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

IDP Número 31 (Octubre, 2020)

Revista de los Estudios de Derecho y Ciencia Política de la UOC

Universitat Oberta de Catalunya

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

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

www.uoc.edu/idp

IDP Número 31 (Octubre, 2020)

ARTÍCULOS

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

www.uoc.edu/idp

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

www.uoc.edu/idp

ARTÍCULO

Las soluciones europeas a la desinformación y su riesgo de impacto en los derechos fundamentales

Raquel Seijas
Universidad de Málaga

Fecha de presentación: junio de 2019
Fecha de aceptación: noviembre de 2019
Fecha de publicación: abril de 2020

Resumen

En una investigación anterior planteaba algunos de los nuevos retos a los que se enfrentaba la Unión Europea (UE) en la elaboración de políticas de comunicación debido a la expansión de desinformación. La UE, alarmada por la difusión masiva de noticias falsas durante las elecciones presidenciales de 2016 en Estados Unidos, o sobre el Brexit en el Reino Unido, comenzó a trabajar para detener este fenómeno en Europa. El primer paso fue reconocer la magnitud del problema, para poder afrontarlo: al respecto, el Parlamento Europeo adoptó en junio de 2017 una resolución en la que instó a la Comisión Europea a analizar el marco jurídico existente en la lucha contra la desinformación, valorándose incluso la posibilidad de intervenir a nivel legislativo a fin de detener este fenómeno. Luchar contra la desinformación es una carrera de fondo que difícilmente va a la velocidad de los avances tecnológicos y de consumo de noticias, pero es fundamental mantener la legalidad en las acciones para frenarla porque pueden convertirse en justificación para limitar la libertad de expresión o la privacidad, poniendo en peligro derechos humanos fundamentales.

Palabras clave

desinformación, noticias falsas, UE, libertad de expresión, derechos fundamentales

European solutions to disinformation and how they may impact on fundamental rights

Abstract

In previous research, I outlined some of the new challenges that the European Union was facing in producing communication policies due to the increase in disinformation. The EU, alarmed by the mass dissemination of fake news during the presidential elections of 2016 in the USA or around Brexit in the UK, began work on stopping this phenomenon in Europe. The first step was to recognise the magnitude of the problem, and in order to face it, in June 2017 the European Parliament adopted a Resolution in which it urges the European Commission to analyse the legal framework existing in the fight against disinformation, and also the possibility of intervening at a legislative level in order to check this phenomenon was assessed. Fighting against disinformation is a longdistance race in which it is hard to keep up to the speed of technological advances and the consumption of news, but it is fundamental to maintain legality in actions in order to put a brake on this disinformation as these actions can become a justification for limiting freedom of expression or privacy, putting fundamental human rights at risk.

Keywords

disinformation, fake news, EU, freedom of expression, fundamental rights

1. Introducción

Hace tiempo que existen evidencias sobre la repercusión de la desinformación en la ciudadanía (Allcott y Gentzkow, 2017; Watanabe, 2018). La desinformación es un fenómeno con origen y solución multifactorial que ha crecido, entre otras razones, debido a la transformación de contenidos informativos forzados por los gustos de los usuarios y por la presión de ser viralizados siguiendo exigencias de rapidez y generación de tráfico. La captación de los usuarios a través de tretas publicitarias como el *clickbaiting*[1] es responsable de lanzar contenidos no acordes a las funciones sociales del periodismo ni con la visión de este como servicio público (Loreto-Echeverri, Romero-Rodríguez y Pérez Rodríguez, 2018). La expansión de la desinformación es difícil de controlar porque pueden generarla tanto usuarios de redes sociales como regímenes políticos (López y Cabrera, 2015).

Tras el impacto que la desinformación tuvo en las elecciones presidenciales de Estados Unidos en 2016 y en las del Brexit del Reino Unido, la UE, consciente de que no se trata de un fenómeno aislado, comprueba su importancia en Europa mediante una consulta pública relativa a noticias falsas, un Eurobarómetro[2] para analizar las percepciones de la ciudadanía en torno a la desinformación y un grupo de expertos de alto nivel para investigar y asesorar sobre

1. El *clickbait* (ciberanzuelo) es contenido en línea cuyo objetivo responde a criterios publicitarios y no informativos, pues intenta atraer la atención de las personas para que hagan clic en enlaces que dirigen a sitios web concretos. El fin no es informar sino mantener al receptor en la página durante el mayor tiempo posible (García Orosa, Gallur Santorun y López García, 2017).
2. Eurobarómetro sobre Fake News y Desinformación en línea 2018. https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/flash/surveyky/2183

iniciativas políticas. La desinformación es, según el Eurobarómetro de 2018, una fuente de preocupación en Europa: un 85% de la ciudadanía europea cree que las noticias falsas son un problema en su país y en general para la democracia.

La importancia de este estudio radica en que proporciona una doble panorámica muy reciente. Tanto de las acciones y medidas impulsadas por la UE respecto a la desinformación como de los cambios regulatorios, examinando de qué manera pueden afectar a los derechos fundamentales. Ambas perspectivas ofrecen respuestas al objetivo de este análisis sobre si las medidas y acciones contra la desinformación que se están llevando a cabo pueden estar implementándose –de manera consciente o no– a expensas de derechos fundamentales.

2. Metodología

Nuestra investigación efectúa, por un lado, una aproximación descriptiva al problema de la desinformación examinando las acciones y medidas políticas emprendidas por la UE respecto a la desinformación. Y por otro, analiza las posibles implicaciones de las decisiones europeas adoptadas para limitar la expansión de desinformación en el ámbito de los derechos fundamentales.

El trabajo se sustenta en la revisión documental de investigaciones científicas, normativas, informes, recomendaciones, comunicaciones, directivas europeas o publicaciones en diarios de prestigio. La investigación documental es una base metodológica apropiada para este estudio puesto que los datos recopilados tras la revisión de documentos proporcionan una perspectiva analítica y reflexiva que completa el análisis crítico. He realizado un análisis general de bibliografía referente a la reciente difusión de desinformación en Europa con el objetivo de determinar el problema. El siguiente paso ha consistido en revisar las acciones contra la desinformación desde la UE, considerando la normativa común europea; y por último he analizado las posibles implicaciones jurídicas de las acciones, medidas y normativa comunitaria a partir de estudios e investigaciones jurídicas.

3. La desinformación en Europa: acciones y medidas contra la desinformación en la UE

La UE ha estructurado un plan con el objetivo de evitar la desinformación y su impacto sobre los procesos democráticos y los debates sociales[3]. La Comisión Europea, reconociendo la importancia de este fenómeno, ha tomado iniciativas en diferentes direcciones: a través de un grupo de expertos, de un foro sobre la desinformación, de estudios para examinar la aplicabilidad de las reglas de la UE, de la identificación de contenidos, de la creación de *fact checkers* europeos independientes, del uso de inteligencia artificial y *blockchain*, etc. Son medidas necesarias, pero, tal y como expresa el informe del Center For European Policy Studies (CEPS)[4], deben ser monitorizadas de manera que se puedan estudiar alternativas que eviten soluciones que afecten a la libertad de expresión, incurriendo en censura. Antes de las iniciativas impulsadas por la UE contra la desinformación, existían directivas y reglamentos que constituyen las bases de un marco regulatorio ampliado con nuevas propuestas en la lucha contra la desinformación. Estas son algunas de las más importantes por el contenido que regulan: en 2013 la Directiva 2010/13/UE establece requisitos sobre el reconocimiento de comunicaciones comerciales audiovisuales y prohíbe las comunicaciones encubiertas, mientras que la Directiva 2005/29/CE veda la publicidad de pago no declarada para promover bienes y servicios en el contenido editorial. Asimismo, la UE dispone de un entorno regulador que permite interacciones electrónicas seguras y para ello se desarrollan el Reglamento n.º 910/2014 y la Directiva 2002/58/CE, que regula las comunicaciones no solicitadas, garantiza la confidencialidad y protege la información almacenada en el equipo de un usuario. En la Directiva 2013/40/UE se armonizan las definiciones de los delitos contra los sistemas de información planteando la posibilidad de llevar a cabo sanciones penales si los ataques son contra procesos electorales. El Reglamento 2016/679 establece el nombramiento de autoridades independientes de supervisión de protección de datos que hacen cumplir las disposiciones del reglamento para evitar ser objeto de decisiones basadas en

3. Plan de Acción contra la desinformación. https://eeas.europa.eu/sites/eeas/files/disinformation_factsheet_es.pdf
4. The legal Framework to address «fake news»; possible policy actions at the EU level. http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/619013/IPOL_IDA(2018)619013_EN.pdf

tratamientos automatizados y elaboración de perfiles. La Directiva UE 2016/1148 surge para lograr seguridad en las redes y sistemas de información: cada Estado debe crear su propia red nacional en materia de elecciones en donde se apliquen normas para actividades en línea que pueden incidir en el contexto electoral. Existen en la UE autoridades de control (artículo 51 del Reglamento 2016/679) cuya función es informar a partidos y fundaciones políticas del coste de la vulneración de las normas en materia de datos personales. Al respecto, el CEPS (Centro Europeo de Estudios Sociales y Políticos) realiza una evaluación de las iniciativas adoptadas por la Comisión calificándolas como propuestas significativas pero incompletas. Las políticas emprendidas como respuesta a la desinformación deben pasar por una alfabetización mediática, por el empoderamiento y comportamiento responsable de los usuarios y por medidas de carácter político que promuevan el pluralismo. El problema es que actualmente existe un medio muy rico en informaciones con múltiples efectos adversos materializados en burbujas de contenido, noticias falsas no intencionadas y noticias falsas o desinformación con intención de manipular a la opinión pública. En marzo de 2018 la UE presentó el informe del grupo de expertos sobre desinformació[5], que recomienda: transparencia de noticias online, promover medios confiables, desarrollar herramientas para empoderar a usuarios y periodistas, salvaguardar la diversidad y sostenibilidad del ecosistema mediático europeo e impulsar investigaciones sobre el impacto de la desinformación en Europa a fin de evaluar las medidas que han tomado los diversos actores. En este mismo informe los expertos afirman que las plataformas en línea están realizando esfuerzos para implementar respuestas a la distribución de desinformación, dando los primeros pasos para identificar y eliminar cuentas; también están integrando señales para la credibilidad y confianza incluyendo recomendaciones de contenido alternativo, y finalmente intentan desmonetizar la fabricación de información falsa colaborando con fuentes independientes y organizaciones del *fact checking*.

3.1 Acciones políticas de la UE durante 2017-2018

Una vez reconocido el problema –y en paralelo al grupo de expertos– comienzan a establecerse recomendaciones, comunicaciones y directivas que conforman un marco general en la lucha contra la desinformación durante estos últimos años. Existe una regulación sobre contenidos ilícitos en línea, la Recomendación (UE) 2018/334 de la Comisión, de 1 de marzo de 2018, que intenta orientar a los Estados miembros acerca de cómo frenar los abusos en la difusión de información por parte de terceros. Los prestadores de servicios en línea deberían asumir más responsabilidad social en cuanto a estos contenidos: al respecto, la retirada o bloqueo de los contenidos ilícitos es esencial, pero hay que tomar medidas y decisiones rápidas para impedirlos. Los contenidos ilícitos en línea siguen siendo un problema y, para intentar evitarlos, en la Resolución del 15 de junio de 2017 se realizó un llamamiento para que las empresas adoptaran una mayor proactividad en la defensa de los usuarios. La Comunicación del 28 de septiembre de 2017 orienta sobre la responsabilidad de los prestadores de servicios en línea en relación con los contenidos ilícitos. Hay actos de Derecho de la UE con el objetivo de establecer un marco jurídico relativo a los contenidos ilícitos en línea: en la Recomendación 2018/334 se orienta acerca de cómo manejar, denunciar y retirar contenidos ilícitos, pero es la Directiva (UE) 2017/541 la que contiene disposiciones respecto a contenidos en línea que constituyan delito de terrorismo. Esta directiva aborda el tema de la difusión de contenido ilícito, pero no es marco competente para aplicar de manera general a la desinformación porque esta no comporta necesariamente contenidos ilícitos, de modo que la Directiva 2011/93/UE y la Directiva 2017/541 no son suficientes para frenar la desinformación. La Comunicación 236 de abril de 2018 deja claro que la difusión de desinformación se debe al modo de consumir noticias en la UE, siendo las redes sociales y los motores de búsqueda los principales lugares a los que acude la ciudadanía europea para informarse. Para contrarrestar la desinformación es fundamental el compromiso de los agentes estatales con la libertad de expresión y la libertad de medios de comuni-

5. Informe del grupo de expertos sobre desinformación: Final report of the High Level Expert Group on Fake News and Online Disinformation (12 de marzo de 2018).
A multidimensional approach to disinformation Report of the independent High level Group on fake news and online disinformation.
https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation

cación. Esta comunicación pone énfasis en la cooperación entre la sociedad civil y el sector privado, entendimiento que se manifiesta con la aparición del Código de buenas prácticas. En la Recomendación 5949 del 12 de septiembre de 2018, se reclama un mayor rendimiento de cuentas por parte del ecosistema en línea y más transparencia en el origen de los mensajes. Para completar este marco jurídico, desde la UE se unifican esfuerzos estableciendo un Plan de Acción el 5 de diciembre de 2018 con el objetivo de tomar medidas para proteger a los sistemas democráticos desde una perspectiva europea.

3.2 Medidas de la UE: Plan de Acción, Código de buenas prácticas, RGPD y Directiva (UE) 2019/790

3.2.1. El Plan de Acción

El Plan de Acción[6] supone una respuesta coordinada a la desinformación sustentada en cuatro pilares básicos: 1) aumento de recursos para frenar la desinformación y mejorar las capacidades de la UE para detectarla, analizarla y desenmascararla; 2) respuestas coordinadas a través de infraestructuras tecnológicas, estableciendo el Rapid Alert System (RAS) entre instituciones de la UE y Estados miembros para facilitar el intercambio de información; 3) cumplimiento del Código de buenas prácticas por parte de las plataformas en línea, movilizar al sector privado en su implicación en la lucha contra la desinformación y cooperar con las regulaciones audiovisuales nacionales y los fact-check independientes. Estos últimos son clave en la comprensión de las estructuras que sostienen la desinformación y los mecanismos que posibilitan su diseminación en línea; y 4) crear grupos para verificar y contrastar datos, concienciar y mejorar la resiliencia social.

3.2.2. El Código de buenas prácticas

El Código de buenas prácticas es una de las medidas más importantes de la UE. Los firmantes de este código se comprometen, entre otras cosas, a limitar los ingresos publicitarios de cuentas y sitios web que tergiversen información, a proporcionar herramientas para reducir la desinformación, a disponer de una política clara y accesible sobre bots, a cerrar cuentas falsas o a ofrecer información y herramientas para ayudar a la ciudadanía a tomar decisiones, facilitando el acceso a diversos puntos de vista. Firmado en octubre de 2018, el código tuvo una primera evaluación el 29 de enero de 2019 gracias a los informes emitidos por los firmantes[7] (Google, Twitter, Facebook, Mozilla y otras asociaciones empresariales de la información), que recogen las medidas tomadas por estos para cumplir con el código. En general, hay avances en la eliminación de cuentas falsas y en la visibilidad de sitios que difunden desinformación, pero no existe una excesiva transparencia en cuanto a la propaganda política en línea. Al respecto, sería necesario establecer disposiciones que garantizaran más transparencia, el acceso a datos con fines de investigación y una mayor cooperación. De todas las medidas adoptadas hasta diciembre de 2018 hay que destacar la retirada de cuentas falsas por parte de las empresas, sobre todo Facebook, si bien estas se quedan atrás en detallar herramientas para verificar datos o empoderar a los consumidores. Al respecto, Google ha dispuesto instrumentos para controlar la propaganda política, estos no están presentes en todos los países; Twitter prioriza el cierre de cuentas falsas y la lucha contra los *bots*, y Mozilla lanza una versión de su navegador que bloquea por defecto el *cross-site tracking*, aunque se desconoce de qué forma limita la información de las actividades de los usuarios que pueden utilizarse para campañas de desinformación[8]. Con todo, a pesar de que desde la UE se han hecho muchos esfuerzos para difundir el Código de buenas prácticas, aún hay pocas empresas entre los firmantes.

