relaciones tributarias en el desarrollo de un sistema tributario inteligente*. Barcelona: Atelier. DOI: https://doi.org/10.71237/MjvRAb4M

LONGÁS LAFUENTE, A. (2017). «Suministro inmediato de información en la gestión de los libros del IVA». *Revista de Contabilidad y Tributación*, n.º 408. DOI: https://doi.org/10.51302/rcyt.2017.4387

PÉREZ TENA, J.R. (2021). «La lucha contra el software de doble uso en la Ley General Tributaria: un ensayo de infracciones tributarias permanentes». *Revista de Contabilidad y Tributación*, n.º 463. DOI: https://doi.org/10.51302/rcyt.2021.7437

RUIZ ZAPATERO, G. (2017). «Base legal de la obligación de suministro electrónico a la administración de todos los registros de facturación». *Revista Quincena Fiscal*, n.º 10.

SÁNCHEZ GALLARDO, F.J. (2025). *Memento Experto Verifactu*. Madrid: Lefebvre.

SÁNCHEZ PEDROCHE, J.A. (2021). «Comentarios a la nueva Ley de represión del fraude fiscal». *Revista de Contabilidad y Tributación*, n.º 461-462. DOI: https://doi.org/10.51302/rcyt.2021.7425

SANZ CASTAÑO, J.F. (2025). «Digitalización y tecnologías disruptivas, de la interconexión técnica a la integración normativa: ¿hacia un ordenamiento jurídico tributario europeo?». *Revista Quincena Fiscal*. n.º 11. DOI: https://doi.org/10.69592/2952-1955-EXTRA-MAYO-2025-ART-2

SERRANO ANTÓN, F. (2022). «La digitalización como factor de cambio en los sistemas de facturación y suministro de información: hacia una tributación fluida basada en el data analytics y la inteligencia artificial». *Revista Nueva Fiscalidad*, n.º 2.

Cita recomendada

OLIVER CUELLO, Rafael (2026). «Algunas consideraciones sobre los sistemas informáticos de facturación». *IDP. Revista de Internet, Derecho y Política*, núm. 44. UOC. [Fecha de consulta: dd/mm/aa]. DOI: http://dx.doi.org/10.7238/idp.v0i44.9800374

Sobre el autor

Rafael Oliver Cuello
Catedrático de Derecho Financiero y Tributario. Universitat Internacional de Catalunya
roliver@uic.es

Catedrático de Derecho Financiero y Tributario. Decano de la Facultad de Derecho. Universitat Internacional de Catalunya. Profesor colaborador en la Universitat Oberta de Catalunya y en ESERP. Doctor en Derecho (Universitat de Barcelona, 1997). Colegiado en el Ilustre Colegio de la Abogacía de Barcelona. Anteriormente, catedrático en ESERP - Universitat de Vic (2014-2024), profesor agregado en la Universitat Pompeu Fabra (2004-2013), profesor titular en ESADE - Universitat Ramon Llull (2001-2004), profesor titular interino en la Universitat de Lleida (1997-2001).

IDP
REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Cuestiones sobre la fiscalidad de los creadores de contenido e *influencers*: criterios de sujeción y aplicación del correspondiente convenio para evitar la doble imposición entre España y Andorra

Antoni Bergas Forteza
Universidad de las Illes Balears

Fecha de presentación: julio 2025
Fecha de aceptación: noviembre 2025
Fecha de publicación: marzo 2026

Resumen

El presente trabajo analiza el régimen fiscal aplicable a los creadores de contenido digital, con especial atención a los denominados *youtubers* e *influencers* que trasladan su residencia a jurisdicciones con menor carga tributaria, como el Principado de Andorra. La investigación parte del fenómeno migratorio digital y examina su trasfondo legal, económico y ético, abordando la normativa española y andorrana del IRPF, así como el convenio para evitar la doble imposición suscrito entre ambos Estados. El autor argumenta que, más allá del lugar de residencia formal, debe atenderse a la naturaleza artística de la actividad y al lugar de realización de la misma –criterios fundamentales en el marco del derecho tributario internacional–. Asimismo, se introduce el papel determinante de la audiencia y de los ingresos derivados de la notoriedad en un país determinado como elementos clave para fijar la sujeción tributaria. En este sentido, se plantea una interpretación funcional del principio de territorialidad fiscal, especialmente aplicable en un contexto de digitalización y de globalización de los modelos de negocio.

Palabras clave

plataformas digitales; creadores de contenido; *youtubers*; *influencers*; Andorra; convenio para evitar la doble imposición; fiscalidad

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Issues regarding the taxation of content creators and influencers: criteria for determining being subject to and implementing the agreement to prevent double taxation between Spain and Andorra

Abstract

This paper examines the tax system applicable to digital content creators, with particular focus on so-called YouTubers and influencers who relocate their residence to jurisdictions with lower tax burdens, such as the Principality of Andorra. The study begins with the digital migration phenomenon and explores its legal, economic, and ethical background, analysing the Spanish and Andorran regulations of the IRPF, as well as the agreement to avoid double taxation signed between both states. The author contends that, beyond the formal place of residence, the artistic nature of the activity and the location where it is performed must be considered – essential criteria within the framework of international tax law. Furthermore, the influential role of the audience and the income generated by notoriety in a particular country are introduced as key factors in determining the taxation. In this regard, a functional interpretation of the principle of tax territoriality is proposed, especially relevant in a context characterised by digitization and globalization of business models.

Keywords

digital platforms; content creators; YouTubers; influencers; Andorra; double taxation avoidance agreement; taxation

Introducción

La migración de los creadores de contenido digital, comúnmente denominados *youtubers* (por ser esta plataforma digital donde se comparte el material audiovisual creado), e *influencers*[1] desde España hacia Andorra[2] ha generado un intenso debate en los últimos años.[3] Este fenómeno pone de manifiesto las complejidades fiscales y éticas que rodean a los creadores de contenido digital y su contribución al sistema tributario de sus países de origen, además de mostrar un cambio en los modelos económi-

1. Existen numerosas definiciones del término «creador de contenido» o del de «influencer», sin embargo, todos ellas reúnen las mismas características: para el caso de un creador de contenido, es el material audiovisual o de texto que comparte esta persona a través de distintas plataformas digitales o redes sociales, ya sea para entretener o informar, destinado a una audiencia; a partir de este material compartido y de la gran audiencia y seguidores que aglomeran, existe por parte de esta persona la posibilidad de influir sobre otros, comportando ello su correspondiente atractivo comercial. Véase, entre otros, Freberg, Graham, McGaughey y Freberg (2011), Hudders, de Jans y de Veirman (2021) y Joshi, Lim, Jagani y Kumar (2023).
2. Las estadísticas del Gobierno de Andorra muestran como en los últimos años (de 2021 a 2024) la mayor inmigración recibida ha sido por parte de nacionales españoles, siendo la franja de edad más común de 20 a 29 años y de 30 a 39 años. Estos datos alimentan la idea de la migración de los creadores de contenido (profesionales jóvenes y españoles) hacia Andorra en busca de unas condiciones fiscales más favorables. Pueden consultarse dichas estadísticas oficiales en: https://www.estadistica.ad/portal/apps/sites/#/estadistica-ca/pages/estadistiques-i-dades-detall?Idioma=ca&N2=605&N3=630&DV=1250
3. Este debate se aviva cada vez que un youtuber o influencer anuncia su traslado a Andorra, justificándolo o no en base a un ahorro fiscal. Por ejemplo, pueden consultarse los artículos periodísticos de Daniel Lara y Laura Delle Femmine de fecha 18 de enero de 2021 en el periódico *El País* titulado «El Rubius anuncia que se muda a Andorra y reabre el debate sobre el pago de impuestos de los "influencers"»; o, el del periódico *elDiario*, de fecha 27 de octubre de 2025, titulado «La influencer Cocina con Coqui da explicaciones sobre su mudanza a Andorra tras perder miles de seguidores».

cos y de entretenimiento actuales,[4] una digitalización del entretenimiento. Una de las principales motivaciones para este traslado es la significativa diferencia en la carga fiscal entre ambos países. En España, en líneas generales y a modo orientativo, el Impuesto sobre la Renta de las Personas Físicas (IRPF) es progresivo, alcanzando un tipo impositivo de hasta un 47 % para ingresos anuales superiores a 300.000 euros. En contraste, Andorra establece un tipo impositivo máximo del 10% para rentas superiores a 40.000 euros. Esta disparidad representa un atractivo considerable para quienes perciben ingresos elevados a través de plataformas digitales.

No obstante, establecer la residencia fiscal en Andorra implica cumplir ciertos requisitos legales. Es esencial residir de forma efectiva en el país al menos 183 días al año y demostrar que el centro de intereses económicos y personales se encuentra en el Principado –a semejanza de la residencia fiscal española a efectos de IRPF–. El incumplimiento de estas condiciones puede derivar en sanciones por parte de la Agencia Tributaria española, que puede llegar a considerar que, de no existir esta residencia efectiva, la potestad tributaria para gravar la obtención de determinadas rentas le corresponde a España. Ahora bien, estos criterios de residencia de personas físicas comportan que este sistema de sujeción pueda considerarse desactualizado (Sánchez-Archidona Hidalgo, pág. 107) y obsoleto, más aún a la luz de los nuevos modelos económicos y de la capacidad de operar en otros territorios sin presencia «física» alguna.

La comunidad de creadores de contenido, así como la opinión de la ciudadanía española, presenta posturas diversas respecto a esta práctica. Este éxodo de creadores de contenido digital también puede tener sus implicaciones económicas y sociales.[5] Mientras que Andorra busca revitalizar su economía atrayendo a estos profesionales, España se enfrenta a la posible disminución de sus ingresos tributarios y al debate sobre la equidad fiscal. Además, como se ha advertido, la opinión pública se muestra dividida, con sectores que critican la falta de solidaridad de quienes buscan reducir su carga impositiva y otros que entienden la decisión como una respuesta legítima a la alta presión fiscal y al uso más o menos eficiente de los recursos públicos.

La decisión de los *youtubers* e *influencers* de trasladar su residencia fiscal a Andorra es un tema complejo que involucra aspectos legales, éticos, económicos y, sobre todo, fiscales. Mientras algunos priorizan la optimización fiscal, otros valoran los beneficios y los servicios que ofrece su país de origen. Este fenómeno continúa alimentando el debate sobre la justicia tributaria y la responsabilidad social de los nuevos profesionales digitales. Ahora bien, aunque el traslado efectivo de la residencia fiscal de España a Andorra parezca una decisión firme e irrefutable a los efectos de someter a tributación las rentas generadas por estos *youtubers* o influencers por su creación de contenido digital, debe estudiarse con detalle lo establecido en el correspondiente convenio fiscal para evitar la doble imposición entre España y Andorra y analizar las distintas consideraciones y elementos fiscales que integran la regulación de este tipo de actividades.

El propósito de este trabajo será analizar la situación fiscal entre España y Andorra, estudiar la consideración, a efectos tributarios, que tienen estos creadores de contenido digital y sus beneficios económicos, así como plantear posibles elementos que permitan sujetar dichos beneficios a imposición en el Estado de la fuente. De este modo, desde una perspectiva estrictamente fiscal, el análisis se centrará en examinar tres cuestiones fundamentales. En primer lugar, determinar las cuestiones previas y la relación fiscal entre España y Andorra. En segundo lugar, se estudiará la calificación jurídica de los rendimientos obtenidos, diferenciando entre ingresos procedentes de actividades económicas, cesión de derechos de imagen o posibles rentas artísticas, con el fin de precisar su tratamiento impositivo tanto en el IRPF español como en el IRPF andorrano. Finalmente, se abordará la aplicación práctica del principio de

4. «[L]a movilidad y posibilidades de trabajar desde cualquier lugar del mundo que permiten estas profesiones puede llevar aparejado el traslado de residentes españoles a otros Estados. De aquí pueden extraerse dos ideas. La primera, y obviando el hecho de que puede haber razones extrafiscales para esos desplazamientos (como simplemente conocer otros lugares), cabría reflexionar sobre si la «huida» hacia otros territorios se debe a regímenes fiscales más favorables fuera de nuestras fronteras. Esto es, si nuestro sistema tributario es lo suficientemente competitivo para retener talento. Segundo, la no permanencia en territorio español no impediría que esa persona siguiera teniendo la condición de residente fiscal en España si mantiene aquí su centro de intereses económicos o un nexo familiar. Lo que implicaría acudir al CDI en cuestión (si lo hubiera) para resolver el posible conflicto de doble residencia» (Gil García, 2022).
5. «Los *influencers* –individuos con muchos seguidores– desempeñan un papel fundamental a la hora de influir en las normas sociales en materia de cumplimiento tributario» (di Gioacchino y Fichera, 2022).

fuente en el entorno digital, analizando hasta qué punto la localización de la audiencia y la consideración de artista del creador de contenido o *influencer* pueden justificar la tributación en el Estado donde se genera el valor económico real. Estas cuestiones fiscales resultan esenciales para comprender la interacción entre las normas nacionales, los convenios internacionales y las nuevas formas de obtención de rentas en la economía digital.

1. Cuestiones previas y relación fiscal entre España y Andorra

Aunque el traslado de determinados profesionales del ámbito del entretenimiento digital para lograr mayores ventajas fiscales suscite en la opinión pública la consideración de que Andorra es un paraíso fiscal, esta idea debe ser rechazada desde el principio.

La disposición adicional primera de la Ley 36/2006, de 29 de noviembre, de medidas para la prevención del fraude fiscal, contiene la definición de paraíso fiscal, de nula tributación y de efectivo intercambio de información tributaria. Respecto de la definición de paraíso fiscal sus apartados 1 y 2 establecen:

«1. Tienen la consideración de paraísos fiscales los países y territorios que se determinen reglamentariamente [periódicamente, el Ministerio de Hacienda y Función Pública publica un listado de países que tiene la consideración de paraísos fiscales o jurisdicciones no cooperativas].

2. La relación de países y territorios que tienen la consideración de paraísos fiscales se podrá actualizar atendiendo a los siguientes criterios:

La existencia con dicho país o territorio de un convenio para evitar la doble imposición internacional con cláusula de intercambio de información, un acuerdo de intercambio de información en materia tributaria o el Convenio de Asistencia Administrativa Mutua en Materia Fiscal de la OCDE y del Consejo de Europa enmendado por el Protocolo 2010, que resulte de aplicación.

Que no exista un efectivo intercambio de información tributaria en los términos previstos por el apartado 4 de esta disposición adicional.

Los resultados de las evaluaciones inter pares realizadas por el Foro Global de Transparencia e Intercambio de Información con Fines Fiscales».

De esta forma, la condición de paraíso fiscal no vendrá marcada tanto por sus condiciones fiscales más o menos favorables, sino por su efectivo intercambio de información económica y tributaria. Al respecto, en 2011 entró en vigor el Acuerdo entre el Reino de España y el Principado de Andorra para el intercambio de información en materia fiscal de 14 de enero de 2010, lo que implicó que Andorra dejase de ser considerado como paraíso fiscal o jurisdicción no cooperativa para España.[6]

Posteriormente, ya en 2015, se firmó entre ambos países –España y Andorra– un convenio para evitar la doble imposición en materia de impuestos sobre la renta y prevenir la evasión fiscal.

Este conjunto de trabajos y la remodelación tributaria por parte de Andorra también tuvieron su repercusión a nivel europeo. Andorra, al formar parte de la Unión Aduanera de la Unión Europea y tener convenio en materia monetaria, y después de los acuerdos adoptados con España, llegó, en 2016, a un Acuerdo con la Unión Europea respecto a la transparencia fiscal exigida en el resto de la Unión. Dicha cooperación en materia de información y transparencia fiscal comportaría, ya en 2018, un intercambio efectivo de información. La ley nacional de Andorra que permitió llevar a la práctica dicho Acuerdo fue la *Llei 10/2017, del 25 de maig, d'intercanvi d'informació mitjançant sol·licitud prèvia i d'intercanvi d'informació espontani en matèria fiscal* y su correspondiente reglamento (*Decret del 31-05-2017 d'aprovació del Reglament de desenvolupament de la Llei 10/2017, d'intercanvi d'informació mitjançant*

6. Puede consultarse la lista actual de jurisdicciones no cooperativas para España en el siguiente enlace: https://sede.agenciatributaria.gob.es/Sede/ayuda/manuales-videos-folletos/manuales-practicos/manual-tributacion-no-residentes/anexos/jurisdicciones-no-cooperativas.html; para el caso de la Unión europea, su lista puede consultarse en: https://www.consilium.europa.eu/es/policies/eu-list-of-non-cooperative-jurisdictions/#0. De ambas listas puede observarse como para el caso de España existe una lista más extensa de jurisdicciones no cooperativas que para la Unión Europea.

sol·licitud prèvia i d'intercanvi d'informació espontani en matèria fiscal).

Con todo, debe partirse de la idea ya indicada de que Andorra no es un «paraíso fiscal», siendo conveniente centrarse ahora en la clasificación, a efectos tributarios, de los rendimientos económicos generados por los conocidos como *youtubers* e *Influencers*. Asimismo, será necesario ubicar dicha obtención de beneficios en el propio convenio tributario aplicable entre España y Andorra.

2. Rendimientos económicos derivados de la profesión de youtuber e influencer

La actividad llevada a cabo por los *youtubers* o *influencers* se caracteriza por ser un trabajo en el que se genera contenido y valor a partir de los medios propios y de la dedicación personal de los profesionales que la desarrollan. Es decir, esta profesión –más allá de posibles contribuciones que puedan hacerse con distintas marcas o demás colaboradores– debe considerarse una actividad económica ejercida por la persona de forma autónoma y no dependiente.[7] A partir de sus propios medios, el creador de contenido digital aporta a una plataforma digital concreta su trabajo, materializado en forma de vídeos o imágenes que comentan, entre otras, aspectos de su vida, situaciones cotidianas, videojuegos, actualidad, etc, y que provoca el entretenimiento del espectador y audiencia que les siguen.[8] Con ello, por una parte, entraría dentro de la definición de actividad económica planteada por la Ley del IRPF, la cual establece que «[s]e considerarán rendimientos íntegros de actividades económicas aquellos que, procediendo del trabajo personal y del capital conjuntamente, o de uno solo de estos factores, supongan por parte del contribuyente la ordenación por cuenta propia de medios de producción y de recursos humanos o de uno de ambos, con la finalidad de intervenir en la producción o distribución de bienes o servicios» (artículo 27 de la Ley). Por otra parte, la Ley del Impuesto sobre la Renta de las Personas Físicas del Principado de Andorra (*Llei 5/2014, del 24 d'abril, de l'impost sobre la renda de les persones físiques*) dispone la misma consideración de las rentas procedentes del trabajo personal y del capital, conjuntamente o por separado.

Cabe concretar que la Ley española hace una especial referencia a la consideración de actividades económicas a aquellas actividades llevadas a cabo, entre otras, por artistas y deportistas. Con ello, ¿puede definirse a los actuales *youtubers* o *influencers* como profesionales que ejercen por su cuenta y con una ordenación autónoma de sus recursos personales y de capital? ¿Realizan, así, una actividad económica sujeta o una explotación de contenido propio? La primera apreciación que debe realizarse respecto a la actividad llevada a cabo por los *youtubers* o *influencers* es que constituye una actividad económica basada en la persona, en su creación de contenido y en su imagen. A partir de aquí, del contenido creado y del uso de la imagen del profesional se derivarán rendimientos económicos de su contenido o de la cesión de los derechos de imagen –a una empresa propia que gestiona dichos derechos o a terceras que utilizan estos derechos de imagen para fines, por ejemplo, comerciales–.

En su caso, es esencial determinar si esta actividad económica llevada a cabo por el *youtuber* o *influencer* puede tener la consideración de actividad artística, al ser determinante esta condición a efectos fiscales y de sujeción de esta actividad en un Estado u otro. Sobre la consideración o definición de «artista», las leyes tributarias estatales no aportan mucha luz al respecto; en su caso, debe acudirse al modelo de convenio de la OCDE para evitar la doble imposición. En concreto, este modelo de convenio advierte de las dificultades prácticas que existen en la determinación de las actividades consideradas artísticas y su consecuente tributación. Asimismo, aunque no sea posible formular una definición precisa –a efectos fiscales– del término «artista», los comentarios al modelo de convenio disponen que «el término "artista" comprende claramente a los artistas escénicos, los actores de cine, y a quienes actúan en un anuncio de televisión (incluyendo, por ejemplo, antiguos deportistas). El artículo puede

7. Respecto a las cuestiones laborales que rodean a la figura del creador de contenido, resulta de especial interés Jover Ramírez (2025).
8. En cuanto a esta actividad profesional realizada por el creador de contenido digital (*youtuber* o/e *influencer*), la Dirección General de Tributos ha venido calificándola de rendimientos de actividades económicas, con su pertinente necesidad de darse de alta en el Impuesto sobre Actividades Económicas (véanse, por ejemplo, las Consultas Vinculantes núm. 0773, de 11 de abril de 2022; y, la núm. 2390, de 21 de noviembre de 2024).

aplicarse también a las rentas generadas por actividades de carácter político, social, religioso o benéfico, cuando incorporen un elemento de espectáculo».[9]

Por ende, ¿pueden considerarse las actividades económicas desarrolladas por los denominados *youtubers* e *influencers* como actividades artísticas? A mi juicio, sí. El uso de la imagen personal como elemento central de su labor, el carácter de entretenimiento o espectáculo que caracteriza la creación de contenido, y la inclusión de publicidad –tanto directa, a través de las plataformas, como indirecta, mediante recomendaciones o promociones incorporadas al contenido– permiten reconocer en estas actividades una dimensión artística propia del entorno digital, que amplía la noción tradicional de artista más allá del cine o la televisión.

Las nuevas formas de entretenimiento, la globalización y el mayor acceso a recursos digitales mediante ordenadores móviles –véanse los *smartphones*– han provocado un cambio en la forma del entretenimiento audiovisual en las nuevas generaciones. Si antiguamente la condición de artista se asociaba, por ejemplo, a presentadores de televisión o actores, todos ellos ligados al mundo del espectáculo; ahora, las nuevas tecnologías aplicadas al ocio generan nuevas figuras del espectáculo –*youtubers* e *influencers*–, nuevos artistas de la pantalla móvil. La condición de artista y sus implicaciones jurídico-tributarias deben ser revisadas y adaptadas a los nuevos tiempos; sin embargo, ello no implica que la actual normativa fiscal aplicable a este tipo de actividades económicas pueda ser interpretada de una forma extensiva o actualizada por parte de determinados organismos administrativos o, incluso, por parte de los tribunales.

Como consecuencia de ello, dicha condición de artista puede comportar un conjunto de consecuencias fiscales para aquellos *youtubers* e *influencers* que se desplazaron a Andorra para sufrir una menor presión fiscal en sus rendimientos económicos, pero que ven cómo la mayor parte de sus espectadores o seguidores están situados en su Estado de origen, esto es, España.

3. La condición de artista de los creadores de contenido e *influencers* y sus consecuencias fiscales a efectos del correspondiente convenio fiscal

En lo que se refiere a la tributación de los artistas, el convenio entre el Reino de España y el Principado de Andorra para evitar la doble imposición en materia de impuestos sobre la renta y prevenir la evasión fiscal y su protocolo, hecho «Ad Referéndum» en Andorra la Vella el 8 de enero de 2015 establece en su artículo 16 que «las rentas que un residente de un Estado contratante obtenga del ejercicio de su actividad personal en el otro Estado contratante en calidad de artista del espectáculo, tal como actor de teatro, cine, radio o televisión, o en calidad de músico, o como deportista, pueden someterse a imposición en ese otro Estado».

De esta forma, el convenio fiscal aplicable entre España y Andorra establece que para aquellos casos en que un artista –entendido como el concepto amplio ya analizado e indicando aquellos casos concretos como los referidos a actores, músicos o deportistas– en el ejercicio profesional de su actividad obtenga rentas de España, siendo residente fiscal en Andorra, estas rentas podrán gravarse por parte de España, y viceversa. Es decir, cuando el sujeto residente en un Estado obtiene rentas derivadas de su actividad profesional y en calidad de artista en otro Estado —véase España o Andorra—, estas últimas podrán someterse a tributación en el Estado donde se han llevado a cabo dichas actividades y han generado un beneficio económico concreto. Si un artista desarrolla su actividad en distintos territorios –independientemente de que tenga su residencia en otro Estado–, las rentas que pueda generar en cada territorio concreto deberán gravarse por el Estado pertinente.

Con ello, el espectáculo y entretenimiento que deriva de la actividad de los denominados *youtubers* o *influencers* comporta, en primer lugar, la posibilidad de considerar di-

9. Al respecto, como bien aclara Toribio Bernárdez (2018), «se debería presuponer que los contenidos publicados por parte del YouTuber son susceptibles de generar entretenimiento o diversión en los consumidores» (Toribio Bernárdez, 2018, p. 210). Ahora bien, advierte este mismo autor de la necesidad de diferenciar entre aquellos supuestos en donde el profesional que crea el contenido digital es parte del entretenimiento, interviniendo de forma personal y directa, y aquellos contenidos en donde el profesional exclusivamente realiza una tarea de edición, diseño y dirección; distinguiendo así aquellas actividades artísticas de otros rendimientos por actividades profesionales.

cha actividad como artística y a los sujetos que la ejercen como artistas a sus plenos efectos jurídicos y fiscales; en segundo lugar, deberá observarse el origen del beneficio o valor, esto es, la fuente de los rendimientos económicos. Ahora bien, debe hacerse una importante apreciación; el convenio establece que «las rentas [en calidad de artista] que un residente de un Estado contratante obtenga del ejercicio de su actividad personal en el otro Estado contratante [...] pueden someterse a imposición en ese otro Estado». Por ende, el elemento esencial para determinar el Estado competente para gravar dichas rentas, a mi modo de ver, no será tanto el origen de las rentas, sino la ubicación o el lugar de realización de la actividad personal y artística que las origina. Deberá observarse el lugar donde se realiza la actividad, más que el origen de la retribución, al ser la creación de contenido, el espectáculo o el entretenimiento en o para un territorio concreto el que ha provocado la generación de un valor económico.

Será el lugar donde se desarrolla la actividad artística, fuente y origen de los posteriores rendimientos económicos que se deriven, lo que determinará el Estado competente para gravar dichos beneficios. Aunque esta situación en el marco de la economía tradicional –lugar donde se desarrolla la actividad y origen de las rentas– pueda no plantear cuestiones conflictivas, al ser en la mayoría de las ocasiones el mismo lugar, en la economía digital dicha situación puede comportar algún tipo de conflicto. Piénsese en aquellas situaciones en que la empresa tecnológica principal que paga a los creadores de contenido por su actividad se sitúa en otros países como, por ejemplo, Irlanda o Estados Unidos –véase el caso de Google Ireland Ldt, Google, LLC o YouTube, LLC–, pero la actividad profesional artística se desarrolla principalmente, por ejemplo, en España. En estas situaciones, parece, en mi opinión, que prima el ejercicio de la actividad personal desarrollada por el *youtuber* o *influencer* en un territorio concreto frente al origen del pago.

No obstante, no debe confundirse el lugar de realización de la actividad personal con el lugar de residencia y, en el caso de los creadores de contenido digital, un factor crucial en la determinación del lugar de realización de la actividad «artística» puede ser la audiencia o los seguidores que consumen el contenido digital de entretenimiento. Así pues, el hecho de que un creador de contenido resida habitualmente en Andorra, bajo mi punto de vista, no implica per se que su actividad profesional de entretenimiento se desarrolle única y exclusivamente en Andorra, sino que deberá estarse ante el origen de la audiencia y seguidores para poder concluir que esta actividad se lleva a cabo en un Estado u otro.

Por todo ello, resulta de especial interés determinar el papel que desempeña la audiencia o los «seguidores», a los efectos de concluir el lugar de realización de la actividad y el correspondiente Estado con derecho a gravar las rentas que se deriven de esta actividad «artística». Más aún en los casos que se refieren a *youtubers* o *inflencers* para los que el número de visualizaciones, el número de seguidores y el origen de estos son factores determinantes para la creación de valor y atractivo comercial. Asimismo, deberán analizarse otras circunstancias que permitan apreciar mayormente que la actividad es llevada a cabo en un territorio o en otro.

4. El papel fundamental de la audiencia o seguidores en la determinación del lugar de ejercicio de la actividad personal y artística

Hasta el momento, dos elementos esenciales determinan la fiscalidad de los *youtubers* e *influencers* desplazados a terceros países para buscar una regulación fiscal más favorable; estos son la consideración de su actividad como artística, o la consideración de artistas de dichos profesionales del entretenimiento digital, y el lugar de realización de dicha actividad personal. Con ello, si ambos elementos coinciden en un mismo territorio –aunque el profesional que la ejerce sea residente en otro país–, previsiblemente el Estado donde dicha actividad se realiza, está enfocada o se destina, podrá tener, en mi opinión, la capacidad y derecho de gravar los beneficios que se deriven.

Ahora bien, por una parte, como ya se ha comentado, la consideración de artista de un *youtuber* o *influencer* será una cuestión interpretativa y de adaptación de los modelos de entretenimiento tradicionales –presentadores, actores o personajes de televisión– a los nuevos modelos de espectáculo y entretenimiento digital. De esta forma, nada impide dicha consideración por parte de organismos públicos o Estados. Por otra parte, el hecho de considerar una actividad personal y artística distribuida de forma digital por parte de una plataforma digital como realizada en un Estado concreto puede ser más dificultoso.

Debe partirse de la consideración de que hasta el momento el atractivo fiscal que motivaba el traslado de estos profesionales del entretenimiento moderno a Andorra era la posibilidad de tributar menos por su renta mundial –es decir, todos los beneficios generados en distintos territorios–, sobreentendiéndose que su actividad se desarrollaba principalmente en Andorra, aunque su contenido creado se distribuyese a diferentes países por una empresa digital con residencia en otro Estado. Sin embargo, ¿cómo puede entenderse una actividad artística como realizada en un Estado concreto sin presencia física en él? ¿Cómo puede entenderse un contenido de entretenimiento como creado en España si se distribuye por una empresa digital sede fiscal en Irlanda o en Estados Unidos? Aquí es donde el papel de la audiencia y los seguidores puede desempeñar un papel fundamental a efectos de entender la actividad profesional realizada en un territorio concreto.

Desde mi punto de vista, la actividad puede entenderse realizada en el país donde se destina o al que está enfocada dicha actividad.[10] Por ejemplo, imagínese que un deportista famoso residente fiscal en España realiza y actúa en un anuncio en Japón; previsiblemente, el convenio fiscal aplicable entre el Estado español y Japón permitirá que las rentas derivadas de esta actividad «artística» puedan gravarse por el país nipón. Dicha posibilidad se fundamenta en el destino de la actividad artística, del producto o del contenido audiovisual que se produce. A similitud con este ejemplo, se podría entender un contenido creado por un *youtuber* o *influencer*, destinado a un público específico y ubicado, en su mayoría, en un país concreto, independientemente del territorio de residencia del «artista».

¿Acaso puede tener algún tipo de relevancia económica y fiscal un *youtuber* o *influencer* con menos de 90.000 seguidores? La población de Andorra no llega a los 90.000 habitantes.[11] ¿Puede entenderse la actividad de entretenimiento desempeñada por estos creadores de contenido digital como realizada exclusivamente en Andorra y para los habitantes de este país? La respuesta, entiendo, debe ser absolutamente negativa. El lugar de realización de la actividad personal y artística debe entenderse realizada donde se sitúa su audiencia y seguidores. Consecuentemente, el Estado con potestad para gravar los beneficios económicos que se deriven de dichas actividades de entretenimiento y creación de contenido digital será el Estado donde se halla la mayoría de la audiencia y los seguidores del profesional. En el caso de plataformas digitales de distribución de contenido audiovisual y entretenimiento digital, plataformas como YouTube o Twitch[12] permiten identificar la ubicación de la audiencia, esto es, el lugar donde se visualiza mayormente el contenido.

Asimismo, pueden tenerse en consideración otros factores a efectos de entender que la actividad artística se realiza en un Estado concreto y se destina a la ciudadanía de dicho territorio. Un ejemplo de ello puede ser el uso de la lengua oficial del lugar en la creación de contenido digital por parte de *youtubers* o *influencers*, o, incluso, el propio lugar donde se realizan estos vídeos –véanse vídeos grabados con frecuencia en una ciudad española cercana al país de Andorra–. En el caso de la lengua, puede ser difícil de entender que un contenido se realiza y distribuye en Andorra cuando la lengua usada con más frecuencia es la española; la lengua oficial del Principado de Andorra es el catalán.

Siguiendo con el ejemplo descrito anteriormente, ¿puede entenderse un anuncio como realizado en Japón cuando se lleva a cabo íntegramente, por ejemplo, en español? Si el anuncio se graba, maqueta y emite en Japón, pese al idioma, no habría inconveniente en considerar la actividad artística como llevada a cabo en Japón. Sin embargo, si este mismo anuncio se graba en Estados Unidos, el idioma

10. Así lo establece la jurisprudencia del Tribunal Superior de Justicia de la Unión Europea en su sentencia de 19 de febrero de 2009, asunto C-1/08, Athesia Druck Srl. en referencia al Impuesto sobre el Valor Añadido; asimismo, el Tribunal Económico Administrativo Central en su resolución de 22 de julio de 2020 (procedimiento 00-01532-2017) concluye que «[e]l TJUE, por tanto, establece claramente que en prestaciones de servicios de publicidad, el país en el que se realiza la utilización y explotación efectivas es aquel desde el que se difunden los mensajes publicitarios, con independencia de que esa utilización la haga el destinatario inicial de la operación, o el destinatario ulterior en la cadena».
11. Según fuentes del propio gobierno de Andorra, en septiembre de 2025 la población de Andorra era de 88.649 habitantes. Datos consultables en: https://sig.govern.ad/Sigdde.Public//Inici?Idioma=ca&Pag=PAG_Inici
12. La plataforma Twitch –perteneciente a Amazon, Inc.– permite otro tipo de apoyo económico (distinto de YouTube) a los denominados *streamers*, aquellos creadores de contenido que comparten mediante la plataforma digital. En concreto, se permite el apoyo económico a la tarea de estos profesionales mediante donaciones económicas por parte de los espectadores. Con ello, como advierte Egea Pérez-Carasa (2021, pág. 34), estos ingresos podrían considerarse donaciones a los efectos del Impuesto de Sucesiones y Donaciones.

del anuncio es el español y se publicita en Japón, aunque sea más difícil, podría seguir entendiéndose la actividad como realizada en aquel lugar en el que se pueda derivar una consecuencia económica, una audiencia, consumidor y posterior beneficio comercial. De este modo, extrapolando este mismo supuesto al caso de los *youtubers* e *influencers*, aunque el lugar de residencia sea Andorra, si el lugar donde se consume mayormente el contenido digital es España, el idioma utilizado es el oficial de España –y no el de Andorra– y existen otros elementos que permiten a la audiencia identificar las costumbres o hábitos propios del país, la actividad personal y artística debe considerarse, a mi parecer, realizada en España. Asimismo, también será indicativo de que dicha actividad se desarrolla en un Estado determinado cuando de la notoriedad del artista y de su creación de contenido en el Estado en cuestión se deriven contratos publicitarios. Esto es, «las actividades de un artista o de un deportista no se limitan a su participación en un espectáculo o en un acto deportivo en un cierto Estado, sino que incluyen igualmente, por ejemplo, su aparición en entrevistas o en anuncios publicitarios en ese Estado que estén estrechamente relacionados con dicha participación» (Comentarios al Modelo de Convenio de la OCDE, artículo 17, párrafo 9.1). Esta posibilidad de que de la notoriedad del artista en un territorio determinado se puedan derivar contratos publicitarios está recogida en el propio Convenio entre España y Andorra, considerándose igualmente obtenidas por artistas y deportistas «[l]as rentas a que se refiere este artículo comprenden las de carácter accesorio derivadas de prestaciones relacionadas con la notoriedad personal de un artista o deportista residente de un Estado contratante, siempre que se obtengan con motivo de su presencia en el otro Estado contratante y provengan de ese otro Estado» (artículo 16.3 del Convenio).[13]

Los contratos publicitarios que puedan resultar de la popularidad de un creador de contenido digital en un país no serán más que un reflejo de los destinatarios principales y del lugar de realización de la actividad de entretenimiento. Si, además de esta publicidad realizada en un Estado concreto por parte del *youtuber* o *influencer*, la actividad realizada por este creador de contenido de entretenimiento puede considerarse artística o llevada a cabo por un artista, podrá estarse ante una plena sujeción de los rendimientos económicos originados en el Estado de la fuente.

En consecuencia, será España quien, en mi opinión, podrá tener el derecho de gravar los beneficios económicos o las rentas que se deriven de la creación de este contenido digital y de entretenimiento por parte de los creadores de contenido desplazados a Andorra, ello en base a lo dispuesto por el propio convenio fiscal de aplicación entre España y Andorra. El destino y audiencia de la creación de contenido generado por los denominados *youtubers* o *influencers* comporta la necesidad de estar ante la fuente de beneficios, pudiéndose calificar dichos beneficios generados por estos creadores de contenido como rendimientos sujetos en España. El artículo 13 de la LGT establece que «[l]as obligaciones tributarias se exigirán con arreglo a la naturaleza jurídica del hecho, acto o negocio realizado, cualquiera que sea la forma o denominación que los interesados le hubieran dado, y prescindiendo de los defectos que pudieran afectar a su validez». Por ende, dicha posibilidad y calificación deberán venir marcadas por una reinterpretación del convenio, ya sea de forma unilateral –por ejemplo, por la propia Administración tributaria española– o mediante un acuerdo de ambos Estados, que permita a España sujetar las rentas de aquellos sujetos pasivos que trasladaron su residencia fiscal a Andorra en busca de mejores condiciones tributarias. De la misma forma, se propone, al igual que se hace con la figura de actor, deportista o músico, incluir en el artículo 16 del convenio entre España y Andorra el concepto de creador de contenido e *influencer*; dicha inclusión permitiría una atribución de potestades tributarias consensuada y falta de ambigüedades.