3.2.3. El Reglamento General de Protección de Datos (RGPD)

El RGPD creó falsas expectativas en cuanto a su potencial para impedir la desinformación y la libre disposición de datos. Se esperaba más control sobre las compañías de redes sociales y su comercio de datos, pero la entrada en

6. Action Plan against Disinformation (5 de diciembre de 2018). https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf
7. Declaración de la Comisión europea: Código de buenas prácticas contra la desinformación: la Comisión reconoce los esfuerzos de las plataformas de cara a las elecciones europeas (Bruselas, 17 de mayo 2019).
8. Fourth intermediate results of the EU Code of Practice against disinformation. https://ec.europa.eu/digital-single-market/en/news/fourth-intermediate-results-eu-code-practice-against-disinformation

vigor del reglamento en mayo de 2018 solo provocó que empresas como Facebook trasladaran su domicilio social de Irlanda a Estados Unidos y, en consecuencia, no tener que modificar en profundidad ninguno de sus términos de uso. El intento de la UE para controlar a las grandes empresas que incumplan el RGDP falla. Según el periodista Adrian Chen, al dueño de Facebook se le demanda más transparencia y responsabilidad en lo referente al uso de datos personales, porque estos son la llave de la persuasión política, pero Facebook tiene escasa habilidad, pocas ganas o es incapaz de controlar su propia plataforma[9]. Facebook, al igual que otras empresas, ha intentado delimitar la difusión de la desinformación verificando la identidad que hay detrás de los anuncios políticos, gestionando grandes páginas, disponiendo de un archivo público de todos los anuncios políticos para que la gente pueda ver a quién iban dirigidos y cuánto pagaron por ello, pero sin garantías de que agencias como Cambridge Analytica puedan utilizar perfiles ideológicos, pues no existe ningún cambio que lo impida[10]. En definitiva, las herramientas empleadas para aumentar la transparencia de las actividades políticas en la red son básicamente una defensa, no la solución del problema.

3.2.4 Los derechos de autor digital: Directiva (UE) 2019/790

Esta directiva no se ha planteado como una respuesta a la desinformación, pero puede contribuir a disminuir la difusión de noticias falsas gracias al con-trol sobre la autoría y la exigencia de filtros. La directiva sobre derechos de autor digital se aprobó este año no exenta de polémica debido a las posibles implicaciones e impacto que puede tener con respecto a algunos derechos fundamentales. Con la Directiva (UE) 2019/790[11] sobre derechos de autor y derechos afines en el mercado único digital, que modifica las Directivas 96/9/CE y 2001/29/CE, la UE pretende unificar normativa, adaptando los derechos de propiedad intelectual al nuevo modo de acceder a los contenidos y a las nuevas formas de creación, producción y distribución, que han variado notablemente con los avances tecnológicos.

Las plataformas en línea tendrán responsabilidad en el contenido por derechos de propiedad intelectual que suben los usuarios, de modo que no pueden difundir o disponer de obras o creaciones protegidas por derechos de autor sin autorización. En el caso de los agregadores de noticias, la reproducción de los fragmentos de estas deberá ser autorizada por el titular de derechos. Los editores de prensa podrán negociar en nombre de los periodistas con los agregadores de noticias para autorizar o no la difusión de contenidos garantizando la retribución de los autores. Por su parte, las empresas de intercambio de contenido se responsabilizarán de lo publicado incluyendo filtros u otros criterios para limitar los contenidos que distribuyen los usuarios. La directiva ha sido muy controvertida si se pretende que internet siga siendo una red abierta: los artículos más espinosos han sido el 11 (15 en la redacción final) y el 13. En el artículo 15 se demandan impuestos a redes sociales y agregadores a pagar por fragmentos de publicaciones, mientras que en el artículo 13 se obliga a empresas de internet más grandes con usuarios que cargan contenido a trabajar con los editores por si la información que aportan infringe sus derechos de autor, de modo que se detecte antes de su publicación. Puede apreciarse que de implementarse estos mecanismos de filtro de contenidos hay altas posibilidades de que afecten a derechos fundamentales como la libertad de empresa o de información, la privacidad o el manejo correcto de datos personales con el pretexto de que se protege a los autores (Acosta-González, 2019).

4. Implicaciones jurídicas

Las TIC impactan en el Derecho en diversas facetas. Las implicaciones jurídicas surgidas del manejo individual de las redes sociales y sus regulaciones son importantes, pues la seguridad digital es central en este momento en el que las noticias falsas afectan a los usuarios de internet, al manejo de su privacidad y a su regulación jurídica. Aparecen nuevas situaciones con múltiples aspectos a abordar desde el punto de vista del Derecho que van desde la violación de reglas de privacidad debido al incumplimiento de los acuerdos de consentimiento sobre la privacidad de

9. https://www.newyorker.com/tech/annals-of-technology/what-was-missing-from-mark-zuckerbergs-first-day-of-congressional-testimony
10. https://www.eldiario.es/tecnologia/Zuckerberg-garantizar-integridad-elecciones-herramientas_0_885061993.html
11. https://www.boe.es/doue/2019/130/L00092-00125.pdf

los usuarios, a la contratación de firmas forenses digitales para determinar si los datos recopilados de las personas utilizados sin su consentimiento son borrados o no (Ruelas, 2019). Es posible que la implementación de medidas contra la desinformación suponga una amenaza a la libertad de expresión, la seguridad digital, el manejo de la privacidad o la libertad del público para estar claramente informado, pero de ninguna manera deben afectar a derechos primordiales tal y como se consigna en la Carta de Derechos Fundamentales de la UE (2000/C 364/01, artículo 11.1). Es bastante complejo definir una normativa común contra la desinformación sin situarse en la frontera de la vulneración de la libertad de expresión o la intromisión en las políticas de cualquier Estado. Aunque existe una guerra de la información y operaciones psicológicas cuyo objetivo es imponer puntos de vista específicos, la dificultad de atribuir una autoría a las informaciones que recibimos conduce a una cierta impunidad que requiere una revisión de la Directiva de Medios Audiovisuales del 2010 y del Convenio de 1989 sobre televisión transfronteriza (Galán, 2018). Lejos de ser resueltas, existen dificultades para proteger los derechos de los usuarios, la dignidad humana y los derechos personales, hoy en día amenazados por los ataques a los ordenadores privados, correos electrónicos o bases de datos. La vigilancia individual por parte de las autoridades policiales y la vigilancia masiva que llevan a cabo las agencias de inteligencia, así como el espionaje entre Estados y Gobiernos, pueden afectar el ejercicio de derechos y libertades fundamentales y dañar nuestras democracias. Por otro lado, hay procesos democráticos y elecciones amenazados por ciberataques y desinformación masiva a través de los *social media,* que manipulan a las masas de manera sistemática usando datos de sus perfiles individuales (Pernice, 2017). Para González de la Garza (2018), los riesgos acaban de empezar, afectando sobre todo a la libertad de expresión mediante la autocensura. En el ejercicio de la «libertad de expresión vigilada» existe un debilitamiento de la privacidad en las redes; los datos son de acceso fácil a empresas y Estados, y la «información clasificada» de la sociedad conlleva su posible manipulación por los poderes económicos, empresas privadas y políticos: el hombre se transforma de sujeto en objeto de derechos, alterando su dignidad como persona.

4.1. Vulneración de derechos fundamentales

Existe un marco jurídico en la UE que intenta evitar la vulneración del derecho a la privacidad y protección de datos. Esta cobertura legal facilita y protege el manejo de nuestros datos personales y la accesibilidad a una información veraz, abogando por la transparencia de las empresas de comunicación o que ofrecen noticias. Pero no todo es tan sencillo; continuamente aparecen situaciones que requieren una acción rápida y coordinada para salvaguardar los derechos fundamentales.

En la UE existía un contenido dogmático-normativo sobre valores y derechos fundamentales en los que se apoya la propia UE. El tratado de Lisboa refuerza el fundamento dogmático de la UE definiendo valores fundamentales (enunciados en el artículo 2 del Tratado de la Unión Europea (TUE): respeto a la dignidad humana, la libertad, la democracia, los derechos humanos...), objetivos y derechos fundamentales de su ciudadanía que forman parte también de su identidad política. Los valores de la UE están protegidos por el artículo 7 del TUE y el artículo 51 de la Carta, pero, sin embargo, al producirse vulneraciones graves de aquellos, la UE no ha sabido utilizar el mecanismo sancionador previsto en el artículo 7 (Bar Cendon, 2014) debido a su operatividad. En una primera fase de aplicación correspondiente del artículo 7.1 el Consejo de la UE determina si hay riesgo de violación grave de valores de la UE. Tras esta medida, el Consejo resuelve la aplicación del artículo 7.2 si ha habido violación grave y persistente de estos valores, y, luego de este paso, puede decidir por mayoría cualificada aplicar el 7.3, lo que supone imponer una sanción al Estado refractario que puede llegar a la suspensión de derechos, como el de voto en el Consejo[12]. Desde la Comisión existe la creencia de que es preferible considerar el artículo 7 desde el punto de vista de la prevención[13], si bien, de todas formas, para activar la sanción hasta último término todos los países deben secundarla casi de manera unánime, siendo esta una cuestión difícil. Se deberían diseñar nuevos modos de protección general de los valores fundamentales dirigidos más a prevenir que a sancionar evitando las violaciones de los mismos. El Estado de derecho está basado en mecanismos que

12. https://www.europarl.europa.eu/news/es/headlines/eu-affairs/20180222STO98434/estado-de-derecho-como-funciona-el-procedimiento-del-articulo-7-infografia
13. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52003DC0606&from=ES

protegen los derechos humanos fundamentales, derechos definidos en la UE en la Carta, de obligado cumplimiento para todos los Estados miembros tal y como establece el artículo 52(3)[14]. La UE dispone del Tribunal Europeo de Derechos Humanos (TEDH), cuya jurisprudencia es esencial en el desarrollo y la interpretación de derechos fundamentales. Hay un compromiso de protección de estos asumido por la UE, pero, como apunta Ortega (2017), partimos de un problema de abordaje amplio por lo multifactorial de la desinformación, y la regulación jurídica es complicada. Las empresas de comunicación deberían poner límites, aunque lo cierto es que las presiones económicas parecen ser más eficientes que las medidas de orden jurídico. Las redes sociales están sometidas al control del Derecho, pero estas, como nueva forma de comunicación, crean nuevos problemas jurídicos. Es necesario establecer una diferencia entre comunicar e informar porque ambas acciones no tienen un mismo tratamiento jurídico; a nivel internacional las regulaciones jurídicas no establecen una precisión entre estos dos conceptos, de manera que el grado de confusión es alto y la regulación de la desinformación se acaba complicando aún más. Por otro lado, y a pesar de contar con normativa suficiente, el derecho humano a la privacidad va desapareciendo en manos de la publicidad, siendo el daño a las poblaciones irreversible y la situación muy difícil de retrotraerse. La responsabilidad de grandes corporaciones como Facebook ha de ser tomada sin relativismos puesto que sirve en bandeja a sus empresas asociadas los datos personales de sus usuarios (Vercelli, 2018). Luchar por una información veraz y transparente sin vulnerar derechos fundamentales complica aún más el margen de acción: limitar la difusión de desinformación es moverse en terrenos de arduo desempeño. Es difícil su puesta en marcha sin que se infrinjan, o puedan llegar a hacerlo, tales derechos. Como ejemplo, la iniciativa de establecer una mayor responsabilidad en los contenidos puede ser peligrosa porque, aunque las redes sociales tienen parte de responsabilidad a la hora de filtrar noticias, puede someter a internet y sus contenidos a parámetros empresariales (Pauner Chulvi, 2018). Otro caso lo encontramos en el tipo de información transmitida que puede incidir en ámbitos íntimos, por lo que debe existir más cautela en la difusión de noticias (Lorente López, 2015). Es importante mencionar que ahora mismo la responsabilidad y la ética están relacionadas con la Inteligencia Artificial (IA) y la utilización de *bots* en redes sociales y otras publicaciones basadas en el intercambio y difusión de noticias, sobre todo si tenemos en cuenta que tanto algoritmos como otras herramientas de la IA pueden redactar y generar texto, imágenes y vídeos de manera más rápida que los humanos. Otorgar personalidad jurídica a los robots sin referencia humana última comportaría una renuncia al carácter antropocéntrico del concepto y a la tradición cultural que lleva aparejada. De ahí que haya que comenzar a plantear una regulación de los avances tecnológicos fundamentada en principios éticos, en la transparencia y la responsabilidad (Petit, 2018). La publicación de noticias en internet embrolla aún más el asunto, pues al límite o el origen de responsabilidades se une la búsqueda de un reequilibrio entre la expresión libre de opiniones, el derecho al honor, la protección de datos personales y el ejercicio de la libertad de expresión e información. Añádase a esto la colisión con los derechos a la intimidad, el honor y la propia imagen, que han de ser reinterpretados de acuerdo con el contenido del derecho a la protección de datos (Domínguez-Garriga, 2016).

4.1.1 La Declaración Conjunta de la Organización para la Seguridad y la Cooperación en Europa (OSCE): el respeto a los derechos humanos y la desinformación

Las propuestas para contrarrestar la desinformación han estado orientadas al control de sitios de internet y a la verificación de noticias, pero muchas de estas acciones podrían poner en peligro la libertad de expresión y la privacidad. Ante este hecho, expertos para la libertad de expresión de la ONU, la OSCE, la Comisión Interamericana de Derechos Humanos (CIDH), la Organización de los Estados Americanos (OEA) y la Comisión Africana de Derechos Humanos emiten en el 7 de marzo de 2017 una Declaración Conjunta sobre libertad de expresión y noticias falsas, desinformación y propaganda que pretende, por un lado, identificar principios y buenas prácticas que han de ser respetados conforme a derecho internacional sin que ninguno de los derechos humanos se vea afectado por ello; y, por otro, advertir de iniciativas preocupantes provenientes del sector público y privado que intentan poner

14. http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493031/IPOL-LIBE_ET%282013%29493031_EN.pdf

coto a la desinformación mediante la supresión de la libre expresión[15], la libre circulación de ideas y el disenso, por lo que podríamos estar ante medidas contrarias al derecho internacional de los derechos humanos.

La lucha contra la expansión de la desinformación no debe realizarse a costa de derechos fundamentales. Los principios generales de la Declaración Conjunta recuerdan que las restricciones a la libertad de expresión solo pueden hacerse desde el derecho internacional conforme a los requisitos estipulados como la prohibición de la apología del odio, la violencia, la discriminación o la hostilidad de acuerdo con el artículo 20.2 del Pacto Internacional de Derechos Civiles y Políticos (PIDCP). En el caso de acuerdos con intermediarios, la Declaración Conjunta deja claro que no son los responsables de contenidos de terceros a menos que intervengan en ellos, teniendo que considerar además la necesidad de proteger a las personas de responsabilidad legal solo por distribuir noticias o informaciones que no crearon. En cuanto a los bloqueos a direcciones IP o sitios web, son medidas de carácter extremo y se realizarán cuando venga estipulado por ley o resulte necesario para proteger un derecho humano. Y, por último, los sistemas de filtrado de contenido controlados por los Gobiernos y no por los usuarios finales suponen una restricción no justificada de la libertad de expresión. Esta ha de aplicarse sin fronteras y la cancelación de derechos de transmisión es legítima solo cuando un tribunal de justicia lo determine. El control de la desinformación debe cumplir unos estándares: no prohibir la difusión de información basándose en conceptos imprecisos y ambiguos como los de *fake news;* las leyes sobre difamación deben ser derogadas por suponer restricciones desproporcionadas al derecho a la libertad de expresión; y los Estados deben promover un entorno de comunicaciones libre, independiente, y no distribuir información falsa, mientras que los medios y periodistas deben ofrecer una cobertura crítica de la desinformación y la propaganda, sobre todo en períodos electorales.

Existen aspectos a reforzar en las medidas contra la desinformación para no vulnerar derechos fundamentales: garantizar que en las decisiones automatizadas sobre personas se extremen las garantías legales y que exista transparencia y consentimiento del interesado, porque medidas como el tratamiento de datos personales pueden afectar a los derechos fundamentales de respeto a la vida y de protección de tales datos, como se vio en la sentencia, de 13 de mayo de 2014, del TJUE respecto del Asunto C-131/12 (Domínguez, 2016). Que los proveedores de acceso a internet no ponderen los intereses afectados por las políticas de bloqueo de contenidos porque lo que está en juego es la restricción de determinados derechos fundamentales es algo que solo los tribunales o un juez deberían poder decidir (López Richart, 2017).

Conclusiones

La desinformación sigue siendo un fenómeno creciente y preocupante para los ciudadanos europeos. Al respecto, se han instaurado algunas soluciones que pasan por establecer marcos jurídicos que intentan controlar las tecnologías y las empresas sobre las que se apoyan los nuevos modos de crear, producir y consumir información, implementando planes de alfabetización mediática para los usuarios y el establecimiento de filtros, o, como recuerda Pauner Chulvi (2018), combatiendo la propaganda con información real contrastándola a través de herramientas digitales. En general, se trata de recomendaciones que no incluyen políticas regulatorias apoyadas en la RGPD, la Directiva de Servicios Audiovisuales o los mecanismos estatales, así que no dejan de ser medidas blandas de mejora (Martens, Aguiar, Gómez y Muller, 2018). En este sentido, las iniciativas desarrolladas desde la UE en cooperación con medios de comunicación o grandes empresas, como por ejemplo el Código de buenas prácticas, están siendo insuficientes porque la problemática va transformándose y evolucionando al mismo ritmo que las herramientas tecnológicas en las que se apoya la desinformación. Y, por otra parte, la respuesta tampoco puede ceñirse solo a la elaboración de nuevas leyes ni a la censura, porque es un problema que no tiene un único abordaje dada su com-

15. El derecho a la libertad de expresión e información está recogido en el artículo 10 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales y en el artículo 11 de la Carta de Derechos Fundamentales de la UE. La libertad de expresión incluye la de opinión y la libertad de recibir o comunicar informaciones o ideas sin que haya injerencia de autoridades públicas sin consideración de fronteras. El derecho a la libertad de expresión incluye el derecho de acceso a internet, derecho inherente al derecho de acceso a la información y a la comunicación, protegido en las Constituciones nacionales.

plejidad. Sea como sea, la división europea está servida entre quienes propugnan el control de las noticias falsas a través de legislación de obligado cumplimiento y los que no son partidarios de medidas legales punitivas (Castro Ruano, 2018). Es complicado establecer herramientas de control de la desinformación orientadas a la vigilancia de los sitios de internet y la verificación de noticias sin poner en peligro la libertad de expresión y la privacidad. La evolución de la comunicación en red puede tomar direcciones inesperadas, amplificar riesgos conocidos o crear otros nuevos, por lo que el abanico de situaciones a regular desafía a los poderes establecidos creciendo más allá de las previsiones.

Referencias bibliográficas

ACOSTA-GONZÁLEZ, D. (2019). «Consideraciones en torno a la normativa sobre los prestadores de servicios en línea y editoriales de prensa propendida por la nueva directiva europea sobre derechos de autor y derechos afines en el mercado único digital». *Revista La propiedad inmaterial*, núm. 27, págs. 95-119.

ALLCOTT, H.; GENTZKOW, M. (2017). «Social media and fake news in the 2016 election». *Journal of economic perspectives,* vol. 31, núm. 2, págs. 211-236.

ARTEAGA, F. (2018). «Lecciones aprendidas durante la tramitación de la Directiva NIS: análisis de la directiva 2016/1148». *Ciber ElCano,* núm. 34. Madrid: Real Instituto Elcano. http://www.realinstitutoelcano.org/wps/portal/rielcano_es/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_es/zonas_es/ari75-2018-arteaga-lecciones-aprendidas-durante-tramitacion-directiva-nis.

BAR CENDON, A. (2014). «La Unión Europea como unión de valores y derechos: teoría y realidad-The European Union as a union of fundamental values and rights: theory and reality». *Teoría y Realidad Constitucional,* vol. 1, núm. 33.

MARTENS, B.; AGUIAR, L.; GÓMEZ HERRERA, E.; MULLER, F. (2018). «The digital transformation of news media and the rise of disinformation and fake news». EU Science Hub. https://ec.europa.eu/jrc/communities/sites/jrccties/files/dewp_201802_digital_transformation_of_news_media_and_the_rise_of_fake_news_final_180418.pdf

BRADSHAW, SAMANTHA, HOWARD, PHILIP, N. (2017). «Computational Propaganda Research Project». Working Paper No. 2017.12 Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation.

CARRERA, S.; GUILD, E.; HERNANZ, N. (2013). «The Triangular Relationship between Fundamental Rights, Democracy and the Rule of Law in the EU: Towards an EU Copenhagen Mechanism» (November 20, 2013). CEPS Paperbacks, 2013. Available at SSRN: https://ssrn.com/abstract=2360486

CASTRO RUANO, J. L. (2018). «La desinformación como instrumento político en la Sociedad Internacional actual: las respuestas desde la Unión Europea». *Unión Europea Aranzadi,* núm. 7.

DOMÍNGUEZ GARRIGA, A. (2016). «Límites del derecho a la protección de datos personales. Especial referencia a las libertades de expresión e información». En:. *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua.* Madrid: Dykinson, págs. 114-145.

GALÁN, C. (2018). «Amenazas híbridas: nuevas herramientas para viejas aspiraciones». Documento de trabajo 20/2018.

http://www.realinstitutoelcano.org/wps/wcm/connect/b388b039-4814-4012-acbf-1761dc50ab04/DT20-2018-Galan-Amenazas-hibridas-nuevas-herramientas-para-viejas-aspiraciones.pdf?MOD=AJPERES&CACHEID=b388b039-4814-4012-acbf-1761dc50ab04

GARCÍA OROSA, B.; GALLUR SANTORUN, S.; LÓPEZ GARCÍA, X. (2017). «Use of clickbait in the online news media of the 28 EU member countries». *Revista Latina de Comunicación Social,* núm. 72, págs. 1.261-1.277.
http://www.revistalatinacs.org/072paper/1218/68en.html

GONZÁLEZ DE LA GARZA, L. M. (2018). «La crisis de la democracia representativa: nuevas relaciones políticas entre democracia, populismo virtual, poderes privados y tecnocracia en la era de la propaganda electoral cognitiva virtual, el *microtargeting* y el *big data*». *Revista de Derecho Político,* núm. 103.

LÓPEZ, M.; CABRERA, T. (2015). «Campaña política a través de redes sociales». *ComHumanitas*, vol. 5, núm. 1, págs. 65-72.

LÓPEZ RICHART, J. (2017). Ordenes de bloqueo de páginas web: ¿ hasta dónde llega el deber de colaboración de los proveedores de acceso a internet en la lucha contra la piratería?. *Ordenes de bloqueo de páginas web: ¿hasta dónde llega el deber de colaboración de los proveedores de acceso a internet en la lucha contra la piratería?*, 211-271.

LORENTE LÓPEZ, M.ª CRISTINA (2015). «Los derechos al honor, a la intimidad personal y familiar y a la propia imagen en la jurisprudencia más reciente». En: *Los derechos a la intimidad y a la privacidad en el siglo XXI*. Madrid: Dykinson, págs. 131-155.

LORETO-ECHEVERRI, G.; ROMERO-RODRÍGUEZ, L.; PÉREZ-RODRÍGUEZ, M. (2018). «Fact-checking vs. Fake news: periodismo de confirmación como componente de la competencia mediática contra la desinformación». *índex. comunicación,* vol. 8, núm. 2, págs. 295-316.
http://journals.sfu.ca/indexcomunicacion/index.php/indexcomunicacion/article/view/370/399

ORTEGA, D. (2017). «Comunicación, tecnología y Derecho. Confusión entre el derecho a la comunicación y el derecho a la información». En: *Retos de la libertad de información*. Madrid: Dykinson, págs. 57-73.

PAUNER CHULVI, C. (2018). «Noticias falsas y libertad de expresión e información. El control de los contenidos informativos en la Red». *Teoría y Realidad Constitucional*, núm. 41, págs. 297-318.
http://revistas.uned.es/index.php/TRC/article/view/22123/18051

PERNICE, I. (2017). Risk Management in the Digital Constellation–A Constitutional Perspectiv Pernice, Ingolf, Risk Management in the Digital Constellation – A Constitutional Perspective (October 2017). HIIG Discussion Paper Series No. 2017-07. Available at SSRN: https://ssrn.com/abstract=3051124

PETIT, M. (2018). «Por una crítica de la razón algorítmica. Estado de la cuestión sobre la inteligencia artificial, su influencia en la política y su regulación». *Quaderns del CAC,* núm. 44 («Fake news, algoritmos y burbujas informativas»), págs. 5-15.

RUELAS MONJARDÍN, A. (2019). «Metodología jurídica digital: conceptualización y problemáticas para su construcción». *Derecho y Cambio Social,* núm. 55, págs.1-36. https://lnx.derechoycambiosocial.com/ojs-3.1.1-4/index.php/derechoycambiosocial/article/view/10/11

UFARTE RUIZ, M. J. (2016). «El rumor como base de la noticia en los medios digitales». *Libro de actas del III Congreso Internacional de Ética de la Comunicación: Desafíos éticos de la comunicación en la Era digital*. Madrid: Dykinson, págs. 105-117.

VALERO, P. P.; OLIVEIRA, L. (2018). «Fake news: una revisión sistemática de la literatura». *Observatorio (OBS*),* vol. 12, núm. 5.

VERCELLI, A. (2018). «La (des)protección de los datos personales: análisis del caso Facebook Inc.Cambridge Analytica». *XVIII Simposio Argentino de Informática y Derecho* (SID 2018). http://sedici.unlp.edu.ar/handle/10915/71755

WATANABE, K. (2018). «Conspiracist propaganda: How Russia promotes anti-establishment sentiment online». *ECPR General Conference*. Hamburgo.

YOUJUNG JUN; RACHEL MENG; GITA VENKATARAMANI JOHAR (2017). «Perceived social presence reduces factchecking». *PNAS,* vol. 114, núm. 23), págs. 5.976-5.981. https://www.pnas.org/content/114/23/5976.full#sec-29

Informes y documentos de la UE:

Estudio sobre desinformación y propaganda: «Disinformation and propaganda impact on the functioning of the rule of law in the EU and its Member States». Policy Department for Citizens' Rights and Constitutional Affairs Directorate General for Internal Policies of the Union PE 608.864, febrero de 2019.
http://www.statewatch.org/news/2019/mar/ep-study-rule-of-law.pdf

«The legal Framework to address "fake news"; possible policy actions at the EU level». Andrea Renda (CEPS-Centre for European Policy Studies and College of Europe). Policy Department for Economic, Scientific and Quality of Life Policies. Directorate-General for Internal Policies PE 619.013, junio de 2018.
http://www.europarl.europa.eu/RegData/etudes/IDAN/2018/619013/IPOL_IDA(2018)619013_EN.pdf

Informe final del Grupo de expertos de alto nivel sobre noticias falsas y desinformación en línea: «A multidimensional approach to disinformation Report of the independent High level Group on fake news and online disinformation. Directorate-General for Communication Networks, Content and Technology, 12 de marzo de 2018. http://sites.les.univr.it/cybercrime/wp-content/uploads/2017/08/Amulti-dimensionalapproachtodisinforma-tion-ReportoftheindependentHighlevelGrouponfake-newsandonlinedisinformation.pdf

Resultados del «Summary report of the public consultation on mesures to further improve the effectiveness of the fight against ilegal content online», septiembre de 2018.
https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-measures-further-improve-effectiveness-fight-against-illegal

Plan de Acción contra la desinformación, diciembre de 2018.
https://eeas.europa.eu/sites/eeas/files/disinformation_factsheet_es.pdf

Reglamentos, directivas, comunicaciones, recomendaciones y resoluciones de la UE:

Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). https://www.boe.es/doue/2002/201/L00037-00047.pdf

Directiva 2005/29/CE del Parlamento Europeo y del Consejo de 11 de mayo de 2005 relativa a las prácticas comerciales desleales de las empresas en sus relaciones con los consumidores en el mercado interior, que modifica la Directiva 84/450/CEE del Consejo, las Directivas 97/7/CE, 98/27/CE y 2002/65/CE del Parlamento Europeo y del Consejo y el Reglamento (CE) n.º 2006/2004 del Parlamento Europeo y del Consejo. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32005L0029&from=ES

Directiva 2010/13/UE de 10 de marzo de 2010 sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas a la prestación de servicios de comunicación audiovisual (Directiva de servicios de comunicación audiovisual). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32010L0013&from=EN

Directiva 2013/40/UE del Parlamento Europeo y del Consejo de 12 de agosto de 2013 relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo. https://www.boe.es/doue/2013/218/L00008-00014.pdf

Directiva 2016/1148 de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad en las redes y sistemas de información en la UE. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016L1148&from=ES

Directiva (UE) 2017/541 del Parlamento Europeo y del Consejo de 15 de marzo de 2017 relativa a la lucha contra el terrorismo y por la que se sustituye la Decisión marco 2002/475/JAI del Consejo y se modifica la Decisión 2005/671/JAI del Consejo. https://www.boe.es/doue/2017/088/L00006-00021.pdf

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX:32016R0679

Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo de 17 de abril de 2019 sobre los derechos de autor y derechos afines en el mercado único digital. https://www.boe.es/doue/2019/130/L00092-00125.pdf

Reglamento UE N.º 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. https://www.boe.es/doue/2014/257/L00073-00114.pdf

Resolución del Parlamento Europeo, de 15 de junio de 2017, sobre una Agenda Europea para la economía colaborativa. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0271+0+DOC+XML+V0//ES

Recomendación UE 2018/334, de 1 de marzo de 2018, sobre medidas para combatir eficazmente los contenidos ilícitos en línea. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32018H0334&from=GA

COM 236/04/2018. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: «La lucha contra la desinformación en línea: un enfoque europeo». https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018DC0236&from=EN

Comunicación: Joint Communication to the European Parliament, the European Council, the Council, The European Economic and Social Committee and the committee of the Regions. Action Plan against Disinformation. Bruselas, 5 de diciembre de 2018. https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf

Recommendation C (2018) 5949 on election cooperation networks C82028) 5949 Final. Recomendación de la Comisión relativa a las redes de cooperación electoral, la transparencia en línea, la protección contra los incidentes de ciberseguridad y la lucha contra las campañas de desinformación en el contexto de las elecciones al Parlamento Europeo. Bruselas, 12 de septiembre de 2018. https://ec.europa.eu/transparency/regdoc/rep/3/2018/ES/C-2018-5949-F1-ES-MAIN-PART-1.PDF

Cita recomendada

SEIJAS, Raquel (2020). «Las soluciones europeas a la desinformación y su riesgo de impacto en los derechos fundamentales». *IDP. Revista de Internet, Derecho y Política.* N.º 31, págs. 1-14. UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i31.3205

Sobre la autora

Raquel Seijas
seijas.raquel@gmail.com

Raquel Seijas es doctora en Periodismo por la Universidad Complutense de Madrid y máster en Derechos Humanos y Democracia por la UOC.