Conclusiones

La fiscalidad de los creadores de contenido digital exige una relectura crítica de las categorías tributarias tradicionales, particularmente en lo que respecta a la determinación del lugar de realización de la actividad económica y, por ende, del Estado con potestad tributaria sobre las rentas obtenidas. La irrupción de nuevos modelos de entretenimiento, disociados en buena parte de la presencialidad física, obliga a repensar conceptos como «actividad

13. Sobre esta cuestión, resulta de interés Báez Moreno (2022).

artística», «fuente de renta» o «territorialidad» desde una perspectiva funcional y adaptada a las dinámicas del entorno digital.

En primer lugar, ha quedado evidenciado que la actividad profesional de los *youtubers* e *influencers* no puede considerarse una mera prestación de servicios. Por el contrario, se trata de una actividad estrechamente vinculada al uso de la imagen personal, a la creación de contenido original y a la interacción constante con una audiencia masiva. Estas características permiten calificar su labor, en muchas ocasiones, como una verdadera actividad artística en los términos amplios reconocidos por el Modelo de Convenio de la OCDE, y, en particular, por el artículo 16 del convenio suscrito entre España y Andorra.

Esta calificación no es meramente académica, sino que conlleva consecuencias fiscales relevantes. Como se ha argumentado en el trabajo, cuando un creador de contenido digital obtiene rentas derivadas de su actividad personal como artista, estas rentas pueden someterse a imposición en el Estado donde se haya realizado dicha actividad, aun cuando el contribuyente resida formalmente en otro país. Así lo establece expresamente el citado artículo 16, lo que refuerza la necesidad de interpretar la noción de «residencia fiscal» de manera sustantiva y no meramente formal.

En este sentido, no basta con constatar que un *youtuber* o *influencer* resida más de 183 días en Andorra y cumpla con los requisitos legales internos para adquirir allí la residencia fiscal. Es imprescindible evaluar el lugar efectivo de desarrollo de la actividad artística. Aquí cobra especial relevancia el concepto de la audiencia, entendido como el conjunto de usuarios[14] que consumen el contenido digital y que constituyen la razón de ser del negocio de la creación de contenido digital. Si la mayor parte de los seguidores, visualizaciones y beneficios publicitarios provienen de un país determinado –como ocurre en numerosos casos con España–, puede sostenerse, con base en el principio de fuente, que es en ese territorio donde se realiza en esencia la actividad económica y artística.

De igual forma, la importancia de la audiencia se proyecta no solo sobre la plataforma de publicación del contenido, sino también sobre los ingresos derivados de contratos publicitarios, colaboraciones con marcas[15] o presencia en medios de comunicación. Cuando estas actividades tienen lugar en función de la notoriedad alcanzada en un Estado concreto, pueden y deben considerarse extensiones de la actividad artística principal y, por tanto, gravables en dicho territorio, conforme al artículo 16.3 del convenio entre España y Andorra.

Asimismo, el uso del idioma, los referentes culturales, los lugares donde se graban los vídeos y la geolocalización de la interacción en redes sociales son factores que contribuyen a fijar el nexo territorial entre la actividad y un determinado Estado. Se ha podido indicar, de forma atinada, que difícilmente puede sostenerse que un contenido producido en español y orientado a una audiencia española esté «realizado» en Andorra, aun cuando el creador haya fijado allí su residencia fiscal.

Otro aspecto crucial abordado en el trabajo es el papel de las plataformas digitales y su ubicación fiscal. Aunque los ingresos se perciban de entidades con sede en Irlanda o en Estados Unidos (como es el caso de Google o YouTube), lo relevante a efectos fiscales no es el origen del pago, sino el lugar donde se realiza la actividad generadora del valor económico. En el caso de los *youtubers* e *influencers*, ese valor surge de la interacción con una audiencia localizada territorialmente, no de la empresa que intermedia o remunera la actividad. Este enfoque, basado en la economía del destino y en el principio de realidad económica, ofrece una interpretación más coherente con los fines del derecho tributario internacional.

14. Autores como Becker y Englisch (2019, pág. 161) proponen establecer un derecho impositivo en el marco del derecho tributario internacional con base en una relación sostenida de usuario, como reflejo de la fuente de beneficios en el marco de la economía digital. La audiencia supone el origen de los rendimientos económicos de plataformas como YouTube o Instagram y, en consecuencia, estos usuarios o audiencia constituyen el origen de la rentabilidad de estos creadores de contenido o *influencers*. Por ende, en el marco de la economía digital, la localización del usuario debería comportar el nacimiento de un derecho de imposición por parte del Estado de la fuente; en este sentido, Devereux, Auerbach, Keen, Oosterhuis, Schön y Vella (2021, pág. 76).
15. «[E]xiste una clara coincidencia entre los académicos de que los perfiles de influencia sí son uno de los nuevos canales a través de los cuales las marcas se comunican con sus públicos y por ello, ya juegan un papel crucial dentro de sus estrategias de comunicación digital» (Arcos Valls y Torres-Romay (2024, pág. 591).

Cabe destacar que el presente análisis no implica desconocer el derecho del contribuyente a optimizar su carga fiscal dentro de los límites de la legalidad. Sin embargo, ello no puede hacerse en fraude de ley ni mediante el uso abusivo de figuras jurídicas como la residencia fiscal formalmente adquirida pero materialmente inexistente. En este contexto, la Agencia Tributaria española, de conformidad con el artículo 13 de la Ley General Tributaria, puede actuar contra los montajes artificiosos destinados a obtener un beneficio fiscal ilegítimo, como sería el caso de una supuesta residencia en Andorra sin desvinculación real del territorio español ni traslado efectivo del centro de intereses económicos. Identificar la correcta naturaleza jurídica del hecho, acto o negocio realizado, cualquiera que sea la forma o denominación que los interesados le hubieran dado, y prescindiendo de los defectos que pudieran afectar a su validez.

La evolución del derecho tributario en esta materia requiere también una actuación coordinada a nivel internacional. La OCDE y la Unión Europea han iniciado procesos de revisión de las normas sobre fiscalidad digital, que deben desarrollarse con mayor profundidad para evitar fenómenos de erosión de las bases imponibles. No es razonable que creadores de contenido que generan millones en ingresos a partir de una audiencia localizada en España puedan tributar exclusivamente en Andorra, reduciendo así su contribución al sostenimiento de los servicios públicos del país donde efectivamente se benefician de infraestructuras, mercado y reputación.

En conclusión, el estudio realizado pone de manifiesto la necesidad urgente de adaptar los conceptos jurídicos tributarios clásicos a los nuevos escenarios digitales. Frente al reto de la fiscalidad de los *youtubers* e *influencers*, el derecho debe avanzar hacia soluciones interpretativas que prioricen la sustancia sobre la forma, la realidad económica sobre las apariencias y el principio de equidad fiscal sobre los privilegios artificiales. El criterio de audiencia-consumidores, la calificación como artistas y la localización efectiva de la actividad deben convertirse en los ejes centrales de un modelo fiscal que responda a los desafíos de la era digital y que garantice una distribución justa de la carga tributaria. Solo así podrá asegurarse la sostenibilidad del sistema fiscal y el respeto al principio de solidaridad en un contexto cada vez más globalizado e interconectado. Esta adaptación debe venir marcada por una reinterpretación del convenio suscrito entre España y Andorra y la noción de artista; o, en su caso, por una referencia explícita a este tipo de profesionales dedicados a la creación de contenido –al igual que se hace respecto a los actores, deportistas o músicos–; solo así podrá existir un derecho de imposición y reparto de potestades tributarias consensuado entre ambos Estados.

Reconocimientos

El autor agradece profundamente las observaciones y sugerencias aportadas por los evaluadores, las cuales han contribuido al enriquecimiento de este estudio. De igual forma, reconoce la gran labor del equipo editorial en la corrección y maquetación del trabajo.

Referencias bibliográficas

ARCOS VALLS. N.; TORRES-ROMAY, E. (2024). «De creadores de contenido a influencers. Contenidos propios frente a contenidos promocionales de marca. Estado de la cuestión». En: DAFONTE GÓMEZ, A.; MÍGUEZ GONZÁLEZ, M. I. (coords.). *Comunicación digital en la era de la inteligencia artificial*, págs. 578-594. Dykinson, España.

DEVEREUX, M-P.; AUERBACH, A. J.; KEEN, M.; OOSTERHUIS, P.; SCHÖN, W.; VELLA, J. (2021). *Taxing Profit in a Global Economy*. Oxford University Press. DOI: https://doi.org/10.1093/oso/9780198808060.001.0001

BÁEZ MORENO, A. (2022). «Un sistema fiscal del siglo XIX frente a un contribuyente del siglo XXI: el irrefrenable éxodo fiscal de los youtubers al Principado de Andorra». *Revista de Contabilidad y Tributación. CEF*, n.º 466, págs. 43-86. DOI: https://doi.org/10.51302/rcyt.2022.7491

BECKER, J.; ENGLISCH, J. (2019). «Taxing Where Value Is Created: What's 'User Involvement' Got to Do with It?». *Intertax*, vol. 47, n.º 2, págs. 161-171. DOI: https://doi.org/10.54648/TAXI2019015

CASTRO DACOSTA, K.; BLANCO NÚÑEZ, D. (2024). «Twitch, YouTube y Streamers. Aspectos relevantes de su fiscalidad». *Quincena Fiscal*, n.º 3 (recurso electrónico).

DI GIOACCHINO D.; FICHERA D. (2022). «Tax evasion and social reputation: The role of influencers in a social network». *Metroeconómica*, vol. 73, n.º 4, págs. 1048-1069. DOI: https://doi.org/10.1111/meca.12391

EGEA PÉREZ-CARASA, I. (2021). «Tributación de los "influencers": normas tradicionales para nuevos y rentables modelos de negocio de las nuevas generaciones». *Cuadernos de derecho y comercio*, n.º 75, págs. 15-112.

FREBERG, K.; GRAHAM, K.; MCGAUGHEY, K.; FREBERG, L. A. (2011). «Who are the social media influencers? A study of public perceptions of personality». *Public relations review*, vol. 37, n.º 1, págs. 90-92. DOI: https://doi.org/10.1016/j.pubrev.2010.11.001

GIL GARCÍA, E. (2022). «La residencia fiscal de las personas físicas indeterminación, ubicuidad y deslocalización». *Revista Española de Derecho Financiero*, n.º 193 (recurso electrónico).

HUDDERS, L.; DE JANS, S.; DE VEIRMAN, M. (2021). «The commercialization of social media stars: a literature review and conceptual framework on the strategic use of social media influencers». En: NILS S. BORCHERS (ed.). *Social media influencers in strategic communication*, págs. 24-67, primera edición. Routledge: Nueva York. DOI: https://doi.org/10.4324/9781003181286-3

JOSHI, Y.; LIM, W. M.; JAGANI, K.; KUMAR, S. (2023). «Social media influencer marketing: foundations, trends, and ways forward». *Electronic Commerce Research*, vol. 25, págs. 1199-1253. DOI: https://doi.org/10.1007/s10660-023-09719-z

JOVER RAMÍREZ, C. (2025). «Los creadores de contenido digital. ¿Una nueva zona gris del Derecho del trabajo?». *LABOS Revista De Derecho Del Trabajo Y Protección Social*, vol. 6, n.º 2, págs. 109-134. DOI: https://doi.org/10.20318/labos.2025.9668

SÁNCHEZ-ARCHIDONA HIDALGO, G. (2022). «La tributación de los modelos de negocio basados en la generación de contenido y streaming: soluciones analógicas a paradigmas digitales». *Revista Técnica Tributaria*, n.º 137, págs. 81-112. DOI: https://doi.org/10.48297/rtt.v2i137.2294

TORIBIO BERNÁRDEZ, L. (2018). «Tributación de las rentas obtenidas por los "YouTubers": cuestiones problemáticas en torno a su calificación en el IRPF». En: GARCÍA-HERRERA BLANCO, C. (dir.). *VI Encuentro de Derecho Financiero y Tributario "Tendencias y retos del Derecho Financiero y Tributario"* (2.ª parte), págs. 197-213. Instituto de Estudios Fiscales.

Cita recomendada

BERGAS FORTEZA, Antoni (2025). «Cuestiones sobre la fiscalidad de los creadores de contenido e influencers: criterios de sujeción y aplicación del correspondiente convenio para evitar la doble imposición entre España y Andorra». *IDP. Revista de Internet, Derecho y Política*, núm. 44. UOC. [Fecha de consulta: dd/mm/aa]. DOI: http://dx.doi.org/10.7238/idp.v0i44.9800309

Sobre el autor

Antoni Bergas Forteza
Profesor ayudante de Derecho Financiero y Tributario de la Universidad de las Illes Balears
antoni.bergas@uib.es
ORCID: https://orcid.org/0000-0003-1335-8039

Graduado en Derecho, máster en Hacienda Pública, Sistema Impositivo y Procedimientos Tributarios y máster en Abogacía por la Universitat de les Illes Balears. Ha cursado diferentes cursos de especialización en el ámbito tributario internacional, de intervención y financiación pública en, entre otros, centros educativos como la Universidad de Leiden, el Instituto de Estudios Fiscales o el Centro de Estudios Financieros. Cursa estudios de doctorado en Derecho, siendo su línea de investigación el Derecho Tributario Internacional y la fiscalidad en el marco de la economía digital. Es autor de varios capítulos de libro y artículos publicados en revistas de carácter nacional e internacional. Ha participado en proyectos de investigación e innovación docente. Asimismo, ha realizado estancias de investigación en el Max Planck Institute for Tax Law and Public Finance de Múnich (Alemania) y en el Institute for Tax Law de la Universidad de Münster (Alemania).

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Navigating the AI legal landscape. Gender implications of large language models in legal text generation

Cristina Blasi Casagran
Autonomous University of Barcelona

Lidia Ballesta Martí
Autonomous University of Barcelona

Santiago Robert Guillén
Autonomous University of Barcelona

Eduard Blasi Casagran
Autonomous University of Barcelona

Date of submission: March 2025
Accepted in: October 2025
Published in: March 2026

Abstract

Large language models (LLMs) are AI systems capable of generating and analysing natural language texts. They have been utilized across various fields, including, among others, legal text generation, where they can aid lawyers in drafting litigation-focused documents such as contracts, pleadings, and motions, or even assist them with ideas and legal research for preparing legal reports or memos. However, the use of LLMs in legal text generation raises ethical and legal concerns, such as responsibility, accountability, and liability for the generated texts, as well as potential algorithmic discrimination and gender biases amongst others. In this article, we review the current state of LLMs in legal text generation, focusing on the strengths and limitations of AI-powered legal research software used by law firms based in the EU. We also discuss gender implications of using LLMs for legal text generation and offer some recommendations and best practices to ensure the quality, reliability and fairness of the generated texts.

Keywords

large language models; legal text generation; gender biases; algorithmic discrimination; AI Act

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Navegar por el panorama legal de la IA. Implicaciones de género en los modelos extensos de lenguaje en la generación de texto legal

Resumen

Los modelos extensos de lenguaje (LLM, por sus siglas en inglés) son sistemas de IA capaces de generar y analizar textos en lenguaje natural. Se han utilizado en varios campos, incluyendo, entre otros, la generación de texto legal, donde pueden ayudar a los abogados a redactar documentos centrados en litigios, como contratos, alegatos y mociones, o incluso a proporcionarles ideas e investigación legal para preparar informes o memorandos legales. Sin embargo, el uso de los LLM en la generación de texto legal plantea preocupaciones éticas y legales, como la responsabilidad y la obligación por los textos generados, así como la posible discriminación algorítmica y los sesgos de género, entre otros. En este artículo, revisamos el estado actual de los LLM en la generación de texto legal, centrándonos en las fortalezas y limitaciones del software de investigación legal impulsado por IA utilizado por bufetes de abogados con sede en la UE. También analizamos las implicaciones de género del uso de los LLM para la generación de texto legal y ofrecemos recomendaciones y mejores prácticas para garantizar la calidad, la fiabilidad y la imparcialidad de los textos generados.

Palabras clave

modelos extensos de lenguaje; generación de texto legal; sesgos de género; discriminación algorítmica; Ley de IA

Introduction

The advent of Artificial Intelligence (AI) signifies a paradigm shift in the legal sector, heralding automated mechanisms for drafting and critical review of legal documentation. The legal sector is a professional sphere that manages a great volume of information. Therefore, the potential of AI in this sector is tremendous. AI is thus being increasingly used by law firms to automate routine tasks and streamline workflows, ultimately leading to enhanced efficiency and cost savings by reducing time spent on manual tasks and generating ideas from scratch (Clio, 2024). This has the benefit of democratizing access to legal advice, particularly for underserved communities, by lowering economic and knowledge barriers. With AI, law professionals can focus on higher value creative tasks or those that require critical judgement; dimensions that to date are beyond the reach of AI systems.

Large Language Models (LLMs), such as OpenAI's ChatGPT-5 and Google's Gemini Advanced, can generate natural language text from various inputs, such as keywords, queries, or existing documents. These models hold the potential to transform the creation of litigation-focused legal documents – contracts, pleadings, motions, briefs, and memoranda – by providing relevant information, recommendations, and structural templates. However, defining the scope of AI application within legal practice reveals a complex landscape. In fact, such a profession is so diverse (including different kinds of work based on organizational size and type) that it is impossible to generalize about how AI benefits everyday legal work (Legg & Bell, 2020). Specific benefits will, of course, be realized, but they will depend on the particular use case and AI application.

At the same time, the use of AI for legal drafting can present challenges and risks, particularly because deploying AI systems often involves handling large amounts of data, potentially including personal information. In fact, the recent adoption of the AI Act (European Union, 2024) in the European Union (EU highlights the urgent need to establish regulatory frameworks for AI technologies, taking into account the ethical and fundamental rights involved. Furthermore, the rise of cybersecurity and data protection concerns in using AI LLMs for legal text generation cannot be overlooked, especially given the EU's strict data protection regulations, such as the General Data Protection Regulation (GDPR) (European Union, 2016). Additionally, one of the most urgent yet underexplored risks in legal AI systems is their potential to reinforce or worsen gender bias in legal language and representation, an issue that this article thoroughly examines.

Within this context, this study aims to provide a thorough analysis of the current state and future prospects of using AI LLMs for generating litigation-focused legal text. It will explore which AI LLMs are most utilized by legal

professionals for drafting purposes and examine the key gender-related implications associated with their use in legal writing.

To fulfil these objectives, this study has reviewed a large number of AI tools and bots for lawyers using a mixed-methods approach, combining qualitative and quantitative data from sources such as literature reviews, surveys and semi-structured interviews. It contributes to the existing literature on AI and law by providing a novel and in-depth analysis of the use of AI LLMs for generating litigation-focused legal text, highlighting the opportunities, challenges, and implications for the legal profession and society.

Furthermore, to strengthen the legal perspective of this study, the analysis consistently focuses on the EU's regulatory framework, especially the AI Act (Regulation (EU) 2024/1689), as well as the ethical and professional duties outlined in national codes of conduct for lawyers. These instruments are employed not only to define the challenges posed by AI in legal practice but also to evaluate the effectiveness of safeguards against risks such as algorithmic discrimination and professional liability. By situating the discussion within this legal context, the paper aims to make a meaningful contribution to the ongoing debate on the lawful and ethical integration of AI into the legal profession.

The structure of this paper follows a progressive argumentative logic, moving from a descriptive analysis of the tools available (Section 2) to a discussion of the necessity of human oversight and ethical responsibility in their use (Section 3), and finally to a critical reflection on the specific risks of algorithmic discrimination and gender bias in legal LLMs (Section 4). This sequence aims to demonstrate that implementing AI in legal practice is not simply a technical challenge but one that demands strong ethical and legal safeguards, especially concerning equality and non-discrimination. The concluding sections (5 and 6) bring these themes together by providing practical recommendations and exploring avenues for further legal regulation and professional responsibility.

Ultimately, the paper adopts a multidisciplinary approach to explore how legal LLMs are being implemented in law firms across the EU, with a particular focus on the gender-related risks and legal challenges they pose, aiming to contribute to both empirical understanding and the ethical-regulatory debate.

1. Main LLMs for legal text generation used by lawyers

Previous studies demonstrate that, although some lawyers are aware of the AI-based legal technology tools available to them, this awareness is not universal (Weinstein, 2022). In fact, compared to other professionals, lawyers are often seen as conservative and more resistant to change than the average (Legg & Bell, 2020; Waisberg & Hudek, 2021), which makes them less inclined towards innovative technologies, including AI tools.

However, in recent years, legal practitioners have shown increasing interest in using AI tools to complete some procedural and substantive tasks. Although the legal profession is traditionally a conservative sector, lawyers are gradually becoming more aware of the advantages that AI offers to support their work, such as accessing and quickly scanning large databases or developing fair legal arguments in their daily practice. An increasing number of legal professionals now recognize the transformative potential of AI in streamlining both procedural tasks and substantive legal analyses. These tools not only facilitate access to and analysis of extensive databases but also assist in formulating equitable legal arguments, thereby enhancing the efficiency of daily legal practices. In essence, lawyers seeking AI assistance in their work can choose from three options: **1)** Lawbots (GPTs), which are legal AI applications that automate general legal tasks like document automation and legal research, ranging from smart searches and step-by-step forms to chatbots; **2)** specialized AI-driven tools for lawyers, which are task-focused tools that streamline specific legal processes, improve efficiency, and enhance particular legal tasks; and **3)** locally-supported AI tools for lawyers, which are customized tools developed within a law firm to help lawyers find relevant case law, statutes, and legal opinions more efficiently.

Using lawbots as assistants for legal tasks can be the most cost-effective option for legal practitioners. Since January 2023, over 20 bots or GPTs have been developed with support from ChatGPT, trained by OpenAI, Poe and Ora. There are some differences in how these three platforms are utilized. While bots provided by Poe and Ora are free, bots built on the OpenAI platform (GPTs) are only accessible to ChatGPT Plus subscribers. This is because, unlike Poe's and Ora's bots, which that are built on GPT-3.5 model, OpenAI employs ChatGPT 5, a far more powerful and capable model than the free version. The economic models underpinning these bots differ: Poe and Ora offer free access, whereas

OpenAI's more advanced GPT-4-based bots require a ChatGPT Plus subscription. However, using bots developed with ChatGPT 3.5 offers two advantages: it is free to use and provides a faster writing experience (ChatGPT 4 is more powerful). Currently, there are seven main lawbots available under OpenAI, Poe, and Ora: **1)** "Abogado Digital", which supports lawyers with any technology-related issue; **2)** "Lex Copilot", which assists with tasks such as legal research, drafting contracts and other legal documents, and improving the drafting of any legal text; **3)** "Lex Tutor", which helps with understanding and applying the Mexican legal framework; **4)** "Lex Informatica" (still in pilot phase), which addresses issues related to digital rights, intellectual property, cybersecurity, and personal data protection; **5)** "Lex Mentor", which aids lawyers in negotiations, conciliation, mediation, and arbitration; **6)** "Lex Advisor", an AI assistant specialized in detecting, evaluating, and mitigating legal risks; and 7) "CoNaProCi", a bot specialized in national civil and family legal procedures (Gómez, 2024).

Another option is to purchase one of the several AI-driven tools for lawyers available on the market (Matich & Lenon, 2024). Their cost can range from 7 to 2,500 euros per month (York, 2024), and their primary functions include summarising legal research, automatically generating new legal tasks, reviewing contracts, creating legal documents or emails, drafting contracts, organising deals for new clients, and suggesting legal strategies for litigation. The most popular large-scale tools and their uses are listed in Table 1. The inclusion of these models illustrates the growing integration of large language models (LLMs) into legal practice and provides context for the legal and ethical issues discussed in this paper. These tools were chosen based on their market relevance, range of functionality, and visibility in recent legal tech analyses (Matich & Lenon, 2024; York, 2024). Although their technical operations differ, most depend on transformer-based architectures that enable natural language processing tasks such as summarising, classification, and generation. Legally, these tools raise important questions about confidentiality, liability, bias, and compliance with professional standards – especially since their outputs may influence contractual terms or litigation strategies.

Table 1. List of selected companies offering AI LLMs for lawyers

	Main purpose of the AI LLM	Summarizing legal research	Automatically generating new tasks	Contract review process automator	Emails, reports, documents, summaries and updates generator	Draft contracts & templates	Organize deals	Suggestions for legal strategies
ClickUp	AI as a national security asset	•	•		•			
Lawgeex	Review and redline contracts in accordance with the company's policies and guidelines.			•				
Amto	Create templates.			•	•	•		
Detangle.ai	Summarize lengthy legal research.	•						
Ansarada	Manage workflows and collaborate on critical tasks such as deals.		•				•	

	Main purpose of the AI LLM	Summarizing legal research	Automatically generating new tasks	Contract review process automator	Emails, reports, documents, summaries and updates generator	Draft contracts & templates	Organize deals	Suggestions for legal strategies
Lex Machina	Analytics platform.	•			•			
Latch	AI legal assistants within MS Word.	•			•			•
PatentPal	Generate documents for intellectual property.				•	•		
HumataAI	Summarize documents.	•						
GenIA-L	Automatically generate questions that will help you delve deeper into cases or explore new lines of investigation.	•			•			•

Source: own creation

By using these AI LLMs, lawyers can automate routine tasks, make legal services leaner and more competitive, take on more clients as their personal time is freed up, and improve the speed and accuracy of outcomes in the client's favour (Legg & Bell, 2020). Such investments promise to recalibrate the competitive landscape of legal services, enhancing operational efficiency, expanding client reach, and improving the precision and speed of legal results. From Table 1, it can be seen that most of these LLMs provide functions for either summarizing legal research or automatically generating legal documents, reports and emails. Some of these AI tools clearly drive a paradigm where the effectiveness of legal practice is significantly enhanced by AI's ability to analyse, condense, and generate legal documents. This shift goes beyond mere efficiency, signalling a deeper, more fundamental transformation in how legal professionals engage with the corpus of legal knowledge. These tools, with their skill in simplifying complex legal narratives and facilitating intricate deal structuring, demonstrate AI's role as a powerful driver of innovation within legal frameworks. Their capacity to translate dense legal discourse into accessible insights not only streamlines workflows but also broadens access to nuanced legal analysis, thereby strengthening the strategic capabilities of legal practitioners. Notably, three out of these ten tools also offer legal strategy functionalities. Such legal strategy formulation is made possible by the enhancement of an ever-evolving legal database filled with detailed case information and documentation, which ultimately acts as a cornerstone for delivering precise legal analytics. This approach unquestionably provides legal professionals with relevant data-driven insights, representing a significant departure from traditional, intuition-based strategies and enriching the strategic foundation of legal practice with empirical accuracy.

A third option, less affordable for small firms, is the development of local, bespoke AI software by law firms and legal companies. One benefit of this approach is that it overcomes the challenge of ensuring alignment with the correct legal system and current legislation. Existing global chatbots and legal AI assistants may offer answers based on laws that exist but belong to a different jurisdiction than the one relevant to the user's query. Additionally, they may reference legislation that has already been repealed or

amended, which can lead to serious errors in legal interpretation or advice. In contrast, bespoke AI software guarantees jurisdictional accuracy and legal up-to-dateness, which are crucial when applying AI in legal contexts.

These tools assist in gathering data to enhance understanding of legal precedents and aid in complex tasks such as preparing court filings. For the present study, three AI tools developed by law firms of different sizes were selected: AI tool 1 (developed by a global law firm), AI tool 2 (from a large national firm), and AI tool 3 (owned by a small or medium-sized enterprise). The tools' names remain confidential for proprietary reasons. From a methodological standpoint, the study employed a qualitative case-study approach for this part of the research. Data about each of the three AI tools were collected through semi-structured interviews with key informants from the respective law firms, supplemented by analysis of internal documentation and publicly available materials (e.g., press releases, white papers). These three tools (N=3) form the core data points of the study, selected from a broader survey of AI tools to represent a diverse range of law firm types (a global firm, a large national firm, and an SME). This purposive selection ensured that the analysed instruments offer a comparative perspective across different organizational sizes, chosen for their representativeness and the availability of detailed information on their development and use. The findings were analysed qualitatively, focusing on aspects such as transparency, human oversight, and gender representation, consistent with previous literature on legal AI systems (Legg & Bell, 2020; Weinstein, 2022).

Table 2. Comparative analysis of three tailor-made AI tools created by law firms[1]

Tool	Uses	Pros	Cons	Info for clients	Servers	Supervision	Gender bias in terminology	Proposal for improvement
AI tool 1	Contract revision, redlining, summaries of judgments, draft of legal documents.	Trained in a specific legal domain; answers much more accurate within the legal field.	None.	Info published in press; workshops held with several clients; included in the general T&C.	EU.	Always requires an expert review by the IT and Knowledge Department. Expert lawyers always review the answers and improve them.	Answers depend a lot on the prompting. It is key to train in how to ask the tool.	Ensure final review and work to be able to train with own knowledge base.
AI tool 2	Analysis of legal document, proposal of ideas or strategies, preparation of legal documents, resolution of specific legal issues.	Generative AI model specifically trained in the legal field, faster than other LLMs, capable of synthesizing in just 2 minutes the positions of the seller/buyer in complex business purchase/sale contracts based on a "mark-up" prepared by the seller on the buyer's initial draft. Very good at doing legal translations.	The users need to invest some time in learning how the system works.	No, but the system is used only as an assistant in developing some tasks, never for final work. All work is ultimately performed by a lawyer.	EU.	A team of experts supervises the system.	Allows text with a split option.	It is a matter of time before these systems improve and perform more complex tasks. It is crucial that lawyers help train the system.

1. The information in this table is based on semi-structured interviews with senior staff members from each firm, internal documentation shared under confidentiality agreements, and publicly available sources such as press releases and technical briefings. A qualitative comparative approach was used to identify shared patterns and divergences in functionality, oversight and ethical safeguards.

Tool	Uses	Pros	Cons	Info for clients	Servers	Supervision	Gender bias in terminology	Proposal for improvement
AI tool 3	Contract drafting, case law gathering, drafting lawsuits/ court documents, analysis of documents for due diligence or audit, analysis of specifications to quickly know if it can be submitted to tender.	The quality of the answers, the legal rigor and broader knowledge of database. Allows users to be more effective, efficient and focus on valuable tasks.	Necessary to provide users training to get the most out of it.	Info via real practical cases from daily life and through demos.	EU.	Yes, able to correct possible errors, hallucinations, as well as introduce improvements based on learning.	Allows text with a split option.	Involve more lawyers, consultants, etc. to better detect needs and to expand the tool's uses.

Source: own creation

Although these AI tools were developed by firms with varying turnovers, their scope is remarkably similar. They perform tasks such as contract revisions, legal document drafting, judgment analysis, and due diligence audits. For example, AI tool 1 focuses on contract redlining and summarizing judgments, while AI tool 2 synthesises buyer and seller positions in business contracts. AI tool 3 supports contract drafting and case law collection. Regarding the benefits, all three tools are customized to the firms' specific legal areas, enabling greater accuracy and relevance when handling legal content. AI tool 2, for instance, was reported to quickly synthesize complex legal contracts, providing speed and precision unmatched by other LLMs. All tools also allow legal teams to concentrate on higher-value tasks by automating document analysis and synthesis, thereby increasing overall efficiency. Regarding disadvantages, two of the tools require substantial initial staff training, which can divert resources from immediate income-generating activities. AI tool 3, in particular, needs extensive training to ensure users can fully utilize its potential. Despite these challenges, human expertise remains essential in all cases. For example, AI tool 1 depends on the firm's IT and knowledge departments to supervise its use, ensuring that legal experts always validate the tool's outputs before finalising documents.

A key issue pointed out in this study is how unclear firms are about their use of AI in legal services. Only two out of three firms actually tell clients they use AI, and none mention it in their contracts. This lack of transparency raises several important concerns. Firstly, clients have a right to know how their legal matters are being handled, including when AI tools are involved. Secondly, they need to trust that using AI – especially LLMs – will not compromise the quality or professionalism of the service. Thirdly, there are ethical concerns, as AI can sometimes produce biased or inaccurate results, which could unfairly affect individuals based on gender, race, or social background. Fourth, accountability is an issue – firms must be clear about who is responsible for work carried out with AI. Finally, it is crucial to ensure that these tools do not perpetuate existing inequalities or discrimination.

Consequently, law firms must adopt clear communication strategies and ethical safeguards when deploying AI tools. Transparent client communication, proper oversight, and careful management of training data are essential steps to ensure AI's responsible and ethical integration into legal practice.

2. The importance of human intervention in the use of legal AI LLMs

While AI LLMs can provide considerable advantages for legal drafting, such as speed, accuracy, and efficiency, they always require human intervention and oversight to maintain quality, reliability, credibility, and ethics. Human intervention is essential for several reasons:

First, AI tools are not infallible. They may generate errors, inconsistencies, or inaccuracies in the outputs, especially when dealing with complex or novel legal issues. It is also common to encounter a phenomenon called "hallucination," where the AI tool provides an answer containing false or misleading information presented as fact. In this context, a study by BCG found that generative AI reduced the likelihood of correct answers in complex problem-solving tasks by 19% (Layne, 2023). Such errors and hallucinations highlight the importance of human oversight, not just for correcting mistakes but as a fundamental part of a responsible AI usage framework that upholds ethical standards and professional responsibility. Human lawyers should therefore always review and verify the outputs of AI LLMs and correct any errors or gaps, reinforcing the symbiotic relationship between AI technologies and legal professionals.

The use of AI by legal professionals can also raise issues of contractual liability. Contractual liability pertains to the obligation to compensate for damages resulting from breach or defective performance of a contract. For example, a lawyer might provide a client with a contract entirely generated by AI that contains erroneous clauses or ambiguous information. When it comes to AI, initial questions may arise about who is responsible for damages caused by its use – whether it is the provider of the AI system, the user, or the system itself. Although most professional codes in EU Member States suggest that legal professionals have an obligation to supervise all content produced by AI, clear guidelines and oversight mechanisms to address potential damages from inaccuracies in AI-generated legal texts are not yet established. For instance, in Spain, Article 21 of the code of ethics of the Spanish legal profession regarding the use of information technologies (Consejo General de la Abogacía, 2019) states that the use of information and communication technologies does not exempt practitioners from complying with deontological norms governing the profession or obligations imposed by regulators of the information society, but the code makes no specific reference to responsibility for AI content and decisions. It is important to clarify, however, that while the AI Act does not impose explicit human oversight duties for all legal applications, it requires human-in-the-loop mechanisms for high-risk AI systems, especially those used in the administration of justice. Although legal LLMs used by law firms typically do not fall under this category, their outputs could still impact fundamental rights or democratic processes – such as in cases of discriminatory outcomes – thereby necessitating human intervention under the AI Act.

Moreover, AI tools are not impartial. Recent evidence shows that lawyers should not automatically trust what is produced by large LLMs and AI chatbots such as ChatGPT when preparing a plaintiff or a legal brief (Novak, 2023; Farah, 2023). As discussed in the next section, AI tools may mirror or accentuate biases and prejudices from their developers, users, or data sources. For example, DoNotPay, a chatbot that used ChatGPT to offer legal assistance, faced controversy and ceased its legal services after allegations of discrimination, misinformation, and malpractice (Cerullo, 2023). Consequently, human lawyers must always supervise and assess the potential effects of AI tools and address any issues related to fairness, diversity, and inclusion.

Finally, AI tools are not autonomous. They rely on human inputs, instructions, and feedback to function properly and improve over time. As shown in Table 1 above, one of the most hyped and rapidly growing sectors of innovation in the legal field is the use of AI to predict the outcome of legal cases and thereby inform legal strategies, such as how to approach litigation (Legg & Bell, 2020). However, such predictions cannot be automated without human intervention. In this context, the AI Act sets out key principles and guidelines for the development and use of AI within the EU, including compliance, privacy, transparency, and accountability. The Act aims to foster an ecosystem where AI tools, including those in the legal sector, are developed and deployed in a manner that upholds the highest ethical and legal standards, addressing the complex fundamental rights considerations inherent to AI's integration into legal practices. Therefore, human lawyers must establish and adhere to clear and ethical rules and standards for the use of AI tools, ensuring their alignment with the legal system and societal values.

Human intervention is therefore crucial for using legal AI tools, as it guarantees the quality, reliability, credibility, and ethics of the generated texts. Human lawyers should not delegate their professional responsibilities or judgment to AI tools; instead, they should utilize them as complementary and supportive resources. In fact, human supervision remains essential, as the issue of liability for AI errors is still unresolved within the EU. The AI Act does not address this concern, and the proposed AI Liability

Directive (European Commission, 2022) has recently been withdrawn by the Commission, leaving cases of responsibility for damages caused by autonomous AI decisions uncertain; thus, human oversight is vital. Building on these legal and ethical considerations, the next section delves deeper into one of the most persistent and structural risks associated with legal LLMs: gender bias and algorithmic discrimination, particularly in relation to linguistic representation and fairness.