Profesora del Departamento de Periodismo de la Universidad de Málaga. Paralelamente a la actividad académica ha desarrollado actividad laboral en Fundación Secretariado Gitano y ha coordinado proyectos de IAP con CIMAS. Entre sus líneas de investigación activas se encuentran: minorías, desinformación y medios de comunicación, análisis del discurso, migraciones y derechos humanos.

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

www.uoc.edu/idp

ARTÍCULO

Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales según el Tribunal de Justicia de la UE[1]

Susanna Oromí i Vall-llovera
Universitat de Girona

Fecha de presentación: junio de 2019
Fecha de aceptación: marzo de 2020
Fecha de publicación: abril de 2020

Resumen

El Tribunal de Justicia de la UE reconoce que el acceso, la conservación y cesión de datos personales electrónicos, una de las diligencias de instrucción cada vez más utilizada en el proceso penal, constituye una injerencia en los derechos fundamentales a la vida privada y familiar y a la protección de datos de carácter personal, de forma que si una autoridad pública pretende obtener tales datos precisa de una autorización judicial que debe respetar en todo caso el principio de proporcionalidad y establece, como criterio de apreciación de la proporcionalidad, la gravedad de los delitos. Parece, pues, que el acceso a datos personales electrónicos en la investigación penal deberá limitarse estrictamente a fines de prevención y detección de delitos graves o el enjuiciamiento de tales delitos. De ahí surge la duda que se pretende resolver en este trabajo: ¿el juez de instrucción únicamente puede autorizar la obtención de datos personales electrónicos conservados por prestadores de servicios de comunicaciones cuando se estén investigando delitos graves?; o, en una investigación penal, ¿cabe autorizar una diligencia de obtención y acceso a datos personales electrónicos cuando el delito no es grave? El TJUE ha dado recientemente una respuesta que es preciso analizar, pues sirve para fijar importantes criterios que debe utilizar el juez de instrucción en el juicio de proporcionalidad que fundamenta la autorización de este tipo de diligencias de instrucción.

Palabras clave

datos personales electrónicos, protección de datos de carácter personal, vida privada, diligencias de instrucción, investigación penal

1. Este trabajo se ha realizado en el marco del Proyecto de I+D (DER2017-82146-P).

Access to personal data held by electronic communications service providers in criminal investigations according to the Court of Justice of the EU[1]

Abstract

The EU Court of Justice recognises that accessing, holding and transferring electronic personal data, pretrial proceedings which are becoming more and more commonly used in criminal proceedings, constitutes interference in the fundamental rights to private and family life and to personal data protection, and therefore if a public authority attempts to obtain such data, it requires judicial authorisation which must in all cases respect the principle of proportionality and establishes, as a criterion of the evaluation of proportionality, the seriousness of the crimes. It seems, then, that access to electronic personal data in criminal investigation must be strictly limited to the purposes of prevention and the detection of serious crimes, or the trial of such crimes. This leads to the doubt which we attempt to resolve in this work: Can only the examining judge authorise obtaining electronic personal data held by communications service providers when serious crimes are being investigated? Or, in a criminal investigation, should proceedings for obtaining evidence and access to electronic personal data be authorised when the crime is not serious? The CJEU recently gave a response which requires analysis, as it serves to set important criteria that the examining judge must use in the judgement of proportionality which gives the foundation for the authorisation of these kinds of criminal pretrial proceedings.

Keywords

electronic personal data, personal data protection, private life, criminal pre-trial proceedings, criminal investigation

1. This work was carried out within the framework of the R+D Project (DER2017-82146-P).

1. Introducción

Uno de los medios de investigación cada vez más utilizados en la fase de instrucción de los procesos penales, tanto si se persigue la presunta comisión de delitos graves como de los que no revisten tal gravedad, es el acceso y obtención de datos de tráfico y localización de las comunicaciones electrónicas, en especial las que derivan de la telefonía móvil o internet. Tales datos tienen la consideración de datos personales de los ciudadanos y quedan amparados por el derecho a la protección de datos de carácter personal[2], por lo que se precisa autorización judicial para obtenerlos (artículo 588 *ter j* LE-Crim). El uso generalizado de la telefonía móvil en la sociedad ha propiciado que estas diligencias sumariales se hayan convertido en uno de los instrumentos más importantes de que dispone la policía judicial, la fiscalía y los jueces para perseguir la criminalidad. Lo habitual es que sea la policía judicial la que solicite al juez instructor tal diligencia de obtención y cesión de datos personales, siendo una de las medidas de investigación usada con mayor asiduidad en los últimos tiempos.

El Tribunal de Justicia de la UE (en adelante, TJUE) reconoce que la conservación y cesión de datos personales de tráfico constituye una injerencia en los derechos a la vida privada y familiar y a la protección de datos de carácter personal, garantizados en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea (en adelante, la Carta), de forma que si una autoridad pública pretende obtener tales datos debe respetar en todo caso el principio de proporcionalidad y establecer, como criterio de apreciación de la proporcionalidad, la gravedad de los delitos como justificación de la obtención y cesión de los datos para las investigaciones penales[3]. Parece, pues, que el acceso de las autoridades competentes a los datos y su utilización ulterior en un proceso penal deberán limitarse estrictamente a fines de prevención y detección de delitos graves o el enjuiciamiento de tales delitos.

De ahí surge la duda que se pretende resolver en este trabajo: ¿el juez de instrucción únicamente puede autorizar la obtención de datos personales electrónicos conservados por prestadores de servicios de comunicaciones cuando se estén investigando delitos graves?; o, en una investigación penal, ¿cabe autorizar una diligencia de obtención y cesión de datos personales electrónicos cuando el delito no es grave?

El TJUE ha dado recientemente una respuesta que es preciso analizar, pues sirve para fijar importantes criterios que deben utilizar los juzgados de instrucción en el juicio de proporcionalidad que fundamenta la autorización de este tipo de diligencias de instrucción[4]. Es otra muestra de cómo el uso de la tecnología en la sociedad –y de forma extensiva en la criminalidad– incide en la eficacia y la eficiencia de los procesos judiciales.

2. Por lo que se deben respetar las previsiones de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
3. STJUE de 8 de abril de 2014, *Digital Rights Ireland* y otros (C 293/12 y C 594/12, EU:C:2014:238), declaró la invalidez de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicación, donde afirma: «Además, en cuanto al acceso de las autoridades nacionales competentes a los datos y su utilización posterior, la Directiva 2006/24 no precisa las condiciones materiales y de procedimiento correspondientes. El artículo 4 de la Directiva, que regula el acceso de dichas autoridades a los datos conservados, no dispone expresamente que el acceso y la utilización posterior de los datos de que se trata deberán limitarse estrictamente a fines de prevención y detección de delitos graves delimitados de forma precisa o al enjuiciamiento de tales delitos, sino que se limita a establecer que cada Estado miembro definirá el procedimiento que deba seguirse y las condiciones que deban cumplirse para tener acceso a los datos conservados de conformidad con los requisitos de necesidad y proporcionalidad».
4. STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), que tiene por objeto una petición de decisión prejudicial planteada por la Audiencia Provincial de Tarragona.

2. Injerencia en los derechos fundamentales al respeto de la vida privada y a la protección de datos de carácter personal

Como se ha apuntado, el acceso por parte de autoridades públicas a datos personales de tráfico y localización de las comunicaciones electrónicas representa una injerencia en los derechos fundamentales al respeto de la vida privada y a la protección de datos personales, garantizados en los artículos 7 y 8 de la Carta. Así lo ha reiterado el TJUE en varias ocasiones, según se examina a continuación.

La injerencia en estos derechos fundamentales puede producirse a través de la comunicación, acceso y conservación de datos de carácter personal con vistas a su utilización por parte de las autoridades públicas o cualquier otra persona. Y esta injerencia se produce cualquiera que sea el uso posterior de la información comunicada o conservada. En este sentido, la injerencia en el derecho fundamental al respeto de la vida privada y familiar, consagrado en el artículo 7 de la Carta, se ocasiona con independencia de que la información sobre la vida privada tenga o no carácter sensible y sin que sea relevante que los interesados hayan padecido algún perjuicio o inconveniente. No es necesario, por tanto, que se trate de una injerencia grave en la vida privada de los ciudadanos, sino que cualquier tipo de acceso a datos personales electrónicos produce la vulneración del derecho fundamental[5].

Es más, tal comunicación, conservación y accesos a datos personales conservados por proveedores de servicios de comunicaciones electrónicas, sea cual sea su utilización posterior, también constituyen tratamientos de datos de carácter personal, por lo que configuran asimismo una injerencia en el derecho fundamental a la protección de datos de carácter personal garantizado por el artículo 8 de la Carta[6].

Ni que decir tiene que, si el acceso de datos personales conservados por proveedores de servicios de comunicaciones electrónicas supone una injerencia en los derechos fundamentales a la vida privada y a la protección de datos de carácter personal, representa, a mi juicio, una vulneración de tales derechos; por tanto, cuando una autoridad pública pretenda acceder a estos datos, justificándolo en actuaciones de investigación de delitos, precisará en todo caso autorización judicial, y en el caso de que se practique la diligencia sin esta autorización cabrá alegar la ilicitud de la prueba en juicio oral.

Sentada, pues, la injerencia en los derechos fundamentales, procede examinar cuándo las autoridades públicas pueden acceder a datos personales electrónicos justificándolo en el desarrollo de investigaciones penales.

3. Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales por delitos graves

A la luz de todo lo expuesto, no hay ninguna duda que el acceso y obtención por autoridades policiales o judiciales, en el marco de investigaciones penales, de datos personales conservados por los proveedores de servicios de comunicaciones electrónicas, representan una injerencia en los derechos fundamentales garantizados en los artículos 7 y 8 de la Carta. Pero esta excepción al principio de confidencialidad de las comunicaciones electrónicas se encuentra amparada por el artículo 15.1 de la Directiva 2002/58, que establece de forma exhaustiva los objetivos que permiten el acceso de autoridades públicas a tales datos, entre los que se encuentra «la prevención, investigación, descubrimiento y persecución de delitos». Cabe recordar que el TJUE ha reconocido que cualquier limitación a la confiden-

5. En relación con el artículo 7 de la Carta, lo viene señalando el TJUE en las siguientes sentencias: de 20 de mayo de 2003, Österreichischer Rundfunk y otros (C-465/00, C-138/01 y C-139/01, EU:C:2003:294), apartados 74 y 75; de 8 de abril de 2014, Digital Rights Ireland y otros (C 293/12 y C 594/12, EU:C:2014:238), apartados 33 a 35; de 6 de octubre de 2015, Schrems (C 362/14, EU:C:2015:650), apartado 87; y, de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 51.
6. Véanse, en este sentido, las sentencias del TJUE de 17 de octubre de 2013, Schwarz (C 291/12, EU:C:2013:670), apartado 25; de 8 de abril de 2014, Digital Rights Ireland y otros (C 293/12 y C 594/12, EU:C:2014:238), apartado 36; y, de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 51.

cialidad de las comunicaciones electrónicas y de los datos de tráfico relativos a ellas debe interpretarse en sentido estricto, de forma que la conservación de datos de tráfico y de localización solo debe realizarse durante un plazo limitado y justificado, por lo que no es posible articular un sistema de conservación y cesión generalizada e indiscriminada de estos datos[7]. Sentada esta premisa, al establecer la investigación criminal como un motivo que justifica el acceso y obtención de datos personales, han surgido dudas, en particular sobre si los delitos deben revestir un cierto nivel de gravedad para permitir la injerencia en los derechos fundamentales, que han llevado a recientes pronunciamientos del TJUE al respecto, los cuales son objeto de análisis en el presente trabajo.

El TJUE ha declarado que cuando el acceso a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas comporta una injerencia grave a los mencionados derechos fundamentales, tal injerencia únicamente puede autorizarse para luchar contra la delincuencia grave[8]. Esto hace que el juez de instrucción, en el momento de dictar su resolución motivada para autorizar esta diligencia, deba realizar un juicio de proporcionalidad entre, por un lado, la gravedad de la injerencia en los derechos fundamentales, con lo que tendrá que tener en cuenta la naturaleza de los datos que se quieren obtener, y, por otro lado, la gravedad de los hechos delictivos. Así las cosas, solo cuando los delitos son graves debe admitirse el acceso a datos electrónicos de carácter personal que provoquen una injerencia grave en los derechos a la vida privada y familiar y a la protección de datos personales.

Llegados a este punto, surge la necesidad de analizar los dos extremos necesarios para realizar el juicio de proporcionalidad: en primer lugar, qué criterios deben utilizarse para valorar que la injerencia en los derechos fundamentales es grave; y, en segundo lugar, cuándo un delito tendrá la consideración de grave. La importancia de saber estos extremos radica en que un juez de instrucción únicamente podrá autorizar el acceso a datos personales si puede motivar este juicio de proporcionalidad.

3.1. ¿Qué criterios deben utilizarse para valorar que una injerencia en los derechos fundamentales a la vida priva y familiar y a la protección de datos de carácter personal es grave?

El TJUE ha interpretado que cuando una norma regula el acceso a datos personales conservados por los proveedores de servicios de comunicaciones electrónicas, en materia de prevención, descubrimiento, investigación y persecución de delitos, debe guardar relación con la gravedad de la injerencia de los derechos fundamentales en cuestión[9], de forma que solo puede justificar una injerencia grave el objetivo de luchar contra la delincuencia también considerada como grave. De ahí que surja el interés por determinar qué se entiende por injerencia grave en los derechos fundamentales a la vida privada y familiar y a la protección de datos de carácter personal.

Una injerencia grave en los derechos fundamentales mencionados es aquella que permite extraer conclusiones precisas y concretas sobre la vida privada de las personas, cuyos datos han sido conservados por los proveedores de servicios de comunicaciones electrónicas. Así lo ha venido entendiendo el TJUE en varias de sus sentencias[10]. Por lo tanto, tienen la consideración de injerencia grave: acceder a las comunicaciones efectuadas con un teléfono móvil; conocer la fecha, la hora, la duración o los destinatarios de las comunicaciones efectuadas; obtener los lugares en que estas comunicaciones tuvieron lugar o la localización del terminal; o, saber la frecuencia de estas comunicaciones con determinadas personas durante un período concreto[11].

7. STJUE de 22 de noviembre de 2012, Probst (C-119/12, EU:C:2012:748), apartado 23. STJUE (Gran Sala), 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C 203/15 y C 698/15, EU:C:2016:970). En este sentido, T. Armenta Deu (2018, pág. 70); I. Colomer Hernández (2018, págs.77-78); J. Delgado Martín (2019); E. Frías Martínez (2019); Mª. I. Gónzalez Cano (2019, págs. 1.331 y sigs.); A. E. Gudín Rodríguez-Magariños (2017); M. Richard González (2018, págs. 475 y sigs.); y A. Sánchez Rubio (2018, págs. 506 y sigs.).
8. STJUE (Gran Sala), 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C 203/15 y C 698/15, EU:C:2016:970), apartado 99. STJUE de 8 de abril de 2014, Digital Rights Ireland y otros (C 293/12 y C 594/12, EU:C:2014:238). STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 56.
9. STJUE (Gran Sala), 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C 203/15 y C 698/15, EU:C:2016:970), apartado 115.
10. STJUE (Gran Sala), 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C 203/15 y C 698/15, EU:C:2016:970), apartado 99. STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 56.
11. STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 60.

Todas estas actuaciones permiten extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados, constituyendo una injerencia grave en los derechos a la vida privada y familiar y a la protección de datos de carácter personal.

Una injerencia de estas características únicamente queda justificada si se persigue la prevención, el descubrimiento, la persecución o la investigación de delitos graves. Por lo que es importante determinar también cuándo un delito tiene la consideración de grave, como se verá en el siguiente apartado.

3.2. ¿Cuándo un delito tiene la consideración de grave?

El TJUE no se pronuncia sobre este extremo de forma expresa, pese a la pregunta formulada en cuestión prejudicial por la Audiencia Provincial de Tarragona[12]. La STJUE (Gran Sala), de 21 de diciembre de 2016, tampoco recoge una definición cerrada de «delincuencia grave» y se limita a relacionarla con la delincuencia organizada y el terrorismo[13]. A nadie escapa que existen otras conductas delictivas consideradas como graves.

La duda planteada es procedente, pues cabe preguntarse si para considerar la gravedad de un delito únicamente debe tenerse en cuenta la pena que pueda imponerse o deben valorarse particulares niveles de lesividad en la conducta delictiva sobre determinados bienes jurídicos o el perjuicio causado a las víctimas; y, en el caso de que se opte por solo utilizar el criterio de la gravedad de la pena, entendiendo que la pena de prisión es la más grave que cabe imponer, ¿cuántos años de prisión como mínimo deben poder imponerse para considerar que el delito es grave?

La cuestión no es baladí en el sistema penal español, pues la legislación aplicable puede inducir a diferentes interpretaciones. Según el artículo 33.2 del Código Penal, son penas graves la prisión permanente revisable y la prisión superior a cinco años, entre otras. Pero conforme al artículo 588 *ter a* de la LECrim, que se remite al 579.1 del mismo texto legal, para precisar los delitos que pueden investigarse con este tipo de diligencias, fija el umbral mínimo de tres años de prisión. Una parte de la doctrina, que considero más razonable, entiende que, para fijar la gravedad de un delito en materia de cesión de datos, también deben utilizarse otros criterios como las circunstancias concretas de la conducta delictiva y el perjuicio causado a las víctimas[14].

El TJUE, empero, entiende que la mencionada cuestión prejudicial planteada por la Audiencia Provincial de Tarragona tiene por objeto apreciar si la norma nacional en la que se basa la solicitud de la policía judicial persigue un objetivo que puede justificar una injerencia en los derechos fundamentales a la vida priva y familiar y a la protección de datos de carácter personal[15], y no entra en determinar qué debe entenderse por delincuencia grave como criterio ponderativo. Parece pues que deja a la normativa y jurisprudencia interna de los Estados miembros la determinación de esta cuestión.

Así las cosas, sin perjuicio de que también deberían tenerse en cuenta otras circunstancias, delito grave en el sistema penal español es el que impone una pena grave, que según el artículo 33.2 del Código Penal es la de prisión superior

12. STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 26: «1) ¿La suficiente gravedad de los delitos como criterio que justifica la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta puede identificarse únicamente en atención a la pena que pueda imponerse al delito que se investiga o es necesario, además, identificar en la conducta delictiva particulares niveles de lesividad para bienes jurídicos individuales y/o colectivos?; 2) En su caso, si se ajustara a los principios constitucionales de la Unión, utilizados por el [Tribunal de Justicia] en su sentencia de 8 de abril de 2014 [Digital Rights Ireland y otros, C 293/12 y C 594/12, EU:C:2014:238] como estándares de control estricto de la Directiva, la determinación de la gravedad del delito atendiendo solo a la pena imponible ¿cuál debería ser ese umbral mínimo? ¿Sería compatible con una previsión general de límite en tres años de prisión?».
13. STJUE (Gran Sala), 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C 203/15 y C 698/15, EU:C:2016:970), apartado 103.
14. J. L. Rodríguez Lainz (2012); L. Vázquez Seco (2017, págs. 19-24); J. Ortiz Pradillo (2017); y M. Bahamonde Blanco (2018); J. Pérez Gil (2019). La misma problemática la plantea M. Marchena Gómez (2014) en la ponencia presentada en el Observatorio de Derecho Penal Económico 2014.
15. STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 49: «la petición de decisión prejudicial no tiene por objeto determinar si los datos personales de que se trata en el litigio principal han sido conservados por los proveedores de servicios de comunicaciones electrónicas de conformidad con los requisitos establecidos en el artículo 15, apartado 1, de la Directiva 2002/58, interpretado a la luz de los artículos 7 y 8 de la Carta». En este sentido, J. L. Rodríguez Lainz (2018).

a cinco años. Por tanto, los delitos dolosos castigados con pena con límite máximo de, al menos, tres años de prisión e inferior a cinco años de prisión, cuya investigación también admite una diligencia de acceso y obtención de datos personales obrantes en archivos automatizados de los prestadores de servicios, no tiene la consideración de delito grave, pues están castigados con penas menos graves según el artículo 33.3 del Código Penal. En consecuencia, parece, a simple vista, que si se investigan estos últimos delitos no se debe autorizar la diligencia de investigación, al no estar fundada esta en un tipo de delincuencia considerada grave[16]. De ahí surge la siguiente pregunta.

3.3. ¿El juez de instrucción únicamente puede autorizar la obtención de datos personales electrónicos conservados por prestadores de servicios de comunicaciones cuando se estén investigando delitos graves?

De lo expuesto hasta este momento, se podría concluir que la única posibilidad que tiene un juez de instrucción para autorizar esta diligencia es cuando la obtención de los datos personales electrónicos represente una injerencia grave en los derechos fundamentales y se encuentre justificada por la gravedad del hecho delictivo. Esto es lo mismo que decir que siempre que el delito sea considerado grave el juez de instrucción debe autorizar esta diligencia de obtención de datos personales, con independencia de que la injerencia en los derechos fundamentales sea grave o no. Nadie puede poner en duda esta premisa, pues así debe acordarlo el juez en todo caso. Cabe preguntarse, empero, por qué es importante saber cuándo una obtención de datos representa una injerencia grave en los derechos fundamentales, pues parece que lo transcendente a tales efectos es fijar la gravedad del delito. La importancia surge, como se tendrá ocasión de comprobar en el siguiente apartado, cuando se solicita esta diligencia sumarial en procesos penales en los que se persiguen delitos que no son graves, casos muy habituales y donde se precisan tales diligencias de investigación por el amplio uso de la telefonía móvil y de la tecnología en la sociedad. Esto provoca que presuntos hechos delictivos no puedan llegar a ser esclarecidos dado que la única diligencia posible para acreditarlos es la obtención de datos electrónicos conservados por prestadores de servicios.

La respuesta a la pregunta planteada es obviamente negativa. El juez de instrucción puede autorizar la obtención de datos personales electrónicos conservados por prestadores de servicios de comunicaciones electrónicas en los procesos que se estén investigando delitos graves, motivándolo en la lucha contra la delincuencia grave. Ahora bien, no puede hacerlo únicamente en estos procesos penales por delitos graves, pues cuando se persiguen delitos que no son graves, si concurren los criterios que analizaremos a continuación, también puede autorizar este tipo de diligencias de investigación.

4. Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales por delitos no graves

Ha quedado claro, de lo expuesto hasta este momento, que una injerencia grave en los derechos fundamentales previstos en los artículos 7 y 8 de la Carta, causada por una solicitud policial o de fiscalía de acceso y obtención de datos personales conservados por prestadores de servicios de comunicaciones electrónicas, solo puede justificarse en la persecución, investigación o descubrimientos de delincuencia grave. Ahora bien, también es posible que esta clase de diligencias de investigación se soliciten en procesos penales por delitos no graves y cabe examinar si es posible su autorización, sin perder de vista, de entrada, que si esta solicitud comporta una injerencia grave en los derechos a la vida privada y familiar o a la

16. Esto es lo que sucedió en la investigación de un robo con violencia de un teléfono móvil que da origen a la cuestión prejudicial planteada por la Audiencia Provincial de Tarragona, resuelta por la STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788): ante la solicitud de la policía judicial de que se ordenase a determinados proveedores de servicios de comunicaciones electrónicas la transmisión de los números de teléfono activados, desde el 16 de febrero hasta el 27 de febrero de 2015, con el código IMEI del teléfono móvil sustraído, así como el nombre, apellidos y dirección de los números de teléfono correspondientes a las tarjetas SIM activadas con dicho código, el juez de instrucción denegó la diligencia considerando que esta cesión de datos se limita a los delitos graves, y los hechos presuntos del caso no eran constitutivos de tal tipo de delito.

protección de datos de carácter personal, el juez no la podrá autorizar, pues los hechos delictivos no revisten la gravedad suficiente para motivar la injerencia grave en los derechos fundamentales, de acuerdo con el principio de proporcionalidad. Pero ¿qué ocurre cuando la injerencia en los derechos fundamentales puede considerarse como no grave?

Cabe recordar, llegados a este punto, que una de las excepciones al principio de confidencialidad de las comunicaciones electrónicas, que permite el acceso de las autoridades públicas a los datos conservados por los proveedores de las comunicaciones electrónicas, establecidas con carácter exhaustivo en el artículo 15 de la Directiva 2002/58[17], se refiere al objetivo de la prevención, investigación, descubrimiento y persecución de delitos[18]. Pues bien, este artículo no limita el acceso de las autoridades públicas a datos de carácter personal en los supuestos de persecución de delitos graves, sino que lo permite cuando se trate de cualquier tipo de delito, sea grave o no lo sea[19].

De ahí que cuando la policía judicial solicita al juez de instrucción el acceso y obtención de datos personales electrónicos conservados por prestadores de servicios de comunicaciones, si el contenido de esta solicitud puede ser calificado como una injerencia no grave de los derechos fundamentales a la vida privada y familiar y a la protección de datos de carácter personal, el juez puede autorizarlo, justificándolo en la prevención, investigación, descubrimiento y persecución de delitos, incluso cuando estos no sean graves. Así lo ha reconocido el TJUE: «En cambio, cuando la injerencia que implica dicho acceso no es grave, puede estar justificada por el objetivo de prevenir, investigar, descubrir y perseguir "delitos" en general»[20].

En concreto, en un apartado anterior hemos señalado supuestos de acceso y obtención de datos de carácter personal conservados por proveedores de servicios de comunicaciones electrónicas, considerados por el TJUE como injerencias graves de los derechos fundamentales garantizados en los artículos 7 y 8 de la Carta. En el mismo sentido, el TJUE indica casos en que tal solicitud de acceso y obtención de datos no tendrá la consideración de injerencia grave sino una mera injerencia en los derechos fundamentales: cuando se solicita identificar a los titulares de las tarjetas SIM activadas durante un determinado período de tiempo con el número IMEI de un concreto teléfono móvil, con objeto de tener los datos personales o de filiación de los titulares de dichas tarjetas, como su nombre, apellidos y dirección.

Ahora bien, la jurisprudencia española ha entendido que este tipo de diligencias de identificación de SIM y número IMEI no implica obtener datos vinculados a un proceso de comunicación, por lo que no comportaría vulneración del derecho a la intimidad o al secreto de las comunicaciones, de forma que su autorización no precisa resolución judicial motivada, y así se ha establecido en el artículo 588 *ter m* LECrim[21]. Parece, por tanto, que existe una contradicción evidente entre la doctrina del TJUE, que considera este tipo de acceso a datos personales como una injerencia no grave de los derechos fundamentales a la protección de datos de carácter personal y a la vida privada y familiar, y el sistema español, lo que hace surgir la duda sobre si el artículo 588 *ter m* LE-Crim es conforme al derecho de la Unión Europea. A mi juicio, pese a que la injerencia no es grave, sigue siendo una vulneración de los derechos fundamentales de los ciudadanos que debe precisar de autorización judicial, pues motivos de eficiencia judicial, esto es, el gran número de diligencias que deban autorizar los jueces provocando gran volumen de trabajo para los juzgados de instrucción, no puede justificar una injerencia en derechos fundamentales sin resolución judicial, aunque tenga la consideración de no grave.

17. «Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas» (Directiva sobre la privacidad y las comunicaciones electrónicas). DOCE (31 de julio de 2002), L 201/37.
18. Sobre el carácter exhaustivo de tales objetivos, ver la STJUE (Gran Sala), 21 de diciembre de 2016, Tele2 Sverige y Watson y otros (C 203/15 y C 698/15, EU:C:2016:970), apartados 90 y 115.
19. Así lo ha interpretado el TJUE en su sentencia (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 53.
20. STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartado 57.
21. STS (Sala de lo Penal, Sección 1.ª) núm. 492/2010 de 18 mayo (RJ 2010\5814); STS (Sala de lo Penal, Sección 1.ª), núm. 1344/2009 de 16 diciembre (RJ 2010\308), entre otras. Para un análisis en profundidad véase A. Peralta Gutiérrez y P. Aguirre Allende (2019). En cambio, J. L. Rodríguez Laiz (2019) considera que no se producen comunicaciones electrónicas cuando se obtiene información sobre la asociación entre terminal físico y tarjeta SIM.

Lo que se deja claro es que esta injerencia no grave en ningún caso puede comportar conocer las comunicaciones efectuadas con el teléfono móvil ni su localización, pues en este último caso estaríamos ante una injerencia grave de los derechos fundamentales mencionados, cuya autorización judicial solo cabe realizarse para la investigación o descubrimiento de delitos graves. En este sentido, toda petición de obtención de datos de carácter personal que no comporte «extraer conclusiones precisas sobre la vida privada de las personas cuyos datos se ven afectados»[22], puede autorizarse al representar una injerencia no grave en los derechos fundamentales de los artículos 7 y 8 de la Carta. Si estamos ante este tipo de injerencias no graves, el juez de instrucción puede autorizar motivadamente la diligencia de investigación solicitada, aunque el delito objeto de investigación no sea grave. Por tanto, la falta de gravedad del delito no puede justificar, por sí sola, la no autorización judicial de estas diligencias.

5. Conclusiones: juicio de proporcionalidad del juez de instrucción

Es preciso sentar, antes de incidir en la proporcionalidad que debe apreciar el juez, que cuando una autoridad pública, como la policía judicial o el fiscal, pretenda acceder a datos personales conservados por proveedores de servicios de comunicaciones electrónicas, justificándolo en la investigación de algún delito, precisará en todo caso de autorización judicial, por lo que, en caso de practicar tal diligencia sin la oportuna resolución judicial, la parte afectada podrá alegar la ilicitud de la prueba en juicio oral por obtención de prueba vulnerando derechos fundamentales.

Así las cosas, cabe concluir que lo importante para poder decidir si se debe autorizar el acceso y obtención de datos personales conservados por proveedores de servicios de comunicaciones electrónicas es el juicio de proporcionalidad que debe realizar el juez de instrucción, valorando, de un lado, la gravedad de la injerencia en los derechos fundamentales y, de otro, la gravedad de los hechos delictivos. Solo así se podrá tener en cuenta el nivel de afectación o injerencia en los derechos fundamentales relacionados con la protección de datos de carácter personal y con la vida privada y familiar en el ámbito de la confidencialidad de las comunicaciones.

En efecto, lo primero que debe hacer el juez es determinar si la diligencia concreta de acceso a datos personales electrónicos que solicita la policía judicial o la fiscalía, a efectos de la investigación de un delito, debe considerarse una injerencia grave en los derechos fundamentales reconocidos en los artículos 7 y 8 de la Carta, o si no reviste tal gravedad; y, una vez determinada la gravedad de la injerencia, es preciso fijar si la delincuencia objeto de investigación es grave o no. Debe realizar tal juicio de proporcionalidad, pues el juez de instrucción únicamente puede autorizar una diligencia de investigación que suponga una injerencia grave en los derechos fundamentales cuando los hechos objeto de investigación puedan tener la consideración de delito grave. Si se trata de un delito que no revista tal gravedad y la diligencia comporta una injerencia grave en los derechos fundamentales, no cabrá autorizar su práctica.