3. Discrimination and gender bias considerations

The increasing use of AI by legal professionals raises important ethical questions, particularly regarding discrimination and gender. This section examines how AI tools could introduce bias or discrimination, including gender bias, in legal practice across the EU. Although the terms discrimination and bias are closely related but refer to different phenomena, especially in social sciences, law, and AI. Therefore, while bias is a prejudiced *attitude* or tendency that influences judgment or perception (e.g., believing that women are less competent in STEM fields), discrimination involves *actions or behaviours* that result in unfair treatment of individuals or groups (e.g., not hiring a woman for a tech role despite her qualifications, because of her gender) (Barocas, Hardt & Narayanan, 2019).

3.1. Algorithmic discriminations in the EU laws

Algorithmic discrimination is clearly included within the legal concept of discrimination, but it has some distinct features. The legal definition of discrimination encompasses any unfair treatment of an individual or group, or the disproportionately harmful effects of a measure or policy on a specific group. Consequently, the term *discrimination* is broader than the legal concept of *algorithmic discrimination*, as the former refers to any kind of disadvantage that may be viewed as ethically or morally wrong, even if it is not illegal (Gerards & Xenidis, 2021). The challenge, therefore, is to improve AI tools with the ability to recognize and compensate for these subtle discriminations, ensuring their operation aligns with the ethical standards established by the legal community. Such improvements might include algorithmic modifications based on ongoing learning from diverse data sets and the implementation of ethical guidelines to govern AI behaviour within legal contexts. For some scholars (Gerards & Xenidis, 2021), the term algorithmic discrimination also includes any form of algorithmic bias that is problematic from the perspective of EU equality and non-discrimination laws.

Previous studies have already raised concerns about the potential of algorithmic discrimination to create challenges in the decision-making processes of the legal profession (Kleinberg *et al*., 2018, Colomina Saló et al., 2024), and such algorithmic risk assessments may continue if existing biases are present in historical data sets (Legg & Bell, 2020). The concept of algorithmic discrimination should be adapted to the legal framework that safeguards the principle of equality under the law. In the context of EU equality and non-discrimination law, and according to Article 19 TFEU, algorithmic discrimination should refer to any discrimination based on sex, race or ethnic origin, disability, sexual orientation, religion or belief, and age, as these are the grounds listed in that provision. However, the grounds for algorithmic discrimination appear to be broader under Article 21 of the Charter of Fundamental Rights of the EU (CFREU), which prohibits any discrimination based on any ground. The CFREU thus provides an open list of grounds for discrimination, including examples beyond those specified in Article 19 TFEU, such as social origin, genetic features, language, political or other opinions, membership of a national minority, property or birth.

Despite the extensive list of grounds of discrimination in the CFREU on which algorithmic discrimination could be based, the main issue is that such discriminations are sometimes not easily detectable, as they only indirectly discriminate against individuals or social groups. In the context of algorithmic decision-making, if an algorithm's design or implementation results in discriminatory outcomes – such as biased decisions on hiring, promotion, or pay – it could be regarded as indirect discrimination. The fact that it is indirect means it is not based on variables that the algorithm itself directly uses, but rather on the disadvantage or the different impact the algorithmic application has on members of protected groups (Morondo Taramundi, 2022). For example, if an AI-powered contract-drafting system used by law firms to produce employment agreements is trained on historical contracts, those contracts could reflect gender biases. If past contracts consistently underpaid female employees compared to their male counterparts, the AI might unintentionally adopt this discriminatory pattern. Consequently, organizations deploying algorithms must ensure

transparency, fairness, and accountability to prevent the reinforcement of gender-based disparities.

A law firm implementing an AI system has the responsibility to integrate this system carefully, strictly control access to its information and algorithms, and select solutions that offer strong safeguards in accordance with relevant data protection laws. Additionally, a law firm must choose the most suitable processing platforms or systems based on the sensitivity of the information they handle and use in their algorithms. For example, a law firm might, due to the nature of its data, opt for a local AI system with decentralized processing to prevent unsupervised algorithms, data leaks, or unauthorized third-party access.

However, there is an important caveat: if the algorithm's impact is objectively justified by a legitimate aim and the means used are appropriate and necessary, it may not be considered discrimination under EU laws. In those cases, we are dealing with "algorithmic bias" rather than "algorithmic discrimination", as explained in the following section. For example, algorithms may contain biases related to protected characteristics like age, race or gender. Some restrictions on employment, such as age requirements for physically demanding jobs, may be considered reasonable and necessary and, therefore, justified. Although there may be an age bias, it does not constitute discrimination because, in this case, the difference is justified and aligns with the legal framework. Therefore, when assessing the legal implications of an algorithm, it is important to consider the specific context and purpose for which it is used (FRA, 2022).

3.2. Gender biases when using LLMs for drafting legal documents

Algorithmic bias, described as "a systematic error of any kind in the outcome of algorithmic operation" (Bellamy, 2018), includes various types of errors – statistical, cognitive, societal, structural, or institutional – that can potentially lead to discrimination. In legal contexts, these biases are particularly troubling when they systematically disadvantage unprivileged groups, as emphasized in the concept of "algorithmic fairness" (Bellamy, 2018). This section examines how biases, especially gender biases, manifest in LLMs used for drafting legal documents, urging legal practitioners to consider how these biases may impact legal fairness and representation.

Biases in LLMs can be categorized into two main types: **a)** data bias, which occurs when the training data itself is biased (Navas Navarro 2023). For example, if an AI system for legal drafting is trained on historical case law where custody rulings predominantly favoured women; and **b)** outcome bias, which occurs when the results reflect unequal ground truths, even if the data is unbiased. This type of bias can surface when an LLM underrepresents certain demographics, resulting in skewed outputs in legal processes. While algorithmic bias does not necessarily surpass the bias already present in society, it can reproduce and amplify existing societal inequalities at scale, especially when deployed without sufficient oversight (Barocas, Hardt & Narayanan, 2019). Additionally, even the use of grammatically generic masculine terms can foster representational imbalance, reinforcing normative assumptions about professional roles and underrepresenting women in high-status legal contexts (Franzoni, 2023).

Furthermore, biases can be divided into three subcategories commonly found in LLMs (Crawford, 2017): **i)** Allocational bias, where the model allocates resources or opportunities unfairly, such as favouring certain demographics in legal rulings; **ii)** Representational bias, which occurs when social groups are underrepresented or stereotyped. For example, LLMs may disproportionately depict women in lower-status professions like secretaries rather than high-status professions like lawyers; and **iii)** Linguistic bias, which occurs in languages with grammatical gender, where LLMs may generate text that defaults to masculine forms, reinforcing male-centric perspectives (Franzoni, 2023).

To systematically explore how gender biases manifest in legal LLMs, this study has evaluated both the main commercially available LLMs for legal professionals and the main custom-made AI tools created by law firms, to identify linguistic and representational biases in both generic and domain-specific LLMs. The evaluation has focused on the presence of masculine defaults in gendered languages like Spanish, where grammatical gender can influence legal drafting. For instance, when generating legal documents in Spanish, tools may default to masculine forms for nouns and titles, reinforcing gender stereotypes. Table 3 provides an evaluation of gender bias in the Spanish language for the ClickUp AI tool, listed above. As demonstrated in the table, ClickUp exhibits diverse types of gender bias, with some prompts offering split options to mitigate bias, while others default to masculine terms without providing neutral or feminine alternatives

Table 3. Gender bias in ClickUp's AI Tool

Prompt #	Prompt (Spanish)	Translation	Gender bias detected	Options for avoiding bias
1	*Escrito de Demanda por despido improcedente.*	Lawsuit application for unjustified dismissal.	No.	Split options for gender.
2	*Contrato de trabajo a tiempo parcial.*	Part-time work contract.	Masculine form (*trabajador*).	N/A.
3	*Contrato laboral de personal directive.*	Work contract for manager position.	Masculine form (*trabajador*).	N/A.
4	*Demanda por denegación de permiso para cuidado de hijos.*	Lawsuit application for unjustified denial of a child-care leave.	Masculine form (*trabajador*).	Split options for some words (*hijo/hija*).
5	*Convenio de divorcio con custodia de hijos a favor de una de las partes.*	Divorce agreement with child custody to one party.	Masculine form (*abogado*).	Uses neutral form (*cónyuge*).
6	*Acuerdo Económico de Capitulaciones Matrimoniales.*	Prenuptial property agreement.	Masculine form (*abogado*).	Uses neutral form (*cónyuge*).
7	*Demanda de divorcio contencioso con de custodia de hijos, pensión de alimentos y pensión compensatoria.*	Divorce petition with custody and compensatory claims.	Masculine form (*abogado*).	Uses neutral form (*cónyuge*).
8	*Contrato de Alquiler de Vivienda.*	Residential rental agreements.	Masculine form (*arrendador/arrendatario*).	Split option for titles (*Sr./Sra*) but incorrect gender alignment.

Source: own creation

The biases found in ClickUp reflect wider patterns in LLMs used for legal practice. Many of these tools tend to default to masculine forms for roles such as "lawyer" (*abogado*) or "landlord" (*arrendador*), thereby reinforcing gender stereotypes in legal settings. However, these biases are not limited to Spanish. In English, legal LLMs frequently default to masculine terms like "landlord" without providing gender-neutral options like "lessor" or split forms such as "landlord/landlady".

A systematic assessment of various LLMs, including those created by law firms, showed that biases are often embedded in the training data, reflecting historical and cultural inequalities. For example, in prestigious professions such as law or medicine, LLMs tend to favour masculine terms, whereas in caregiving roles or lower-status jobs, feminine terms are more prevalent. This bias is problematic because it can result in underrepresentation or stereotyping, thereby reinforcing damaging societal norms.

To address gender bias in LLMs, we can take a few simple yet essential steps. First, it is crucial to use balanced training data that fairly represents all genders, especially in how various professions are depicted. Next, legal professionals should learn to craft prompts in a gender-neutral manner or clearly specify when gender-specific information is necessary. Regularly reviewing and updating the systems to identify and replace gendered language with more neutral options is also beneficial. Lastly, transparency is important: law firms should inform clients when AI tools are used and be transparent about any limitations or potential biases of these tools. By ensuring training data is balanced and designing LLMs with gender neutrality in mind, developers and legal professionals can reduce the risk of reinforcing gender biases in legal document generation. Although this type of transparency does not eliminate bias entirely, it promotes accountability and encourages law firms to actively monitor and address gender bias.

4. Gaps and areas for improvement in the current practice

As AI begins to integrate into the daily tasks of lawyers, it is crucial to establish best practices to ensure the quality, reliability, and fairness of the generated texts. This section offers recommendations for lawyers and legal practition-

ers on how to use AI LLMs and tools responsibly and to meet their professional obligations.

First, legal practitioners should uphold their professional duties such as competence, independence, and safeguarding client confidentiality (Legg & Bell, 2020). Recently, the number of official requests asking for clarification on guidelines for lawyers regarding the use of generative AI in managing cases has increased significantly (for instance, USPTO 2024). In this sense, one area where legal professionals using AI could dedicate more effort and resources is the development and implementation of Rules of Conduct for AI use in legal practice. Although each Member State within the EU has its own code of conduct for lawyers, the Council of Bars and Law Societies of Europe (CCBE) has issued a Model Code of Conduct for European Lawyers (CCBE, 2021), which, unfortunately, does not reference the use of AI or technological tools within the document. Therefore, codes in EU countries could explicitly outline the ethical responsibilities related to the use (or non-use) of AI by lawyers, including duties of competence (and diligence), communication, confidentiality, and supervision (Cerny *et al*., 2019). For example, updated codes could include clauses that require lawyers to inform clients about the risks and limitations of any AI they consider using, and to oversee work assisted by AI (Gordon & Ambrose, 2017).

Furthermore, in the changing landscape of legal documentation, the use of AI in drafting processes requires a reassessment of transparency standards. Introducing a watermark or a clear indicator showing that no human intervention was involved in fully AI-generated documents could be a solution. A pioneering step might be the introduction of "AI Transparency Certificates" for documents created with AI support, offering a detailed report on the AI's role, the data it was trained on, and the human oversight involved. This approach aligns with the transparency principle (recital 58 GDPR), ensuring all parties are aware of the document's origin and the level of AI involvement. It acts as a safeguard against ethical issues, such as undisclosed automation, and preserves the integrity of the legal process. Additionally, it clarifies responsibility and accountability, especially in cases where legal outcomes are challenged. As AI continues to integrate into legal practices, such indicators will be vital in maintaining the values of honesty and transparency that underpin trust in legal institutions and their outputs.

Service contracts between lawyers and clients could also include a few clear clauses. These might cover whether AI will be utilized in the client's case, how their data will be kept confidential, and a commitment that human professionals will always supervise AI decisions. The contract could also describe how the firm adheres to ethical AI standards, give clients the option to agree or opt out of AI use, and clarify who is responsible if something goes wrong with an AI-driven decision.

Moreover, there is a need for AI training specifically dedicated to legal professionals. Currently, very few specialized postgraduate courses for lawyers cover AI, and many lawyers using AI within their law firms lack sufficient training on the software they utilise. In this context, lawyers working with AI should be required to develop an understanding of the technical assumptions and foundations of AI to anticipate future advancements (Legg & Bell, 2020). Specifically, legal professionals need to understand the capabilities and limitations of AI tools, and proper training ensures they comprehend how AI algorithms function, interpret results, and make informed decisions. Without appropriate training, lawyers risk misusing or misinterpreting AI-generated outputs, which could lead to errors or unintended consequences. Additionally, as mentioned earlier, AI tools may inadvertently reinforce biases or produce discriminatory outcomes, so legal experts should be aware of the ethical considerations involved. Training can help lawyers navigate legal and regulatory frameworks related to AI, ensuring compliance with non-discrimination laws and privacy regulations. In conclusion, legal experts should see AI as a collaborative tool rather than a substitute. Adequate training fosters a mindset that combines human expertise with AI capabilities.

Finally, there is a need for monitoring bodies and mechanisms that assess the effects of algorithm-based legal decisions (Morondo Taramundi, 2022). Although Table 2 above shows that all three tailor-made tools include a supervisory team of AI experts who monitor the functioning of the tool, such a role could be established in law in the same way that companies processing the personal data of EU citizens are required to incorporate a data protection officer under the terms of the GDPR. Another additional mechanism could be the implementation of regular audits of the AI models to ensure that the algorithms minimize potential biases in the use of legal documents that display discriminative elements based on race, sex, religion, national origin, ethnicity, disability, age, sexual orientation,

gender identity, marital status, or socioeconomic status. Ultimately, the need for lawyers to understand how AI generates outputs is important for reducing bias and providing sound counsel to clients (Cerny, 2019).

Conclusions

This article identifies and examines the main LLMs used by lawyers. Despite the differences among these LLMs, this study demonstrates that integrating AI LLMs into legal practices signals a transformative era, moving beyond traditional methods to redefine efficiency, accuracy, and innovation in legal work. This shift signifies a major change towards increasing productivity, automating complex legal tasks, and enabling deep analytical insights. The use of AI in areas such as, but not limited to, drafting legal documents, reviewing contracts, or researching specific legal issues highlights the significant benefits of technology in improving legal service delivery to a range of clients.

These technologies, despite their varied applications, collectively highlight a paradigm where legal operations are not just optimized but reimagined. AI's role in enhancing the drafting of documents, streamlining contract reviews, and providing predictive analytics exemplifies the strategic integration of digital intelligence into the heart of legal workflows. This move towards a more data-driven, automated, and intellectually enriched legal practice aims to raise the standard of legal services, making them more accessible, accurate, and client-centred.

However, the legal community must address existing concerns around algorithmic discrimination and gender bias to promote fairness in AI-assisted legal decisions. This article has thoroughly analysed potential risks associated with using LLMS for legal purposes, particularly in relation to algorithmic discrimination and gender biases. To reduce such risks, transparency between law firms and their clients regarding AI use in legal matters is crucial for maintaining trust and ethical standards. Furthermore, establishing watchdogs to monitor AI applications within the legal sector will help ensure compliance with non-discrimination and privacy regulations.

This study highlights the urgent need to update and define the ethical and gender-based rules that govern the use of AI in the legal profession. To implement these rules effectively, education and training are essential for legal professionals to integrate AI tools into their daily practices responsibly, as if AI were a colleague. Understanding both the capabilities and the limitations of AI can help lawyers use technology to support their expertise rather than replace human judgment. Essentially, lawyers must employ these technologies carefully, ensuring their use aligns with the fundamental principles of justice and fairness that underpin their professional responsibilities. Additionally, open communication between law firms and clients regarding AI adoption is vital to foster trust, ensure compliance, and uphold ethical standards in the legal field.

Therefore, in light of the evident integration of AI into the legal landscape, it is imperative that the legal community proactively defines the parameters and guidelines for AI adoption. Ultimately, AI should not replace human expertise but rather augment the capabilities of the legal profession. While the future undoubtedly involves lawyers and law firms collaborating with AI systems, the critical task lies in delineating the ethical, regulatory, and practical boundaries within which AI operates, so that the legal sector can take advantage of the opportunities offered by technological advances while mitigating its risks.

References

1. Doctrine

BAROCAS, S.; HARDT, M.; NARAYANAN, A. (2019). *Fairness and Machine Learning: Limitations and Opportunities* [online]. Available at: https://fairmlbook.org/

BELLAMY, R.K.E.; DEY, K.; HIND, M.; HOFFMAN, S.C.; HOUDE, S.; KANNAN, K.; LOHIA, P.; MARTINO, J.; MEHTA, S.; MOJSILOVIC, A.; NAGAR, S.; NATESAN, RAMAMURTHY, K.; RICHARDS, J.; SAHA, D.; SATTIGERI, P. (2018). "AI Fairness 360: An Extensible Toolkit for Detecting, Understanding, and Mitigating Unwanted Algorithmic Bias". *arXiv*. DOI: https://doi.org/10.48550/arXiv.1810.01943. [Accessed: 01 March 2025].

COLOMINA SALÓ, C.; INNERARITY, D.; CANTERO GAMITO, M. (2024). "Desigualdad algorítmica: gobernanza, representación y derechos en la IA". *Revista CIDOB d'Afers Internacionals*, no. 138.

FRANZONI, V. (2023). "Gender Differences and Bias in Artificial Intelligence". In: Vallverdú, J. (eds.). *Gender in AI and Robotics. Intelligent Systems Reference Library*, vol. 235. Springer. DOI: https://doi.org/10.1007/978-3-031-21606-0_2

KLEINBERG, J.; LUDWIG, J.; MULLAINATHAN, S.; SUNSTEIN, C.R. (2018). "Discrimination in the Age of Algorithms". *Journal of Legal Analysis*, vol. 10, pp. 113-174. DOI: https://doi.org/10.1093/jla/laz001

LEGG, M.; BELL, F. (2020). *Artificial Intelligence and the Legal Profession*. 1st ed. New York: Hart Publishing. DOI: https://doi.org/10.5040/9781509931842

MORONDO TARAMUNDI, D. (2022). "Discrimination by Machine-Based Decisions: Inputs and Limits of Anti-discrimination". In: Bart Custers, B. & Fosch-Villaronga, E. (eds.). *Law and Artificial Intelligence. Regulating AI and Applying AI in Legal Practice*, 1st ed. Leiden: Springer. DOI: https://doi.org/10.1007/978-94-6265-523-2

NAVAS NAVARRO, S. (2023). *ChatGPT y modelos fundacionales. Aspectos jurídicos de presente y futuro*. Madrid: Editorial Reus.

PARK, J. (2020). "Your Honor, AI". *Harvard International Review*, vol. 41, no. 2, pp. 46-48 [online]. Available at: https://www.jstor.org/stable/26917302

SAVOLDI, B.; GAIDO, M.; BENTIVOGLI, L.; NEGRI, M.; TURCHI, M. (2021). "Gender Bias in Machine Translation". In: *Transactions of the Association for Computational Linguistics*, vol. 9, pp. 845-874. DOI: https://doi.org/10.1162/tacl_a_00401

WAISBERG, N.; HUDEK, A. (2021). *AI for lawyers. How artificial intelligence is adding value, amplifying expertise and transforming careers*. 1st ed. Hoboken: Wiley.

WEINSTEIN, S. (2022). "Lawyers' Perceptions on the Use of AI". In: Bart Custers, B. & Fosch-Villaronga, E. (eds.). *Law and Artificial Intelligence. Regulating AI and Applying AI in Legal Practice*. 1st ed. Leiden: Springer. DOI: https://doi.org/10.1007/978-94-6265-523-2

2. Legal documents

EUROPEAN COMMISSION (2022). *Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive)*, COM(2022) 496 final, 28.09.2022.

EUROPEAN COMMISSION (2008). *Proposal for a Council Directive on implementing the principle of equal treatment between persons irrespective of religion or belief, disability, age or sexual orientation (Directive against discrimination beyond the workplace)*, COM/2008/0426 final, 02.07.2008 - CNS 2008/0140.

EUROPEAN UNION (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, OJ L 119, 04.05.2016, pp. 1-88.

EUROPEAN UNION (2024). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations* (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU,

(EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance) PE/24/2024/REV/1, OJ L, 2024/1689, 12.07.2024, pp. 1-144.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2022). *Bias in Algorithms: Artificial Intelligence and Discrimination, Report*. Luxembourg: Publications Office of the European Union [online]. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2022-bias-in-algorithms_en.pdf. Accessed on 26.02.2025

CONSEJO GENERAL DE LA ABOGACÍA (2019). *Código Deontológico de la Abogacía Española. Aprobado por el Pleno del Consejo General de la Abogacía Española*, 6 of March of 2019. Abogacía [online]. Available at: https://www.abogacia.es/wp-content/uploads/2019/05/Codigo-Deontologico-2019.pdf. [Accessed: 08 February 2025].

UNITED STATES PATENT AND TRADEMARK OFFICE (2024). *The applicability of existing regulations as to party and practitioner misconduct related to the use of artificial intelligence*, 6 February 2024. USPTO [online]. Available at: https://www.uspto.gov/sites/default/files/documents/director_guidance_ai_use_legal_proceedings.pdf. [Accessed: 14 February 2025].

3. Reports, news and websites

CERULLO, M. (2023). "AI-powered 'robot' lawyer won't argue in court after jail threats". *CBS News* [online]. Available at: https://www.cbsnews.com/news/robot-lawyer-wont-argue-court-jail-threats-do-not-pay/. [Accessed: 07 February 2025].

CERNY, J.; DELCHIN, S.; NGUYEN, H. (2019). "Legal Ethics in the Use of Artificial Intelligence". [Online]. Available at: https://download.pli.edu/WebContent/pm/249218/pdf/02-22-19_1600_115843_LegalEthics.pdf. [Accessed: 22 February 2025].

CLIO (2024). "What is AI and How Can Law Firms Use it?". *Clio* [online]. Available at: https://www.clio.com/resources/ai-for-lawyers/lawyer-ai/. [Accessed: 13 February 2025].

COUNCIL OF BARS AND LAW SOCIETIES OF EUROPE (2021). *Model Code of Conduct for European Lawyers*. *CCBE* [online]. Available at: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_CoC/EN_DEONTO_2021_Model_Code.pdf. [Accessed: 22 February 2025].

CRAWFORD, K. (2017). "Deconstructing Gender Prediction in NLP". In: *Conference on Neural Information PROCESSING SYSTEMS (NIPS) – Keynote*, Long Beach, USA [online]. Available at: https://www.youtube.com/watch?v=fMym_BKWQzk. [Accessed: 01 March 2025].

FARAH, H. (2023). "Court of appeal judge praises 'jolly useful' ChatGPT after asking it for legal summary". *The Guardian* [online]. Available at: https://www.theguardian.com/technology/2023/sep/15/court-of-appeal-judge-praises-jolly-useful-chatgpt-after-asking-it-for-legal-summary. [Accessed: 13 January 2025].

GÓMEZ, J. (2024). "Lawbots". *Joel Gomez* [online]. Available at: https://joelgomez.abogado.digital/lawbots/. [Accessed: 16 February 2025].

GERARDS, J.; XENIDIS, R. (2021). *Algorithmic discrimination in Europe: Challenges and opportunities for gender equality and non-discrimination law. A special report*. Luxembourg: Publications Office of the European Union [online]. Available at: https://ai.equineteurope.org/system/files/2021-04/EELN_Algorithmic-discrimination_GERARDS%20and%20XENIDIS_2021.pdf

GORDON, D.L.; AMBROSE, R. (2017). "The Ethics of Artificial Intelligence". In*: The Jackson Lewis Corporate Counsel Conference. The Future of Work. Lexology* [online]. Available at: https://www.lexology.com/library/detail.aspx?g=0d-9dc2d0-bb79-4983-8dbf-13df60b9a566. [Accessed: 01 February 2025].

LAYNE, R. (2023). "Humans vs. Machines: Untangling the Tasks AI Can (and Can't) Handle". *Harvard Business School* [online]. Available at: https://hbswk.hbs.edu/item/humans-vs-machines-untangling-the-tasks-ai-can-and-cant-handle. [Accessed: 07 February 2025].

MATICH, T.; LENON, J. (2024). "The Best Free Legal Research Tools". *Clio* [online]. Available at: https://www.clio.com/blog/best-free-legal-research-tools/. [Accessed: 13 January 2025].

NOVAK, M. (2023). "Lawyer Uses ChatGPT In Federal Court And It Goes Horribly Wrong". *Forbes* [online]. Available at: https://www.forbes.com/sites/mattnovak/2023/05/27/lawyer-uses-chatgpt-in-federal-court-and-it-goes-horribly-wrong/?sh=1a6d49643494. [Accessed: 13 February 2025].

YORK, A. (2024). "10 Legal AI Tools for Legal Practices and Professionals in 2024". *ClickUp* [online]. Available at: https://clickup.com/blog/ai-tools-for-lawyers/. [Accessed: 16 February 2025].

Recommended citation

BLASI CASAGRAN, Cristina; BALLESTA MARTÍ, Lidia; ROBERT GUILLÉN, Santiago; BLASI CASAGRAN, Eduard (2025). "Navigating the AI legal landscape. Gender implications of large language models in legal text generation". *IDP. Internet, Law and Politics Journal*, no. 44. UOC [Accessed: dd/mm/yy]. DOI: http://dx.doi.org/10.7238/idp.v0i44.432721

About the authors

Cristina Blasi Casagran
Autonomous University of Barcelona
cristina.blasi@uab.cat
ORCID: https://orcid.org/0000-0002-4327-2212

Cristina Blasi Casagran has a PhD in Law from the European University Institute (Florence) and is currently an Associate Professor at the Law Faculty of the Universitat Autònoma de Barcelona (UAB), specializing in EU law, AI governance, and data protection. She coordinated the H2020 project ITFLOWS and has published widely on migration, digital rights, and the societal impacts of emerging technologies as well as AI regulation. Cristina regularly contributes policy insights for European initiatives and multi-stakeholder fora, bridging research and practice to promote trustworthy, rights-respecting AI across public and private domains.

Lidia Ballesta Martí
Autonomous University of Barcelona
lidia.ballesta@uab.cat
ORCID: https://orcid.org/0009-0002-5547-1566

Dr. Lidia Ballesta Martí is a researcher and Lecturer in Public International Law and European Union Law at the Autonomous University of Barcelona (UAB). She holds a PhD in International Law and a master degree in European Integration from the Autonomous University of Barcelona (UAB). Her current research focuses on EU Law, gender, non-discrimination, and digital law. In addition to her academic work, she has practised as a lawyer and legal advisor for over twelve years.

Santiago Robert Guillén
Autonomous University of Barcelona
santiago.robert@uab.cat
ORCID: https://orcid.org/0000-0002-6919-6801

PhD in Law. Faculty member in the Department of Private Law at the Universitat Autònoma de Barcelona (UAB) and Associate Lecturer at the Universitat Oberta de Catalunya (UOC). Academic Director of the master Programme in Artificial Intelligence and Digital Law at UAB. Member of the Association for the Study and Teaching of Copyright (ASEDA).

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Eduard Blasi Casagran
Autonomous University of Barcelona
eduard.blasi@dataguardians.net
ORCID: https://orcid.org/0009-0003-0155-8989

Legal scholar and practitioner specializing in technology law, privacy, and data protection. He holds a Law degree from the Universidad Autónoma de Barcelona (Spain) and a postgraduate diploma in Protection of Data and Privacy from the Universidad de Murcia. He has been Vice President (3º) of the Asociación Profesional Española de Privacidad (APEP) (2016-2025) and is currently a lecturer on IA regulation and digital law at the Autonomous University of Barcelona.

IDP
REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Manufacturer's liability for continuous product learning

Guillem Izquierdo Grau
Universitat Autònoma de Barcelona

Date of submission: July 2025
Accepted in: October 2025
Published in: March 2026

Abstract

This paper aims to explore a novel aspect of Directive (EU) 2024/2853 (PLD): the manufacturer's liability for continuous product learning. This is a new criterion for evaluating product defectiveness that integrates artificial intelligence. The PLD pays limited attention to this matter, so the study aims to identify the conditions under which a product's continuous learning might be deemed defective. Firstly, it is argued that this basis for assessing whether a product is defective should be understood to apply to generative AI systems, rather than to AI systems that do not change their behaviour after deployment. Secondly, the ten-year limitation period for holding the manufacturer liable, starting from the time the product was placed on the market or put into service, seems unsuitable for products that undergo continuous learning, as their features may change over time. Thirdly, the crucial factor enabling the manufacturer's liability is that the product remains within the manufacturer's control, allowing modifications to correct defects caused by continuous learning.

Keywords

manufacturer liability; continuous product learning; autonomous learning; product liability

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Responsabilidad del fabricante por el aprendizaje continuo del producto

Resumen

El objetivo de este documento es explorar un aspecto novedoso de la Directiva (UE) 2024/2853 (PLD): la responsabilidad del fabricante por el aprendizaje continuo del producto. Este es un nuevo criterio para evaluar la falta de calidad del producto que integra inteligencia artificial. El PLD presta una atención limitada a este asunto, por lo que el estudio tiene como objetivo identificar las condiciones en las que el aprendizaje continuo de un producto podría considerarse defectuoso. En primer lugar, se argumenta que esta base para evaluar si un producto es defectuoso debe entenderse como aplicable a los sistemas de IA generativos, en lugar de a los sistemas de IA que no cambian su comportamiento tras la implementación. En segundo lugar, el período de limitación de diez años para responsabilizar al fabricante, a partir del momento en que el producto se comercializó o se puso en servicio, parece inadecuado para productos que se someten a aprendizaje continuo, ya que sus características pueden cambiar con el tiempo. En tercer lugar, el factor crucial que permite hacer responsable al fabricante es que el producto permanece bajo su control, lo que permite realizar modificaciones para corregir defectos derivados del aprendizaje continuo.

Palabras clave

responsabilidad del fabricante; aprendizaje continuo del producto; aprendizaje autónomo; responsabilidad del producto

Introduction

Products with digital elements that include AI systems have emerged in the market and are in high demand by consumers who wish to use such products to enhance the effectiveness of certain actions or tasks. The development of new product technologies and generative artificial intelligence (AI) has made Directive 85/374/EEC obsolete. In this context, the OJEU of 18 November 2024 published Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products, repealing Council Directive 85/374/EEC (PLD),[1] given that, in the field of product liability, the increasing technical complexity of products is leading to greater difficulties in obtaining compensation for damage caused by defective products, particularly due to the challenges in gathering the evidence needed to hold the manufacturer liable for the damage.

The potential for a product to become defective due to the AI system integrated within it is specifically mentioned in Article 7.2.c) PLD, which refers to "the effect on the product of any ability to continue to learn or acquire new features after it is placed on the market or put into service". The PLD pays little attention to this aspect, that is, how AI may contribute to a product being classified as defective, as can be observed from a careful reading of its articles and recitals, despite it being one of the newest considerations to be included in the Directive.

Therefore, this work aims to analyse the impact of a product's continuous learning on manufacturer liability after it is placed on the market or put into service, examining how continuous product learning occurs and the extent of measures manufacturers should adopt to mitigate or eliminate the risks associated with AI systems embedded in their products.

1. Hardware, software and artificial intelligence: what characterizes a product that incorporates AI?

1.1. A new understanding of products

The main reason for adopting a new directive in this area is to update regulations in response to the complex nature of new products entering the market: namely goods with digital elements that may include AI systems. The key feature of

1. Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC (OJEU No. 2853 of 18 November 2024).

these goods is that they can be classified as either tangible movable goods (hardware) or digital elements. Moreover, in the digital era, not all products are tangible, as digital products or services (such as operating systems, computer programmes, applications or AI systems) have been introduced that are not necessarily part of a tangible movable good but can be downloaded and later integrated into products outside the manufacturer's control (Recital 13 PLD).

The issues concerning the classification of this type of goods as a product under Directive 85/374/EEC are well known (Wanderhorst, 2021, pp. 64-66). This is why the PLD aims to resolve the existing doctrinal debate by including software, digital services, and content within the scope of the new regulation, regardless of how they are supplied. In this regard, Art. 4.1) PLD defines the concept of product as follows: "'product' means all movables, even if integrated into, or interconnected with, another movable or an immovable; it includes electricity, digital manufacturing files, raw materials, and software".

The definition of "product" in the proposed Directive is based on the definition contained in Directive 85/374/EEC. The core element of the new definition of product is that it is movable and can be integrated into another movable or immovable good. So far, the definition in the PLD does not introduce anything new. However, the definition then adds two new concepts not present in the definition of product given by Directive 85/374/EEC, in addition to electricity: digital manufacturing files, raw materials such as gas and water, and software (Recitals 16 and 17 PLD).

Recital 16 PLD provides guidance on interpreting what is meant by "digital manufacturing files", as opposed to "digital files". The former includes "the functional information necessary to produce a tangible item". Therefore, digital manufacturing files are those that contain the information required to create new products. In contrast, according to Recital 16 PLD, digital files cannot be classified as products. These are files that do not contain coded information to produce new items, such as photographs and video or audio files (Recital 13 PLD in fine). The PLD might have referred to such digital files as mere digital content, a concept used by Art. 2(1) Directive (EU) 2019/770 (DCDS) for files of this kind, thereby ensuring internal coherence with other European legislation on contractual and non-contractual liability.

For its part, Recital 17 PLD refers to digital services. Art. 4 PLD does not contain a definition of the concept of digital services, meaning that the guidance given by Recital 17 PLD is particularly relevant for correctly tackling this concept. However, it is a concept that is also defined in Art. 2.2) DCDS.[2]

According to Recital 17 PLD, in the case of digital services, the criterion of integration into or interconnection with tangible products must be satisfied if the provisions of the PLD are to be applied to this type of product. Although Recital 17 PLD states that it should not apply to digital services as such, its effects should be extended to digital services when these are integrated into or interconnected with products in a way that the product could not perform its functions without them, and within the manufacturer's control. To this effect, Recital 17 PLD mentions, for example, the continuous supply of traffic data in a navigation system. Therefore, in my view, the criterion of whether software or digital services are integrated into or interconnected with products is crucial if the PLD is to apply to damage caused by digital services, especially when these services are a key factor in the product's safety or functionality.

However, a more contentious issue would be an AI chatbot that, unlike the examples provided in Recital 17 PLD, does not determine a product's safety or functionality. In this case, the chatbot is not an AI system that determines a product's safety or functionality; rather, it is a type of software distributed as a service ("software as a service," or SaaS) that could harm the user as a result of information entered into the system via a dialogue box. For instance, consider a user with a fever asking an AI chatbot for medical advice. In this case, the manufacturer of the computer or smartphone would not be liable under the PLD. Furthermore, Recital 13 PLD clarifies that information shall not be regarded as a product.[3]

2. Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (OJEU no. 136 of 22 May 2019).
3. In the same regard, see Herbosa Martínez (2024, p. 74) and Wagner (2023, p. 203). "Imagine a 'digitised' version of the Krone case: if the incorrect treatment advice had been published in an electronic newspaper, the publisher would be liable for this under general tort law, but not the manufacturer of the smartphone under the Product Liability Directive".

Recital 13 PLD clarifies that software, such as firmware, computer programmes, applications or AI systems, are products, regardless of how they are supplied, i.e. whether they are incorporated into the market as standalone products or integrated into other products as components. They are intangible products that fall within the definition of a product in Art. 4(1) PLD. With this categorization, the European legislator closes one of the debates surrounding the definition of product provided in Directive 85/374/EEC.[4] The clarification is welcome for the purpose of increasing legal certainty for injured parties and those affected by defective products: both tangible and intangible products are considered products for all purposes of the PLD.

However, Recitals 13 and 17 PLD must be contrasted, as the concepts of "product" (Art. 4(1) PLD), "related service" (Art. 4(3) PLD), and "component" (Art. 4(4) PLD) have distinct meanings. If intangible elements such as computer programmes, applications, or AI systems are regarded as products (Art. 4.1 *in fine* PLD in conjunction with Recital 13 PLD), it broadens the idea of a product to include intangible products that were excluded from this concept in Directive 85/374/EEC. Now that the concept of a product has been expanded to include intangible products, such items as computer programmes, applications, or AI systems should be considered either as a "related service" or a "component", since they will be part of devices or machines regarded as products (Art. 4.1 PLD).

Regarding the AI systems elevated by Recital 13 PLD to the category of products, the interdependence or interconnection of these systems with a product, which is the basis for them being considered as a related service or component, follows from the definition in Art. 3(1) AI Act, which emphasises that an AI system is a "machine-based system," meaning that such systems can also function as a related service or as a component of a tangible product.[5]

Therefore, intangible products such as computer programmes, applications, or AI systems are, beyond any doubt, considered products for the purposes of the PLD, which represents a step forward from the definition of product given in Directive 85/374/EEC. However, these intangible products must be added to a machine or device, which is why they should be regarded as being incorporated or interconnected as a "related service" or "component" within a tangible or movable product, as long as they are not distributed as SaaS and do not compromise the security or functionality of a product that relies on internet connection services.