Así parece indicarlo el mismo artículo 588 *ter j* de la LECrim, cuando establece que la solicitud de la diligencia de investigación debe precisar «la naturaleza de los datos que hayan de ser conocidos y las razones que justifican la cesión», pues «la naturaleza de los datos» servirá para valorar la gravedad de la injerencia en los derechos fundamentales y «las razones de la cesión» determinará el nivel de gravedad de los hechos delictivos. Con estos extremos, el juez puede realizar el juicio de proporcionalidad para decidir si autoriza o no la diligencia de investigación.

Se observa que es importante valorar cuándo la injerencia en los derechos fundamentales no es grave o cuándo reviste una especial gravedad. El TJUE, como se ha tenido ocasión de comprobar, ha ido señalando supuestos concretos de injerencia grave y no grave. En este sentido, ha entendido que cuando se solicita identificar a los titulares de las tarjetas SIM activadas durante un determinado período de tiempo con el número IMEI de un concreto teléfono móvil, con el objeto de tener los datos personales o de filiación de los titulares de dichas tarjetas, como su nombre, apellidos y dirección, no se trata de una injerencia grave en los derechos fundamentales. En estos casos, el artículo 588 *ter m* LECRim no exige

22. STJUE (Gran Sala), de 2 de octubre de 2018 (C-207/16, EU:C:2018:788), apartados 59, 60 y 62.

resolución judicial motivada para acceder a estos datos, cosa que parece contradictoria con la interpretación del TJUE y hace surgir dudas sobre si esta regulación es conforme con el derecho de la Unión Europea. Pese a que la injerencia en los derechos fundamentales no es grave, no deja de ser una injerencia, de forma que su práctica precisa autorización judicial, pues motivos de eficiencia judicial, como son el gran número de estas diligencias que deban autorizar los jueces, las cuales aumentarían su volumen de trabajo, no pueden justificar una injerencia en derechos fundamentales sin resolución judicial, aunque tenga la consideración de injerencia no grave.

En consecuencia, como se ha tenido ocasión de comprobar, cuando el juez entienda que la injerencia en los derechos fundamentales a la vida priva y familiar o a la protección de datos de carácter personal no es grave, puede autorizar la diligencia de acceso y obtención de datos con el objeto de prevenir, descubrir, investigar o perseguir delitos en general, sin necesidad de valorar la gravedad de los hechos delictivos; en cambio, cuando se trate de injerencias graves en los derechos a la vida privada y familiar y a la protección de datos de carácter personal, tal injerencia solo puede fundamentarse en la persecución, descubrimiento, prevención o investigación de delitos graves. Ahora bien, la falta de gravedad del delito no puede justificar, por sí sola, la no autorización judicial de una de estas diligencias de investigación.

Referencias bibliográficas

ARMENTA DEU, T. (2018). «Regulación legal y valoración probatoria de fuentes de prueba digital (correos electrónicos, WhatsApp, redes sociales): entre la insuficiencia y la incertidumbre». *IDP. Revista de Internet, Derecho y Política,* núm. 27, págs. 67-79. https://doi.org/10.7238/idp.v0i27.3149

BAHAMONDE BLANCO, M. (2018). «Medidas de investigación tecnológica a la luz de los Derechos Fundamentales, una cuestión pendiente». *Diario La Ley*, núm. 9.160.

COLOMER HERNÁNDEZ, I. (2018). «La cesión de datos de las comunicaciones electrónicas para su uso en investigaciones criminales: una problemática en ciernes». En: F. JIMÉNEZ CONDE (dir.). *Adaptación del Derecho Procesal español a la normativa europea y a su interpretación por los tribunales*. Valencia: Tirant lo Blanch, págs. 77 y sigs.

DELGADO MARTÍN, J. (2019). «Protección de datos y prueba en el proceso». *Diario La Ley,* núm. 9.383.

FRÍAS MARTÍNEZ, E. (2019). «Obtención de datos personales en procesos penales y administrativos». *Diario La Ley,* núm. 9.404.

GONZÁLEZ CANO, M.ª I. (2019). «Cesión y tratamiento de datos personales en el proceso penal. Avances y retos inmediatos de la Directiva (UE) 2016/680» [en línea]. *Revista Brasileira de Direito Processual Penal, Porto Alegre*, núm. 3(5), págs. 1.331-1.384. https://doi.org/10.22197/rbdpp.v5i3.279.

GUDÍN RODRÍGUEZ-MAGARIÑOS, A. E. (2017). «La protección de datos en el tratamiento procesal de los dispositivos de almacenamiento masivo de información». *La Ley Penal*, núm. 125.

MARCHENA GOMEZ, M. (2014). «El futuro de las diligencias probatorias relacionadas con las nuevas tecnologías de la información y la comunicación, a partir de los contenidos del Borrador de Código Procesal Penal» [en línea]. *Observatorio de Derecho Penal Económico 2014*. Madrid: Universidad Rey Juan Carlos- KPMG. http://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAUszEONTtbLUouLM_DxbIwNDEwNzQwuQQGZapUtckhlQaptWmJOcSoAPL5kezUAAAA=WKE [Fecha de consulta: 14 de marzo de 2020].

ORTIZ PRADILLO, J. (2017). «Comunicaciones, tecnología y proceso penal: viejos delitos, nuevas necesidades». En: J. M. ASENCIO MELLADO (dir.). *Justicia penal y nuevas formas de delincuencia.* Valencia: Tirant lo Blanch, págs. 23-28.

PERALTA GUTIÉRREZ, A.; AGUIRRE ALLENDE, P. (2019). «El TJUE y el acceso a los datos de abonado en el seno de la instrucción penal». *Diario La Ley*, núm. 9.420.

PÉREZ GIL, J. (2019). «Exclusiones probatorias por vulneración del derecho a la protección de datos personales en el proceso penal». En: F. JIMÉNEZ CONDE; F. BELLIDO PENADÉS (dirs.). *Justicia: ¿garantías versus eficiencia?* Valencia: Tirant lo Blanch, págs. 399 y sigs.

RICHARD GONZÁLEZ, M. (2018). «La conservación y utilización de datos de las comunicaciones en la investigación criminal. Problemas que resultan de la aplicación de la doctrina del TJUE». En: F. JIMÉNEZ

CONDE (dir.). *Adaptación del Derecho Procesal español a la normativa europea y a su interpretación por los tribunales.* Valencia: Tirant lo Blanch, págs. 475 y sigs.

RODRÍGUEZ LAINZ, J. L. (2012). «Hacia un nuevo entendimiento de gravedad del delito en la Ley de conservación de datos relativos a las comunicaciones electrónicas». *Diario La Ley*, núm. 7.789.

– (2018). «El régimen legal español en materia de conservación y cesión de datos para la investigación de delitos». *Diario La Ley,* núm. 9.291, Sección Doctrina.

SÁNCHEZ RUBIO, A. (2018). «La necesaria adecuación del derecho interno a la normativa europea sobre tratamiento de datos de las comunicaciones electrónicas en la investigación penal». En: F. JIMÉNEZ CONDE (dir.). Adaptación del Derecho Procesal español a la normativa europea y a su interpretación por los tribunales. Valencia: Tirant lo Blanch, págs. 506 y sigs.

VÁZQUEZ SECO, L. (2017). «Incorporación de datos al proceso. Vigencia de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a redes públicas e interpretación de la ley a la luz de la reforma operada por la LO 13/2015». Madrid: Centro de Estudios Jurídicos. Universidad Complutense de Madrid, págs. 19-24.

Cita recomendada

OROMÍ I VALL-LLOVERA, Susanna (2020). «Acceso a datos personales conservados por proveedores de servicios de comunicaciones electrónicas en investigaciones penales según el Tribunal de Justicia de la UE». *IDP. Revista de Internet, Derecho y Política*. N.º 31. UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i31.3206

Sobre la autora

Susanna Oromí i Vall-llovera
soromi@uoc.edu
Universitat de Girona

Licenciada en Derecho (1996) y doctora en Derecho (2000) por la Universitat de Girona. Ha sido becaria FI de la Generalitat de Catalunya y profesora ayudante, también en la Universitat de Girona. Ha realizado estancias de investigación predoctoral en el Institut für Bürgerliches Recht und Zivilprozeβrecht (Universidad de Múnich, Alemania) y posdoctoral en la Universidad Paris X-Nanterre. En la actualidad es profesora titular de Derecho Procesal y directora del Departamento de Derecho Público de la Universitat de Girona. Asimismo, forma parte del Grup de Recerca Consolidat de la Generalitat de Catalunya «Cuestiones actuales de Derecho Procesal», y centra su investigación en la Administración de Justicia y en los procesos civil y penal. Entre sus publicaciones destacan: El ejercicio de la acción popular o Intervención voluntaria de terceros en el proceso civil. Ha sido coordinadora científica del proyecto europeo financiado por la Comisión Europea (Action grant, sobre «The protection of the victims in the European criminal justice systems»), además de haber participado activamente, como IP o como miembro, en más de una decena de proyectos de investigación nacionales y europeos.

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

www.uoc.edu/idp

ARTÍCULO

La desconexión digital de los trabajadores. Reflexiones a propósito de su calificación como derecho y su instrumentación

David Gutiérrez Colominas
Universitat Autònoma de Barcelona

Fecha de presentación: julio de 2019
Fecha de aceptación: diciembre de 2019
Fecha de publicación: mayo de 2020

Resumen

La desconexión digital ha sido regulada en la reciente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, como un derecho reconocido legalmente de los trabajadores en aras de garantizar el respeto del tiempo de descanso. Sin embargo, su contenido no ha sido definido por el legislador y traslada esta responsabilidad a los agentes sociales y a los empleadores, quienes, a través de la negociación colectiva y la elaboración de políticas empresariales internas, están llamados a desempeñar un papel fundamental en la configuración y exigencia de este nuevo derecho. Ante tal escenario, este artículo aborda si la calificación como derecho ofrece una solución ajustada al propósito que se persigue con la desconexión digital, añadiendo además un análisis crítico del papel que desempeñan la negociación colectiva, la representación de los trabajadores y los empresarios, así como sus implicaciones jurídicas, en la regulación de la desconexión digital.

Palabras clave

desconexión digital, representación de los trabajadores, negociación colectiva, política interna empresarial, tiempo de trabajo

Tema

Derecho del Trabajo

The digital disconnection of workers. Reflections concerning its description as a right and its implementation

Abstract

Digital disconnection was regulated in the recent Organic Law 3/2018, of December 5, on Protection of Personal Data and Guarantee of Digital Rights, as a legally recognised right for the workers in order to guarantee observance of rest times. However, its content has not been defined by the legislator, and transfers this responsibility to social agents and employers, who, through collective negotiation and the production of internal business policies, are called upon to play a fundamental role in the configuration and requirements of this new law.

In the light of these circumstances, this article addresses whether the description as a right offers a solution adjusted to the proposal that is pursued with digital disconnection, also adding a critical analysis of the part that collective negotiation and the representation of workers and business owners plays, as well as the legal implications of this in the regulation of digital disconnection.

Keywords

digital disconnection, representation of the workers, collective negotiation, internal business policy, work time

Subject

Labour Law

Introducción

Las tecnologías de la información y la comunicación (TIC) nacieron para facilitar el intercambio de información y las conexiones interpersonales, si bien han generado nuevas amenazas para la salud de la especie humana, concretadas en la sobreexposición a un exceso de información, o infoxicación[1]. La sobrecarga informativa es el precio que pagamos por integrar las ventajas de la tecnología en nuestras vidas, pero el problema se agrava por la expansión descontrolada de las TIC en el ámbito laboral. En este sentido, el informe «Working anytime, anywhere: The effects on the world of work» pone de manifiesto que uno de cada tres trabajadores utiliza las TIC para realizar tareas relacionadas con su trabajo fuera del horario laboral[2]. Esta circunstancia evidencia la existencia de solapamientos entre tiempo de trabajo y tiempo de descanso que hace resurgir una cuestión clásica del Derecho del Trabajo[3]: la protección de la seguridad y la salud.

Sin embargo, desde una perspectiva europea, no hay previsión de regular este fenómeno. No existe a día de hoy propuesta alguna de reglamento o directiva que pretenda ofrecer una solución común en la UE a la conciliación de la vida laboral tecnológica y familiar. No obstante, la protección de los riesgos que generan las TIC se halla incardinada actualmente en dos grandes líneas de actuación: la delimitación del tiempo de trabajo, prevista en 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 y la protección de la salud y seguridad en el trabajo al amparo de la Directiva 89/391/CEE del Consejo, de 12 de junio de 1989, referente a la aplicación de medidas para promover la mejora de la seguridad y de la salud de los trabajadores en el trabajo. Cuestiones como los períodos de descanso diarios y semanales (artículos 3 y 5 de la Directiva 2003/88/CE) y la definición de los límites máximos de tiempo de trabajo (artículo 6 de la Directiva 2003/88/CE), así como la necesidad de que el empresario consulte con los representantes de los trabajadores la introducción de nuevas tecnologías (artículo 6.3.c de la Directiva 89/391/CE) y ofrezca la formación adecuada para esta (artículo 12 de la Directiva 89/391/CE), constituyen el marco de protección actual frente a los riesgos tecnológicos de las TIC.

A nivel nacional, se evidencia un escenario en el que los países han tomado conciencia de la importancia de esta cuestión. Así, por ejemplo, Francia ha sido el primero en legislar explícitamente sobre este fenómeno[4], tendencia a la que se ha sumado Italia[5], si bien otros países también han procurado incrementar la protección contra los riesgos derivados del trabajo con las TIC mediante la regulación legal del teletrabajo[6].

1. Alemán Páez, F. (2017). «El derecho a la desconexión digital. Una aproximación conceptual, crítica y contextualizadora al hilo de la *Loi Travail* N.o 2016-1088». *Trabajo y Derecho*, vol. 30, págs. 3 a 6.
2. Eurofound and the International Labour Office, «Working anytime, anywhere: The effects on the world of work», Publications Office of the European Union, Luxembourg, and the International Labour Office, Ginebra, 2017, pág. 4, que identifica este fenómeno bajo las siglas «T/ICTM» y lo define como: «[...] use of information and communications technologies (ICT), such as smartphones, tablets, laptops and/or desktop computers, for work that is performed outside the employer's premises».
3. García-Perrote Escartín, I.; Mercader Uguina, J. R. (2016). «El permanente debate sobre la jornada laboral: una cuestión clásica (reducción del tiempo de trabajo) y otra reciente (el derecho a la desconexión del trabajo)». *Revista de información laboral*, vol. 10, pág. 7; Molina Navarrete, C. (2017). «Jornada laboral y tecnologías de la infocomunicación... "desconexión digital"...», *op. cit., Temas laborales: Revista andaluza de trabajo y bienestar social,* vol. 138, pág. 255; Tascón López, R. (2018). «El derecho de desconexión del trabajador (potencialidades en el ordenamiento español». *Trabajo y Derecho*, núm. 41, págs. 1-3.
4. El artículo L2242-8 del Code du Travail, que fue modificado por la Loi 2016-1088 de 8 de agosto de 2016, introdujo el droit à la déconnexion, que surge con el objetivo de garantizar a los trabajadores la conciliación de la vida laboral y familiar. Para un estudio en profundidad, véase Alemán Páez, F. (2017). «El derecho a la desconexión digital...», op. cit., págs. 9-18; y Cialti, P. (2017). «El derecho a la desconexión en Francia: ¿más de lo que parece?». Temas laborales: Revista andaluza de trabajo y bienestar social, núm. 137, págs. 163-181.
5. Taléns Visconti, E. E. (2018). «La desconexión digital en el ámbito laboral: un deber empresarial y una nueva oportunidad de cambio para la negociación colectiva». Información Laboral, vol. 4, págs. 8-9.
6. Tal y como señala el informe Eurofound and the International Labour Office, «Working anytime, anywhere: The effects on the world of work», Publications Office of the European Union, Luxembourg, and the International Labour Office, Ginebra, 2017, págs. 45-51, Suecia, el Reino Unido y Holanda han optado por implementar una sólida regulación del teletrabajo. Ahora bien, también existen otros países que han preferido trasladar esta responsabilidad al diálogo social, como por ejemplo Alemania o Finlandia, entre otros.

España también se incluye dentro del reducido número de países que han decidido regular el derecho a la desconexión digital de los trabajadores. Concretamente, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LO 3/2018) incluye la regulación del citado derecho en el marco del artículo 88, que en virtud de la Disposición Final 13 LO 3/2018 ha introducido el artículo 20.bis en el 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, TRLET), que consta de tres apartados, de innegable inspiración francesa[7]. El primero de ellos afirma la existencia de un derecho a la desconexión digital de los trabajadores fuera del tiempo de trabajo legal, con el objetivo de garantizar el respeto del tiempo de descanso, así como la intimidad personal y familiar. La segunda sección flexibiliza la configuración del derecho, atendiendo a la naturaleza y objeto de la relación laboral, introduciendo la intervención de la negociación colectiva o, en su defecto, los pactos entre empresa y representantes de los trabajadores. Por último, el tercer apartado obliga a los empleadores a elaborar una política interna en materia de desconexión digital, estableciendo las modalidades del ejercicio de este derecho y las acciones de formación y de sensibilización de los dispositivos tecnológicos, con especial atención a aquellos casos en los que el trabajo se desarrolle a distancia o en el domicilio de la persona trabajadora.

Así, este estudio parte de la hipótesis de que la protección europea de los riesgos derivados del uso de las TIC no se halla actualizada, y que, en consecuencia, la intervención nacional se convierte en absolutamente necesaria para garantizar la protección de la salud de los trabajadores. Por lo tanto, el objetivo de esta contribución consiste en examinar la eficacia y efectividad de la configuración española mediante el estudio de dos aspectos claves: los efectos de su regulación como derecho y el papel de los sujetos que intervienen en la configuración de las modalidades de ejercicio de este derecho. Para ello, se analizará si la desconexión digital es un derecho de los trabajadores o una obligación empresarial, así como la eficacia de su configuración, valorando críticamente el papel conferido a la negociación colectiva, la representación de los trabajadores y la autonomía empresarial.

1. La desconexión digital: ¿derecho de los trabajadores u obligación de los empleadores?

Como ya se ha puesto de relieve, la desconexión digital surge como una necesidad ante las consecuencias negativas derivadas del uso de la tecnología que, traspasando la frontera de lo laboral, afectan especialmente a la esfera personal. En el ámbito español, el artículo 88.1 de la LO 3/2018 se ha encargado de plasmar esta cuestión sobre la base de la construcción de un derecho a la desconexión digital de los trabajadores que obedece a la necesidad de garantizar el respeto de su tiempo de descanso, permisos y vacaciones, así como su intimidad personal y familiar.

Sin ánimo de analizar el contenido del derecho, materia esta ya abordada en diversas ocasiones por la doctrina[8], el aspecto sobre el que conviene detenerse es si la categorización de la desconexión digital como un derecho se ajusta al propósito de la norma, o, en otras palabras, si ofrece más garantías que su conceptualización como obligación empresarial. La clasificación como derecho u obligación a la desconexión digital de los trabajadores es una cuestión de una importancia capital, ya que su incardinación en una u otra categoría conlleva distintas implicaciones, tanto en su construcción como en su exigencia.

En efecto, la designación como derecho, que es la tesis mayoritaria adoptada por los distintos legisladores que

7. Baylos Grau, A. (2019). «El derecho a la privacidad en el trabajo en la nueva Ley Orgánica de Protección de Datos: una mala regulación». *Ciudad del Trabajo*, vol. 14, pág. 8, entre muchos otros.
8. Molina Navarrete, C. (2017). «Jornada laboral...», *op. cit.*, págs. 270-274; Igartua Miró, M. 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, vol. 432, págs. 66-71; Tascón López, R. (2018). «El derecho de desconexión...», *op. cit.*, págs. 5-15; Vallecillo Gámez, M. R. (2018). «El derecho a la desconexión, ¿novedad digital o esnobismo del viejo derecho al descanso?». *Estudios financieros. Revista de trabajo y seguridad social: Comentarios, casos prácticos: recursos humanos,* vol. 418, págs. 174-175; Serrano Argüeso, M. (2019). «*Always on.* Propuestas para la efectividad del derecho a la desconexión digital en el marco de la economía 4.0». *Revista Internacional y Comparada de Relaciones laborales y derecho del empleo*, vol. 7, núm. 2, págs. 182-189.

han regulado la desconexión digital, reconoce la facultad de cualquier trabajador a desconectarse digitalmente de sus obligaciones laborales fuera del horario de trabajo. El planteamiento ofrece, pues, una libertad en su ejecución. Dicho de otra manera, la categoría de derecho no vela por exigir en cualquier caso la desconexión digital, sino por un reconocimiento que no se acompaña de ningún tipo de obligación empresarial. Ello tiene una implicación clave: otorga una cierta libertad para reclamar o no su cumplimiento. Libertad esta que se halla limitada enormemente por la posición de inferioridad propia de cualquier persona trabajadora en el marco de una relación laboral, a lo que debe sumarse el correspondiente riesgo de sufrir represalias por el ejercicio del derecho.

Esta circunstancia, que puede ser considerada como menor, tiene importantísimas consecuencias a nivel práctico que, en mi opinión, no son coherentes con la finalidad de garantizar una efectiva implementación de la desconexión digital de los trabajadores. La estandarización de la desconexión digital y la lucha frente a los riesgos que supone para las personas dejan de ser una responsabilidad de los poderes públicos y se traslada a los propios trabajadores. Los efectos de este planteamiento son devastadores para su cumplimiento efectivo, ya que no se contemplan medidas o sanciones derivadas del incumplimiento de este derecho. En consecuencia, el planteamiento legal adoptado pivota sobre la voluntad del trabajador.

Por el contrario, abordar la desconexión digital como una obligación empresarial reivindicaría, en mi opinión, un planteamiento basado en el carácter imperativo no disponible con el que debe abordarse este fenómeno. Los riesgos que la permanente conexión tecnológica genera para la salud de los trabajadores exigen una actuación normativa que impida que las personas empleadoras puedan requerir una conexión permanente con el entorno de trabajo. Y la forma más efectiva de introducir este enfoque transita en torno al establecimiento de una prohibición empresarial que constate explícitamente la imposibilidad de que el empresario pueda ordenar la utilización o consulta de medios digitales fuera del tiempo de trabajo. Es cierto que la plasmación como derecho exige como contrapartida un deber empresarial de respeto, pero la exigencia siempre vendrá motivada por la reivindicación del titular del derecho, que puede verse coartada ante la posición contractual en la que se encuentra. El carácter imperativo de una obligación empresarial sería más acorde con la finalidad que persigue la implementación efectiva de la desconexión digital, ya que omite el carácter optativo del derecho —o la decisión de no ejercer este para evitar represalias empresariales— y lo transforma en una imposición normativa insalvable que admitiría un mayor control de su cumplimiento por parte de los poderes públicos.

Si trasladamos esta discusión al escenario legal español, se observa la debilidad del planteamiento normativo basado en la configuración de la desconexión digital como un derecho, más aún cuando su concreción se remite a la negociación colectiva y al poder de dirección empresarial (política interna), así como la conveniencia de reformularlo como obligación empresarial o ampliar su formulación mediante la constatación expresa del contenido obligacional desde el punto de vista empresarial. El artículo 88.1 de la LO 3/2018 ha seguido la estela de otros países y ha reconocido el derecho de los trabajadores a la desconexión digital, pero no ha acompañado su formulación con medidas dirigidas a garantizar su cumplimiento o, como mínimo, definiendo las implicaciones o límites empresariales para respetar el ejercicio de este derecho.

Esta circunstancia otorga a este precepto un carácter reactivo cuya activación solo se produce si la persona titular decide ejercer el derecho a la desconexión digital. En otras palabras, la norma no dota a este derecho de medidas que impidan de forma preventiva la producción de vulneraciones de este derecho, sino que plasma un reconocimiento sin contenido cuya infracción implica la judicialización del incumplimiento a instancia del trabajador, que podrá incluso optar por la extinción del contrato de trabajo *ex* artículo 50 del TRLET[9]. Tal planteamiento dificulta la materialización de la desconexión digital en el ámbito laboral, ya que no se procura una protección efectiva del derecho por parte de la norma, sino un mero reconocimiento sometido a la judicialización por parte del trabajador en caso de incumplimiento, y de ahí su carácter reactivo. Si a ello le añadimos que la defensa de los denominados derechos digitales no se acompaña de ningún tipo de garantía procesal que proteja a la persona trabajadora denunciante de

9. Sobre esta cuestión, véase el apartado 2.2.

la vulneración, más allá de los mecanismos ya existentes[10], nos encontramos ante un reconocimiento legal más cercano conceptualmente a un instrumento de *soft law* que a un derecho.

Ahora bien, existe un elemento que necesariamente debe introducirse en el marco de esta discusión: el posible carácter fundamental del derecho a la desconexión digital. En efecto, su calificación dentro de esta categoría ofrecería ciertas garantías que facilitarían la reivindicación del derecho a la desconexión digital por parte de los trabajadores[11] y reforzarían la conveniencia del planteamiento de la desconexión digital como derecho. La LO 3/2018 clasifica el derecho a la desconexión digital en el ámbito laboral como uno de los derechos digitales de los ciudadanos, al amparo del artículo 18.4 de la Constitución española[12]. Un examen a primera vista permitiría afirmar que nos encontramos ante un derecho fundamental, y de ahí la inclusión de su regulación en una ley orgánica.

Sin embargo, el propio artículo 1.b de la LO 3/2018, relativo al objeto de la ley, efectúa una distinción de interés, diferenciando entre la regulación del derecho fundamental a la protección de datos personales y la regulación de los derechos digitales, de conformidad con el mandato del artículo 18.4 de la Constitución española. Como puede advertirse, el legislador no acompaña la calificación «fundamentales» a la expresión «derechos digitales», hecho este que también puede apreciarse si acudimos a los preceptos concretos que regulan los distintos derechos[13]. *De facto*, el contenido del artículo 18.4 de la Constitución proclama la necesaria limitación legal del uso de la informática «para garantizar el honor y la intimidad personal y familiar» de los ciudadanos, pero en ningún caso reconoce explícitamente ninguno de los derechos digitales de la LO 3/2018. Así pues, no nos encontramos ante derechos de alcance constitucional, sino derivados de una limitación constitucional.

Es cierto que una lectura amplia del artículo 18.4 de la Constitución permitiría incardinar aquellos derechos digitales encaminados a defender alguno o varios de los tres bienes jurídicos constatados en el texto constitucional, pero el derecho a la desconexión digital quedaría excluido de tal categorización. El objeto de protección del derecho a la desconexión digital en el ámbito laboral pretende procurar principalmente el respeto del tiempo de descanso, permisos y vacaciones, constatándose además la intimidad personal y familiar en el marco del artículo 88.1 de la LO 3/2018. Sin embargo, esta última mención, que es la única conexión que presenta con el artículo 18.4 de la Constitución y habilitaría su calificación como fundamental, no es significativa. El objeto de protección del derecho se extiende a trabajador y empresario, y pretende proteger a aquel de injerencias derivadas de la relación laboral durante su tiempo de descanso, ostentando una escasa significación la protección a la intimidad personal y familiar, que aparecen como bienes jurídicos desconectados de la finalidad protectora principal del derecho.

En consecuencia, el derecho a la desconexión digital presenta una cierta base constitucional, justificada en la necesaria limitación legal del uso de la informática formulada en clave general *ex* artículo 18.4 de la Constitución española. No obstante, en mi opinión no merece la calificación de fundamental, si bien sería deseable, en tanto que el propio texto constitucional no lo reconoce explícitamente, y, de hecho, la incardinación como derechos fundamentales es especialmente restrictiva, solo reservada a los derechos constatados en el capítulo segundo del título primero, al amparo del artículo 53.1.

Ante la eficacia limitada del derecho a la desconexión en el ámbito laboral, aparece un argumento más para abogar por una reformulación hacia una obligación empresarial a la desconexión digital. El carácter de obligación empresa-

10. La garantía de indemnidad, surgida como manifestación del derecho a la tutela judicial efectiva (artículo 24.1 de la Constitución española), es la única protección que ostenta cualquier persona trabajadora frente a la adopción de medidas de represalia por la reclamación de la vulneración del derecho a la desconexión digital.
11. Así, a título de ejemplo, la existencia de un procedimiento específico para la tutela de los derechos fundamentales y libertades públicas en el marco de la Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social, que incluye la inversión de la carga de la prueba (artículo 181.2) o la posibilidad de solicitar una indemnización reparadora, es una de las principales ventajas que presenta la calificación del derecho a la desconexión digital como fundamental.
12. Véase el apartado V del preámbulo de la LO 3/2018.
13. Los derechos digitales se hallan regulados en los artículos 80 a 96 de la LO 3/2018, e incluyen desde la protección a la neutralidad de internet (artículo 80), el acceso universal a internet (artículo 81) y la seguridad digital (artículo 82) hasta el derecho al olvido en las búsquedas de internet (artículo 93), entre un total de trece derechos.

rial es más acorde con la finalidad preventiva que persigue la desconexión digital y con la perspectiva limitadora del artículo 18.4 de la Constitución Española, que pretende limitar legalmente la utilización de la informática en pro de una serie de bienes jurídicos. Y es precisamente en el carácter de limitación legal donde una obligación empresarial a la desconexión digital de sus trabajadores encuentra su razón de ser; no nos encontramos ante una facultad, sino ante una necesidad, por razones de salud y seguridad en el trabajo, de limitar la sobreexposición a los dispositivos digitales, limitación esta que cuenta con el apoyo constitucional del artículo 18.4 de la Constitución. Por lo tanto, sería conveniente suprimir el carácter optativo propio del derecho a la desconexión digital e integrar una obligación empresarial que impida al empresario el ejercicio de cualquier manifestación del poder directivo por medios digitales fuera de la jornada laboral, cuyo incumplimiento debe ser controlado y sancionado por la autoridad pública, desplazando a un segundo plano el papel de la reclamación del trabajador.

2. Los instrumentos de regulación del derecho a la desconexión digital de los trabajadores

La configuración del derecho a la desconexión digital de los trabajadores no es de origen legal, sino que se reserva a la negociación colectiva, a la iniciativa empresarial y, en menor medida, a la representación de los trabajadores. El contenido de la LO 3/2018 se ha encargado de reservar un papel especial a la representación de los trabajadores y a la negociación colectiva en relación con el derecho a la desconexión digital, olvidando a otros sujetos[14]. Tanto los artículos 88 de la LO 3/2018 como, de forma más general, el 91 abren vías interesantes de intervención que conviene examinar, a fin de constatar si sus aportaciones pueden incrementar la eficacia del derecho a la desconexión digital.

En líneas generales, el legislador ha conferido un papel preponderante a la negociación colectiva en la regulación del derecho a la desconexión digital mediante la exigencia de respeto al contenido relativo a las modalidades de ejercicio del derecho (artículo 88.2 de la LO 3/2018) y, más generalmente, a través de la posibilidad de establecer garantías adicionales en el ejercicio y salvaguarda de los derechos digitales en el ámbito laboral. También se introduce un segundo actor, a saber, la representación de los trabajadores, pero su actuación es menos ambiciosa. En efecto, la intervención de los representantes de los trabajadores se traslada a un segundo plano, pues actuarán en la audiencia que ha de conferir el empleador en la elaboración de la política interna (artículo 88.3 de la LO 3/2018) y en el acuerdo para con la empresa relativo a las modalidades de ejercicio del derecho a la desconexión digital, exigido por el artículo 88.2 de la LO 3/2018, si bien este último solo se producirá si la negociación colectiva no se ha pronunciado.