Once the concept of product is clearly understood based on the definition in the PLD, it becomes necessary to examine the characteristics of products with digital elements, including AI systems, to understand the risks and impacts of their continuous learning.

1.2. Artificial intelligence applied to products

Products, as understood at the time of adopting Directive 85/374/EEC, were subject to the control of the individual, who used them to satisfy his or her needs in accordance with the intended use of the product (Art. 6.1.b) Directive 85/374/EEC). Even if they were equipped with software, this, although integrated into the product, was preprogrammed and carried out its functions based on the commands of the individual. Currently, software in products has gained new functionalities, to the point where it can make decisions without following a strict, pre-set, and unidirectional pattern. In other words, the product can make its own decisions depending on its circumstances and the external stimuli it receives (Wagner, 2023; Abbot, 2020, pp. 32-35). This fact indicates that a product containing an AI system can cause harm to third parties due to its unpredictable behaviour. The PLD does not establish different levels of liability based on the AI system's degree of autonomy in continuous learning, in accordance with Art. 3(1) AI Act.[6] There are deterministic computational AI systems where the outcome or prediction is entirely predictable because the system has no autonomous learning capability after deployment. However, deep-learning AI systems can continue learning after deployment, making

4. Supra, note 2.
5. Gómez Ligüerre (2025). "las víctimas de los sistemas de inteligencia artificial lo serán con motivo del uso de un producto, artefacto o aparato que incorpore, de manera principal o como uno de sus componentes operativos uno de tales sistemas que, como los define el artículo 3.1 del Reglamento de IA están 'basados en una máquina'".
6. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (OJEU no. 1689 of 12 July 2024).

it difficult or impossible to trace the final result. In my view, continuous learning as a basis for defectiveness should specifically apply to generative AI systems – those that keep learning from their environment. In contrast, AI systems that do not change their behaviour once on the market cannot be regarded as genuinely engaging in continuous learning. Therefore, I believe this ground for defectiveness should refer to generative AI, which adapts to the operational environment in which the product is deployed (Navas Navarro 2022, 2-5).

2. Legal status of the manufacturer: brief reference to the AI Act

On 14 May 2024, the Council endorsed a proposed regulation on artificial intelligence, following its approval by the European Parliament on 13 March 2024. Finally, the ordinary legislative procedure was completed with the publication of the Artificial Intelligence Act (AI Act) in the OJEU on 12 July 2024. One of the key new features of the AI Act is that, in order to protect users and consumers, it will apply to product manufacturers who place on the market or put into service an AI system along with their product and under their own name or trademark (Art. 2.1.e). The European legislator aims to require manufacturers of products incorporating AI to adhere to the obligations of the AI Act when the AI system is integrated or installed in the product.

However, in light of the provisions of Recital 87 AI Act, it appears that the AI Act distinguishes between different functions of an AI system once integrated into a product, specifically recognizing whether the AI system is a "safety component" or not. Recital 87 AI Act emphasises the role of the AI system as a safety component. The concept of 'safety component' is defined in Art. 3(14) AI Act as follows: "'safety component' means a component of a product or of an AI system which fulfils a safety function for that product or AI system, or the failure or malfunctioning of which endangers the health and safety of persons or property". Based on these considerations, an AI system functioning as a safety component within a product is responsible for controlling the product's operation, preventing it from endangering the health and safety of persons.

The fact that the AI system therefore acts as a safety component is one of the factors to consider when determining that the product manufacturer should be required to comply with the obligations set out in the AI Act (Art. 6.2 AI Act, together with Annex III). However, there are AI systems that do not function as a product safety component, in the sense that they cannot compromise the health or safety of individuals, but which are classified as high-risk by the AI Act. An example of these are consumer creditworthiness assessment AI systems. In such cases, Art. 2.2 AI Act significantly reduces the legal requirements that manufacturers must meet for products falling under Section B of Annex I AI Act, without affecting the provisions of sectoral legislation applicable to these products.

Art. 25.3 of the AI Act addresses this issue and states that, when a high-risk AI system functions as a safety component of a product listed in Section A of Annex I of the AI Act, the manufacturer must act as the provider of the AI system and comply with the obligations set out in Art. 16 of the AI Act. Examining the harmonized legislative acts listed in Section A of Annex I of the AI Act, they relate to products the malfunctioning of which could be particularly dangerous for people's health and safety, such as machines, toys, recreational craft, lifts, safety components and others. For this reason, adhering to the legal requirements of Art. 16 of the AI Act is crucial.

This does not mean that the AI Act only covers systems that are safety components of products that fall within the scope of the harmonisation legislation in Section A of Annex I AI Act, rather than an AI system can be classified as high-risk according to the AI Act criteria, but integrated into products mentioned in Section B of Annex I AI Act. In this case, Art. 2.2 AI Act relaxes the obligations of manufacturers whose products include AI systems mentioned in Section B of Annex I. This applies to manufacturers of motor vehicles, which may contain AI systems that serve as safety components.

Accordingly, it is evident that the AI Act mainly focuses on AI systems integrated into products as safety components. When these are classified as high-risk and are incorporated into products mentioned in Section A of Annex I, manufacturers must adhere to the requirements for high-risk AI systems outlined in the AI Act. Otherwise, if the AI systems are classified as high-risk but are included in devices listed in Annex B, only the obligations under Articles 6 (1), 102-109, and 112 of the AI Act apply (Art. 2.2 AI Act). Notwithstanding the above, in the case of the high-risk AI systems listed in Annex B AI Act, compliance with the legal requirements enforceable under sectoral

legislation is mandatory (Recital 64 AI Act). Thus, the AI Act aims to establish general provisions, without affecting sectoral legislation that imposes additional requirements on those deploying AI systems.

3. Continuous learning of the product after being placed on the market or put into service

The continuous learning of a product after it is introduced to the market or put into service is a trait of products with digital elements that include generative AI systems. Art. 7.2.c) PLD refers to this aspect when assessing a product's defectiveness: "the effect on the product of any ability to continue to learn or acquire new features after it is placed on the market or put into service." Although this ability to keep learning or acquiring new features may significantly impact the manufacturer's liability, there are no further references to this aspect in the PLD. Only Recital 32 offers some insight into it.

"The effect on a product's safety of any ability to learn or acquire new features after it is placed on the market or put into service should also be taken into account to reflect the legitimate expectation that a product's software and underlying algorithms are designed in such a way as to prevent hazardous product behaviour. Consequently, a manufacturer that designs a product with the ability to develop unexpected behaviour should remain liable for behaviour that causes harm."

The above recital provides some elements for assessing the potential defectiveness of a product resulting from continuous learning after it has been placed on the market or put into service, namely, the acquisition of new features and the AI system's ability to avoid hazardous product behaviour. These elements and their impact on the product will be discussed in the following pages. Furthermore, a product which causes damage due to unexpected behaviour will not constitute a circumstance that exonerates the manufacturer of liability.[7] Therefore, a decision made autonomously by the product cannot nullify or lessen the manufacturer's liability, as the product remains under the manufacturer's control and the manufacturer is still liable for any behaviour or decision taken autonomously by the product (Recital 32 PLD).[8]

Therefore, considering the provisions of the text of the PLD, the following premises are set out for further analysing this question:

1. An aspect that must be considered when assessing a product's defectiveness is its capacity for continuous learning, which can manifest in multiple facets, such as the product's ability to acquire new properties and mitigate risks.
2. In general, the appropriate time to assess a product's defectiveness due to its continuous learning ability is when it is placed on the market or put into service. However, since products with digital elements that can be updated or upgraded may remain within the manufacturer's control, it is necessary to consider the moment when the product is no longer within the manufacturer's control.
3. The legitimate expectation of consumers or users should be used as a basis for assessing the self-learning ability of the product to avoid hazardous behaviour and acquire new features or characteristics.

7. Recital 32 of the Product Liability Directive refers to "unexpected behaviour" as a potential manifestation of harmful conduct resulting from the product's continuous learning. In my view, continuous learning cannot be equated with unexpected behaviour, although the former may indeed give rise to the latter. It is perfectly conceivable that unexpected behaviour may result from a malfunction in the processing or execution of training models or input data available to the product. Nonetheless, the product will have been trained according to behavioural patterns that confer a certain degree of autonomy in its decision-making processes. This autonomy limits the scope of what can be considered truly unexpected behaviour and enables the attribution of liability to the manufacturer. Kim (2023, p. 159). Hartmann, Jueptner, Matalonga, Riordan and White (2023, pp. 35-36).
8. Atienza Navarro (2025, pp. 17-18). This author contends that the threshold for finding a product defective on account of its learning capability must be assessed by reference to whether that capability delivers a substantial reduction of risk, using as the benchmark the level of risk that would obtain if the relevant action or activity were performed by a human being. Herbosa Martínez (2024, pp. 65-66). Navas Navarro (2022, p.171). For their part, these authors advocate the "reasonable alternative" criterion, meaning that a product will be deemed defective as a consequence of the algorithm's unpredictable behaviour if the manufacturer could have avoided or mitigated it by adopting a reasonable alternative.

3.1. Some general considerations

3.1.1. A product that is capable of continuous learning is subject to the manufacturer's control

In the current context, in which digital elements are prevalent in products, it is essential to see a product as something that can change. In other words, a product that causes harm to a third party because it is faulty may not have the same features as when it was first placed on the market or put into service. Conversely, its characteristics may have altered because the manufacturer continues to control the product for safety updates or because it has gained new features. Therefore, the idea of 'manufacturer's control' is very important in evaluating the manufacturer's liability.

This concept is defined in Art. 4.(5) PLD and has undergone significant changes due to the amendments proposed by the Council. Thus, it is seen that the product remains under the manufacturer's control whether the manufacturer itself intervenes or a third party acts with its authorisation to modify the product. In the first case, the manufacturer or an authorised third party acting on its behalf integrates, connects, or supplies a product component or makes a modification to the product. In the second case, the manufacturer or an authorised third party supplies product updates or upgrades, so that in both cases the product changes its properties and remains under the manufacturer's control after being placed on the market; hence, the PLD holds the manufacturer liable for any damage.

Furthermore, it should be noted that, if the damage occurs after a third party's intervention, the third party can attempt to exempt itself from liability if it proves that the damage is unrelated to its intervention (Art. 11.1(f) PLD) or is due to instructions given by the manufacturer. This potential exemption from liability can only be claimed by a third party acting within the manufacturer's control (Art. 8.1(b) PLD). If the third party operates outside the manufacturer's control, this third party will also be regarded as the manufacturer (Art. 8.2 PLD) for the purpose of attributing liability for damage resulting from its intervention in the product.

3. 1.2. Continuous learning and assessment of product defectiveness

Regarding when the defectiveness of a product is assessed, the concept of the manufacturer's control remains crucial in determining liability. Since products with AI systems are constantly evolving, their defectiveness cannot be judged solely based on their condition at the time they were first marketed or put into service. Art. 7.2(e) PLD states that, in such cases, the defectiveness must be evaluated at the moment the product left the manufacturer's control. Therefore, changes to the product's software or AI system that could make it defective should not be judged based on the condition when initially market or put into service, because, among other reasons, the properties of the product have altered.[9] In such cases, the relevant moment is when the product ceased to be under the manufacturer's control.

When the continuous learning of a product is due to the fact that it contains a high-risk AI system, Art. 8.2 AI Act obliges the system provider to comply with the general requirements imposed on high-risk AI systems (Art. 8.1 AI Act). In developing these requirements, Articles 9.2 and 15.1 AI Act state, respectively, that the AI provider must manage the risks of the AI system throughout the product's lifecycle, and that the provider must also ensure its accuracy, robustness and cybersecurity throughout its lifecycle. Accordingly, when high-risk AI that enables continuous learning is embedded in a product and acts as a safety component thereof, it is the manufacturer who must comply with the obligations imposed on providers, meaning that the manufacturer that has equipped its products with such an AI system will be responsible for controlling the risks caused by the continuous learning of

9. Wagner (2023, p. 206). This author states that taking the moment the product leaves the manufacturer's control for the purposes of assessing its defectiveness is only applicable to software (in particular, its security features), and not to hardware, whose defectiveness must be assessed according to its state at the time it was placed on the market or put into service.

the product (Recital 87 AI Act and Art. 25.3 AI Act).[10] However, if the product leaves the manufacturer's control, for instance due to a significant modification carried out by a third party outside their control or acting without their authorisation, then it seems reasonable to say that the original manufacturer can be exempt from liability if the substantial modification has affected the AI system. Conversely, if the substantial modification has not altered the AI system, it is clear that under Art. 9.2 and 15.1 AI Act, the original manufacturer remains liable (Recital 84 AI Act).

The performance of a significant product modification by a third party, through a remanufacturing or refurbishing process outside the control of the original manufacturer and acting without its authorisation, will result in the third party gaining the status of manufacturer (Art. 8.2 PLD). Furthermore, in accordance with Recital 84 AI Act, the economic operator who has carried out the significant modification will be obliged to comply with the obligations imposed by the AI Act, as they will also be regarded as a manufacturer.

3.1.3. The 10-year limitation period on the manufacturer's liability: how should it be applied in the case of damage attributable to the continuous learning of the product?

Although products with digital elements that include AI, which can learn, improve and upgrade over time while under the manufacturer's control, are dynamic and changing in nature, the manufacturer's liability for damage caused by the defective product has a static limit over time (Art. 17 PLD). The manufacturer is not liable for damage caused by the product beyond ten years after the moment it is placed on the market or put into service, unless there is a substantial modification to the product. When this occurs, the product is considered to have been newly introduced onto the market, and the manufacturer's period of liability therefore runs once again from this moment (Art. 17.1(b) PLD).

The expected continuous evolution of the product due to software updates and continuous learning after being placed on the market or put into service is not easily compatible with setting a static limit to the manufacturer's liability, especially as Art. 9.2 and 15.1 AI Act oblige the producer to manage the risks of the AI system during the entire product lifecycle (Navas Navarro, 2022, pp. 93-94).

Art. 17.1 PLD refers to the possibility of restarting the manufacturer's liability in case of significant modifications. Therefore, considering the safety obligations imposed on providers of AI systems throughout the entire product lifecycle by the AI Act, it follows that the 10-year period would hardly apply to damage caused by AI and continuous product learning, unless continuous learning qualifies as a significant modification, in which case the expiry period would restart (Art. 17.1.b) PLD).[11] In any case, the relentless progress of technology means that products become obsolete quickly, so a ten-year limitation period may be sufficiently long to protect both consumers' right to compensation for damage caused by a defective product and manufacturers' interests, by allowing product-liability insurance and the internalisation of innovation costs (Fairgrieve, 2016, p. 96).

3.1.4. Product defectiveness and consumer expectations

The defectiveness of a product must be assessed according to the legitimate safety expectations for that product, a criterion that was already adopted by Directive 85/374/

10. Art. 25.3 AI Act therefore determines that the manufacturer of a product shall be considered the supplier of the high-risk AI system and thus subject to the provisions of Art. 16 AI Act, when such system acts as a safety component of the product, and the product is listed in Section A of Annex I, provided that the high-risk AI system is marketed together with the product under the trademark or name of the product manufacturer. However, the situation is different for high-risk AI systems that are integrated into products not listed under Section A of Annex I and which do not act as a safety component. In these cases, the supplier of the high-risk AI system should be subject to compliance with the legal requirements of the AI Act and, therefore, the product manufacturer should not be subject to such compliance, as it would not be considered as the supplier of the AI system. There would be two subjects with different obligations regarding the treatment of the AI incorporated in the product.
Despite the lack of clarity provided by the AI Act in this area, the solution adopted for the purposes of damage caused by defective products fulfils the aim of providing legal certainty to the affected parties: Art. 12 PLD provides for the joint and several liability of all economic operators when they are liable for the same damage (Recital 53 PLD), without prejudice to the provisions of Art. 12.2 PLD.
11. ELI (2023). ELI (2022). The European Law Institute (ELI) proposed introducing a reversal of the burden of proof such that the ten-year limitation period would not apply to damage caused by machine learning if the manufacturer could not prove that the defect was inherent in the product when it was placed on the market or put into service. However, that amendment was not adopted in the PLD.

EEC and which now remains in force with the PLD regulation (Art. 7.1 PLD and Recital 30 PLD) (Stapleton, 1994, p. 234; Borghetti, 2023, p. 33).

At this point, one might question whether the continued learning of a product that includes an AI system could lead the public to reasonably expect potential defectiveness. Recital 30 PLD highlights certain factors that should be considered when assessing the defectiveness of the product in relation to public expectations. From this viewpoint, the public could legitimately expect that continued product learning after deployment might enable the product to perform new functions or enhance its properties or features. In other words, it is an inherent characteristic of such products to adapt to new circumstances and thus serve new purposes or rectify errors in task execution. Consequently, ongoing product learning is a factor that influences the reasonable expectations of the public at large regarding product safety (Recital 32 PLD).[12]

3.2. Manifestations of product defectiveness due to continuous learning

Correction of errors and performance of functions

At the time of adopting Directive 85/374/EEC, products were regarded as tools fully controlled by humans, used by individuals to satisfy their needs in line with the reasonably expected use of such products (Art. 6(1)(b) of Directive 85/374/EEC). Even when products included software, that software was typically embedded, preprogrammed, and operated strictly in accordance with the user's instructions. In contrast, today's technological environment is characterized by the evolution of product software towards greater autonomy. Software now embedded in products may no longer follow a fixed, predetermined sequence of commands, but can instead make autonomous decisions. This shift is driven by the advent of continuous learning – the capacity of products to modify their functioning through experience after being placed on the market or put into service – and by the wider development of artificial intelligence systems.

Continuous learning is the process by which a product can acquire new characteristics or perform new tasks through continuous exposure to a large amount of data (Huberman, 2021, p. 109). As the product interacts with more data and is trained, its algorithm can improve its performance to better fulfil its functions (Vallor & Bekey, 2017, p. 340). The learning ability of products that include AI enables them to operate with partial independence from the instructions set by their programmers. The increasing autonomy of these products is therefore due to the algorithm's capacity to detect statistical patterns in the data it analyses and to automatically build models without manual programming (Surden, 2014, pp. 89-95). Despite the growing autonomy of the product, the software must initially be programmed to perform certain functions when it is launched or put into service, although its learning ability later allows it to adopt new solutions. However, the data, decisions made by the product, and its evolving characteristics as a result of its learning capacity will influence its potential for defectiveness. In this regard, legal doctrine has contributed several insights concerning defective continuous learning (Cormen, 2013, pp. 2-4):

a) The inaccuracy of the data that feeds the machine learning system on which the algorithm relies. In this case, the system has not been provided with up-to-date data and has therefore made an incorrect decision due to the use of outdated data or parameters.

b) Error of the algorithm concerning the decision made, meaning the algorithm fails to follow the instructions provided by the user when there are multiple possible procedures. For example, a GPS navigation system where the user wants to choose the fastest route. If the system ignores certain information about the current traffic conditions, the route selected may not be the quickest, as there could be other options.

c) Defective execution of new functions. The idea that products with embedded AI are completely hard-coded to perform their functions must be discarded. These products are, or should be, capable of performing new func-

12. Pazos Castro (2025, p. 6). The author considers that the continuous and rapid evolution of technology may prove problematic for the purposes of assessing consumers' legitimate safety expectations. Some users may have formed reasonable expectations in line with the earlier state of the art and, therefore, their expectations will be more than met if the product is capable of learning after deployment. By contrast, other consumers may hold higher expectations and feel unprotected if the product is unable to integrate new functionalities. In such a case, the product should not be deemed defective where economic operators have not incorporated the legitimate expectations of the public at large.

tions that, at the time they are placed on the market or put into service, are still unknown, or of making decisions according to an unprogrammed data pattern. In this case, the product is not ready to perform its functions from the outset; however, it can learn to do so if permitted by the algorithm and machine learning (Desai & Kroll, 2017, pp. 26-27). In other words, the product must continuously learn to perform new functions by analysing available data and developing new patterns. In this case, the continuous learning process is governed by the AI provider's data and methods, meaning that the product's performance is not fully autonomous (Art. 10 AI Act). In other words, regardless of the source of the data on which the product's continuous learning is based (be it the user, the provider or the deployer), Art. 16 AI Act, in conjunction with Art. 10 AI Act, imposes on the provider of the high-risk AI system a duty to govern the system's data. Therefore, as mentioned above, if there is a duty to govern the data of the high-risk AI system, the AI provider will be able control the data that feeds the continuous product learning.

The above groups make it possible, albeit schematically, to outline the possible defects that a product may have that affect its continuous learning capacity. In all of them, the AI manufacturer or provider can exercise control, in the sense of correcting any errors in the system's data, improving the algorithm's decision-making process or preparing the product so that it can acquire new features. Therefore, the PLD's premise of concentrating liability on the manufacturer for damages caused by defective products remains appropriate (Recital 32 PLD).

The main beneficiary of the joint and several liability of economic operators outlined in Art. 12 PLD is the user, because the product is presented as a complete entity, including hardware and software. This means the user does not need to prove which economic operator is responsible for the damage. Consequently, both the manufacturer and the AI provider would be held jointly and severally liable for any harm caused by the product due to defective continuous learning.

Conclusions

First: continuous learning of the product must be understood as referring to products incorporating generative artificial intelligence, which enables the product to alter its properties and acquire new characteristics after being placed on the market or put into service. By contrast, products equipped with non-generative artificial intelligence are not capable of modifying their characteristics after being placed on the market, which brings them closer to pre-programmed, deterministic software.

Second: the PLD has elevated software, applications, and AI systems to the status of products (Recital 13 PLD). This reform is undoubtedly welcome, as it puts an end to the ambiguity surrounding the definition of "product" under Directive 85/374/EEC, which previously did not include intangible items. Despite their classification as products, AI systems will generally function as a related service or component of another product, to which they are added or with which they are interconnected, such that, without the AI system, the product could not perform its functions or would fail to deliver the safety level expected by the public (Recital 17 PLD). However, their integration or interconnection with a tangible product may result in liability being attributed to the manufacturer, especially if the AI system either enables the product to perform its functions or compromises its safety, regardless of how it is supplied, thereby acting as a related service or component.

Third: one characteristic of products with digital elements with embedded generative AI is that, when they are released to the market or put into service, the manufacturer continues to exercise control over the product. This control allows for periodic updates to fix software errors, add new features, or enhance security. Understanding the concept of the manufacturer's control is essential for grasping manufacturer liability related to continuous product learning. Therefore, since products with generative AI remain under the manufacturer's control, the product's defectiveness must be assessed once it is no longer under the manufacturer's control.

Fourth: continuous product learning is also a factor influencing the duration of the manufacturer's liability. Art. 17.1 PLD states that the manufacturer's liability lasts for ten years after the product is placed on the market or put into service. However, the ten-year liability period specified in Art. 17.1 PLD does not suit products with generative AI that remain under the manufacturer's control after being marketed or deployed, and which are regularly updated and capable of learning after deployment. Therefore, it is proposed to interpret Art. 17.1 PLD together with Art. 7.2.e) PLD so that the manufacturer's liability begins when the product leaves the manufacturer's control. Otherwise,

even though the AI Act requires providers to monitor AI systems throughout their entire lifecycle, the manufacturer's liability for damage caused by AI products would be limited to ten years from market placement or deployment, ignoring the fact that the product might develop defects from continuous learning beyond that period.

Acknowledgments

This article is published within the framework of the R&D&I project Conducción autónoma y seguridad jurídica del transporte/Autonomous Driving and legal certainty of transport. PI: Eliseo Sierra Noguero.

References

ABBOTT, Ryan (2020). *The Reasonable Robot*. London: Cambridge University Press. DOI: https://doi.org/10.1017/9781108631761

ATIENZA NAVARRO, María Luisa (2025). "¿Una nueva responsabilidad por productos defectuosos? Notas a la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre responsabilidad por daños causados por productos defectuosos de 28 de septiembre de 2022 (COM/2022/495)". *Indret*, no. 3, pp. 1-53.

BORGHETTI, Jean-Sébastien (2023). "Taking EU Product Liability Law Seriously: How Can Product Liability Directive Effectively Contribute to Consumer Protection". *French Journal of Legal Policy*, no. 1, pp. 1-41.

CORMEN, Thomas H. (2013). *Algorithms Unlocked*. London: The MIT Press.

DESAI, Deven R.; KROLL, Joshua A. (2017). "Trust but Verify: A Guide to Algorithms and the Law.". *Hardward Journal of Law & Technology*, no. 31, pp. 1-64.

ELI (EUROPEAN LAW INSTITUTE) (2023). *European Commission's Proposal for a Revised Product Lia→bility Directive. Feedback of the European Law Institute*. Vienna: European Law Institute [online]. Available at: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Feedback_on_the_EC_Proposal_for_a_Revised_Product_Liability_Directive.pdf

ELI (EUROPEAN LAW INSTITUTE) (2022). *ELI Draft of a Revised Product Liability Directive. Draft Legislative Proposal of the European Law Institute.* Vienna: European Law Institute [online]. Available at: https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Draft_of_a_Revised_Product_Liability_Directive.pdf

FAIRGRIEVE, Duncan, *et. al*. (2016). "Product Liability Directive". In: Machnikowski P. (ed.). *European Product Liability: An Analysis of the State of the Art in the Era of New Technologies*. Principles of European Tort Law, pp. 17-108. Intersentia. DOI: https://doi.org/10.1017/9781780685243.002

GÓMEZ LIGÜERRE, Carlos (2025). "Responsabilidad por daños causados por la inteligencia artificial". *Indret*, no. 1, pp. 1-3.

HARTMANN, Jacques; JUEPTNER, Eva; MATALONGA, Santiago; RIORDAN, James; WHITE, Samuel (2023). "Artificial Intelligence, Autonomous Drones and Legal Uncertainties". *European Journal of Risk Regulation*, no. 14, pp. 31-48. DOI: https://doi.org/10.1017/err.2022.15

HERBOSA MARTÍNEZ, Inmaculada (2024). "Encaje de los sistemas de IA en la definición de producto en la legislación de productos defectuosos Análisis de la legislación vigente con la vista puesta en la Propuesta de Directiva del Parlamento europeo y del Consejo de 28 de septiembre de 2022 (COM/2022/495)". *Indret*, no. 3, pp. 52-98. DOI: https://doi.org/10.31009/InDret.2024.i3.02

HUBERMAN, Pinchas (2021). "Tort Law, Corrective Justice and the Problem of Autonomous-machine-Caused Harm". *Canadian Journal of Law & Jurisprudence*, no. 1, pp. 105-147. DOI: https://doi.org/10.1017/cjlj.2020.3

KIM, Daria (2023). "Artificial Intelligence Should Not Become a 'Black Hole' for Human Agency in Tort Law". *Tort Law Review*, no. 29, pp. 152-168.

NAVAS NAVARRO, Susana (2020). "Robot Machines and Civil Liability". In: EBERS, Martin, NAVAS NAVARRO, Susana (eds.). *Algorithms and Law,* pp. 153-177. Cambridge University Press. DOI: https://doi.org/10.1017/9781108347846.006

NAVAS NAVARRO, Susana (2022). "Seguimos necesitando normas de responsabilidad en caso de daños ocasionados por sistemas de inteligencia artificial de alto riesgo". *Revista CESCO de derecho de consumo*, pp. 1-5 [online]. Available at: https://portalrecerca.uab.cat/es/publications/seguimos-necesitando-normas-de-responsabilidad-civil-en-caso-de-d/

NAVAS NAVARRO, Susana (2022). *Daños ocasionados por sistemas de inteligencia artificial. Especial atención a su futura regulación*. Granada: Comares, pp. 93-94. DOI: https://doi.org/10.55323/edc.2022.21

PAZOS CASTRO, Ricardo (2025). "El carácter defectuoso del producto en la nueva Directiva europea 2024/2853". *Revista d'Internet, Dret i Política*, no. 43, pp. 1-15. DOI: https://doi.org/10.7238/idp.v0i43.433093

EXPERT GROUP ON LIABILITY AND NEW TECHNOLOGIES (2019). *Liability for Artificial Intelligence and Other Emerging Digital Technologies*, pp. 1-70. Luxembourg: European Commission [online]. Available at: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2020/01-09/AI-report_EN.pdf

STAPLETON, Jane (1994). *Product Liability*, p. 234. Butterworths.

SURDEN, Harry (2014). "Machine Learning and Law". *Washington Law Review*, no. 89, pp. 87-115.

VALLOR, Shannon; BEKEY, George A. (2017). "Artificial Intelligence and the Ethics of Self-Learning Robots". In: LIN, Patrick, ABNEY, Keith and JENKINS, Ryan (eds.). *Robot Ethics 2.0: From Autonomous Cars to Artificial Intelligence*, pp. 338-353. Oxford University Press. DOI: https://doi.org/10.1093/oso/9780190652951.003.0022

WAGNER, Gerhard (2023). "Liability Rules for the Digital Age". *Journal of European Tort Law*, vol. 13, no. 3, p. 193. DOI: https://doi.org/10.1515/jetl-2022-0012

WANDEHORST, Christiane (2021). "Safety and Liability Related Aspects of Software". Luxembourg: European Commission, pp. 1-99.

Recommended citation

IZQUIERDO GRAU, Guillem (2026). "Manufacturer's liability for continuous product learning". *IDP. Internet, Law and Politics Journal*, no. 44. UOC [Accessed: dd/mm/yy]. DOI: http://dx.doi.org/10.7238/idp.v0i44.433369

About the authors

Guillem Izquierdo Grau
Universitat Autònoma de Barcelona
guillem.izquierdo@uab.cat

He is an associate professor of Civil Law at the Universitat Autònoma de Barcelona. He was awarded the Ferrer Eguizabal legal prize in 2019 on Catalan Civil Law for the work "La división y la temporalidad del dominio: la propiedad temporal del Código civil de Cataluña", which is the result of his doctoral thesis. He has carried out several research stays at international universities (University of Osnabrück and University of Leiden). His main lines of research currently focus on the Law of Obligations and Contracts and the Law of Torts, two lines of research on which several articles have been published in national and international journals in recent years.

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Challenges of using digital evidence in pretrial investigations of online fraud: lessons for Kazakhstan from international practice

Nurdaulet Apsimet
Al-Farabi Kazakh National University, Kazakhstan

Yerbol Alimkulov
Al-Farabi Kazakh National University, Kazakhstan

Bakytkul Konysbay
Al-Farabi Kazakh National University, Kazakhstan

Akynkozha Zhanibekov
Mukhtar Auezov South Kazakhstan Research University, Kazakhstan

Alua Muratova
Gumilyov Eurasian National University, Kazakhstan

Date of submission: April 2025
Accepted in: November 2025
Published in: March 2026

Abstract

In the context of digital evidence, the issues of admissibility, authenticity, reliability, and compliance with procedural standards remain contentious in the legislation and judicial practice of many countries worldwide. The existing challenges in the use of digital evidence in pretrial investigations highlight conflicts between safeguarding personal data and the need for its use in investigations. These challenges are worsened by the increase in cybercrime, with online fraud ranking prominently among other forms. This paper aims to analyse current challenges related to the use of digital evidence in online fraud investigations and propose potential solutions. The above issues are examined in terms of their relevance to the legal system and regulatory framework of Kazakhstan. The findings reveal that in the current circumstances, the primary challenges in the field under study are both issues typical of conventional forensics (e.g., the absence of a court warrant or sanctions for collecting digital information, non-adherence to data retention and analysis requirements) and more recent problems (e.g., disruptions to the chain of digital evidence, the use of unlawful methods for collecting digital evidence). The modern demands of the forensics industry necessitate a thorough reassessment of approaches to training forensic investigators, with the establishment of a separate specialization.

Keywords

blockchain; cybercrime; digital data; digital evidence; digital forensics

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Desafíos del uso de pruebas digitales en las investigaciones previas al juicio sobre el fraude en línea: lecciones para Kazajistán a partir de la práctica internacional

Resumen

En el contexto de las pruebas digitales, las cuestiones de admisibilidad, autenticidad, fiabilidad y cumplimiento de las normas procesales siguen siendo un tema polémico en la legislación y la práctica judicial de muchos países de todo el mundo. De los desafíos existentes en el uso de pruebas digitales en investigaciones previas al juicio, destacan los conflictos entre la protección de los datos personales y la necesidad de su uso en dichas investigaciones. Estos desafíos empeoran debido al aumento de los ciberdelitos, entre los que destaca el fraude en línea sobre otras formas. Este artículo tiene como objetivo analizar los desafíos actuales relacionados con el uso de pruebas digitales en investigaciones de fraude en línea y proponer posibles soluciones. Las cuestiones anteriores se examinan en términos de su relevancia para el sistema jurídico y el marco normativo de Kazajistán. Los hallazgos revelan que, en las circunstancias actuales, los principales desafíos en el campo en estudio son tanto problemas típicos de los análisis forenses convencionales (p. ej., ausencia de una orden judicial o sanciones para recopilar información digital, incumplimiento de los requisitos de conservación y análisis de datos) como problemas más nuevos (p. ej., interrupciones en la cadena de pruebas digitales, uso de métodos ilegales para recopilar pruebas digitales). Las demandas modernas de la industria forense requieren una reevaluación exhaustiva de los enfoques para capacitar a los investigadores forenses, así como el establecimiento de una especialización independiente.

Palabras clave

cadena de bloques; ciberdelitos; datos digitales; evidencia digital; análisis forense digital

Introduction

With the rapid digitalization of economies and social interactions, crime has also evolved, adopting new forms and methods. In recent years, cybercrime, and more broadly, online crime (from a criminal law perspective, these two concepts are often seen as complementary), has shown steady growth, while traditional types of crime have either declined or remained stable globally. This is due to the transformation (evolution) of tools and methods used to commit some traditional crimes (Murphy, 2024). As early as 2022, according to estimates from major fintech and telecom companies such as Stripe and Juniper, global losses from online payment fraud in 2020 amounted to 130 billion US dollars. Moreover, they forecast that by 2027, cumulative global losses over four years, starting in 2023 will reach approximately 340 billion US dollars (Juniper Research, 2022; Stripe, 2023). In 2024, the Global Anti-Scam Alliance (GASA), in collaboration with Feedzai, published its report on the current state of online fraud worldwide, revealing staggering data on the prevalence and impact of fraud globally. The report, based on data from various regions, highlights the substantial economic losses incurred by consumers due to online fraud. In 2024 alone, approximately 1.03 trillion US dollars were stolen worldwide, which is comparable to the annual budgets of large countries (Rogers, 2024). Despite statistical discrepancies and differing methodologies for calculating damage and classifying crimes, it is evident that the trend indicates to a steady increase in cybercrime. One of the most common crimes in the virtual space is online fraud, which includes various schemes of deception, from phishing and fraudulent online stores to complex financial manipulations involving cryptocurrencies. Online fraud (also referred to as internet fraud and cyber-enabled crime/fraud) is traditionally considered a criminal offence, as it is characterized by direct intent, a degree of public danger typical of criminal offences (crimes), and other features that distinguish online fraud from other types of wrongful actions.

The rise of cybercrime has created new challenges for criminal investigations, particularly in the collection and analysis of digital evidence (DE). The lack of standard, unified protocols for handling digital evidence complicates its admissibility in court and leads to errors in law enforcement and judicial assessments of evidence (Rakha, 2024). Effective investigation of such crimes is impossible without the use of digital evidence – data obtained from

electronic sources, including messenger platform communications, network activity logs, IP addresses, transaction information and other digital footprints. However, their use in pretrial investigations entails a range of problems related to both the technical aspects of collection and analysis and the legal issues of admissibility and reliability of such evidence. Against the backdrop of increasing cybercrime, the use of DE for investigative purposes is becoming increasingly important for many countries, including the Republic of Kazakhstan (RK). The use of evidence involves the handling of evidence for the purpose of providing proof. The criminal law doctrine in post-Soviet countries holds that the use of evidence encompasses both its examination and evaluation (Meretukov, 2015). The term "electronic evidence" began to be actively used in judicial practice after the adoption of the Federal Rules of Evidence (FRE) 1001 (Graham, 2016) in the United States, which specified the admissibility of electronic data in court. The Budapest Convention on Cybercrime has enshrined the term in international law. The widespread use of the concept in criminal investigations, including digital evidence from mobile devices and cloud services, became prevalent from 2005 to 2010. In 2019, the Committee of Ministers of the Council of Europe adopted guidelines aimed at facilitating the use of electronic evidence in civil and administrative proceedings. These guidelines cover the collection, seizure, transfer, storage and preservation of electronic evidence, and also address issues of admissibility and reliability.

Currently, online fraud is one of the most common types of cybercrime, and without electronic evidence, its investigation is practically impossible. Because fraudsters operate remotely, digital footprints are the only means of establishing their guilt and holding them accountable. In the context of pretrial investigations, the proper evaluation and management of electronic evidence is of paramount importance. Modern studies explore various aspects related to the application of digital evidence in pretrial investigations. The works in this field focus on the competence of prosecutors and investigators in the use of digital evidence (Miller, 2023) and on the collection of evidence using blockchain to detect cybercrimes (Balmiki, 2023). Some studies examine potential directions for digital transformation in pretrial investigations through the lens of protecting individuals' rights and legal interests (Demura *et al*., 2020). Factors leading to the commission of internet fraud have been analysed in the Republic of Kazakhstan (Namysov, 2024). Other critical issues that have received research attention include the admissibility of digital evidence (Yeboah-Ofori & Brown, 2020), the automation of forensic examination systems for websites (Vidya *et al*., 2022) and sources of error in digital forensics (Horsman, 2024).

The relevance of this research topic stems primarily from the need to examine challenges in personal data protection in the digital age. It is also necessary to address numerous threats to businesses and the nonprofit sector posed by the theft and leakage of commercial information and personal data. The aim of this paper was to analyse the current challenges associated with the use of digital evidence in the investigation of online fraud and to identify potential solutions.

1. Materials and methods

The documentary and analytical basis of this research includes international acts on the handling of digital evidence in pretrial investigations as well as on the collection of evidence from ICT systems (Convention on Cybercrime, 2001,[1] United Nations Convention against Cybercrime, 2024,[2] Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings, The Council of Europe Recommendation No. R (95) 13, Appendix, IV. Electronic evidence). The study also employed ISO/IEC standards (27037, 27042, 27043), data from analytical reports by Europol (Internet Organised Crime Threat Assessment (IOCTA) 2024) and OSCE (Stoilkovski, 2022), as well as analytical materials from legal firms and companies in the field of digital forensics (Eclipse Forensic. Breaking the Chain: Common Mistakes in Digital Evidence, etc.). The methodological foundation of the research is system analysis, which involves considering various aspects of digital evidence (DE) and their interdependencies in the context of their application in pretrial investigations. Problems related to the collection and analysis (or processing, in a broader sense) of DE were examined from two perspec-

1. The Council of Europe Convention on Cybercrime, 2001.
2. United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes.

tives: as indicators pointing to both the evolution of cybercrime and the evolution of forensics as a science, field of knowledge and applied activity.

Considering theoretical limitations, the work situates its analysis within Kazakhstan's national legislation, focusing on issues of digital evidence admissibility mainly through the perspective of national procedural practice. International regulations and precedents are referenced to identify global trends and approaches to managing digital evidence.

2. Results

The concepts of evidence and proof are fundamental to civil and criminal proceedings. Proof consists of gathering, verifying, evaluating evidence and using it to establish facts relevant to the case, as well as justifying the conclusions drawn from them (Vapniarchuk *et al*., 2018). The emergence of the term "electronic (digital) evidence" has somewhat changed the perception of evidence as a material object. Digital evidence (DE), in turn, is a derivative product of certain crimes (criminal offences) with a complex taxonomy; these crimes share a common feature – they are committed using electronic equipment and typically in the internet environment. In these conditions, traditional forensics requires new skills and knowledge from specialists. Law enforcement agencies always strive to obtain as much data as possible to support any ongoing investigations. Circumventing complex security schemes incentivizes law enforcement to invest resources in knowledge and expensive equipment for advanced forensic examinations to respond to various challenges. Investigative agencies also focus their efforts and investments on identifying and exploiting security vulnerabilities to circumvent security controls and obtain digital evidence. For example, in the United States, law enforcement policy in this area aims to strengthen the role of digital forensics and expand the participation of digital forensic experts in countering cybercrime (particularly corporate cybercrime), despite numerous practical obstacles (Cybersecurity and Infrastructure Security Agency, 2022; U.S. Attorney's Office, Central District of California, 2022). Although other countries have implemented similar measures, the United States and the European Union lead in this area. In these countries, forensic science, as a component of the system for protecting and safeguarding human rights, has traditionally been of great significance (Stoilkovski, 2022). In the glossary of digital forensics, the concept of DE occupies a central place. Based on a combination of definitions, DE can be conceptualized as any information in digital form that has probative value and can be used as reliable evidence in court. According to the Council of Europe, electronic evidence means "any evidence derived from data contained in or produced by any device, the functioning of which depends on a software programme or data stored or transmitted over a computer system or network" (Committee of Ministers of the Council of Europe, 2019). In scientific sources, this definition is considered similarly. In a broader sense, electronic evidence is any probative information stored in electronic form on any type of computer device that can be used as evidence in legal proceedings (Casey, 2011; Volonino, 2003).

The problems of using digital evidence in pretrial investigations of online fraud can be conditionally divided into three main categories – technical, legal and organizational. The first category includes the complexity of extracting digital data, their mutability and instability, the lack of unified standards in digital forensics, and the difficulty of identifying the criminal due to the specific tools (instruments) used to commit a crime (electronic means and systems). The practice of criminal investigations in different countries demonstrates that digital evidence is frequently found on servers outside the country where the investigation takes place. Moreover, the information is stored in encrypted form or in data clouds, access to which is difficult. Electronic footprints can be easily forged, deleted, or altered without proper documentation, making their use in court even more challenging. Digital forensics also lacks unified standards – methods of collecting and analysing digital evidence may vary, affecting their reliability. At the same time, the use of VPNs, anonymizers, TOR networks, fake accounts, and cryptocurrencies by criminals to conceal their identity poses additional challenges to forensic investigators.

The second category – legal problems – encompasses the ambiguous status of digital evidence, as many countries have yet to enact clear regulations on their admissibility in criminal proceedings. Additionally, this category includes issues such as authenticity and reliability, as well as the absence of international mechanisms for investigative cooperation. Thus, courts may doubt the authenticity of digital evidence due to its mutability. Typically, online fraud is cross-border in nature, but the process of obtaining digital data from abroad entails bureaucratic complexities. In

addition to the aforementioned aspects, there is the problem of insufficient regulation of data collection from private sources. This problem implies potential conflicts between the protection of personal data and the necessity of its use in investigations.

The third category (conditionally titled organizational problems) refers to insufficient training of law enforcement agencies, issues of interaction with the private sector and lengthy investigation periods. The lack of expertise in cybercrime investigations and digital forensics among modern forensic investigators is a long-standing and acute issue, stemming from the specific nature of the educational programmes rooted in legal studies. Regarding the limitations of technical resources, there is a systemic opposition between "private" and "public": the operational tools of private actors often outpace the inertia of the state. In other words, state agencies generally lag behind fraudsters in terms of technology and tools for analyzing digital footprints. In this situation, the state tends to adopt a "reactive" approach, which forces the state (represented by law enforcement agencies) to implement countermeasures. In contrast, the position of fraudsters is generally proactive. Regarding the problems of interaction with the private sector, participants in investigative actions, in one or another procedural capacity (in this case, internet companies, banks, and communication operators), may refuse to provide data or do so with delays. In conclusion, it is worth noting that the extended duration of investigations can lead to data loss or to an inability to identify offenders. Although this issue is not exclusive to online fraud, it is equally prevalent in this area as it is in cases of "traditional" offences.

The reports by Europol (2024) and the Global Anti-Scam Alliance (Singapore) (Rogers, 2024), as well as analytical data from British and American cybersecurity companies (CYBSAFE, 2024; Palatty, 2025), identify the most common types of online fraud. These include:

- Phishing – one of the most common types of cybercrime. According to the Anti-Phishing Working Group (APWG), the monthly volume of phishing attacks worldwide was approximately 250-300 thousand in 2024;
- Financial pyramid schemes and investment fraud are the largest-scale crimes in terms of financial losses. Fake investment projects (cryptocurrency schemes, HYIPs) promise high returns, with new investors paying the returns of earlier participants. In 2022, in the United States alone, losses from investment fraud amounted to $3.3 billion (based on data from the FBI's Internet Crime Complaint Center) (Federal Bureau of Investigation, 2022);
- Extortion and blackmail. Extortionists threaten to publish personal data, photos, or videos, demanding money to prevent it. Criminals also use ransomware that blocks access to the victim's files until a "ransom" is paid. Theft of personal data and its resale;
- Organization and maintenance of fake online stores and services;
- Telephone fraud (especially via IP telephony, which classifies these as cyber-enabled crimes), as well as sending SMS messages containing malicious links to phishing sites;
- Cryptocurrency fraud – arguably the newest and most "technological" of all crimes related to online fraud. These crimes involve fake ICOs (initial coin offerings), pyramid schemes disguised as DeFi projects, theft of private keys, and hacking of cryptocurrency wallets. This category also includes offers for "remote (cloud) mining" (Finance Magnates, 2023).

As can be seen, online fraud is constantly evolving, and it is currently difficult to predict the "bifurcation point" at which a new evolutionary leap will occur. However, it is evident that two components will definitely be involved in this process – social engineering and technological development enhanced by the capabilities of artificial intelligence (AI). Although the latter is not yet widely cited in reports as a factor *hic et nunc*, its impact is clearly inevitable.

In light of the above, it is important to understand the criteria for admissible (legit) digital evidence. In criminal investigations of online fraud, legit digital evidence may include data from correspondence and online communications, records of telephone conversations and VoIP calls, data on financial transactions and similar information. A necessary condition is the confirmation that their collection and processing are carried out in accordance with the legislative requirements and procedures of the countries where such collection and processing occur. At the international level, these issues are partially regulated by ISO/IEC standards, such as ISO/IEC 27037, 27042 (ISO, 2012, 2015). Although these standards are essentially recommendatory documents without regulatory authority, they generally serve as the basis for preparing instructions for

digital forensics experts. An analysis of these standards can discern parameters that render digital evidence admissible for investigations and juridical proceedings. Thus, proper evidence may include:

- Data from correspondence and online communications. These are typically chats and messages on messaging platforms, correspondence on social networks, and emails (with preserved headers, metadata and delivery routes). Such data must be authenticated (e.g., through judicial requests to platforms) and must not be altered or falsified;
- Records of telephone conversations and VoIP calls (audio recordings of calls on Skype, Zoom, etc.), as well as call log files from communication providers. General requirements include the need to obtain a court warrant for access to such data, as well as to ensure confirmed sources of the recordings;
- Data on financial transactions and cryptocurrencies, e.g., bank transfers, bank statements, transactions from cryptocurrency exchanges, data on wallets and cryptocurrency addresses. As a general requirement, data must contain information about the sender and recipient. Access of competent services to such data is primarily determined by judicial decisions;
- Data on account logins (logins, IP address history of the suspect's account logins, geolocation data, cookies and metadata from websites). Such data can only be provided upon official request to internet service providers and web services, and must be in compliance with the rules of storage (analysis, processing) of the chain of custody necessary for the investigation of relevant categories of cases;
- Data from the suspect's devices obtained through physical access (files on a hard drive or flash drive, browser history, cached pages, saved passwords, autofill forms);
- Log files from servers and hosting platforms (records of activity on websites used to conduct fraudulent activities), data on payments on specialized platforms (e.g., PayPal) and information on domain registration and changes of ownership. Forensic experts must confirm the immutability of log files when working with them;
- Video recordings of suspects (e.g., webcam recordings, recordings of video conferences conducted during fraudulent activities, videos from ATMs or stores confirming the withdrawal of money by the fraudster). Evidence must be collected lawfully (for instance, surveillance camera recordings must be obtained through a request), and it must be clear and identifiable. As in previous cases, access to such materials may require a court warrant (or a prosecutor's warrant, depending on the jurisdiction). All the above data can be used in the investigation of online fraud if they are collected legally, authenticated and not subject to manipulation. At the same time, non-compliance with procedural norms may lead the court to deem them inadmissible when considering cases.

In order to identify the main problems encountered in the collection and processing of DE, it is necessary to analyse materials from the OSCE Guidelines on Cybercrime Investigation (Stoilkovski, 2022), UNODC (United Nations Office on Drugs and Crime, 2024), Information Commissioner's Office Guidance on the use of storage and access technologies impact assessment (Information Commissioner's Office, 2024), as well as materials from private organizations specializing in digital forensics (Cyber Centaurs, 2024; Lucid Truth Technologies, 2024). In pretrial investigations of online fraud, common procedural violations include the collection of DE without a court-issued warrant, breaches in the chain of custody for DE, and insufficient authentication of DE. In addition, illegal methods of collecting DE (i.e., those that contravene established procedures) and failure to adhere to required timeframes for DE storage and analysis are also prevalent. The absence of a court warrant often arises during the seizure of digital storage devices (computers, smartphones, servers, etc.), in cases involving access to correspondence in messenger platforms, email, or cloud storage without court permission, as well as during wiretapping and internet activity monitoring without proper procedural grounds. In the United States, the case United States v. Warshak established a legal precedent, with the court ruling that law enforcement agencies' access to a suspect's emails without a warrant constituted a violation of the Fourth Amendment and was therefore unlawful (United States Court of Appeals, 2010).

Breaches in the chain of custody of digital evidence occur in the absence of detailed documentation on who, when and how seized, copied and analysed digital evidence, as well as in cases of non-compliance with digital forensics standards when copying data (particularly, the absence of hashing, making it impossible to verify the integrity of files). This issue is often highlighted by companies specializing in digital forensics (Belkasoft, 2024; Eclipse Forensic, 2024). In procedural terms, a breach in the chain of custody

of evidence can be identified either at the court's initiative or at the parties' request during the evidence examination stage. Present studies provide evidence that this typically occurs when the defence challenges the authenticity or integrity of digital data. If the court finds that the chain of custody has been breached, the relevant evidence may be deemed inadmissible or its probative value significantly reduced (Caianiello & Camon, 2021; IJIS Institute, 2024).

The lack of proper authentication of digital evidence implies using screenshots of correspondence on social networks or messenger platforms (as evidence) without verifying their authenticity, as well as presenting files and logs in court without proof that they have not been altered. Thus, in another case, *United States v. Vayner* (United States, 2014), the court dismissed a VKontakte page as inadmissible evidence because the prosecution failed to establish that the page definitively belonged to the defendant (VLex, 2014). The problem of employing unlawful methods to collect digital evidence generally stems from a broader issue in forensics – the use of illegal practices to obtain evidence. Although this issue is not the only one, it remains one of the most prevalent. In practice, investigative agencies may resort to installing spyware (keyloggers, trojans, etc.) without court authorization, coerce suspects into providing passwords or encryption keys without legal grounds, and collaborate with hackers or private individuals to obtain evidence illegally (TCDI, 2023). Another significant issue is the failure to comply with established protocols for the storage and analysis of digital data. Delays in analysing seized digital evidence can lead to its loss, while the absence of proper backups or the premature destruction of files before the investigation is concluded further exacerbates the problem (Information Commissioner's Office, 2024). As a result, all these errors can lead to the annulment of evidence in court, and investigators may even face charges for procedural violations.

In many jurisdictions, using digital evidence without proper judicial authorization can lead not only to the evidence's inadmissibility but also, in some cases, to the annulment of the entire proceeding (a ground for terminating criminal proceedings). For example, Article 238 of the Spanish Organic Law of Judicial Power (LOPJ)[3] provides for the invalidity of judicial actions taken in violation of fundamental procedural guarantees. Article 11.1 of the LOPJ provides that evidence obtained, directly or indirectly, in violation of fundamental rights and freedoms is null and void. Similar rules are contained in the criminal procedural laws of many other countries (in particular, the Codice di Procedura Penale of Italy,[4] Art. 191). The Polish legislature takes a different position. The country's Code of Criminal Procedure stipulates that evidence cannot be declared inadmissible solely on the grounds that it was obtained in violation of procedural provisions or through a prohibited act.[5] This demonstrates the increasingly close relationship between data protection, procedural legality and the admissibility of digital evidence. Regarding supranational regulation, at the international legal level, some of the main regulatory instruments for combating cybercrime and handling DE are the Council of Europe Convention on Cybercrime (Budapest Convention, 2001) and the UN Convention against Cybercrime (2024). The interaction of these two conventions is generally seen as a set of complementary regimes that lay the foundations of legal regulation and avenues for cooperation (legal, technical, and procedural). At the same time, both conventions entrust national jurisdictions with the implementation of the provisions concerning the admissibility, relevance, reliability and evaluation of DE in criminal proceedings.

Many of the previously mentioned problems regarding admissibility of DE have been noted in earlier analytical studies and institutional reports (American Bar, 2016; Goodison *et al*., 2015). This fact indicates that the issue has become deep-seated and is likely to persist in the foreseeable future. To date, there is no clear evidence that forensic experts face difficulties with the set of technical tools or that regulatory standards inadequately describe the algorithms underlying their actions in obtaining or processing DE. This suggests that the main source of problems is the human factor – namely, the actions of forensic experts. Looking

3. ORGANIC LAW 6/1985, OF 1 JULY, ON THE JUDICIARY [online]. Available at: https://www.legal-tools.org/doc/881df4/pdf/#:~:text=Article%20122%20of%20the%20Spanish,the%20Official%20State%20Gazette%20n%C2%BA
4. Codice di procedura penale Testo del D.P.R. 22 settembre 1988, n. 447 [online]. Available at: https://www.altalex.com/documents/codici-altalex/2014/10/30/codice-di-procedura-penale
5. USTAWA z dnia 6 czerwca 1997 r. Kodeks postępowania karnego [online]. Available at: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/kodeks-postepowania-karnego-16798685

ahead, one might arrive at the surprising conclusion that reducing human involvement could lessen the scope of issues, with certain tasks potentially being automated (for instance, through AI techniques such as digital evidence authentication). However, under the current conditions, this scenario appears unrealistic. Forensic investigation tactics remain largely discretionary, often necessitating *ad hoc* solutions and expertise in human psychology. Forensic practice is highly context-dependent, requiring flexibility, interpretation, and adaptation to the unique circumstances of each case. While artificial intelligence may assist in identifying and prescreening evidence, the final decision regarding the admissibility, consistency and legal relevance of evidence ultimately lies with humans. Moreover, automation fails to address the critical issue of trust. The judicial system demands explicitness and clarity in decision-making. For instance, if an AI system asserts the authenticity or falsity of evidence, it is imperative to understand the rationale behind its conclusion. Unlike humans, algorithms cannot articulate their reasoning in a legally acceptable manner, which restricts their role in legal processes. Thus, while AI can serve as a valuable tool in forensics, it cannot replace human judgment at this stage.

In light of the current circumstances, the most viable solution appears to be strengthening the professional training of experts in the field (primarily criminalists and forensic investigators, and to a lesser degree, prosecutors and judges). For instance, the seminal report of the RAND Justice, a project operating under the auspices of the National Institute of Justice (the United States), focused on digital forensics in the United States. The report highlighted the critical need to train prosecutors to utilize digital evidence more effectively. It observed that many prosecutors lack a comprehensive understanding of the appropriate use and limitations of digital evidence, often leading them to request excessive amounts of data from devices – far beyond what is necessary for a case. This practice creates an unnecessary burden for digital forensic experts. In conclusion, the report recommended expanding federal training programmes to include more prosecutors, thereby improving their understanding of the types and volumes of data required as evidence in different types of cases (Goodison *et al*., 2015).

Practising lawyers (American Bar, 2016; Fynd Academy, 2025) emphasize the educational aspect of forensics (the retraining or additional training of experts), as it is identified as a top priority in the guidelines of international organizations such as the OSCE and Interpol (Interpol, 2021; Stoilkovski, 2022). The issue of retraining criminologists in digital forensics is especially critical for countries experiencing rising levels of cybercrime, which conventional methods cannot effectively address. In particular, in Kazakhstan, by the end of 2024, approximately 17,000 cases of internet fraud were recorded (Turlybek, 2024) – a sharp 40-fold increase from around 500 cases in 2018 (Finprom, 2024).

Nevertheless, the qualifications of many specialists fall short of the requirements for working effectively with digital evidence. Common errors include improper collection and storage of evidence, the possibility of overlooking cryptocurrency transactions, and an inability to identify criminals who use tools such as Tor, VPNs or the darknet (Saniyazova *et al*., 2024; Satbayeva *et al*., 2024). Furthermore, Kazakhstan's legislation in this area remains underdeveloped. While there are standards for protecting personal data, clear regulations for handling digital evidence are insufficient. Furthermore, the country is not a signatory to the Budapest Convention, which hampers international cooperation.

These gaps often result in evidence being declared inadmissible in court due to procedural errors. To address these challenges, specialized training programmes should be introduced within the Ministry of Internal Affairs, Prosecutor's Office, and judicial system of the Republic of Kazakhstan. It is also essential to develop specialized regulations, such as implementing ISO standards in digital forensics and formalizing the principles of digital evidence, as well as establishing local standards for the proper handling of digital evidence.

3. Discussion

Comprehensive and reliable global data on specific issues related to violations of forensic procedures in DE acquisition and analysis (such as breaches in the chain of custody) are currently lacking. However, these issues rank among the most serious challenges in modern criminology, as highlighted by secondary sources – materials from law firms and companies specializing in digital forensics (D'Anna *et al*., 2023; Horsman, 2024).

Modern researchers frequently argue that deviations from standard procedural protocols are the primary cause of DE processing issues (Rakha, 2024; Seo, 2024; Tosza, 2024; Ute-

pov & Zhempiisov, 2022). A growing concern among experts is the integrity of the chain of custody (De Abreu Motta, 2023; Miller & Singh, 2024; Salih & Ibrahim, 2023), particularly given the complexity of certain forensic procedures in DE operations – it is extremely challenging to strictly adhere to forensic protocols. At the same time, breaches in the chain of custody can undermine the probative value of DE. Standard methods, such as simple file copying, often fail to meet forensic requirements. Despite this, such methods are still commonly used in practice. Forensic protocols mandate the use of specialized tools (FTK Imager, Autopsy, etc.) to extract data without altering the original source (Salman *et al*., 2023). Specialized studies have rightly emphasized that, within the EU, courts may reject evidence if it was collected in violation of the General Data Protection Regulation (GDPR) or if the procedures for obtaining it were inadequately documented (Antoliš, 2023; Wairimu *et al*., 2024).

Other issues, such as insufficient authentication of digital evidence and noncompliance with time requirements for storing and analysing digital data, have received less attention. These are often perceived as "technical" obstacles that do not require forensic experts to acquire complex new skills in response to industry advancements (Al-E'mari *et al*., 2024; Singh *et al*., 2022). Meanwhile, the use of unlawful methods to obtain digital evidence is typically examined within the broader context of forensic issues (Antoliš, 2023; Li *et al*., 2021).

Addressing crimes such as the theft of private keys and the hacking of cryptocurrency wallets requires forensic experts to possess specialized knowledge and expertise in digital forensics, blockchain technology and cryptography. Given this fundamental premise, it is evident that forensic science, as a practical discipline, must reexamine its methodological foundations for training specialists. Regarding the previously discussed integration of AI tools and their potential role in forensic techniques and strategies, this issue has not received the attention it deserves. The unique nature of forensic activities involving digital evidence demands high technical proficiency, strict adherence to procedural regulations and the use of specialized tools. A review of the methodological framework for training digital forensic experts should be considered a critical step in addressing these challenges, as well as similar issues that may emerge in the future. For many countries, including Kazakhstan, the lack of a specific term to describe professionals in this field of criminology underscores the relevance of this issue. For instance, in Russian-language literature, the term *форензик* (forensic) is increasingly used to denote this professional field, though this may lead to confusion in the future (Mironov & Milaeva, 2024). Simultaneously, it is clear that criminology, as a scientific discipline, is undergoing a transformative phase. This is driven by the evolution of the forensic profession from a purely legal practice to a hybrid domain that combines law and computer science. This shift necessitates specialists possessing not only personal and professional qualities but also expertise in related and even unrelated fields. To train a modern forensic expert, it is essential to equip them with specific knowledge in areas such as cryptography and blockchain technology. Specifically, they must understand the principles of cryptographic key usage and storage in cryptographic wallets, as well as be familiar with symmetric and asymmetric encryption, hashing algorithms and digital signatures. Additionally, expertise in algorithms used for protecting cryptographic data, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), is crucial (Bhadarge & Parkhe, 2024; Cui & Li, 2023). To work effectively in the evolving blockchain industry, forensic experts must also have a foundational understanding of various blockchain platforms, their unique features and the use of smart contracts. Educational programmes designed to train digital forensics experts should include content aimed at enhancing professionals' ability to trace blockchain transactions, analyse blockchains and develop methodologies for detecting fraudulent or illegal transactions. Furthermore, such programmes should provide insights into anonymity-enhancing cryptocurrencies (e.g., Monero and Zcash) and their implications for investigations (Almutairi & Moulahi, 2023).

Other aspects pertain to enhancing knowledge and skills in the analysis of digital evidence. This implies the ability to use digital forensic tools and techniques to extract and analyse data such as log files, blockchain transactions and cryptographic key histories. Specialists must be proficient in employing software solutions that enable them to monitor blockchain transactions and identify connections between addresses. Additionally, it is essential for specialists to utilize cryptocurrency wallets to review transaction histories, identify suspicious activities, and detect patterns indicative of illegal actions (Ahmed & Alabi, 2024). This set of skills also includes a comprehensive understanding of cybersecurity principles, including methods for hacking cryptocurrency wallets, detecting malware (keyloggers or trojans) and analysing malicious attacks. The category conditionally titled "computer and technical skills" involves the ability to work with anonymous services and platforms that may facilitate illegal cryptocurrency transactions, as well as knowledge of

the unique characteristics of darknet marketplaces, where stolen cryptocurrencies are often traded (Anju *et al*., 2022).

Questions related to prevention and investigation methods can be grouped into a separate category. These are closely tied to the methodological rationale for employing modern digital forensic tools. In particular, this category includes techniques for tracking cryptocurrencies (e.g., blockchain analysis to identify unusual or suspicious transactions) and evidence-gathering methods, such as retrieving information from cryptocurrency wallet addresses, obtaining transaction records, and identifying potential suspects. While these aspects align with traditional forensic tactics and procedures, the terminology in this emerging field remains underdeveloped.

Against this backdrop, it is crucial to emphasize the need to incorporate a dedicated module on legal issues into educational programmes – specifically, the legal aspects of working with cryptocurrencies and blockchain technology. The practice of experts in this field invariably involves understanding the laws and regulations governing the use of cryptocurrencies across various jurisdictions, including issues related to confidentiality, monitoring of financial transactions and cryptocurrency exchanges. Moreover, specialists must be proficient in processing court requests, working with standardized forms of appeal, and properly requesting information from exchanges, blockchain platforms and other digital services while ensuring compliance with legal requirements.

Different stages of pretrial investigations demand distinct approaches to digital evidence, ranging from collection and preservation to analysis and presentation in court. Errors at any stage can result in evidence being deemed inadmissible. Without comprehensive training of specialists based on updated methodological frameworks, even the most advanced technical improvements will remain ineffective. Furthermore, the unique nature of forensic activities involving DE requires high technical expertise, strict adherence to procedural rules and the use of specialized software and hardware tools.

Conclusions

It is evident that cybercrime continues to evolve, giving rise to new techniques and methods for committing crimes (criminal offences), and it is difficult to predict where and when the next evolutionary step will occur. Nevertheless, there is reason to believe that social engineering and technological advancements, fueled by rapid technological progress and the integration of artificial intelligence, will play a decisive role in this process. In the current context, the primary challenges in applying DE to pretrial investigations of cybercrimes, such as online fraud, encompass both traditional forensic issues and emerging complexities. Previously, non-compliance with court decisions or warrants for the collection, retention, and analysis of digital data was more prevalent. Digital forensic investigations have led to the emergence of other violations, such as breaches in the chain of custody for digital evidence, the absence of court-issued warrants or orders from competent authorities for collecting digital data, as well as the use of illegal methods to obtain DE. To date, there is no clear evidence suggesting that forensic experts face serious difficulties due to a lack of technical tools or insufficient regulatory standards outlining the procedures for acquiring and processing data. Accordingly, the primary source of error lies in the human factor – specifically, the actions and decisions of forensic experts. At the same time, the role of these experts remains indispensable, requiring flexibility, interpretation, and adaptation to the unique circumstances of each case. In this regard, the most viable solution appears to be enhancing the professional training of experts in the field (primarily criminalists and forensic investigators, and to a lesser degree, prosecutors and judges). The modern demands of the forensic sector necessitate a major overhaul of training approaches for forensic investigators, including the establishment of a separate discipline. This can be achieved by revising educational methodologies in forensics, thoroughly studying international standards for handling digital evidence (ISO/IEC 27037, 27042, 27043), gaining practical experience with certified forensic tools, and developing skills in analysing complex fraud schemes and cryptocurrency transactions. Additionally, enhancing expertise in applying artificial intelligence to criminology is crucial. Educational programs should also place greater emphasis on understanding the legal admissibility of digital evidence and the requirements of national legal frameworks governing its use.

Acknowledgments

This research was funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan within the framework of the program-targeted financing project BR27101389, "The introduction of artificial intelligence tools into the legislative process of the Republic of Kazakhstan to optimize efficiency and enhance the transparency of legislation".

References

AHMED, A. A.; ALABI, O. O. (2024). "Secure and scalable blockchain-based federated learning for cryptocurrency fraud detection: A systematic review". *IEEE Access*, vol. 12, pp. 102219-102241. DOI: https://doi.org/10.1109/ACCESS.2024.3429205

AL-E'MARI, S.; SANJALAWE, Y.; MAKHADMEH, S.; ALQUDAH, H. (2024). "Digital forensics meets blockchain: Enhancing evidence authenticity and traceability". In: *2024 2nd International Conference on Cyber Resilience (ICCR)*. Dubai: IEEE, pp. 1-6. DOI: https://doi.org/10.1109/ICCR61006.2024.10532961

ALMUTAIRI, W.; MOULAHI, T. (2023). "Joining federated learning to blockchain for digital forensics in IoT". *Computers*, vol. 12, no. 8, p. 157. DOI: https://doi.org/10.3390/computers12080157

ALTALEX (1988). "Codice di procedura penale, Testo del D.P.R. 22 settembre 1988, n. 447". *Altalex* [online]. Available at: https://www.altalex.com/documents/codici-altalex/2014/10/30/codice-di-procedura-penale

AMERICAN BAR ASSOCIATION (2016). "Forensic Examination of Digital Devices in Civil Litigation: The Legal, Ethical and Technical Traps". *American Bar Association* [online]. Available at: https://www.americanbar.org/groups/professional_responsibility/publications/professional_lawyer/2016/volume-24-number-1/forensic_examination_digital_devices_civil_litigation_legal_ethical_and_technical_traps/

ANJU, A.; KAUR, C.; KONDAPALLI, S.; HUSSAIN, M.; BEGUM, A.; HASSEN, S. M.; BOUSH, M. S. A.; BENJEED, A. O. S.; ABDALRAHEEM, M. H. O. (2022). "A mysterious and darkside of the darknet: A qualitative study". *Webology*, vol. 18, no. 4, pp. 285-294. [online]. Available at: https://www.webology.org/data-cms/articles/20220224072305pmwebology%2018%20(4)%20-%2073.pdf

ANTOLIŠ, K. (2023). "The challenges of collecting digital evidence across borders". *Policija i Sigurnost*, vol. 32, no. 3, pp. 271-289. DOI: https://doi.org/10.59245/ps.32.3.2

BALMIKI, V. (2023). "An evidence collection using blockchain for cybercrime detection". In: S. J. C, Varma (ed.). *2023 4th IEEE Global Conference for Advancement in Technology (GCAT)*. Bangalore: IEEE, pp. 1-7. DOI: https://doi.org/10.1109/GCAT59970.2023.10353259

BELKASOFT (2024). "Preserving chain of custody in digital forensics". *Belkasoft*, [online]. Available at: https://belkasoft.com/preserving_chain_of_custody

BHADARGE, T.; PARKHE, D. (2024). "Comparing traditional and digital methods for detecting forged signatures in forensic analysis". *International Journal for Research in Applied Science and Engineering Technology*, vol. 12, no. 4, pp. 2073-2086. DOI: https://doi.org/10.22214/ijraset.2024.60271

CAIANIELLO, M.; CAMON, A. (2021). *Digital forensic evidence. Towards common European standards in antifraud administrative and criminal investigations*. San Giuliano Milanese: Wolters Kluwer, pp. 1-272. [online]. Available at: https://iris.unimore.it/bitstream/11380/1230941/2/CAIANIELLO-CAMON%2C%20Digital%20forensic%20evidence.pdf

CASEY, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the internet*. Cambridge: Academic Press.

CYBER CENTAURS (2024). "Exposing Weaknesses in Digital Evidence for Effective Defense". *Cyber Centaurs* [online]. Available at: https://cybercentaurs.com/blog/exposing-weaknesses-in-digital-evidence-for-effective-defense/

COMMITTEE OF MINISTERS OF THE COUNCIL OF EUROPE (2019). "Guidelines of the Committee of Ministers of the Council of Europe on electronic evidence in civil and administrative proceedings". *COE* [online]. Available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680902e0c

CUI, W.; LI, Y. (2023). "An improved algorithm for elliptic curve digital signature". In: *2023 42nd Chinese Control Conference (CCC)*. Tianjin: IEEE, pp. 8830-8833. DOI: https://doi.org/10.23919/CCC58697.2023.10240757

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (2022). "Combating Cyber Crime". *CISA* [online]. Available at: https://www.cisa.gov/combating-cyber-crime

CYBSAFE (2024). "The Annual Cybersecurity Attitudes and Behaviors Report". *Cybsafe* [online]. Available at: https://www.cybsafe.com/whitepapers/oh-behave-the-annual-cybersecurity-attitudes-and-behaviors-report-24-25/

D'ANNA, T.; PUNTARELLO, M.; CANNELLA, G.; SCALZO, G.; BUSCEMI, R.; ZERBO, S.; ARGO, A. (2023). "The chain of custody in the era of modern forensics: from the classic procedures for gathering evidence to the new challenges related to digital data". *Healthcare*, vol. 11, no. 5, p. 634. DOI: https://doi.org/10.3390/healthcare11050634

DE ABREU MOTTA, A. (2023). "The importance of the chain of custody of expert evidence in digital and digitized processes in the civil sphere". *Revista Gênero e Interdisciplinaridade*, vol. 4, no. 1, pp. 458-496. DOI: https://doi.org/10.51249/gei.v4i01.1228

DEMURA, M.; KLEPKA, D.; KRYTSKA, I. (2020). "Ensuring of the rights and legal interests of the person in the conditions of "digitalization" of criminal proceedings". *Law Review of Kyiv University of Law*, vol. 1, pp. 295-301. DOI: https://doi.org/10.36695/2219-5521.1.2020.59.

ECLIPSE FORENSIC (2024). "Breaking the Chain: Common Mistakes in Digital Evidence Handling". *Eclipse Forensics* [online]. Available at: https://eclipseforensics.com/breaking-the-chain-common-mistakes-in-digital-evidence-handling/

EUROPOL (2024). "Internet Organised Crime Threat Assessment (IOCTA)". *Europol* [online]. Available at: https://www.europol.europa.eu/publications-events/main-reports/iocta-report

FEDERAL BUREAU OF INVESTIGATION (2022). "Internet Crime Report". *IC3* [online]. Available at: https://www.ic3.gov/AnnualReport/Reports/2022_ic3report.pdf

FINANCE MAGNATES (2023). "Is Cloud Mining a Scam?". *Finance Magnates*.

FINPROM (2024). "Losses caused by internet fraud in Kazakhstan has reached 7 billion tenge". *Finprom* [online]. Available at: https://finprom.kz/ru/article/usherb-ot-sluchaev-internet-moshennichestva-v-kazahstane-vyros-do-7-milliardov-tenge

FYND ACADEMY (2025). "Chain of Custody in Cyber Security (Digital Forensics): Importance, Process, and Best Practices in 2025". *Fynd Academy*.

GOODISON, S. E.; DAVIS, R. C.; JACKSON, B. A. (2015). "Digital evidence and the US Criminal Justice System". *RAND* Corporation [online]. Available at: https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf

GRAHAM, M. H. (2016). "Handbook of federal evidence". *Miami Law* [online]. Available at: https://repository.law.miami.edu/fac_books/8/

HORSMAN, G. (2024). "Sources of error in digital forensics". *Forensic Science International: Digital Investigation*, vol. 48, 301693. DOI: https://doi.org/10.1016/j.fsidi.2024.301693

IJIS Institute (2024). *Analysis of the Law Enforcement Digital Evidence Imagery Lifecycle*. Law Enforcement Imaging Technology Task Force [online]. Available at: https://ijis.org/wp-content/uploads/2024/05/LEITTF-Digital-Evidence-Whitepaper.pdf

INFORMATION COMMISSIONER'S OFFICE (2024). "Guidance on the use of storage and access technologies impact assessment – DRAFT". *ICO* [online]. Available at: https://ico.org.uk/media/about-the-ico/impact-assessments/4032165/storage-and-access-tech-guidance-final-draft-ia-for-consultation-20241219.pdf

INTERPOL (2021). "Guidelines for Digital Forensics First Responders". *Interpol* [online]. Available at: https://www.interpol.int/content/download/16243/file/Guidelines_to_Digital_Forensics_First_Responders_V7.pdf

ISO (2012). "ISO/IEC 27037:2012. "Information technology. Security techniques. Guidelines for identification, collection, acquisition and preservation of digital evidence". *ISO* [online]. Available at: https://www.iso.org/ru/standard/44381.html

ISO (2015). "EN ISO/IEC 27042:2022 Information technology. Security techniques. Guidelines for the analysis and interpretation of digital evidence". *ISO* [online]. Available at: https://www.iso.org/standard/44406.html

JUNIPER RESEARCH (2022). "Online Payment Fraud Losses to Exceed $343 Billion Globally Over the Next 5 Years". *Juniper* [online]. Available at: https://www.juniperresearch.com/press/online-payment-fraud-losses-to-exceed-343bn/

LI, M.; LAL, C.; CONTI, M.; HU, D. (2021). "LEChain: A blockchain-based lawful evidence management scheme for digital forensics". *Future Generation Computer Systems*, vol. 115, pp. 406-420. DOI: https://doi.org/10.1016/J.FUTURE.2020.09.038

LUCID TRUTH TECHNOLOGIES (2024). "The Perils of Improper Evidence Collection: Safeguarding the Integrity of Digital Forensics". *Lucid Truth Technologies* [online]. Available at: https://lucidtruthtechnologies.com/improper-evidence-collection/

MERETUKOV, A. G. (2015). "Conditions for the use of evidence in procedural decisions on criminal cases". *Society and Law*, vol. 1, no. 51, pp. 187-191. [online]. Available at: https://cyberleninka.ru/article/n/uslovie-ispolzovaniya-dokazatelstv-v-protsessualnyh-resheniyah-po-ugolovnym-delam

MILLER, A.; SINGH, A. (2024). "Chain of custody and evidence integrity verification using blockchain technology". In: J. du Toit, and B. van Niekerk (Eds.). *Proceedings of the 19th International Conference on Cyber Warfare and Security*, pp. 168-176. Johannesburg: Academic Conferences International Limited. DOI: https://doi.org/10.34190/iccws.19.1.2025

MILLER, C. M. (2023). "A survey of prosecutors and investigators using digital evidence: A starting point". *Forensic Science International: Synergy*, vol. 6, 100296. DOI: https://doi.org/10.1016/j.fsisyn.2022.100296

MIRONOV, B. A.; MILAEVA, M. Y. (2024). "Modern perspective on the concept of crime in the field of computer information. Forensic expertise as a component of criminal law regulation of anti-corruption in the Russian Federation". *Student Science Issues*, vol. 10, p. 248. SCIFF [online]. Available at: https://sciff.ru/wp-content/uploads/2024/11/Sciff_10_98-1.pdf#page=248

MURPHY, C. (2024). "Understanding cybercrime". *EPRS* [online]. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760356/EPRS_BRI(2024)760356_EN.pdf

NAMYSOV, E. D. (2024). "Factors determining the commission on Internet fraud in the Republic of Kazakhstan". *Journal of Innovation in Education and Social Research*, vol. 2, no. 1, pp. 138-142 [online]. Available at: https://journals.proindex.uz/index.php/jiesr/article/view/528

Official State Gazette (1985). "ORGANIC LAW 6/1985, OF 1 JULY, ON THE JUDICIARY". *Official State Gazette*, no. 157 [online]. Available at: https://www.legal-tools.org/doc/881df4/pdf/#:~:text=Article%20122%20of%20the%20Spanish,the%20Official%20State%20Gazette%20n%C2%BA

PALATTY, N. J. (2025). "90+ Cyber Crime Statistics 2025: Cost, Industries and Trends". *astra* [online]. Available at: https://www.getastra.com/blog/security-audit/cyber-crime-statistics/

RAKHA, N. (2024). "Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations". *Mexican Law Review*, vol. 16, no. 2, pp. 23-54. DOI: https://doi.org/10.22201/iij.24485306e.2024.2.18892

ROGERS, S. (2024). "International Scammers Steal Over $1 Trillion in 12 Months in Global State of Scams Report 2024". *GASA* [online]. Available at: https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai

SALIH, K.; AND IBRAHIM, N. (2023). "CustodyChainGuardian: Blockchain of custody digital evidence preservation system". In: B. M. Sukojo (ed.). *2023 IEEE Asia-Pacific Conference on Geoscience, Electronics and Remote Sensing Technology (AGERS)*, pp. 168-175. Surabaya: IEEE. DOI: https://doi.org/10.1109/AGERS61027.2023.10490757

SALMAN, M.; BANI-SLMAN, B.; ALJAIDI, M.; SALEEM, R.; ALSARHAN, A.; QASEM, M.; INJADAT, M.; IGRIED, B. (2023). "A study of forensic tools data recovery performance". In: *2023 2nd International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI)*, pp. 1-6. Zarqa: IEEE. DOI: https://doi.org/10.1109/EICEEAI60672.2023.10590383

SANIYAZOVA, Y.; MEDIYEV, R.; SAITOVA, E.; UTEGENOVA, G.; KZYLKHOJAYEVA, A. (2024). "Advancing forensic science in Kazakhstan: The emergence and impact of digital forensics in cybercrime investigation". *Law, State and Telecommunications Review*, vol. 16, no. 2, pp. 48-68. DOI: https://doi.org/10.26512/lstr.v16i2.49190

SATBAYEVA A. M.; ALIMBETOVA A. P.; BEISSENBAYEVA M. T. (2024). "Cybercrime challenges: Experience of international cooperation". *Scientific and Legal Journal «Bulletin of the Institute of Legislation and Legal Information of the Republic of Kazakhstan*, vol. 3, no. 78, pp. 211-221. DOI: https://doi.org/10.52026/2788-5291_2024_78_3_211

SEO, W. (2024). "A study on electronic evidence collection methods in foreign countries and methods for granting evidence". *The Korean Association of Criminal Procedure Law*, vol. 16, no. 1, pp. 209-263. DOI: https://doi.org/10.34222/kdps.2024.16.1.209

SINGH, A.; IKUESAN, R.; VENTER, H. (2022). "Secure storage model for digital forensic readiness". *IEEE Access*, vol. 10, pp. 19469-19480. DOI: https://doi.org/10.1109/ACCESS.2022.3151403

STOILKOVSKI, M. (2022). "Guidelines on cybercrime investigation". *OSCE* [online]. Available at: https://www.osce.org/files/f/documents/a/8/534684.pdf

STRIPE (2023). "Online and ecommerce fraud statistics that are predicting the future of fraud". *Stripe* [online]. Available at: https://stripe.com/resources/more/online-and-ecommerce-fraud-statistics

TCDI (2023). "The Hidden Dangers of Entrusting Forensic Data Collections to Your Internal IT Team". *TCDI* [online]. Available at: https://www.tcdi.com/the-hidden-dangers-of-entrusting-forensic-data-collections-to-your-internal-it-team/

TOSZA, S. (2024). "Mutual recognition by private actors in criminal justice? E-evidence regulation and service providers as the new guardians of fundamental rights". *Common Market Law Review*, vol. 61, no. 1, pp. 139-166. DOI: https://doi.org/10.54648/cola2024005

TURLYBEK, S. (2024). "MVD has explained the types of fraud". *Polisia.kz*. [online]. [online]. Available at: https://polisia.kz/ru/v-mvd-rasskazali-o-vidah-moshennichestva/

U.S. ATTORNEY'S OFFICE, CENTRAL DISTRICT OF CALIFORNIA (2022). "Cyber and Intellectual Property Crimes Section. Retrieved from". *Justice.gov* [online]. Available at: https://www.justice.gov/archives/usao-cdca/cyber-and-intellectual-property-crimes-section

UNITED NATIONS OFFICE ON DRUGS AND CRIME (2024). "Module Series Overview". *Sherloc* [online]. Available at: https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime.html

UNITED STATES COURT OF APPEALS (2010). "Appeal from the United States District Court for the Southern District of Ohio at Cincinnati". *OPN* [online]. Available at: https://www.opn.ca6.uscourts.gov/opinions.pdf/10a0377p-06.pdf

USTAWA z dnia 6 czerwca 1997 r. "Kodeks postępowania karnego". *Wolters Kluwer* [online]. Available at: https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/kodeks-postepowania-karnego-16798685

UTEPOV, D.; ZHEMPIISOV, N. (2022). "Legal basis for collection and attachment of digital information as proof in criminal cases in the Republic of Kazakhstan". *Jurisprudence*, vol. 1, pp. 165-174. DOI: https://doi.org/10.51788/tsul.jurisprudence.2.1./agoo5913

VAPNIARCHUK, V. V.; TROFYMENKO, V. M.; SHYLO, O. G.; MARYNIV, V. I. (2018). "Standards of criminal procedure evidence". *Journal of Advanced Research in Law and Economics*, vol. 9, no. 7.37, pp. 2462-2470 [online]. Available at: https://www.ceeol.com/search/article-detail?id=808866

VIDYA, V.; SALY, K.; BALAN, C. (2022). "Forensic acquisition and analysis of webpage". In: B. S. Anami (ed.). *2022 2nd International Conference on Intelligent Technologies (CONIT)*, pp. 1-6. Hubli: IEEE. DOI: https://doi.org/10.1109/CONIT55038.2022.9848303

VLEX (2014). "United States of America, Appellee, v. Semyon Vayner, aka Sam Vayner, aka Semen, Defendant, Aliaksandr Zhyltsou, Defendant-Appellant". *VLex* [online]. Available at: https://case-law.vlex.com/vid/united-states-v-vayner-885228839

VOLONINO, L. (2003). "Electronic evidence and computer forensics". *Communications of the Association for Information Systems*, vol. 12, no. 1, pp. 457-468. DOI: https://doi.org/10.17705/1CAIS.01227

WAIRIMU, S.; IWAYA, L.; FRITSCH, L.; LINDSKOG, S. (2024). "On the evaluation of privacy impact assessment and privacy risk assessment methodologies: A systematic literature review". *IEEE Access*, vol. 12, pp. 19625-19650. DOI: https://doi.org/10.1109/ACCESS.2024.3360864

YEBOAH-OFORI, A.; BROWN, A. D. (2020). "Digital forensics investigation jurisprudence: Issues of admissibility of digital evidence". *Journal of Forensic, Legal and Investigative Sciences*, vol. 6, no. 1, pp. 1-8. DOI: http://dx.doi.org/10.24966/FLIS-733X/100045

Recommended citation

APSIMET, Nurdaulet; ALIMKULOV, Yerbol; KONYSBAY, Bakytkul; ZHANIBEKOV, Akynkozha; MURATOVA, Alua (2026). "Challenges of using digital evidence in pretrial investigations of nnline fraud: lessons for Kazakhstan from international practice". *IDP. Internet, Law and Politics Journal*, no. 44. UOC [Accessed: dd/mm/yy]. DOI: http://dx.doi.org/10.7238/idp.v0i44.433072

About the authors

Nurdaulet Apsimet
Department of Criminal Law, Criminal Procedure and Criminalistics, Al-Farabi Kazakh National University, Almaty, Kazakhstan
apsimet.nurdaulet@gmail.com

Master of Legal Sciences degree. He is a doctoral student at the Department of Criminal Law, Criminal Procedure and Criminalistics, Al-Farabi Kazakh National University, Almaty, Kazakhstan. His research interests are: cybercrime, internet fraud, criminal law, etc.

Yerbol Alimkulov
Department of Criminal Law, Criminal Procedure and Criminalistics, Al-Farabi Kazakh National University, Almaty, Kazakhstan
erbol.alymkulov@kaznu.edu.kz

Candidate of Legal Sciences degree. He is an associate professor of the Department of Criminal Law, Criminal Procedure and Criminalistics and Deputy Dean of the Faculty of Law at the Al-Farabi Kazakh National University, Almaty, Kazakhstan. His research interests are: criminal procedure, pre-trial investigation, criminal procedure law, etc.

Bakytkul Konysbay
Department of Customs, Financial and Environmental Law, Al-Farabi Kazakh National University, Almaty, Kazakhstan
b.konysbay@kaznu.edu.kz

PhD degree. She is an acting associate professor at the Department of Customs, Financial and Environmental Law, Al-Farabi Kazakh National University, Almaty, Kazakhstan. Her research interests are: financial law, banking law, customs law, etc.

Akynkozha Zhanibekov
Mukhtar Auezov South Kazakhstan Research University, Shymkent, Kazakhstan
zhan.akin@gmail.com

PhD degree. He is a professor of the Faculty of Law and Member of the Board – Vice-Rector for Research and Innovation at Mukhtar Auezov South Kazakhstan Research University, Shymkent, Kazakhstan. His research interests are: criminal procedure, evidence in criminal proceedings, advocacy, etc.

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Alua Muratova
Department of Criminal Law Disciplines, L.N. Gumilyov Eurasian National University, Astana, Kazakhstan
muratova_azh@enu.kz

PhD degree. She is the head of the Department of Criminal Law Disciplines at L.N. Gumilyov Eurasian National University, Astana, Kazakhstan. Her research interests are: cybercrime, online fraud, criminal justice system, etc.

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Copyright or personality rights? A critical analysis of Denmark's approach to deepfakes

Gabriel Ernesto Melian Pérez
Universitat Pompeu Fabra

Laura Herrerías Castro
Universitat Pompeu Fabra

Date of submission: September 2025
Accepted in: January 2026
Published in: March 2026

Abstract

This paper critically examines Denmark's proposed amendment to its Copyright Act, particularly section 73(a), which aims to grant individuals intellectual property protection against the unauthorized sharing of realistic, digitally generated imitations of their physical traits (deepfakes). While recognizing the well-intentioned aim, this study contends that the Danish proposal is fundamentally flawed both conceptually and teleologically. The analysis demonstrates that copyright law is an inappropriate framework for safeguarding elements of personal identity. A significant teleological mismatch exists: copyright law promotes economic and cultural objectives by encouraging the creation of works, whereas personality rights are grounded in the principle of human dignity. This misalignment risks turning intrinsic personality traits into commodities and undermining the coherence of the copyright system. The study proposes that Spain's Organic Act 1/1982 on the civil protection of the right to honour, privacy and one's own image offers a more suitable alternative. Despite its origins in the 1980s, this act's substantive and procedural design effectively addresses technological challenges such as deepfakes without requiring major reforms. The paper concludes that reinforcing existing civil protection mechanisms provides a more consistent solution than relying on copyright law.

Keywords

deepfake; artificial intelligence; copyright; personality rights; right to one's image

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

¿Derechos de autor o de personalidad? Un análisis crítico del enfoque de Dinamarca hacia las falsificaciones deepfake

Resumen

*Este documento examina de forma crítica la enmienda propuesta por Dinamarca a su Ley de Derechos de Autor, en particular la sección 73(a), cuyo objetivo es otorgar a las personas protección de la propiedad intelectual contra el intercambio no autorizado de imitaciones realistas generadas digitalmente a partir de sus rasgos físicos (*deepfakes*). Al tiempo que reconoce el objetivo bienintencionado, este estudio sostiene que la propuesta danesa es fundamentalmente defectuosa tanto conceptualmente como teleológicamente. El análisis demuestra que la ley de derechos de autor es un marco inapropiado para salvaguardar los elementos de la identidad personal. Existe una discordancia teleológica significativa: la ley de derechos de autor promueve los objetivos económicos y culturales fomentando la creación de obras, mientras que los derechos de personalidad se basan en el principio de dignidad humana. Esta desalineación corre el riesgo de convertir los rasgos de personalidad intrínseca en mercancías y socavar la coherencia del sistema de derechos de autor. El estudio propone que la Ley Orgánica 1/1982 de España sobre la protección civil del derecho al honor, la privacidad y la imagen propia constituye una alternativa más adecuada. A pesar de sus orígenes en la década de 1980, el diseño sustantivo y procedimental de esta ley aborda eficazmente desafíos tecnológicos, como los* deepfakes*, sin requerir reformas importantes. El documento concluye que reforzar los mecanismos de protección civil existentes proporciona una solución más coherente que confiar en la ley de derechos de autor.*

Palabras clave

deepfake*; inteligencia artificial; derechos de autor; derechos de personalidad; derecho a la imagen propia*

Introduction

The swift progress of Artificial Intelligence in recent years has driven the surge of deepfakes.[1] This technology can generate or alter images, audio, or voices with extraordinary realism, making it a potential tool for rights violations. Deepfakes differ from other types of digital manipulation because they aim for such authenticity that they can deceive and cause confusion, unlike caricatures or parodies, which exaggerate features or depend on humour and critique without any assertion of authenticity. It is precisely this potential for deception that makes deepfakes particularly relevant in legal, ethical, and social contexts.

Common threats include non-consensual pornography and identity impersonation or identity theft, illustrating the technology's potential to harm both private and public life (Simó Soler, 2023, pp. 500-503). Deepfakes can also be a powerful means of spreading misinformation, allowing people to generate fake content in political, social, or personal contexts to deceive or mislead audiences and consumers. Consequently, this content significantly undermines trust in the media, traditional evidence, and science (Van der Sloot & Wagensveld, 2022, p. 6).

Some jurisdictions have responded to this situation by proposing new norms. In recent months, Denmark's approach has garnered considerable public attention due to

1. According to recital 134 and art. 3.60 of the Artificial Intelligence Act, "'deep fake' means AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful". Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act).

its pragmatic proposal.[2] This initiative aims to amend the Danish Copyright Act to enable individuals to take legal action against the sharing of deepfakes. This is outlined in section 73(a), which states: "General Protection against Deepfakes: Any individual can seek IP protection against the unauthorized sharing of realistic, digitally generated imitations of their physical characteristics (face, voice, etc.)". It is important to highlight that the Danish proposal focuses solely on the distribution of deepfakes, not their mere creation. Therefore, the provision does not constitute a general ban on deepfakes. Private imitations that are not made available to the public remain permitted.[3]

Although the aim of protecting citizens is well-intentioned, the Danish proposal is both conceptually and teleologically flawed. By transforming elements of personal identity into legal assets under a branch of law traditionally reserved for intellectual creations, it distorts the object of copyright and disregards its functions and objectives. Intellectual property is, therefore, an inadequate tool for addressing deepfakes. From a comparative law perspective, more suitable legal solutions exist.[4] Analysing the proposal's conceptual foundations is essential to inform the political debate and ensure that efforts to address deepfakes do not compromise the coherence and integrity of long-established legal institutions.

The paper is structured as follows. The first section discusses why copyright law is an unsuitable framework for protecting aspects of individual identity. It begins by highlighting the differences between the objects of protection (work/performance versus physical attributes). Then, it addresses the fundamental teleological issue: the purpose of copyright law is inherently distinct from that of laws designed to protect the intrinsic features of a person. The second section reviews the provisions of Spain's Organic Act 1/1982. It demonstrates how this legislation provides a clearer and more effective framework for dealing with the challenges posed by deepfakes. Overall, the paper seeks to demonstrate that tackling contemporary issues like deepfakes does not require altering existing legal regimes but can be achieved by relying on well-established legal frameworks.

Before proceeding, please note the following disclaimer. Section 73(a) is not the only amendment. Section 65(a) has also been introduced, which states: "Protection for Performing Artists: Performing artists can claim copyright protection from unauthorized sharing of realistic, digitally created imitations of their artistic performances". The difference between the two provisions lies in their scope of protection. Section 73(a) safeguards the personal identity traits of individuals, while section 65(a) protects specific artistic performances. The latter focuses on performers and their right to control the use of their performances, a matter traditionally covered by neighbouring rights. Consequently, section 65(a) grants performers access to the enforcement mechanisms usually available to holders of such rights, including the ability to issue takedown notices, claim damages, or initiate infringement proceedings against the creators of the deepfake (see section 83).[5] This paper's analysis focuses solely on the problematic section 73(a), rather than on section 65(a), since the latter is neither as controversial nor as innovative. Section 65(a) is less groundbreaking because it does not establish an entirely new legal framework; instead, it extends existing protections under neighbouring rights for performers to the context of deepfakes. The enforcement mechanisms it provides were already available and are merely applied to a new technological setting. In contrast, section 73(a) creates an autonomous protection of personal identity against digital imitations, an area not traditionally addressed by copyright or neighbouring rights. With these clarifications in mind, we now turn to analysing the implications of the newly introduced section 73(a).

2. See https://www.theguardian.com/technology/2025/jun/27/deepfakes-denmark-copyright-law-artificial-intelligence; https://www.nytimes.com/2025/07/10/world/europe/denmark-deepfake-copyright-ai-law.html; https://www.weforum.org/stories/2025/07/deepfake-legislation-denmark-digital-id/. The proposal can be found at https://www.ft.dk/samling/20241/almdel/kuu/bilag/232/3050901.pdf.
3. In fact, nothing prevents realistic digitally generated imitations from being used within the private sphere, for example, at a private party, as specified in the proposal on page 41.
4. According to the European Parliamentary Research Service's Study on "Tackling deepfakes in European policy" (PE 690.039 – July 2021, p. 40): "Since individuals generally do not own a copyright interest in their own image, copyright law is not very suitable for individuals to protect their own persona. However, in some EU Member States there are other legal provisions for the protection of a person's image or portrait. Although the protection of image rights in the EU still remains far from harmonised, most Member States recognise at least some form of legal protection".
5. As we will discuss later, this broad set of remedies is not available to the subjects covered by section 73(a). The Danish proposal does not provide any justification for this distinction.

1. Copyright is not the proper legal framework

1.1. The problem of the object of protection

Copyright protects original expressions of human intellect, such as literary, cinematographic, musical, pictorial, and photographic works, among others.[6] What is protected are not abstract ideas, but rather the concrete and original form in which those ideas are expressed, hence originality in this expression is a prerequisite (Goldstein and Hugenholtz, 2019). According to the doctrine of the CJEU, an expression is original and therefore constitutes a work protected by copyright if it is the author's own intellectual creation[7] (Fritz, 2024). While no high level of creativity or special artistic merit is required,[8] it should allow some room to reflect creative choices or decisions.[9] If there is no room for such decisions, it would lack originality and could not be considered a work protected by copyright.[10] Besides, the notion of "intellectual creation" implies that the work must be the product of human mental activity, i.e., it excludes anything that is purely automatic, natural, or generated without creative intervention by someone (Friedmann, 2024). This implies that a certain degree of conscious choice and creative freedom is required, so that it can communicate a personal touch.

Copyright laws also cover what are known as "Neighboring Rights".[11] These protect performers, phonogram producers and broadcasters. That is, its object of protection is the interpretation or performance of works, phonograms, and radio and television broadcasts. Neighbouring rights safeguard those who, without being the original authors of a work, make a creative, technical, or financial contribution essential for its public dissemination. A key difference between copyright and neighbouring rights is that the latter do not demand "originality" in the strict sense. However, they do involve an act of creative or technical input, such as a musician's performance (Hugenholtz, 2019). A phonogram producer does not create in the artistic sense but organizes and makes technical and economic decisions that produce an object worthy of legal protection. In essence, neighbouring rights aim to ensure the fair exploitation of contributions significant to cultural communication – even if they are not "original" to the extent required for copyright protection.

Although related rights are less strict than copyright, they are not an appropriate parallel for personal traits. Neighbouring rights, while not requiring the same level of creativity as copyright, still involve an act of creation. An actor's or musician's performance, or a phonogram's recording, reflects an individualized creative or technical contribution that involves conscious effort. Conversely, personality traits such as image and voice are inherent qualities of human personality and not the result of free choices. The proposal neglects the core principle of intellectual property, which is the act of creation. Denmark's approach would introduce elements of personality rights into a legal framework designed for intellectual creations, leading to a clear conflict regarding what is protected.

1.2. Copyright and personality rights have limits, but with different rationales

The boundaries of copyright differ substantially from those of personality rights. While copyright protects the author's rights over an original intellectual creation, the right to one's own image aims to safeguard inherent and fundamental attributes of the individual. This distinction forms the foundation upon which their respective limitation regimes are built. Copyright limitations are intended to balance the creator's temporary monopoly with broader societal interests. To ensure access to culture, education, and the encouragement of new works, the law offers exceptions such as quotation, educational or research use, parody, and informational use. These limitations help prevent the protection of a work from hindering cultural development.

6. Art. 2 Berne Convention for the Protection of Literary and Artistic Works, September 9, 1886, as revised at Paris, July 24, 1971, and amended in 1979.
7. Infopaq International A/S v. Danske Dagblades Forening, C-5/08, EU:C:2009:465 (2009).
8. Cofemel v. G-Star Raw CV, C-683/17, EU:C:2019:531 (2019).
9. Painer v. Standard VerlagsGmbH, C-145/10, EU:C:2011:798 (2011); Brompton Bicycle Ltd v. Chedech/Get2Get, C-833/18, EU:C:2020:946 (2020).
10. Football Dataco Ltd v. Yahoo! UK Ltd, C-604/10, EU:C:2012:115 (2012).
11. Rome Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations, 496 UNTS 43 (1961).

These limits are reinforced by the "three-step rule", established in the Berne Convention as a strict control mechanism over copyright exceptions. Consequently, for a limitation to be lawful, it must cumulatively meet three conditions:

1) the limitation must only apply in certain specific cases that are well defined by law;[12]
2) the use covered by the limitation must not interfere with the way in which the author is commercially exploiting his work; and
3) the limitation must not cause disproportionate harm to the legitimate interests of the right holder.

In contrast, the limits of image rights are established through a balancing test between fundamental rights (Dworkin, 1977), which evaluates the legality, proportionality, and necessity of restricting personal rights in favour of others, such as freedom of expression or information. Unlike copyright, the restrictions on image rights are not aimed at fostering third-party creativity or cultural access but are instead designed to weigh these rights against constitutionally protected interests. The ECtHR has outlined nonexhaustive key factors to consider when balancing the right to one's image under art. 8 and freedom of expression under art. 10 ECHR, including: contribution to a debate of public interest, the prominence of the individual concerned,[13] prior conduct of that individual, the content, form, and consequences of the publication, and, where relevant, the circumstances under which the photographs were taken.[14]

The right to information does not protect the dissemination of deepfakes, as these creations, by their very nature, lack factual or informational value given that the content they depict is not real. In certain circumstances, the unauthorized dissemination of a deepfake may be protected by freedom of expression when it involves public figures, poses no risk of confusion, and respects the principle of proportionality, for example, in the cases of parody[15] or social criticism.[16]

In summary, in copyright law, the limits are determined by the law governing the creator's monopoly rights, which permit society to benefit from the work under specific conditions. Conversely, restrictions on image rights stem from a balance of fundamental rights, where the right to one's own image may be overridden by freedom of expression and information, always subject to strict scrutiny of proportionality and relevance. This contrast is clear in practice. With copyright, any excerpt from a film or book can be used without the right holder's permission for purposes such as criticism or analysis, provided the three-step test is satisfied. However, under image rights, reproducing and sharing a clip of an identifiable person without consent would generally be prohibited unless there is a significant public interest justifying it.

1.3. The teleological argument

Copyright law is a set of norms that grant creators of original works a series of exclusive rights over the use and exploitation of their works. Although it may be perceived at first glance as a norm whose objective is to protect authors, its purpose is much broader and more complex, preserving a delicate balance between private and public interests (Ricketson & Ginsburg, 2022; Hugenholtz, 2000).

The fundamental purpose of copyright is based on the theory of economic incentive, which seeks to encourage

12. The doctrine of the CJEU establishes that Member States cannot invoke fundamental rights enshrined in the Charter of Fundamental Rights of the EU to create exceptions or limitations to copyright that are not expressly provided for in the Infosoc Directive. This principle, established in cases such as Spiegel Online (C-516/17, ECLI:EU:C:2019:62 (2019). § 49), confirms that the copyright system operates with a closed list of exceptions, which marks a fundamental difference with the regime for limiting personality rights.
13. Public figures enjoy more limited protection of their image rights than private individuals. Whilst in the former case the press exercises its role of "public watchdog" in a democracy by imparting information and ideas on matters of public interest, that role appears less important in the latter case.
14. ECtHR, *Hannover v Germany (no. 2)* [GC], applications nº 40660/08 and 60641/08 (7 February 2012), §§ 108-113; *Axel Springer AG v Germany* [GC], application nº 39954/08 (7 February 2012), §§ 89-95.
15. Satire is a form of artistic expression and social commentary and, by its inherent features of exaggeration and distortion of reality, naturally aims to provoke and agitate. See ECtHR, *Vereinigung Bildender Künstler v Austria*, application nº 68354/01 (25 January 2007), § 33.
16. Freedom of expression not only protects ideas that are favorably received or regarded as inoffensive, but also those that offend, shock or disturb. See ECtHR, *Castells v Spain*, application nº 11798/85 (23 April 1992), § 42.

creativity by ensuring that authors can obtain fair compensation for their intellectual efforts.[17] By granting a temporary monopoly on reproducing and distributing a work, the law establishes a market mechanism that allows creators to benefit from their efforts. Without this legal fiction, the ease with which original works could be mass-copied would discourage the creation of new works. In this way, copyright acts as a tool to stimulate a constant flow of innovation and expression (Landes & Posner, 1989).

The copyright system does not grant authors absolute control; instead, it operates through a delicate balance between their private interests and the public interest in accessing knowledge and culture. This balance is reflected in the temporality of rights, ensuring that all works eventually enrich the public domain. Likewise, the law establishes limitations and exceptions, such as the right to quote or educational uses, allowing society to use existing works reasonably (Ricketson & Ginsburg, 2022). Therefore, ultimately, the function of copyright transcends the individual benefit of the author to fulfil a higher social objective: the advancement of culture, science, and art. The economic reward for the author serves as a means to an end, which is the construction of a rich and diverse cultural heritage and the continuous advancement of knowledge and art.

On this basis, we must ask: does the protection of individual identity traits rest on the same principles and objectives as copyright? The answer is no. Fundamentally different purposes must guide a legal framework designed to prevent the misuse of personal identifying features. Whereas copyright pursues economic and cultural aims, seeking to incentivize creations through economic rewards, personality rights serve an existential and dignitary function, safeguarding the individual's innermost sphere as a cornerstone of human dignity (López Jacoiste, 1986, pp. 1068-1070; de Cupis, 1956, pp. 32-33). Copyright is justified by utilitarian theories (incentive to create), while personality rights are based directly on the dignity of the human person as the supreme value.

If personality rights protect human dignity and the free development of the individual, then what is necessary is a rule that provides concrete safeguards, a guarantee-oriented provision (or a rights-protective rule). The latter do not aim to promote economic activity or encourage productive behaviour, as is the case with copyright, but rather to ensure that a particular right is effectively protected against infringements.[18] In other words, what is necessary is to establish a system of civil protection against all types of unlawful interference, enabling legal action to seek compensation and remedial measures. This concept of "personal intellectual property" conflicts with the logic of copyright law: the goal is not to reward the authorship of a creation, but to prevent impersonation.

In summary, the Danish proposal presents several risks. First, it may lead to uncontrolled expansion and blurring of copyright, whose scope is already complex and diffuse. Including elements unrelated to the system, such as personal identity traits, could distort the logic and principles of the intellectual property regime, leading to conceptual conflicts and interpretive difficulties.

Secondly, this proposal could influence future European legislation in areas such as copyright, where there is still no complete harmonization on several key issues. This could create further legal uncertainty and disrupt the coherence of the European intellectual property framework by incorporating criteria that are unrelated to the traditional logic of this branch of law.

Thirdly, there could be a potential risk of excessive "commodification" of inherent personality traits. Intellectual property law is intended to "commodify" content and promote its economic exploitation. This approach could

17. The first conceptual obstacle arises when comparing this to personal characteristics. While copyright serves to reward the author for the creative effort invested in producing a work, one might ask: what effort is involved in the mere image of an ordinary person? In this case, the "remunerative function" of copyright is meaningless, since there is no effort involved in possessing certain features when these are given by nature. This argument loses force when it comes to celebrities, whose personal characteristics are often the result of significant effort and financial investment – through marketing strategies and advertising campaigns – aimed at building and consolidating their image.
18. Under the objectives set out in the Danish proposal, it does not seem that the idea is to promote a business model based on the commercialization of images, but rather to ensure that individuals can prevent the unauthorized use of their distinctive features. It would be inconsistent to use a regime whose logic consists precisely in encouraging the dissemination, "commodification", and exploitation of content – as is the case with copyright – to pursue an opposite objective, namely, to prevent deepfakes.

indeed turn deepfakes into a new "licensing opportunity" rather than an illegal activity (Hugenholtz, 2025). In other words, aligning with the logic of IP rights encourages the creation of deepfakes as a possible source of income for individuals, rather than deterring it. Should this be the aim of a new regulation that seeks to limit the harmful effects of deepfakes? This is not the perspective supported by this paper. A regulatory solution should prioritize safeguarding individual dignity and control over aspects of identity, rather than providing incentives for economic exploitation.[19]

Finally, there is also a risk of weakening or neglecting legal frameworks better suited to protect inherent personality rights. Traditionally, these rights have been protected through constitutional and civil mechanisms, which better align with the dignity and safeguarding purpose of these rights than an intellectual property regime. In the second part of this paper, we therefore aim to highlight an approach that we consider more suitable for protecting the interests discussed above.

2. Towards a more suitable legal alternative

2.1. The civil protection of the right to one's image

A person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development and presupposes the right to control the use of that image.[20] The spread of deepfakes endangers this right by removing individuals' control over their image and voice. For instance, deepfakes can falsely attribute statements to someone that oppose their beliefs or be used to mock them. The unauthorised distribution of deepfakes can breach the right to one's image (Trujillo Cabrera, 2024, pp. 92-94), and when such distribution aims to defame the individual depicted, it may also violate the right to honour (Herrerías Castro, 2025, pp. 38-39).[21]

A recent case in Germany illustrates these risks. Manfred Lehmann, a well-known dubbing artist, sued a YouTube channel operator for the unauthorized commercial use of his voice. In its ruling, the Berlin Regional Court (II, 2 O 202/24) found that the YouTube creator had violated Lehmann's right to his own voice by using an AI-generated voice to add narration to videos. Although the voice employed was an artificial reproduction rather than Lehmann's actual voice, the method of production was considered irrelevant. What matters is whether a substantial part of the target audience would believe that Lehmann had authorized the content of the videos.

Section 73(a) of the Danish Proposal Copyright Act protects individuals from the unauthorized publication of deepfakes. This protection remains in force until 50 years after the individual depicted has died. One reason for extending copyright protection to these cases is that, under Danish commercial law, the right to one's own image only covers the commercial use of digitally generated imitations.[22] When there is no commercial purpose, the injured parties must rely on the general rules of non-contractual civil liability.

In contrast, art. 7.5 of the Spanish Organic Act 1/1982, of 5 May, on the civil protection of the right to honour, privacy and one's own image protects individuals, among others, against "the capture, reproduction, or publication by means of photography, film, or any other process, of the image of a person in places or moments of their private

19. It should be noted that although personality rights are traditionally regarded as inalienable, unavailable and non-transferable, their holders may consent to certain uses of their image, typically in exchange for remuneration. See Vendrell Cervantes (2014, pp.132-152).
20. ECtHR, GC, López Ribalda and Others v. Spain, applications nº 1874/13 and 8567/13 (17 October 2019) §§ 87-89.
21. See also Judgements of the Spanish Supreme Court nº 682/2020, of 15 December 2020 (ECLI:ES:TS:2020:4217); nº 209/2020, of 29 May 2020 (ECLI:ES:TS:2020:1537); nº 544/2016, of 14 September 2016 (ECLI:ES:TS:2016:4053); and nº 588/2011, of 20 July 2011 (ECLI:ES:TS:2011:5858).
22. In Spain, see art. 7.6 of the Organic Act 1/1982, of 5 May, which protects individuals against the use of their name, voice, or image for advertising, commercial, or similar purposes.

life or outside of them".[23] The Spanish Supreme Court has interpreted the scope of art. 7 broadly, so that the protection it offers can also be understood to include a person's voice (Ammerman Yebra, 2021, pp. 151-152). The protection of a person's image also extends to neutral photographs, which are images that, while not revealing private details of an individual's life, nonetheless depict their physical appearance in a way that makes them identifiable.[24] This is because the Constitutional Court regards the rights to privacy and to one's own image as separate rights with their own specific content.

The Danish Proposal protects only realistic deepfakes and excludes from its scope of application deepfakes created primarily for purposes such as caricature, satire, parody, pastiche,[25] or social and political criticism, unless the imitation constitutes misinformation. The criterion of realism requires that the imitation has the potential to cause confusion with the person being imitated. For instance, a deepfake showing a person's traits as a fictional character would not be protected, as such an imitation generally cannot cause confusion. Similarly, a realistic deepfake that reveals the content has been artificially created or manipulated would also not entail a risk of confusion.[26] On the contrary, under art. 7 of the Organic Act 1/1982, the mere warning itself does not constitute a legitimate justification for interference with the right to one's image (Extremera Fernández, 2024, pp. 247-248).

As noted above, under the Danish Proposal, caricatures and other forms of protected speech are excluded from its scope of protection unless they pose a risk to the rights of others, such as life, health, privacy, reputation, or property. Similarly, art. 8.2 (b) of the Organic Act 1/1982 states that the right to one's own image shall not prevent the use of caricatures of public persons, in accordance with social custom. A caricature is a visual representation in which a person's image is exaggerated humorously or critically, exercising freedom of expression. A depiction does not qualify as a caricature if the person's image is not distorted or the distortion is not clearly recognizable (de Verda y Beamonte, 2011, pp. 107-108). Consequently, a deepfake cannot be regarded as a caricature when it does not involve a deliberate alteration of a person's image for satirical, humorous, or socially critical aims. For example, linking a person's face with a naked or semi-naked body surpasses the limits of freedom of expression. In this regard, the Judgment of the Spanish Constitutional Court nº 23/2010, of 27 April, held that it is difficult to see any public interest in the use of such manipulated photographs, as they are unrelated to any legitimate purpose of political or social criticism and their publication does not contribute to the formation of free public opinion.

Finally, according to sections 83 and 84 of the Danish Proposal, individuals have no right to compensation for infringements of section 73 a); they can only seek the removal of the deepfake. This contrasts with the broad range of remedies available under art. 9.2 of the Organic Act 1/1982 in cases of infringement of the right to one's own image. In such instances, the injured party may pursue several remedies, such as an injunction ordering the violation to cease and/or prohibiting its future occurrence, a claim for damages to compensate for the harm suffered, an action seeking the publication of the judgment against the defendant, and the appropriation by the injured party of the profit obtained from the infringement of their rights (Santos Morón, 2023, pp. 1324-1334; Yzquierdo Tolsada, 2014).

In summary, despite the Organic Act 1/1982 dating to the 80s, the wording of art. 7, along with its broad judicial interpretation, allows for the inclusion of deepfakes. It should be noted that this provision does not establish a closed list of infringements of the right to honour, to privacy and to one's own image. This open character allows for an adaptation of new instances of infringements to the new requirements posed by technological advances without the need to pass new acts on the subject.

Regarding the limits of the right to one's own image, deepfakes disseminated for humorous or socially critical purposes should be protected under freedom of expression, provided the principle of proportionality is respected.

23. Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen (BOE nº 115, 14/05/1982).
24. Judgement of the Spanish Constitutional Court nº 27/2020, of 24 February 2020 (ECLI:ES:TC:2020:27).
25. On the meaning of the term "pastiche" see the Opinion of AG Emiliou in Pelham, C-590/23, ECLI:EU:C:2025:452 (2025) §§ 81-83.
26. Art. 50.4 of Artificial Intelligence Act.

However, freedom of expression does not extend to the unauthorized dissemination of a person's image – particularly if the individual is not a public figure – when no public interest is involved. Moreover, the Danish Proposal excludes from its scope of protection deepfakes that disclose they have been artificially generated. Even though such deepfakes do not create a risk of confusion, the right to one's image can still be severely infringed, for example, in cases of non-consensual pornography.

2.2. Why should the Organic Act 1/1982 inspire future legislation?

From a procedural standpoint, one of the main advantages of the Spanish legal system is that it allows individuals to seek judicial protection against violations of fundamental rights through the special procedure established in art. 53.2 of the Spanish Constitution. This provision grants all citizens the right to seek protection of their own image before the ordinary courts through a procedure based on the principles of preference and summary resolution. In this regard, art. 249.1.2 of the Civil Procedure Act sets forth that claims seeking protection of the right to honour, privacy, and one's own image shall be given priority. Furthermore, art. 477.2 of the same Act guarantees the possibility of filing an appeal before the Supreme Court in cases involving civil protection of fundamental rights. Finally, the provisional enforcement of judgments safeguarding fundamental rights is also prioritized (art. 524.5), except for compensation awards, for which provisional enforcement is not permitted (art. 535.3).

From a substantive law perspective, art. 9.3 of the Organic Act 1/1982 establishes an irrefutable presumption of nonpecuniary damages, which serves as an exception to the general rules in Spanish law that require the claimant to prove the existence of damage.[27] This presumption is justified both due to the difficulty of proving this type of loss and because the specific nature of the protected interests that have been infringed reasonably suggests that nonpecuniary loss has occurred (Martín-Casals/Solé Feliu, 2005, p. 329).

The assessment of nonpecuniary damage must consider both the circumstances of the case and the seriousness of the harm. The latter requires evaluating the scope of dissemination of the medium through which the infringement occurred, from both a quantitative and qualitative perspective. The quantitative dimension refers to the number of potential recipients,[28] while the qualitative dimension concerns the impact of the infringement on the injured party's personal, professional, or social life. Even when dissemination is limited, the harm may still be severe if the infringement occurs within the area where the injured person resides or conducts their professional activities.[29] In the online context, the Spanish Supreme Court considers various factors when assessing the seriousness of the damage, including the number of followers of an account,[30] the volume of visits or impressions received,[31] and the duration for which the content remained accessible.[32] The ECtHR has also stressed the relevance of the social network account's public or private nature in assessing the extent of the harm caused.[33]

The injured party may claim damages against the individual who disseminates the deepfake and against the online platform that hosts it. In the latter case, the platform becomes civilly liable only when it has actual knowledge or awareness of the content's illegality, usually upon receiving a user notification, and then fails to act promptly to remove it or restrict access (Herrerías Castro, 2025). Until that moment, it may rely on the safe harbour protection provided in art. 6.1 of the Digital Services Act (Arroyo

27. See also art. 27.1 of Act 15/2022 on equal treatment and non-discrimination (Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, BOE nº 167, 13/07/2022).
28. Judgement of the Spanish Supreme Court nº 689/2019, of 18 December 2019 (ECLI:ES:TS:2019:4200).
29. Judgements of the Spanish Supreme Court nº 484/2024, of 10 April 2024 (ECLI:ES:TS:2024:1805); nº 637/2022, of 3 October 2022 (ECLI:ES:TS:2022:3505).
30. Judgement of the Spanish Supreme Court nº 142/2022, of 22 February 2022 (ECLI:ES:TS:2022:632).
31. Judgements of the Spanish Supreme Court nº 1037/2023, of 27 June 2023 (ECLI:ES:TS:2023:2894); nº 682/2020, of 15 December 2020 (ECLI:ES:TS:2020:4217).
32. Judgement of the Spanish Supreme Court nº 1617/2023, of 21 November 2023 (ECLI:ES:TS:2023:5194).
33. ECtHR, *Kozan v. Türkiye*, application nº 16695/19 (1 March 2022) §§ 51 and 66.

Amayuelas, 2025).[34] The injured party might also seek damages from the Generative AI operator itself under Member States' non-contractual liability rules[35], although proving fault can be challenging.[36]

As noted in the previous section, the Danish Proposal grants individuals the right to request the removal of deepfakes from the medium on which they have been published. In accordance with art. 6.4 of the Digital Services Act, the safe harbour protection for hosting service providers does not prevent a judicial authority, following a Member State's legal system, from requiring the online platform to terminate or prevent an infringement.

Pursuant to art. 9.2 a) DSA, any order to act against illegal content must contain the following information:

i) a reference to the legal basis under Union or national law for the order;
ii) a statement of reasons explaining why the information is illegal content, by reference to one or more specific provisions of Union law or national law in compliance with Union law;
iii) information identifying the issuing authority;
iv) clear information enabling the provider of intermediary services to identify and locate the illegal content concerned, such as one or more exact URL and, where necessary, additional information;
v) information about redress mechanisms available to the provider of intermediary services and to the recipient of the service who provided the content;
vi) where applicable, information about which authority is to receive the information about the effect given to the orders. Concerning the territorial scope of such orders, art. 9.2 b) DSA does not exclude global effectiveness, although it states that it must be limited to what is strictly necessary to achieve its objective.[37]

A key issue, however, is that users may reupload deepfakes, and the Danish Proposal does not clarify whether a claim under sec. 84 extends to preventing further infringements.[38] In contrast, art. 9.2(b) of the Organic Act 1/1982 explicitly states that judicial protection includes preventing future infringements.[39] Such prevention may be implemented using automated detection tools, such as hashing technologies (Gorwa, Binns & Katzenbach, 2020, p. 4).

Although injunctions are essential for protecting fundamental rights, they are not always sufficient, given the challenges of preventing content from reappearing after removal. The viral dissemination of a deepfake might cause substantial reputational harm, potentially affecting both personal and professional life. Effective protection of the right to one's image requires that injured parties be entitled to seek both injunctive relief and damages. The Danish proposal, in its current form, is inadequate to achieve this objective, as it expressly excludes compensation claims and fails to address the prevention of future infringements.

34. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (OJ L 277, 27.10.2022, pp. 1-102). It should be noted that safe harbor protections do not affect the obligations imposed by the GDPR on online platform operators. See Russmedia Digital and Inform Media Press, C-492/23, ECLI:EU:C:2025:935 (2025), §§127-136.
35. While the Directive (EU) 2024/2853 of the European Parliament and of the Council of 23 October 2024 on liability for defective products and repealing Council Directive 85/374/EEC classifies AI systems as products, it excludes damages resulting from violations of personality rights from its scope of application (see art. 6 and recital 24).
36. On 11 February 2025, the European Commission announced the withdrawal of the proposal for a Directive on adapting non-contractual civil liability rules to artificial intelligence due to the absence of a foreseeable agreement among the Member States. See Commission work programme 2025. Moving forward together: A Bolder, Simpler, Faster Union, Strasbourg, 11.2.2025, COM(2025) 45 final, p 26.
37. Recital 36 DSA sets forth that: "In particular in a cross-border context, the effect of the order should in principle be limited to the territory of the issuing Member State, unless the illegality of the content derives directly from Union law or the issuing authority considers that the rights at stake require a wider territorial scope, in accordance with Union and international law, while taking into account the interests of international comity". See (Melian Pérez, 2022).
38. *Cf*. Art. 17.4 c) of Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (OJ L 130, 17.5.2019, pp. 92-125)
39. In Glawischnig-Piesczek, C-18/18, ECLI:EU:C:2019:821 (2019) the CJEU stated that it is not contrary to art. 15.1 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (now art. 8 DSA) an injunction ordering a social network to remove information the content of which is identical or equivalent to information which was previously declared to be defamatory, or to block access to that information, irrespective of who the author is.

Conclusion

The Danish proposal, although well-intentioned, makes a conceptual error by bringing the issue of personality rights into the realm of copyright. While intellectual works are, by nature, economic assets, a person's image and characteristics fall better within the sphere of dignity and personality, and therefore require a less commodified approach. Integrating these elements into the logic of intellectual property not only distorts their essence but also threatens to weaken the internal coherence of the copyright system simultaneously.

This analysis demonstrates that more suitable and less disruptive legal remedies are available. Spain's Organic Act 1/1982 provides a fitting framework for dealing with issues like deepfakes. The act's flexible structure and extensive judicial interpretation mean it can adapt to technological advancements without needing major legislative changes. Additionally, it offers injured parties broader and more effective remedies than those proposed in the Danish proposal. While acknowledging that the Organic Act 1/1982 has its critics, its structure and scope offer a more consistent way to regulate deepfakes. Improving existing mechanisms, such as the right to one's own image, the right to honour, and personal data protection, presents a more conceptually sound alternative than expanding copyright law into this area.

To summarize, this contribution reaffirms the conceptual and teleological inadequacy of resorting to copyright law to address deepfakes. The systematic coherence of the legal system requires regulatory solutions that are technologically informed yet respectful of and rigorous with respect to traditional legal categories. This is the only way to avoid hasty legislative responses that, far from solving the problem, end up creating greater distortions.

Acknowledgments

This work was supported by the research project "Digitalización y responsabilidad por producto: análisis de la Directiva (UE) 2024/2853 y de su transposición", funded by the Spanish Ministry of Science, Innovation, and Universities. The European Fund of Regional Development and the Spanish State Research Agency (PID2024-158195OB-I00).

References

AMMERMAN YEBRA, J. (2021). *El derecho a la propia voz como derecho de la personalidad*. A Coruña: Colex.

ARROYO AMAYUELAS, E. (2025). "Article 6 Hosting". In: SCHULZE, R./STAUDENMAYER, D. (ed.). *EU digital law: article-by-article commentary*, pp. 731-757, 2nd ed. Bade-Baden: Nomos.

DE CUPIS, A. (1956). *I Diritti della Personalità*. Milan: Giufrrè editore.

DE VERDA Y BEAMONTE, J. R. (2011). "Intromisiones legítimas en el derecho a la propia imagen autorizadas por la ley". In: DE VERDA Y BEAMONTE, J.R. (coord.). *El derecho a la imagen desde todos los puntos de vista*, pp. 87-120. Cizur Menor: Aranzadi.

DWORKIN, R. (1977). *Taking rights seriously.* Harvard University Press.

EXTREMERA FERNÁNDEZ, B. (2024). "Los *deepfakes* y la intromisión en los derechos de la personalidad (imagen, voz, honor y protección de datos) y sus mecanismos de reparación". In: MORENO MARTÍNEZ/FEMENÍA LÓPEZ (coords.). *Inteligencia artificial y derecho de daños: cuestiones actuales,* pp. 223-259. Madrid: Dykinson.

FRIEDMANN, D. (2024). "Creation and Generation Copyright Standards". *NYU J. Intell. Prop. & Ent. L*, vol. 14, p. 51. DOI: https://doi.org/10.2139/ssrn.4770924

FRITZ, J. (2024). "The notion of 'authorship' under EU law—who can be an author and what makes one an author? An analysis of the legislative framework and case law". *Journal of Intellectual Property Law & Practice*, vol. 19, no. 7, pp. 552-556. DOI: https://doi.org/10.1093/jiplp/jpae022

GOLDSTEIN, P.; HUGENHOLTZ, P. B. (2019). *International copyright: principles, law, and practice*. 4th Edition: Oxford University Press. DOI: https://doi.org/10.1093/9780190060619.001.0001

GORWA, R.; BINNS, R.; KATZENBACH, CH. (2020). "Algorithmic content moderation: Technical and political challenges in the automation of platform governance". *Big Data & Society*, vol 7, no. 1, pp. 1-15. DOI: https://doi.org/10.1177/2053951719897945

HERRERÍAS CASTRO, L. (2025). *El derecho al honor en línea: protección civil y responsabilidad de las plataformas digitales*. Madrid: Aranzadi LALEY.

HERRERÍAS CASTRO, L. (2025). "Liability of online platforms in defamation cases". *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, vol. 16, no. 2, pp. 252-269.

HUGENHOLTZ, B. (2025). "Deepfake Bills in Denmark and the Netherlands: Right idea, wrong legal framework". *Kluwer Copyright Blog* [online]. Available at: https://legalblogs.wolterskluwer.com/copyright-blog/deepfake-bills-in-denmark-and-the-netherlands-right-idea-wrong-legal-framework/. [Accessed: 28 August 2025].

HUGENHOLTZ, B. (2000). "Why the copyright directive is unimportant, and possibly invalid". *European Intellectual Property Review,* vol. 22, no. 11, pp. 499-505.

HUGENHOLTZ, B. (2019). "Neighbouring rights are obsolete". *IIC-International Review of Intellectual Property and Competition Law*, vol. 50, no. 8, pp. 1006-1011. DOI: https://doi.org/10.1007/s40319-019-00864-3

LÓPEZ JACOISTE, J. J. (1986). "Una aproximación tópica a los derechos de la personalidad". *Anuario De Derecho Civil*, vol. 39, no. 4, pp. 1059-1120.

LANDES, W. M.; POSNER, R. A. (1989). "An economic analysis of copyright law". *The Journal of Legal Studies*, vol. 18, no. 2, pp. 325-363. DOI: https://doi.org/10.1086/468150

MARTÍN-CASALS, M.; SOLÉ FELIU, J. (2005). "The protection of personality rights against invasions by mass media in Spain". En: KOZIOL, H. and WARZILEK, A. (eds). *The protection of personality rights against invasions by mass media,* pp. 287-339. New York: Springer.

MELIAN PÉREZ, G. E. (2022). "Global or Local? Freedom of Speech and Some Extraterritorial Court Decisions on the Internet". *Queen Mary Law Journal*, vol. 3, pp. 70-91.

RICKETSON, S.; GINSBURG, J. (2022). *International copyright and neighbouring rights: The Berne Convention and Beyond*. Oxford University Press. DOI: https://doi.org/10.1093/oso/9780198801986.001.0001

SANTOS MORÓN, M. J. (2023). "La tutela de los derechos de la personalidad ante atentados producidos en redes sociales y servicios equivalentes". *Anuario de Derecho Civil*. Tomo LXXVI, fasc. IV, pp. 1297-1374. DOI: https://doi.org/10.53054/adc.v76i4.10303

SIMÓ SOLER, E. (2023). "Retos jurídicos derivados de la Inteligencia Artificial Generativa". *InDret*, vol. 2, no. 22, pp. 493-515. DOI: https://doi.org/10.31009/InDret.2023.i2.11

TRUJILLO CABRERA, C. (2024). "El derecho a la propia imagen (y a la voz) frente a la inteligencia artificial". *InDret*, vol. 1, no. 24, pp. 74-113. DOI: https://doi.org/10.31009/InDret.2024.i1.02

VAN DER SLOOT, B.; WAGENSVELD, Y. (2022). "Deepfakes: regulatory challenges for the synthetic society". *Computer Law & Security Review*, vol. 46, pp. 1-15. DOI: https://doi.org/10.1016/j.clsr.2022.105716

VENDRELL CERVANTES, C. (2014). *El Mercado de los Derechos de Imagen*. Cizur Menor: Thomson Reuters.

YZQUIERDO TOLSADA, M. (2014). "Daños a los derechos de la personalidad (honor, intimidad y propia imagen)". In: REGLERO CAMPOS, L. F. and BUSTO LAGO, J. M. (coords.). *Tratado de Responsabilidad civil,* pp. 1366-1498. 5.ª ed. Tomo II. Cizur Menor: Thomson Reuters Aranzadi.

Recommended citation

MELIAN PÉREZ, Gabriel Ernesto; HERRERÍAS CASTRO, Laura (2026). «Copyright or personality rights? A critical analysis of Denmark's approach to deepfakes». *IDP. Revista de Internet, Derecho y Política*, no. 44. UOC [Accessed: dd/mm/yy]. DOI: http://dx.doi.org/10.7238/idp.v0i44.9800397

About the authors

Gabriel Ernesto Melian Pérez
Predoctoral fellow in the Civil Law Department at the Universitat Pompeu Fabra
gabrielernesto.melian@upf.edu
ORCID: https://orcid.org/0000-0001-9298-5553

He is a predoctoral fellow in the Faculty of Law at the Universitat Pompeu Fabra, Barcelona. He has been a visiting researcher at the Centre for Advanced Internet Studies (Bochum). He holds an LLM in IP and IT from the University of Göttingen and graduated in Law with honours from the University of Havana. He is a member of the project "Contractual and non-contractual liability of online platforms", funded by the Spanish Ministry of Economy, Industry and Competitiveness, the European Fund of Regional Development and the Spanish State Research Agency (PID2021-126354OB-I00).

Laura Herrerías Castro
Postdoctoral Researcher in the Civil Law Department at the Universitat Pompeu Fabra
laura.herrerias@upf.edu
ORCID: https://orcid.org/0000-0003-1975-1499

She is a Postdoctoral Researcher in the Faculty of Law at the Universitat Pompeu Fabra, Barcelona. She has been a visiting researcher at the European University Institute (Florence). She is a member of the projects "Justice, Fundamental Rights and Artificial Intelligence", funded by the EU Justice Programme (101046631, JUST-2021-JTRA); and "Contractual and non-contractual liability of online platforms", funded by the Spanish Ministry of Economy, Industry and Competitiveness, the European Fund of Regional Development and the Spanish State Research Agency (PID2021-126354OB-I00).

IDP REVISTA D'INTERNET, DRET I POLÍTICA
REVISTA DE INTERNET, DERECHO Y POLÍTICA

https://idp.uoc.edu

Identidad cifrada con desencriptación judicial: una solución jurídica para la responsabilidad en entornos *blockchain*

Javier Martínez Boada
Universidad Camilo José Cela (Madrid)

Fecha de presentación: septiembre 2025
Fecha de aceptación: noviembre 2025
Fecha de publicación: marzo 2026

Resumen

La tecnología *blockchain* se posiciona como una de las tecnologías que mayor interés genera en la sociedad actual. Entre sus mayores atractivos se encuentran las características que aporta a las transacciones que efectúan los usuarios en sus sistemas; sin embargo, junto a sus ventajas, también emergen inconvenientes que pueden poner en jaque los ordenamientos jurídicos tal y como están pensados actualmente. En este sentido, la anonimidad con la que son capaces de actuar los usuarios en algunas *blockchain* dificulta la aplicación del derecho, lo que plantea la necesidad de ofrecer alternativas como la implantación de una identidad cifrada que pueda revelarse en determinadas circunstancias y situaciones para garantizar la seguridad jurídica y el cumplimiento de las normas.

Palabras clave

blockchain; identidad; tecnología; anonimidad; derecho

Encrypted identity with judicial decryption: a legal solution for liability in Blockchain environments

Abstract

Blockchain technology is considered one of the most intriguing innovations in today's society. Its key appeal lies in the unique features it offers for user transactions within its systems. However, alongside its benefits, there are also disadvantages that could pose risks to current legal frameworks. In this context, the anonymity that enables users to operate in some Blockchains complicates the application of existing laws. This highlights the need for alternatives, such as implementing an encrypted identity that can be disclosed under certain circumstances to ensure legal certainty and rule compliance.

Keywords

blockchain; identity; technology; anonymity; law

Introducción

Actualmente, las nuevas tecnologías están acaparando el interés del conjunto de la sociedad. Entre ellas, la tecnología *blockchain*, de la cual se espera que durante este año 2026 las transacciones efectuadas en sus sistemas alcancen los 19.900 millones de dólares a nivel mundial, se posiciona como uno de los sistemas más disruptivos, no solo por su capacidad para descentralizar procesos y garantizar la integridad de la información contenida en el sistema, sino también por los desafíos jurídicos y éticos que puede llegar a plantear (Zhang, Xue y Liu, 2019, pág. 2).

Originalmente, la *blockchain* fue creada como base técnica para la criptomoneda Bitcoin con el propósito de evitar el doble gasto en este sistema desarrollado por Satoshi Nakamoto. Gracias a su evolución tecnológica y funcional, la *blockchain*, que inicialmente servía como base de datos distribuida para registrar transacciones, dio paso a las versiones 2.0 y 3.0, lo que la transformó en una infraestructura transversal con aplicaciones en sectores tan diversos como las finanzas, la salud, la energía, la logística, las ciudades inteligentes y la industria 4.0 (Martínez Boada y Rejas Muslera, 2024, pág. 6).

Sin duda, el desarrollo tecnológico y funcional de la *blockchain* permite a los usuarios efectuar transacciones como nunca antes habían imaginado; sin embargo, estos avances no están exentos de desafíos (Torres Cazorla, 2019, pág. 94). Uno de los más significativos es la dificultad para compatibilizar algunas características técnicas de *blockchain*, como el anonimato, con los marcos jurídicos existentes. En este sentido, dentro de las redes *blockchain*, la información fluye de forma descentralizada y los participantes pueden operar sin revelar su identidad real, lo que genera un entorno ideal para preservar la privacidad, pero, por contrapartida, también puede facilitar conductas ilícitas de difícil persecución, pues si no puede conocerse la identidad digital real de los sujetos, difícilmente podrán aplicarse las normas y atribuir responsabilidades (Andola, Raghav, Yadav, Venkatesan y Verma, 2021, pág. 1).

La capacidad que tienen los usuarios en *blockchain* para actuar de forma intrazable utilizando seudónimos que impiden conocer su identidad plantea serias preocupaciones al mundo jurídico, ya que impide, en diversos casos, la aplicación efectiva de los ordenamientos jurídicos. De este modo, deviene imprescindible la propuesta de algún tipo de mecanismo que permita compatibilizar el atractivo que supone la privacidad que poseen los usuarios dentro de los sistemas *blockchain* con la posibilidad de identificarles cuando ocurran actividades ilícitas o, sin ocurrir estas, algún usuario desee entablar acciones legales contra otro por no haber visto respetados sus derechos e intereses (Sun Yin, Langenheldt, Harlev, Mukkamala y Vatrapu, 2019, pág. 37).

La solución no debe consistir simplemente en desmantelar las características básicas de esta tecnología, como,

por ejemplo, prohibir aquellos sistemas en los que no existan identidades tasadas, sino que deben desarrollarse mecanismos o estrategias que permitan equilibrar los caracteres atractivos de la *blockchain* y los derechos y obligaciones de los usuarios.

Ante esta situación, surge la propuesta de implementar dentro de las estructuras *blockchain* un sistema de identidad cifrada capaz de ser descifrado cuando existan condiciones judiciales o legales debidamente autorizadas que lo justifiquen. En este sentido, lo que se busca es continuar garantizando el anonimato en *blockchain* protegiendo la identidad de los usuarios mediante técnicas de cifrado robustas, de manera que dicho anonimato se mantenga en condiciones normales de uso, pero se pueda acceder a su información identificativa bajo condiciones determinadas y con autorización judicial.

1. Panorama general de *blockchain*

1.1. Definición de *blockchain*

Hoy por hoy, no existen normas que se encarguen de definir en qué consiste la tecnología *blockchain* y qué modalidades pueden encontrarse o utilizar los usuarios. En el caso de España, tan solo disponemos de la Proposición de Ley 122/000148 para la Transformación Digital de España[1] que, como la propia palabra indica, únicamente es una declaración de intenciones, pues carece de fuerza normativa al no haber sido debidamente aprobada (Martínez Boada, 2025).

Como ya se ha adelantado, la tecnología *blockchain* emergió durante el año 2008 como el sistema que almacenaba la información de las transacciones efectuadas dentro del protocolo bitcoin con el fin de evitar el doble gasto, pues, sin un registro que archivase las transacciones, los usuarios podían utilizar y gastar las monedas de forma ilimitada (De Filippi y Wright, 2018, pág. 205).

De este modo, y según establece la doctrina, inicialmente *blockchain* fue el sistema que permitió el funcionamiento de la criptomoneda Bitcoin (Ammous, 2016, pág. 1). Sin embargo, es una innovación relativamente reciente que ha cobrado protagonismo en los últimos años, pues ha extendido su uso más allá de las criptomonedas y, por lo tanto, su definición podría variar (Rayenizadeh y Rafsanjani, 2025, pág. 3).

Como se puede observar, la definición de *blockchain* va a depender de la funcionalidad a la que se destine el sistema, por lo que, brevemente a continuación, deberá estudiarse la evolución que ha sufrido esta tecnología y cómo, en consecuencia, varía su concepto (Zīle y Strazdiņa, 2018).

La tecnología *blockchain* ha pasado por tres generaciones denominadas Blockchain 1.0, 2.0 y 3.0, en las que ha sufrido diferentes evoluciones que han variado la manera de concebir este tipo de sistemas (Xu, Chen y Kou, 2019).

Las Blockchain 1.0 se destinaban a almacenar datos y servir como libros de contabilidad distribuidos en los que se registrasen las informaciones de las transacciones de los usuarios, siendo el ejemplo más claro Bitcoin. Posteriormente, surgen las Blockchain 2.0, en las que se va a permitir codificar programas informáticos denominados *smart contracts*, lo que permite observar que la definición de estos sistemas irá un paso más allá de una simple base de datos distribuida. Por último, emergen las Blockchain 3.0 que, sin implementar funcionalidades específicas, permiten a los usuarios utilizar este tipo de ecosistemas en diversos sectores (Sarmah, 2018, pág. 26).

Ante tal evolución, podrá decirse que, dependiendo de cada sistema, la definición podrá variar. Por un lado, existen aquellos que la definen como una base de datos distribuida para registrar informaciones de cualquier tipo (Ibáñez Jiménez, 2018, págs. 36-37). Por otro, quienes la entienden como una enorme computadora mágica en la que pueden codificarse condiciones preestablecidas que, en caso de cumplirse, despliegan unos efectos jurídicos (Davidson, De Filippi y Potts, 2016, pág. 6).

1.2. Estructuras y modalidades de *blockchain*

Junto a la gran variedad de definiciones que puede adoptar esta tecnología, también debe prestarse atención a los tipos de sistemas que pueden constituirse. De igual modo, fruto de los avances tecnológicos que han sufrido estos

1. *Vid*. Congreso de los Diputados. *Proposición de Ley para la Transformación Digital de España*. BOCG-14-B-173-1. 14.ª Legislatura. https://www.congreso.es/public_oficiales/L14/CONG/BOCG/B/BOCG-14-B-173-1.PDF

sistemas, además emergen nuevos entornos con permisos y características diferentes.

Inicialmente, la *blockchain* fue creada para ser un sistema público, abierto y descentralizado en el que los usuarios pudieran transaccionar bajo seudónimos que dificultaran trazar su identidad o, incluso, si se diseñaban expresamente para ello, ser totalmente anónimas (Preukschat y Kuchkovsky, 2017, pág. 27).

Posteriormente, surgen otros entornos que dan lugar, principalmente, a tres tipos de sistemas: públicos, privados e híbridos (Touriño Pena *et al*., 2022, pág. 16).

Según la doctrina, los entornos *blockchain* públicos pueden estar diseñados para ser completamente anónimos. En los sistemas privados, los usuarios normalmente se encuentran debidamente identificados, y los accesos y permisos se encuentran centralizados en una autoridad central; sin embargo, pueden existir entornos privados en los que los usuarios puedan actuar desde el anonimato, si así ha sido diseñado el sistema. En cuanto a los sistemas híbridos, estos combinan características tanto de la *blockchain* pública como de la privada, lo que hace posible configurar el entorno para que los usuarios operen también de manera anónima (Preukschat y Kuchkovsky, 2017, págs. 28-30).

Como puede observarse, a este estudio le interesan todas aquellas arquitecturas *blockchain* que han sido diseñadas para actuar de forma anónima con independencia de su tipología, pues, como ya se ha dicho, cualquiera de los entornos puede haber sido diseñado para que se desconozca la identidad digital fehaciente de los usuarios que operan en este.

2. Características de la tecnología *blockchain*: especial alusión a la anonimidad

La tecnología *blockchain* posee diversos atributos que la diferencian de cualquier otro sistema y que atraen los intereses del conjunto de la sociedad. En general, la doctrina mantiene que las características de *blockchain* son la autonomía, la independencia, la distribución, la inmutabilidad, la seguridad, la transnacionalidad, la rapidez y el pseudoanonimato o anonimato en función del sistema o la intención de los usuarios (Bedecarratz Scholz, 2018, págs. 86-69).

Conviene explicar brevemente cada una de ellas con la finalidad de que el lector entienda los grandes atractivos de este tipo de sistemas y comprenda por qué la tecnología *blockchain* ha despertado tanto interés en diversos sectores.

2.1. Desintermediación

La autonomía o desintermediación permite a los usuarios actuar sin depender de ningún tipo de intermediario o autoridad central. En este sentido, cada nodo actúa de manera independiente cumpliendo con las normas preestablecidas del protocolo, lo que garantiza la confianza entre los usuarios de la red y posibilita que no existan autoridades que regulen sus actuaciones (Pinto Arboleda, Fajardo Bravo, Ortega Mènde, Zambrano Toapanta y Zambrano Recalde, 2025, pág. 500).

2.2. Independencia

La independencia se encuentra estrechamente relacionada con la característica anterior; sin embargo, se centra en la autogestión que poseen los nodos dentro de la red. A este respecto, cada usuario es dueño de sus activos digitales y de su información sin depender de terceros que validen sus transacciones o custodien sus datos (Bedecarratz Scholz, 2018, pág. 86).

2.3. Rapidez

Asimismo, la tecnología *blockchain* aporta rapidez a las transacciones de los usuarios debido a la eficiencia con la que se pueden validar y registrar estas sin la intervención de intermediarios. Aunque el tiempo de confirmación varía según el protocolo y la congestión de la red, en comparación con sistemas tradicionales de transferencia de valor, especialmente en contextos transfronterizos, *blockchain* suele ofrecer mayor velocidad y disponibilidad, incluso operando fuera del horario bancario convencional (Rueda Castañeda, Gallego Gómez, Estanling Cárdenas, Tello y García Pineda, 2024, pág. 10).

2.4. Distribución

La distribución en *blockchain* permite que la información se replique en múltiples nodos, lo que garantiza que todos

accedan al mismo registro, reforzando la transparencia y eliminando un único punto de fallo, lo que, a su vez, incrementa la seguridad (Yaroshenko, Puntus, Chanysheva, Moskalenko y Sliusar, 2025, pág. 248).

2.5. Inmutabilidad

Toda vez que las transacciones se han validado y añadido a la *blockchain*, se vuelven inmutables debido al uso de funciones criptográficas de *hash*[2] y la estructura encadenada de los bloques. En otras palabras, los datos no pueden ser alterados, modificados ni eliminados sin el consenso de la mayoría de la red, lo que ofrece un alto grado de confianza y veracidad a la información almacenada (Hofmann, Wurster, Ron y Böhmecke-Schwafert, 2017, pág. 1).

2.6. Seguridad

Cuando los usuarios eligen utilizar *blockchain* para efectuar sus transacciones, es, entre otras cuestiones, por la seguridad que garantiza este tipo de sistemas. Esta seguridad se sustenta en algoritmos criptográficos avanzados y protocolos de consenso, que dificultan enormemente la alteración de registros o la creación de transacciones fraudulentas (Zhang y Lee, 2020, págs. 94-95).

2.7. Transnacionalidad

La tecnología *blockchain* contribuye a la eliminación de barreras geográficas, regulatorias e institucionales, lo que facilita la interacción directa entre personas y promueve la interoperabilidad entre países y sistemas (Padilla Sánchez, 2020, pág. 187).

2.8. Anonimidad

Como característica más interesante para este estudio, debe destacarse la anonimidad con la que los usuarios pueden actuar dentro de este tipo de sistemas (Huang, Zhang, Mu, Rezaeibagha y Du, 2021, pág. 25).

Precisamente, esta característica genera diversas cuestiones que van más allá de lo meramente tecnológico, abriendo un amplio debate en el ámbito jurídico acerca de la identificación de los intervinientes, la atribución de responsabilidades y la adecuación de estos sistemas a las normativas vigentes en materia de protección de datos, prevención del delito y cumplimiento legal.

En lo que respecta a las normativas sobre protección de datos, la anonimidad y desintermediación que caracteriza a los sistemas *blockchain* imposibilitan enormemente el cumplimiento de las obligaciones de protección de datos como la existencia obligatoria de los denominados responsables del tratamiento y encargados de tratamiento. Al operar sin intermediarios y bajo un modelo descentralizado y anónimo, estos sistemas desdibujan algunas figuras tradicionales previstas en los marcos regulatorios, lo que genera vacíos y desafíos que exigen nuevas soluciones jurídicas (Fink, 2019, pág. 91).

Como puede observarse, aun sin intermediarios ni autoridades, como se viene diciendo, dentro de *blockchain* no existen jerarquías, podrían establecerse estas dos figuras esenciales. Sin embargo, aun existiendo, los nodos no sabrían a quién acudir para ejercer sus derechos de acceso, rectificación, cancelación u oposición, pues, al actuar de forma anónima, se desconocen los datos de identificación de los usuarios y no se puede saber qué usuario asume el papel de responsable o encargado de tratamiento (Pardo Prado, 2022, págs. 153-160).

Por contraparte, puede pensarse que, si los usuarios actúan de forma anónima, la legislación de protección de datos no entra en juego debido a que un dato debidamente anonimizado no se encuentra sujeto a las disposiciones sobre protección de datos por no poderse atribuir a ninguna persona concreta. Sin embargo, sí quedan registrados datos de transacciones asociadas a los usuarios y, en algunas ocasiones, pueden llegarse a vincular a personas concretas, como, por ejemplo, mediante el uso de su dirección IP u otros datos adicionales.

Como ya se ha señalado, en ciertos casos puede llegarse a identificar a los usuarios mediante el uso de información adicional; sin embargo, la anonimidad con la que se actúa en *blockchain* dificulta enormemente, en la gran mayoría de supuestos, la determinación del autor real que se entromete dentro de los derechos e intereses del resto de usuarios (Gimeno Beviá, 2023, pág. 6).

2. Una función *hash* es un algoritmo que convierte datos de cualquier tamaño en una cadena única de longitud fija, lo que permite verificar su integridad al detectar cualquier modificación. *Vid*. González González, 2015, pág. 172.

Adicionalmente, el uso de la tecnología *blockchain* no se encuentra exenta de riesgos, debido a que su estructura puede utilizarse también como mecanismo para cometer delitos, incumplir obligaciones contractuales o vulnerar derechos como, por ejemplo, la propiedad. En este contexto, *blockchain* no escapa a la posibilidad de originar conflictos de naturaleza social o jurídica, tanto en el ámbito privado como en el público, derivados de su uso o de las actividades que en ella se desarrollen (Gimeno Beviá, 2023, pág. 2).

Ante esta situación, la anonimidad desempeña un papel fundamental, ya que puede favorecer la comisión de dichas actuaciones ilícitas y contrarias a los derechos e intereses de las personas, pues, si se desconoce al autor verdadero de los hechos, se dificulta enormemente la atribución de responsabilidades y la posibilidad de emprender cuantas acciones legales sean necesarias. En este sentido, surge la duda de cómo los usuarios van a ser capaces de reclamar responsabilidades ante un entorno anónimo en el que se desconocen las identidades de los usuarios y en el que no hay autoridades centrales que velen por el cumplimiento normativo y el respeto de los derechos e intereses de las personas (Calaza López *et al*., 2023, págs. 3-5).

A su vez, las transacciones en *blockchain* son transnacionales, lo que permite operar sin fronteras y puede implicar la aplicación del derecho internacional, público o privado, según la naturaleza de las partes involucradas (Ortega Giménez, 2019, pág. 60).

Actualmente, las normas que se encargan de regular los fueros de competencia en caso de conflicto entre usuarios, en los que al menos uno de ellos sea de carácter extranjero, gravitan en torno al denominado *criterio tradicional de conexión por proximidad*, cuyo eje es la localización. Es decir, dichas reglas necesitan de una identidad fehaciente y de una ubicación geográfica concreta para poder surtir efectos, lo que es prácticamente imposible cuando la celebración de los acuerdos y las transacciones se realiza en un sistema digital, descentralizado, transnacional y anónimo (Jiménez Blanco y Espinella Menéndez, 2021, pág. 28).

Igualmente, las situaciones críticas pueden surgir desde el inicio, pues Blockchain permite celebrar contratos digitales automáticos, inmutables y anónimos, válidos siempre que cumplan con consentimiento, objeto y causa (Fetsyak, 2020, págs. 208-210).

Ahora bien, verificar si el consentimiento otorgado en un *smart contract* celebrado en *blockchain* es válido o no es relativamente complicado: ¿cómo podrá verificarse que el consentimiento que aportan las partes del contrato es válido jurídicamente si se desconoce la identidad de los usuarios?

Como se puede concluir, resulta difícil observar y garantizar si el consentimiento es plenamente válido o si, por el contrario, se encuentra viciado. A modo de ejemplo, puede ser que en la relación contractual alguna de las partes sea menor de edad o, incluso, que alguna se encuentre incapacitada judicialmente para contratar, lo que se desconocerá en todo momento porque no existen identidades reales.

A su vez, en ocasiones, existen mecanismos de resolución de conflictos dentro de los sistemas *blockchain*. En este sentido, existen plataformas que ofrecen los servicios de arbitraje en línea mediante tecnología *blockchain*; sin embargo, más allá de solucionar los problemas, parecen incrementarse. Dentro de estos sistemas, los árbitros actúan de forma anónima; se desconoce si poseen conocimientos sobre la materia que se está discutiendo o si ni siquiera pueden actuar en este tipo de procesos (Yépez Idrovo, Vela Sevilla y Haro Aillón, 2020, pág. 21).

Además, ya se ha dicho que las partes son anónimas, por lo que vuelve a surgir la duda: ¿cómo podrá verificarse que el consentimiento que aportan las partes a someterse a arbitraje es válido jurídicamente si se desconoce la identidad de los usuarios? y ¿cómo puede comprobarse si el convenio arbitral se ha celebrado respetando los requisitos del debido proceso si las partes son anónimas? (Tasende, 2020, pág. 143).

Considerando estas situaciones, parece necesario un mecanismo que preserve el anonimato en *blockchain* y, al mismo tiempo, ofrezca seguridad jurídica. Por ello, se propone implementar una identidad cifrada que pueda ser legalmente descifrada en caso de controversia o riesgo.

3. Identidad cifrada en *blockchain*: equilibrio entre anonimato y responsabilidad

Según lo señalado, uno de los ejes fundamentales de la tecnología *blockchain* es la capacidad que otorga a los

usuarios para actuar dentro de un entorno anónimo, descentralizado y sin necesidad de autoridades o intermediarios (Nespral y Fernández Hergueda, 2021, pág. 23).

Ante este disruptivo diseño aparecen importantes desafíos para el ámbito jurídico, concretamente en lo referente a la imputación de responsabilidades, al acceso a mecanismos judiciales y la tutela efectiva de derechos. Aunque actualmente se recurre a mecanismos alternativos de resolución de conflictos dentro del ecosistema *blockchain*, como el arbitraje automatizado mediante contratos inteligentes, estos carecen de obligatoriedad, presentan ciertas fallas y, por supuesto, no pueden sustituir al derecho a acceder a la justicia ordinaria (Pérez Campillo, 2025, págs. 2 y 6).

3.1. Propuesta de identidad cifrada

Frente a esta situación, los sistemas *blockchain* que permiten que los usuarios puedan ser completamente anónimos deben evolucionar sin contradecir su esencia, y dotar a sus arquitecturas de soluciones que garanticen seguridad jurídica y mecanismos de verificación que permitan responsabilizar a los actores cuando sea necesario sin comprometer la descentralización ni la privacidad.

Así las cosas, como posible solución a las fallas encontradas, se sugiere la implementación de una identidad cifrada con desencriptación judicial como un modelo intermedio entre la garantía del anonimato que ofrece la *blockchain* y la posibilidad de desvirtuarlo cuando lo exijan los derechos o intereses legítimos de las personas.

Una identidad cifrada es un mecanismo que permite a los usuarios de *blockchain* mantener su anonimato funcional, al interactuar en la red sin revelar sus datos personales reales, pero de manera que exista un método seguro para identificar al titular de la identidad en casos puntuales.

La propuesta de identidad cifrada parte de una premisa clara: preservar el anonimato funcional del usuario dentro del ecosistema *blockchain* y, a su vez, permitir su identificación plena en casos excepcionales debidamente justificados por orden judicial. De este modo, se establece un modelo que persigue el equilibrio entre privacidad y responsabilidad (Pfitzmann y Köhntopp, 2001, pág. 9).

Con ello, se garantiza el anonimato, pues los usuarios no se encuentran obligados a revelar sus datos personales para observar la cadena, participar en transacciones, celebrar *smart contracts* o cualesquiera otras actuaciones que deseen efectuar y, al mismo tiempo, se respetan las exigencias de las normas que, como ya se ha visto, requieren conocer la identidad del sujeto para bien imputar responsabilidades por actos ilícitos o dañosos, o bien comprobar ciertos requisitos contractuales en aras de verificar que las relaciones mantenidas son conforme a derecho (Merchán Murillo, 2022, pág. 1388).

3.2. Beneficios jurídicos y aumento de la seguridad jurídica

Asimismo, dado que los usuarios serían anónimos en todo momento salvo cuando se extralimiten en sus actuaciones, podría reducirse la comisión de delitos como el fraude, el blanqueo de capitales, la evasión fiscal o la financiación ilegal del terrorismo; aspectos fundamentales que cuerpos legales como el Reglamento (UE) 2023/1114 del Parlamento Europeo y del Consejo, de 31 de mayo de 2023, relativo a los mercados de criptoactivos y por el que se modifican los Reglamentos (UE) n.º 1093/2010 y (UE) n.º 1095/2010 y las Directivas 2013/36/UE y (UE) 2019/1937 (MiCA) abordan con estricto celo por razón de la necesidad de proteger a los usuarios y prevenir actividades ilícitas (Martí Miravalls, 2021, pág. 475).

Además, gracias a la implementación de una identidad encriptada, se respetaría mayormente el derecho a la tutela judicial efectiva, consagrado en muchos ordenamientos constitucionales y en instrumentos internacionales, que exige que las personas puedan acceder a un recurso judicial efectivo y que sus derechos sean protegidos en el ámbito de los procedimientos legales, sin que, por ello, el anonimato de los usuarios que actúan en *blockchain* pueda interferir en la posibilidad de establecer responsabilidades en caso de disputas o delitos (Marcheco Acuña, 2020, pág. 93).

3.3. Implementación técnica de la identidad cifrada

A la hora de implementar la identidad cifrada en los entornos *blockchain,* pueden utilizarse las tecnologías ya disponibles en estos sistemas, particularmente las relacionadas con el cifrado asimétrico, los *smart contracts* y los mecanismos descentralizados de almacenamiento (Soledad Cabrera, 2019, págs. 33-36).

Antes de nada, conviene recalcar que el cifrado asimétrico es una técnica criptográfica que utiliza un par de claves: la clave pública, que sirve como identificador del usuario en el *blockchain* y puede compartirse abiertamente, y la clave privada, que permite firmar digitalmente transacciones y *smart contracts*, debiendo mantenerse en secreto.

Para generar la identidad digital cifrada, cada usuario del sistema debe crear este par de claves asimétricas. Con ello, cada usuario deberá crear una clave pública y una clave privada, siguiendo el estándar criptográfico de claves asimétricas: la clave pública servirá como identificador de la identidad del usuario en la *blockchain* y será la que se almacene y utilice para interactuar con otros usuarios o participar en la red, mientras que la clave privada deberá mantenerse en secreto, nunca se revela ni se almacena en la red y permitirá firmar digitalmente las transacciones y *smart contracts* dentro del sistema, garantizando así la seguridad y privacidad de las acciones de los usuarios dentro de la *blockchain (*González y Martínez, 2007, pág. 420).

Tal y como puede observarse, estas claves asimétricas serán la base para mantener el anonimato funcional, porque los usuarios pueden interactuar sin necesidad de revelar su identidad real, lo que garantiza la filosofía de *blockchain* de descentralización y anonimato (Valderrama Hoyos y Araque Cely, 2024, pág. 93).

Toda vez que se ha generado el bloque que contiene la identidad digital del usuario, los datos personales se cifran y se almacenan en una entidad pública o descentralizada que garantice seguridad, integridad y trazabilidad, pudiendo utilizarse como ente custodio una DAO que, mediante contratos inteligentes, gestione el acceso a los datos, preservando la automatización y reduciendo la intervención humana.

Por otro lado, podría recurrirse a una fórmula más tradicional utilizando un notariado criptográfico público o privado, que actúe como un nodo de confianza dentro de la red y pueda certificar, sin revelar su contenido, que los datos cifrados pertenecen a un usuario concreto (García-Ramos Lucero, 2023, pág. 49).

3.4. Desencriptación judicial de la identidad cifrada y posibles desafíos

A la vista de todas las cuestiones planteadas en los sistemas *blockchain* públicos y toda vez que se ha desarrollado su implementación técnica, conviene destacar que la desencriptación judicial es un procedimiento mediante el cual los datos cifrados de un usuario pueden ser revelados solo bajo orden judicial válida, para permitir identificar al titular de la clave pública en casos específicos.

Este mecanismo constituye la propuesta central de este trabajo: un modelo que permite preservar el anonimato funcional dentro de la *blockchain* y, al mismo tiempo, garantizar la responsabilidad jurídica de los usuarios cuando sea necesario. En este sentido, la propuesta se basa en un equilibrio entre privacidad, descentralización y trazabilidad legal, lo que asegura que el acceso a la identidad real del usuario se realice únicamente bajo condiciones estrictamente justificadas y controladas judicialmente (Goel, Bisht, y Chaudhary, 2023, pág. 476).

Uno de los desafíos principales que enfrenta este modelo es el acceso a la identidad cifrada en situaciones en las que se requiere imputar responsabilidad jurídica, realizar una investigación judicial u observar si los requisitos de validez contractual del *smart contract* son conformes a derecho. En este sentido, el sistema debe diseñarse de manera que la desencriptación de los datos solo sea posible mediante una orden judicial válida emitida por una autoridad judicial competente, lo que garantiza que el acceso a la información se haga de acuerdo con la ley y solo en los casos estrictamente necesarios.

En este contexto, la tutela judicial efectiva adquiere un papel central, porque la desencriptación de la identidad cifrada implica inevitablemente la afectación de derechos fundamentales como la privacidad, la protección de datos personales y, en algunos casos, la libertad individual frente al poder del Estado. Por ello, el acceso judicial a la identidad de un usuario solo debería autorizarse cuando existan indicios razonables y proporcionados de la comisión de un delito o una vulneración grave de derechos de terceros (Vidal Fernández, 2025, págs. 221 y ss.).

El juez, como garante último del equilibrio entre seguridad y libertad, debería evaluar la necesidad, idoneidad y proporcionalidad de la medida, verificando que no existan alternativas menos intrusivas. Además, la autorización debería constar en una resolución motivada, dictada conforme a los principios de legalidad y debido proceso, y ejecutarse bajo un sistema de control técnico seguro, como el modelo de firma múltiple propuesto a continuación, que asegure que la desencriptación se realiza exclusivamente

en los términos ordenados judicialmente. En este sentido, la decisión judicial se basaría en la existencia de indicios razonables que justifiquen la intervención, asegurando que la medida solo se adopte cuando haya evidencia fundada de un ilícito, un conflicto contractual o una amenaza a derechos de terceros. De este modo, se protege la privacidad y el anonimato funcional del usuario, limitando la exposición de datos únicamente a lo estrictamente necesario para cumplir con un fin legal concreto, garantizando a la vez la tutela efectiva de los derechos fundamentales involucrados, como la protección de datos, la seguridad jurídica y el acceso a la justicia (Martín Diz, 2025, pág. 57).

Además, como propuesta, el mecanismo de desencriptación debe ser implementado mediante un sistema de firma múltiple o *multisig*, que significa que la identidad cifrada no podrá ser desencriptada sin la intervención de varias partes autorizadas. En este caso, las firmas necesarias podrían incluir las de un juez, un representante del ente que custodia los datos y un auditor independiente o defensor de derechos. De este modo, se asegura que la operación sea supervisada y validada por varias entidades, evitando abusos y garantizando la legalidad del acceso (Goel, Bisht, y Chaudhary, 2023, pág. 476).

Por otra parte, debe tenerse en cuenta que el uso de contratos inteligentes automatizados en *blockchain* puede facilitar la ejecución de este proceso sin necesidad de intermediarios manuales. Al respecto, la orden judicial que activa el mecanismo de desencriptación puede ser programada como un *smart contract* que ejecute el desbloqueo de los datos cifrados bajo condiciones específicas, asegurando eficiencia, rapidez, transparencia y trazabilidad de la acción (Castellano García, 2021, pág. 10).

Toda vez que se ha propuesto la implementación de este sistema y se ha sugerido la forma en la que puede llevarse a cabo, conviene repasar de forma breve las anomalías jurídicas anteriormente expuestas y estudiar cómo este sistema puede resolverlas.

La incorporación de un sistema de identidad cifrada con desencriptación judicial no solo es compatible con los principios fundamentales de la tecnología *blockchain*, como la descentralización, la privacidad y el anonimato, sino que además permite enfrentar de manera eficaz los principales desafíos jurídicos que actualmente obstaculizan la plena integración legal de esta tecnología en los sistemas normativos tradicionales.

Uno de los principales desafíos jurídicos en *blockchain* es la dificultad para determinar quiénes son los encargados y responsables del tratamiento de los datos personales contenidos en la cadena, dado que, en un entorno descentralizado, no existen jerarquías o autoridades que puedan asumir este papel (Espuga Torné, 2021, pág. 2).

El sistema propuesto mitiga este riesgo mediante la custodia externa de los datos cifrados. En este sentido, como ya se ha comentado, la custodia puede recaer en una organización autónoma descentralizada (DAO) o en una entidad confiable de carácter más tradicional que actúe bajo criterios de notariado criptográfico, que pueden asumir el papel de responsable o encargado del tratamiento, según el caso, y garantizar así el cumplimiento de la normativa sobre protección de datos.

No debe olvidarse que el anonimato en *blockchain* puede favorecer la comisión de actividades ilícitas, como el blanqueo de capitales, la evasión fiscal, el fraude o la financiación del terrorismo; sin embargo, la fórmula de identidad cifrada parece proporcionar una solución equilibrada. Por una parte, garantiza el anonimato funcional de los sistemas *blockchain*, y, por otra, permite que, en situaciones de riesgo o delito, las autoridades puedan acceder a la identidad real del usuario mediante un proceso transparente y controlado, manteniendo la privacidad sin que esta se convierta en un obstáculo para la preservación de los derechos e intereses de los usuarios (Aránguez Sánchez, 2020, págs. 75-76).

Asimismo, las normas que conforman el ordenamiento jurídico necesitan que las personas puedan ser identificadas para poder aplicarse e imputar hipotéticas responsabilidades. En este sentido, el sistema propuesto parece permitirlo, pues, mediante una orden judicial, se podrá identificar al titular de una clave pública en la *blockchain*, desvelando su identidad real, lo que abre la puerta a iniciar acciones judiciales, y resolviendo el problema de la inimputabilidad jurídica de sujetos anónimos.

Por otro lado, se ha visto que la *blockchain* carece de fronteras y, por lo tanto, posee carácter transnacional, lo que, junto al anonimato, impide determinar la jurisdicción aplicable cuando existan en la relación elementos extranjeros. En defecto de acuerdo de sumisión a una jurisdicción determinada o juez competente, con la identidad cifrada asociada a un ente que la custodie, se crea

un vínculo jurídico trazable que facilita aplicar las normas del derecho internacional privado. En este sentido, podrá revelarse judicialmente que un sujeto está domiciliado en cierto país y, por tanto, podrá aplicarse el criterio de proximidad geográfica o de conexión significativa, tal y como exigen los principios de territorialidad y competencia en los conflictos internacionales (Calvo Caravaca yCarrascosa González, 2012, pág. 582).

A su vez, se estudió cómo los *smart contracts* se ejecutan automáticamente sin verificación de la voluntad real de las partes, lo que puede generar dudas sobre la validez del consentimiento prestado. Ahora, asociando cada clave pública a una identidad cifrada, evidentemente respaldada por datos reales, será posible verificar, en caso de controversia, si el consentimiento fue prestado por una persona jurídica o física válida y, por supuesto, bajo qué condiciones. De esta manera, el sistema permitirá revisar la formación del contrato conforme a los requisitos legales del consentimiento (capacidad, ausencia de vicios, libre voluntad), y reforzar así la seguridad jurídica de los procedimientos y el cumplimiento de las normas aplicables (Cáceres Malagón, 2024, págs. 164-166).

Además, muchos entornos *blockchain* proponen mecanismos alternativos de resolución de disputas, como, por ejemplo, arbitrajes automáticos en línea, pero sin que sea posible verificar si existe un acuerdo válido entre las partes identificadas o si los árbitros se encuentran capacitados para actuar en el proceso, lo que pone en duda su eficacia legal y el respeto de los requisitos del debido proceso. Mediante la propuesta de identidad cifrada, si una de las partes impugna el acuerdo arbitral, el juez podrá verificar, mediante desencriptación judicial, si los usuarios que suscribieron el convenio de arbitraje son plenamente capaces y si actuaron conforme al debido proceso, para garantizar la validez del pacto y, por tanto, la legitimidad del procedimiento arbitral (Gonzalo Quiroga, 2023, pág. 545).

Igualmente, debe decirse que, al igual que responde a los riesgos concretos señalados, el sistema de identidad cifrada con desencriptación judicial también parece representar una vía intermedia entre dos extremos. Por un lado, el absolutismo del anonimato y el hipercontrol estatal, porque este modelo no impone una vigilancia masiva ni vulnera el principio de privacidad que inspira la Web3, y, por otro, tampoco permite que esa privacidad se convierta en una zona de impunidad digital, porque, en su lugar, habilita un sistema de responsabilidad condicionada, controlado, con garantías procesales y trazabilidad técnica, que puede constituir una referencia normativa para futuras regulaciones internacionales sobre identidad digital (Ramos Gil de la Haza, 2022, págs. 51-52).

En aras de que este sistema funcione de manera efectiva y cumpla con sus objetivos de privacidad, trazabilidad y responsabilidad jurídica, su implementación debe estar necesariamente respaldada por una regulación específica que establezca los límites de acceso a la identidad cifrada, los procedimientos de autorización y las medidas de control técnico. Esta regulación garantizará que la desencriptación judicial solo se realice en situaciones extraordinarias, previamente justificadas por la ley, y deberá articularse bajo las normas existentes, como el Reglamento (UE) 2023/1114 (MiCA), las Directivas 2013/36/UE y 2019/1937, la normativa de protección de datos (RGPD) y los principios de tutela judicial efectiva, para asegurar la compatibilidad del sistema con el marco legal vigente.

Asimismo, hay que tener presente que la *blockchain* es transnacional, lo que permite a los usuarios transaccionar sin limitarse a un solo país o continente. Por ello, para que la desencriptación judicial de la identidad cifrada funcione de manera efectiva y segura, no basta con la regulación europea; es necesario que se creen mecanismos de homogeneidad entre legislaciones, de manera que los criterios de acceso, custodia de datos, autorización judicial y medidas de control técnico sean compatibles en distintas jurisdicciones.

De este modo, el sistema podrá operar en el ámbito global, asegurando que la responsabilidad jurídica se pueda ejercer en cualquier jurisdicción en las que surjan conflictos o delitos, sin que las diferencias entre marcos normativos comprometan la eficacia del procedimiento; cuestión que está ocurriendo actualmente debido a la ausencia de criterios uniformes dentro de este tipo de sistemas.

Conclusiones

La creciente inserción de la tecnología *blockchain* en diversos ámbitos plantea desafíos inéditos para el derecho, especialmente en la atribución de responsabilidad, la protección de derechos fundamentales y el cumplimiento efectivo de la legislación vigente.

Las distintivas características de *blockchain*, como el anonimato, el seudonimato funcional y la transnacionalidad, representan significativos retos para los ordenamientos jurídicos contemporáneos. Sin embargo, estas particularidades no deben convertirse en barreras que imposibiliten la acción del derecho, pues la privacidad que aportan las nuevas tecnologías puede y debe coexistir con la exigencia de responsabilidad jurídica.

En este contexto, el modelo de identidad cifrada con desencriptación judicial se presenta como una propuesta concreta y factible, tanto técnica como legalmente. Su implementación se basa en claves asimétricas, custodia descentralizada de datos cifrados y mecanismos de validación jurídica, como la firma múltiple o *multisig*, activables únicamente bajo una orden judicial válida. Esto permite preservar el anonimato funcional de los usuarios, y evitar la creación de bases de datos centralizadas que concentren riesgos o vulneren derechos, al mismo tiempo que habilita la identificación legal cuando sea estrictamente necesario.

Desde el punto de vista técnico, las herramientas y los actuales estándares criptográficos son capaces de soportar este modelo, y, desde el punto de vista legal, se alinea con normas como el Reglamento MiCA, el RGPD, directivas europeas de supervisión y tutela judicial efectiva y puede ser escalado mediante acuerdos de armonización transnacional, es decir, mediante convenios y tratados internacionales.

A su vez, no debe olvidarse que el anonimato es una de las características más atrayentes en el mundo *blockchain*, por lo que, en términos de aceptación por parte de los usuarios que operan en este tipo de sistemas, este modelo ofrece un valor significativo: protege el anonimato en la mayoría de las interacciones cotidianas, preserva la descentralización de la red y solo introduce intervención jurídica en casos excepcionales, lo que podría favorecer aún más la confianza y la adopción del sistema.

Además, la implementación de esta solución podría incentivar la integración institucional y empresarial de este tipo de sistemas, pues, recordemos que actualmente nos encontramos en la etapa Blockchain 3.0, en la que se pretende aplicar a diversos sectores muy regulados, como las finanzas, la salud y la contratación pública, ámbitos en los que la seguridad jurídica constituye un requisito ineludible y, aunque se pudieran usar *blockchain* privadas en estos sectores, no debe olvidarse la importancia de preservar la desintermediación que caracteriza a los sistemas públicos y que también atrae el interés de los usuarios.

Propositivamente, se sugiere que futuras regulaciones incluyan criterios claros de autorización de desencriptación, límites de acceso, supervisión de terceros independientes y mecanismos transnacionales de coordinación, para garantizar que la responsabilidad jurídica pueda aplicarse globalmente sin comprometer la privacidad de los usuarios ni la efectividad de la tecnología. Junto a ello, también sería recomendable promover estándares técnicos interoperables y auditorías externas para validar la ejecución segura de los procesos de desencriptación judicial y la trazabilidad de los datos.

En conclusión, el modelo de identidad cifrada con desencriptación judicial no solo permite integrar la esencia descentralizada y anónima de *blockchain* con la exigencia de seguridad jurídica, sino que también ofrece soluciones técnicas, legales y operativas concretas que podrían ser aceptadas por los usuarios y aportar un valor real al ecosistema. Se trata de una vía equilibrada que protege los derechos de los usuarios, facilita la atribución de responsabilidades y fortalece la confianza institucional en un entorno tecnológico disruptivo.

Referencias bibliográficas

PREUKSCHAT, A.; KUCHKOVSKY, C. (2017). *Blockchain: la revolución industrial de internet*. España: Gestión 2000.

AMMOUS, S. (2016). «Blockchain Technology: What is it Good for?». *SSRN 2832751*, págs. 1-5. DOI: http://dx.doi.org/10.2139/ssrn.2832751

ANDOLA, N.; RAGHAV; YADAV, V.; VENKATESAN, S.; VERMA, S. (2021). «Anonymity on blockchain based e-cash protocols—A survey». *Computer Science Review*, vol. 40, 100394. DOI: https://doi.org/10.1016/j.cosrev.2021.100394

ARÁNGUEZ SÁNCHEZ, C. (2020). «El bitcoin como instrumento y objeto de delitos». *Cuadernos de Política Criminal: 131, II*, págs. 75-103.

BEDECARRATZ SCHOLZ, F. (2018). «Riesgos delictivos de las monedas virtuales: Nuevos desafíos para el derecho penal». *Revista chilena de derecho y tecnología*, vol. 7 n.º 1, págs. 79-106. DOI: https://doi.org/10.5354/0719-2584.2018.48515

CÁCERES MALAGÓN, J. A. (2024). «¿Sueñan las máquinas con contratar? Un estudio sobre smart contracts y consentimiento algorítmico». *Revista de derecho Privado,* n.º 46, págs. 155-185. DOI: https://doi.org/10.18601/01234366.46.07

CALAZA LÓPEZ, S.; ANGUIANO JIMÉNEZ, J. M.; FERNANDEZ-TRESGUERRES GARCÍA, A.; FELIU REY, J.; GIMENO BEVIÁ, J.; MADRID PARRA, A.; VILALTA NICUESA, A. E. (2023, junio). «Smart Contract: ¿Contrato inteligente o programa informático? ¿Qué son —exactamente— los Smart Contracts? ¿Cuál es su naturaleza, filosofía y principios inspiradores?». *Actualidad Civil,* n.º 6, págs. 1-23. Editorial LA LEY.

CALVO CARAVACA, A. L.; CARRASCOSA GONZÁLEZ, J. (2012). *Derecho del comercio internacional*. Madrid: San Fernando de Henares: Colex.

CASTELLANO GARCÍA, A. (2021). «Conceptualización de los contratos inteligentes o autoejecutables basados en la tecnología blockchain y su encuadre en el ordenamiento jurídico español». *Revista Estudios Jurídicos. Segunda Época,* n.º 21, e6756, págs. 1-41. DOI: https://doi.org/10.17561/rej.n21.6756

DAVIDSON, S.; De FILIPPI, P.; POTTS, J. (2016). «Economics of Blockchain». *SSRN 2744751*, págs. 1-23. DOI: http://dx.doi.org/10.2139/ssrn.2744751

De FILIPPI, P.; WRIGHT, A. (2018). *Blockchain and the Law. The Rule of Code*. Cambridge: Harvard University Press. DOI: https://doi.org/10.2307/j.ctv2867sp

ESPUGA TORNÉ, G. (2021, octubre). «Compatibilidad y encaje legal de la tecnología blockchain con la normativa sobre protección de datos personales». *La Ley mercantil, ISSN-e 2341-4537,* n.º 84.

FETSYAK, I. (2020). «Contratos inteligentes: análisis jurídico desde el marco legal español». *Revista electrónica de Derecho de la Universidad de La Rioja, REDUR,* n.º 18, págs. 197-236. DOI: https://doi.org/10.18172/redur.4898

FINK, M. (2019). «Smart Contracts as a Form of Solely Automated Processing Under the GDPR». *International Data Privacy Law,* vol. 9, n.º 2, págs. 78-94. DOI: https://doi.org/10.1093/idpl/ipz004

GIMENO BEVIÁ, J. (2023). «La resolución de los conflictos «en blockchain» o cuando el código es la leyel difícil reto desde la justicia penal». *La Ley. Mediación y arbitraje,* n.º 16, págs. 1-8.

GOEL, A.; BISHT, V.; CHAUDHARY, S. (2023). «Multisignature Crypto Wallet Paper». *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, págs. 476-479. Coimbatore, India: IEEE. DOI: https://doi.org/10.1109/ICCES57224.2023.10192591

GONZÁLEZ, S.; MARTÍNEZ, C. (2007). «Las matemáticas de la seguridad». *Arbor Ciencia Pensamiento y Cultura*, vol. 183, n.º 735, págs. 419-425. DOI: https://doi.org/10.3989/arbor.2007.i725.114

GONZALO QUIROGA, M. (2023). «La inteligencia artificial en el arbitraje internacional 2.0. Oportunidades y desafíos en un futuro que ya es presente». *CUADERNOS DE DERECHO TRANSNACIONAL*, vol. 15, n.º 2, págs. 516-550. DOI: https://doi.org/10.20318/cdt.2023.8067

HOFMANN, F.; WURSTER, S.; RON, E.; BÖHMECKE-SCHWAFERT, M. (2017). «The immutability concept of blockchains and benefits of early standardization». *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K). IEEE.*, págs. 1-8. DOI: https://doi.org/10.23919/ITU-WT.2017.8247004

HUANG, K.; ZHANG, X.; MU, Y.; REZAEIBAGHA, F.; DU, X. (2021). «Scalable and redactable blockchain with update and anonymity». *Information Sciences*, vol. 546, págs. 25-41. DOI: https://doi.org/10.1016/j.ins.2020.07.016

IBÁÑEZ JIMÉNEZ, J. W. (2018). *Derecho de Blockchain*. Navarra: Aranzadi. DOI: https://doi.org/10.2307/j.ctv346qc0

JIMÉNEZ BLANCO, P.; Espinella Menéndez, Á. (2021). *Nuevos escenarios del derecho internacional privado de la contratación*. Asturias: Tirant lo Blanch.

MARCHECO ACUÑA, B. (2020). «La dimensión constitucional y convencional del derecho a la tutela judicial efectiva (no penal) desde la perspectiva jurisprudencial europea y americana». *Estudios constitucionales: Revista del Centro de Estudios Constitucionales*, vol. 18, n.º 1, págs. 91-142. DOI: https://doi.org/10.4067/S0718-52002020000100091

MARTÍ MIRAVALLS, J. (2021). «La propuesta de reglamento del parlamento europeo y del consejo relativo a los mercados de criptoactivos: la propuesta mica». *Revista de Derecho del Sistema Financiero: mercados, operadores y contratos*, n.º 1, págs. 473-480.

MARTÍN DIZ, F. (2025). «Derechos y garantías procesales penales fundamentales: una lectura en clave tecnológica». *Ius et Scientia*, vol. 10, n.º 1, págs. 52-81. DOI: https://doi.org/10.12795/IESTSCIENTIA.2024.i01.03

MARTÍNEZ BOADA, J. (2025, marzo). «Transformación digital del transporte marítimo: Blockchain para la ventanilla única europea». *Cuadernos de Derecho Transnacional*, vol. 17, n.º 1, págs. 1234-1244. DOI: https://doi.org/10.20318/cdt.2025.9365

MARTÍNEZ BOADA, J.; REJAS MUSLERA, R. J. (2024). «Protección jurídica de Blockchain: Un análisis desde su funcionalidad y naturaleza jurídica según el ordenamiento jurídico español». *Revista Chilena de Derecho y Tecnología*, vol. 13, págs. 1-20. DOI: https://doi.org/10.5354/0719-2584.2024.73869

MARTÍNEZ BOADA, J.; SANTAMARÍA RAMOS, F. J. (2024). «Blockchain: la nueva era de la identificación digital en internet». *Teoría & Derecho. Revista De Pensamiento jurídico*, n.º 37, págs. 258-283. DOI: https://doi.org/10.36151/TD.2024.114

MERCHÁN MURILLO, A. (2022). «La identidad digital en la contratación electrónica: una mirada desde el derecho internacional privado». *Actualidad jurídica iberoamericana*, n.º 16, págs. 1386-1411.

NESPRAL, D.; FERNÁNDEZ HERGUEDA, R. (2021). *Blockchain: El modelo descentralizado hacia la economía digital*. Bogotá: Ra-ma (España) - Ediciones de la U (Colombia).

ORTEGA GIMÉNEZ, A. (2019). *Smart Contracta y Derecho Internacional Privado*. Pamplona: Aranzadi.

PADILLA SÁNCHEZ, J. A. (2020). «Blockchain y contratos inteligentes: aproximación a sus problemáticas y retos jurídicos». *Revista de Derecho Privado,* n.º 39, págs. 175-201. DOI: https://doi.org/10.18601/01234366.n39.08

PARDO PRADO, S. (2022). «Las repercusiones de Blockchain en los derechos de los consumidores». *Hacia una tutela efectiva de consumidores y usuarios,* cap. 7, págs.153-160. Tirant lo Blanch Online.

PÉREZ CAMPILLO, L. (2025). «Implementación de blockchain en el sistema judicial público y en los ADR». *IDP. Revista d›Internet, Dret i Política,* n.º 42, págs. 1-12. DOI: https://doi.org/10.7238/idp.v0i42.429135

PFITZMANN, A.; KÖHNTOPP, M. (2001, septiembre). «Cómo alcanzar un equilibrio entre la prevención del ciberdelito y la privacidad». *Vlex,* n.º 57, págs. 9-18.

PINTO ARBOLEDA, R. A.; FAJARDO BRAVO, N. J.; ORTEGA MÈNDE, J. X.; ZAMBRANO TOAPANTA, A. Y.; ZAMBRANO RECALDE, P. E. (2025). «Análisis del uso de software contable y tecnologías como blockchain». *Sinergia Académica,* vol. 8, especial 2, págs. 499-513. DOI: https://doi.org/10.51736/sa505

POLO ROCA, A. (2021). «Datos, datos, datos: el dato personal, el dato no personal, el dato personal compuesto, la anonimización, la pertenencia del dato y otras cuestiones sobre datos». *Estudios de Deusto: revista de Derecho Público,* vol. 69, n.º 1, págs. 165-194. DOI: https://doi.org/10.18543/ed-69(1)-2021pp211-240

RAMOS GIL de la HAZA, A. (2022). «La web3: una aproximación jurídica». *Revista Jurídica Pérez-Llorca,* vol. 8, n.º 24, págs. 36-59.

RAYENIZADEH, M.; RAFSANJANI, M. (2025). «Chapter 1 - Introduction to blockchain technology». *Digital Twin and Blockchain for Sensor Networks in Smart Cities*, págs. 3-16. DOI: https://doi.org/10.1016/B978-0-443-30076-9.00002-9

RUEDA CASTAÑEDA, J. E.; GALLEGO GÓMEZ, N.; ESTANLING CÁRDENAS, E.; TELLO, J. S.; GARCÍA PINEDA, V. (2024). «Identificación de variables relacionadas a la seguridad informática a partir de tendencias investigativas de la tecnología Blockchain». *Revista Politécnica,* vol. 20, n.º 40, págs. 9-29. DOI: https://doi.org/10.33571/rpolitec.v20n40a1

SARMAH , S. S. (2018). «Understanding blockchain technology». *Computer Science and Engineering,* vol. 8, n.º 2, págs. 23-29.

SOLEDAD CABRERA, C. (2019). «Aproximación a los conceptos de blockchaing, smart contracts y su relación con la función notarial». *Revista De Derecho Notarial Y Registral. Universidad Blas Pascal,* n.º 6, págs. 29-40.

SUN YIN, H.; LANGENHELDT, K.; HARLEV, M.; MUKKAMALA, R.; VATRAPU, R. (2019). «Regulating Cryptocurrencies: A Supervised Machine Learning Approach to De-Anonymizing the Bitcoin Blockchain». *Journal of Management Information Systems,* vol. 36, n.º 1, págs. 37-73. DOI: https://doi.org/10.1080/07421222.2018.1550550

TASENDE, I. (2020). «Blockchain y arbitraje: un nuevo enfoque en la resolución de disputas. Especial énfasis en smartcontracts y criptodivisas». *Revista de Derecho (Universidad Católica Dámaso A. Larrañaga, Facultad de Derecho),* n.º 22, págs. 138-159. DOI: https://doi.org/10.22235/rd22.2127

TORRES CAZORLA, M. I. (2019). «Cuestiones jurídicas Emergentes: Un análisis a Vista De pájaro». *Estudios De Deusto,* vol. 67, n.º 2, págs. 87-102.DOI: https://doi.org/10.18543/ed-67(2)-2019pp87-102

TOURIÑO PENA, A.; VILLASANTE, C.; ARNAIZ, J.; CAMARASA, P.; DÍEZ, J.; GALÁN, J.; TÉLLEZ, H. (2022). *Blockchain y Smart Contracts.* Madrid: Francis Lefbvre.

VALDERRAMA HOYOS, M.; ARAQUE CELY, J. A. (2024). «Aplicación de blockchain en diferentes sectores: revisión literaria». *Revista Ingeniería, Matemáticas y Ciencias de la Información,* vol. 11, n.º 21, págs. 81-98. DOI: https://doi.org/10.21017/rimci.1024

VIDAL FERNÁNDEZ, B. (2025). «Independencia judicial y proceso penal europeo. El derecho a un juez independiente y su incidencia en el espacio de libertad, seguridad y justicia». *Revista de Estudios Europeos,* n.º 85, págs. 221-252. DOI: https://doi.org/10.24197/ree.85.2025.221-252

XU, M.; CHEN, X.; KOU, G. (2019). «A systematic review of blockchain». *Financial Innovation,* vol. 5, n.º 1 , págs. 1-14. DOI: https://doi.org/10.1186/s40854-019-0147-z

YAROSHENKO, O.; PUNTUS, D.; CHANYSHEVA, H.; MOSKALENKO, O.; SLIUSAR, A. (2025). «Integration of blockchain technologies into the social security system: transparency and efficiency». *Revista de derecho de la seguridad social. Laborum,* n.º 42, p. 243-257.

YÉPEZ IDROVO, M. V.; VELA SEVILLA, M. P.; HARO AILLÓN, B. A. (2020, septiembre). «Smart contracts y el arbitraje: hacia un modelo de justicia deslocalizado». *USFQ Law Review,* vol. 7, n.º 1, págs. 1-28. DOI: https://doi.org/10.18272/ulr.v7i1.1698

ZHANG, R.; XUE, R.; LIU, L. (2019). «Security and privacy on blockchain». *ACM Computing Surveys (CSUR),* vol. 52, n.º 3, págs. 1-34. DOI: https://doi.org/10.1145/3316481

ZHANG, S.; LEE, J.-H. (2020). «Analysis of the main consensus protocols of blockchain». *ICT Express,* vol. 6, n.º 2, págs. 93-97. DOI: https://doi.org/10.1016/j.icte.2019.08.001

ZĪLE, K.; STRAZDIŅA, R. (2018). «Blockchain use cases and their feasibility». *Applied Computer Systems,* vol. 23, n.º 1, págs. 12-20. DOI: https://doi.org/10.2478/acss-2018-0002

Cita recomendada

MARTÍNEZ BOADA, Javier (2026). «Identidad cifrada con desencriptación judicial: una solución jurídica para la responsabilidad en entornos *blockchain*». *IDP. Revista de Internet, Derecho y Política*, núm. 44. UOC [Fecha de consulta: dd/mm/aa]. DOI: http://dx.doi.org/10.7238/idp.v0i44.9800435

Sobre el autor

Javier Martínez Boada
Universidad Camilo José Cela (Madrid)
javier.martinez6@ucjc.edu
ORCID: https://orcid.org/0009-0008-5482-4757

Graduado en Derecho por la Universidad Camilo José Cela (2019), máster de Acceso a la Profesión de Abogado por la Universidad Camilo José Cela (2021), abogado colegiado en el ICAM (2021), experto en Derecho y *Compliance* de las TIC's por la Universidad Camilo José Cela (2021), doctor en Derecho por la Universidad Camilo José Cela (2025).