En consecuencia, la norma diseña de forma muy acertada dos niveles de actuación en relación con la regulación de las modalidades de ejercicio de este derecho: el constituido por la negociación colectiva, que actuará como norma de mínimos en virtud del artículo 88.2 de la LO 3/2018, y un segundo escalón constituido por la política interna de la empleadora, que será elaborada por la empresa *ex* artículo 88.3 de la LO 3/2018. De esta manera, la negociación colectiva tiene la posibilidad de establecer una regulación genérica que armoniza cómo debe ejercerse el derecho a la desconexión digital en el ámbito de aplicación del convenio colectivo, mientras que, de forma más particular, la política interna se encargará de colmar las necesidades particulares de cada sujeto empleador.

2.1. La intervención de la representación de los trabajadores y la negociación colectiva en la configuración legal del derecho a la desconexión digital

Sin embargo, el artículo 88.2 y 3 de la LO 3/2018 presenta problemas de aplicación en relación con aquellas empresas que no ostentan representación legal de los trabajadores. Si bien es cierto que la negociación colectiva siempre podrá salvaguardar el posible impacto de esta circunstancia, la norma guarda un extraño silencio a propósito de la participación de trabajadores en aquellas empresas sin representación legal constituida. Técnicamente, la men-

14. El ejemplo más claro es el silencio respecto a la intervención del comité de prevención de riesgos laborales, tal y como señala Vallecillo Gámez, M. R. (2018). «El derecho a la desconexión...», *op. cit.*, pág. 176.

ción expresa a los representantes de los trabajadores no permite la constitución de una comisión *ad hoc* para la negociación o audiencia en el marco de la elaboración de la política interna empresarial sobre el ejercicio del derecho a la desconexión digital. Y esta circunstancia parece un grave descuido del legislador, especialmente si tenemos en cuenta que el número de empresas con una plantilla inferior a seis trabajadores es significativo en el tejido empresarial español[15], y ello sin introducir en la ecuación aquellas empresas que, aun superando la cifra de seis trabajadores, no ostentan representación legal constituida. Sorprende, pues, que el artículo 88.2 y 3 de la LO 3/2018 no ofrezca ninguna solución, como por ejemplo la constitución de una comisión representativa de trabajadores[16] ante este tipo de escenarios, que es probablemente el más común en la práctica. En consecuencia, el marco legal actual impide que los trabajadores que no ostentan representación legal puedan intervenir en la configuración de las modalidades de ejercicio del derecho a la desconexión digital, y, por lo tanto, ofrece un amplio margen de libertad para la elaboración de políticas internas extremadamente flexibles sobre esta materia.

Así pues, la negociación colectiva y la intervención empresarial, junto con la representación legal de los trabajadores, mediante la elaboración de políticas internas *ex* artículo 88.2 de la LO 3/2018, serán los sujetos encargados de regular las modalidades de ejercicio del derecho a la desconexión digital. No obstante, el planteamiento legal presenta diversos interrogantes que no han sido clarificados en la escueta regulación contenida en el artículo 88 de la LO 3/2018.

En primer lugar, conviene abordar cómo se conjuga la intervención de los tres sujetos indicados anteriormente. La actuación de la negociación colectiva y los empleadores se halla delimitada de forma clara en los distintos escenarios, pero el papel que desempeña la representación de los trabajadores presenta algunas zonas oscuras que deberían ser clarificadas por el legislador. En efecto, una lectura de los apartados 2 y 3 del artículo 88 de la LO 3/2018 permite dilucidar dos posibles escenarios, diferenciados por la existencia o no de regulación de las modalidades de ejercicio del derecho a la desconexión digital por parte de la negociación colectiva. En caso de existir regulación, la representación de los trabajadores se limitará a manifestar su opinión en el marco de la audiencia que contempla el artículo 88.3 de la LO 3/2018. Esta situación no plantea especiales problemas, ya que existe un equilibrio razonable en la intervención de los tres sujetos que dota a la norma de una regulación multinivel sumamente flexible, sin comprometer con ello ninguna garantía. Es cierto que en este punto podría haberse introducido la tipificación como sanción de las conductas consistentes en adoptar políticas internas que no se adecuen a lo previsto por la negociación colectiva, pero, en líneas generales, se aprecia un esfuerzo del legislador en evitar que sucedan este tipo de situaciones mediante la audiencia a la representación de los trabajadores en la elaboración de la política interna, que puede advertir de esta circunstancia a la Inspección de Trabajo y de la Seguridad Social.

El escenario verdaderamente problemático es aquel en el que la negociación colectiva no ha establecido ningún tipo de directriz. En estos supuestos, la representación de la empresa y los trabajadores deberán acordar las modalidades de ejercicio del derecho a la desconexión digital y, paralelamente, la representación de los trabajadores tendrá que comparecer en el marco de la elaboración empresarial de la política interna *ex* artículo 88.3 de la LO 3/2018. Queda patente que el legislador ha querido mantener los dos niveles de actuación, uno de alcance general y otro más particular, pero lo cierto es que la figura de la representación de los trabajadores aparece en este tipo de situaciones redundante y vacía de contenido en el marco del segundo nivel, esto es, en la elaboración de la política interna empresarial. Y, de hecho, las incidencias pueden suceder si el empresario se aparta del contenido pactado

15. Según los datos publicados por el INE relativos al número de empresas activas, en el año 2018 existían un total de 3.337.646, de las cuales 910.686 solo tenían entre uno y dos trabajadores, y 303.574 de tres a cinco. Fuente: INE, Empresas activas, Resultados nacionales, Empresas por estrato de asalariados y condición jurídica, 2018.
16. Las comisiones representativas de trabajadores han sido un recurso utilizado en diversas ocasiones en el marco del TRLET como consecuencia del gran número de empresas que, o bien no ostentan representación legal de los trabajadores, o bien no alcanzan el número mínimo de estos para su constitución. Así, por ejemplo, el artículo 40 (movilidad geográfica), 41 (modificación sustancial), 47 (suspensión del contrato o reducción de jornada por causas económicas, técnicas, organizativas o de producción), 51 (despido colectivo) o 82.3 (descuelgue de convenio).

con la representación de los trabajadores, supuesto este que no ostenta ninguna consecuencia legal y para el que el artículo 88 de la LO 3/2018 solo concede un trámite de audiencia no vinculante. En mi opinión, hubiera sido conveniente regular un papel más amplio de la representación de los trabajadores en aquellas situaciones en las que la negociación colectiva no se pronuncie sobre las modalidades de ejercicio del derecho a la desconexión digital.

2.2. El papel de la política interna empresarial como instrumento para concretar el derecho a la desconexión digital

El legislador ha introducido la política interna empresarial en el marco del artículo 88.3 de la LO 3/2018 como una forma de ofrecer flexibilidad en la concreción empresarial del ejercicio del derecho a la desconexión digital y en el diseño de acciones de formación y de sensibilización del personal sobre un uso razonable de las herramientas tecnológicas que eviten el riesgo de fatiga informática. La libertad para configurar su contenido es muy amplia, sobre todo con respecto a las acciones de formación y sensibilización, pero se halla limitada al necesario respeto de las previsiones adoptadas por la negociación colectiva en relación con las modalidades de ejercicio del ya citado derecho *ex* artículo 88.2 de la LO 3/2018. Sin embargo, merece la pena detenerse en la naturaleza y ámbito de exigencia, así como en sus implicaciones, que aparecen como elementos clave para delimitar el ejercicio del derecho a la desconexión digital de los trabajadores.

En cuanto a su naturaleza, la política interna empresarial prevista en el artículo 88.3 de la LO 3/2018 se plasma como una obligación legal[17] cuyo cumplimiento corresponde al empleador. Llama la atención la falta de previsión explícita de sanciones ante situaciones de incumplimiento empresarial, circunstancia esta que, si bien puede ser solventada mediante la incardinación de esta conducta en el artículo 6.4 del Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, desincentiva la elaboración de este instrumento. A propósito de su calificación jurídica, nos encontramos ante una manifestación del poder de dirección empresarial, ejercida al amparo del artículo 20 del TRLET. El empresario tiene un elevado margen de libertad para decidir su contenido, tan solo restringido por los límites del poder de dirección empresarial y el contenido que haya podido establecer la negociación colectiva ex artículo 88.3 de la LO 3/2018. De hecho, el papel de la representación de los trabajadores es anecdótico[18], sin contemplarse legalmente ningún tipo de intervención vinculante. En este punto, hubiera sido conveniente trasladar la exigencia de acuerdo entre empresa y representación de los trabajadores plasmada en el ámbito del artículo 88.2 de la LO 3/2018, a fin de potenciar un instrumento negociado que mantenga un cierto equilibrio entre las necesidades empresariales y las garantías de los trabajadores.

En este punto, conviene precisar que la inclusión de las modalidades de ejercicio del derecho a la desconexión digital en la política interna empresarial tiene diversas implicaciones de interés. La primera de ellas es la calificación del contenido de la política interna como un instrumento que contiene condiciones de trabajo. Nos encontramos ante la concreción de un derecho establecido legalmente, y esta circunstancia supone que las modalidades de ejercicio del derecho a la desconexión digital se conviertan en condiciones de trabajo que se integrarán dentro del patrimonio contractual del trabajador. Tal afirmación nos conduce a la segunda y más importante connotación: la limitación de la posibilidad de modificar unilateralmente el contenido de la política interna empresarial. Si bien es cierto que el empresario goza de una cierta libertad en la plasmación por primera vez de este instrumento[19], las posteriores modificaciones requerirán el cumplimiento de las exigencias legales previstas en el artículo 41 del TRLET. Por último, cualquier conducta empresarial que suponga un incumplimiento del deber legal de respeto al contenido de la política empresarial interna sobre el derecho a la desconexión digital, o incluso la propia no elaboración del mencionado instrumento, permitirá la extinción del contrato de trabajo al amparo del artículo 50.1.c del TRLET. La configuración del derecho a la des-

17. Igartua Miró, M. T. (2019). «El derecho a la desconexión...», *op. cit*., pág. 83.
18. *Ibid*., pág. 84, que señala el limitado papel otorgado a la representación legal de los trabajadores, al preverse únicamente su audiencia, «sin imponer deber de negociar ni emisión de informe alguno».
19. El artículo 88.3 de la LO 3/2018 solo exige la audiencia de los representantes de los trabajadores y, por lo tanto, no será necesario ningún tipo de acuerdo.

conexión digital depende en gran medida del contenido plasmado por el propio empresario en la política interna exigida por el artículo 88.3 de la LO 3/2018. Si valoramos los distintos bienes jurídicos que se persiguen mediante su implementación, pueden observarse puntos de conexión con deberes empresariales establecidos en el TRLET que refuerzan la posibilidad de extinguir el contrato de trabajo a instancia del trabajador. Concretamente, la prevención de los riesgos laborales derivados del uso de las TIC en el trabajo es uno de los deberes que mayor importancia cobra en el marco de esta cuestión, circunstancia esta constatada, de forma más genérica, en el artículo 4.2.d del TRLET. La conveniencia de incorporar esta posibilidad a nuestro ordenamiento jurídico aparece como un aspecto de interés ante la ausencia de sanciones[20], en aras de conferir al correcto desarrollo y cumplimiento del derecho a la desconexión digital de los trabajadores la importancia que requiere.

En relación con el ámbito de exigencia, la norma no se encarga de identificar qué empresarios estarán obligados a elaborarla. El silencio normativo debe entenderse como una expansión generalizada a todos los empleadores, independientemente del número de trabajadores. Si bien este hecho es positivo, hubiera podido afinarse con una regulación que diferenciara entre distintos niveles obligacionales en función de la implementación empresarial de dispositivos digitales. Las necesidades digitales en el mundo empresarial son muy diversas y la norma debería reconocer esta circunstancia adaptando la exigencia de elaborar una política interna sobre desconexión digital al uso habitual que se efectúe de los dispositivos digitales entre empresario y trabajadores. En otras palabras, el artículo 88.3 de la LO 3/2018 exige la presencia de una política interna en los mismos términos para pequeñas y medianas empresas con un uso esporádico o no habitual de dispositivos digitales y para aquellos empleadores que exigen una conexión digital permanente durante la jornada de trabajo. Y precisamente este hecho, que conmina la elaboración de un instrumento jurídico de contenido indeterminado y de forma indiscriminada a todos los empresarios, sacrifica la eficacia por un mayor alcance.

Conclusiones

La desconexión digital ha adquirido una gran importancia en el ámbito del Derecho del Trabajo, pero su configuración está lejos de garantizar la ausencia de intromisiones empresariales durante los tiempos de descanso. Si bien no existe a día de hoy voluntad de armonizar su regulación a nivel europeo, no han sido pocos los países que han regulado esta cuestión en los últimos años, entre los que se incluye España. Todos comparten la regulación de la desconexión digital como un novedoso derecho de las personas trabajadoras, pero nos encontramos ante la reapertura de un viejo debate, enmarcado en la delimitación del tiempo de trabajo y la protección de la salud y seguridad en el trabajo.

El artículo 88 de la LO 3/2018 reconoció el derecho a la desconexión digital de los trabajadores, siguiendo la estela de países como Francia. Sin embargo, una configuración basada en el reconocimiento de un derecho no vela por exigir en cualquier caso la desconexión digital, sino por un reconocimiento desde la perspectiva del trabajador, que no se acompaña de ningún tipo de obligación empresarial. Por lo tanto, traslada la tutela de la delimitación entre tiempo de trabajo y descanso de los poderes públicos a los trabajadores mediante el reconocimiento de un derecho cuyo ejercicio se ve comprometido por la posición de inferioridad propia de estos últimos. Esta circunstancia confiere al derecho un carácter reactivo cuya activación solo se produce si la persona titular decide ejercer el derecho a la desconexión digital, e implica la judicialización del incumplimiento a instancia del trabajador.

La calificación del derecho a la desconexión digital como fundamental ofrecería garantías que facilitarían su reivindicación por parte de los trabajadores, pero el artículo 18.4 de la Constitución española no reconoce su carácter fundamental, ya no solo por la omisión de la calificación explícita de fundamentales, sino por la débil conexión que presenta con el mandato del citado precepto. Este hecho requiere la reformulación hacia una obligación empresarial a la desconexión digital que impida al empresario el ejercicio de cualquier manifestación del poder directivo por medios digitales fuera de la jornada laboral.

20. Vallecillo Gámez, M. R. (2018). «El derecho a la desconexión...», *op. cit.*, pág. 176; y Alemán Páez, F. (2017). «El derecho a la desconexión digital...», *op. cit.*, pág. 14.

En cuanto a la dotación de contenido del derecho, el legislador español ha situado a la negociación colectiva, la iniciativa empresarial y, en menor medida, la representación de los trabajadores como responsables de diseñar sus modalidades de ejercicio. Concretamente, nos encontramos ante dos niveles de actuación: el constituido por la negociación colectiva, que actuará como norma de mínimos en virtud del artículo 88.2 de la LO 3/2018, y un segundo escalón constituido por la política interna, que será elaborada por la empresa, previa audiencia de la representación legal de los trabajadores, según recoge el *ex* artículo 88.3 de la LO 3/2018.

Sin embargo, el artículo 88 de la LO 3/2018 presenta algunos aspectos que reducen su eficacia enormemente. En primer lugar, otorga un reducido papel a la representación de los trabajadores, que solo podrán intervenir en la negociación ante un escenario en el que no exista regulación previa por la negociación colectiva y mediante la audiencia prevista en la elaboración de la política interna empresarial. Situación esta que es agravada por la falta de previsión de soluciones a empresas que no ostentan representación legal de los trabajadores, que constituyen la mayor parte del tejido empresarial español.

Paralelamente, la elaboración de una política interna empresarial se diseña como un instrumento que se encargará de establecer las modalidades de ejercicio del derecho unilateralmente por el empresario. Si bien se halla limitada por el respeto de las previsiones adoptadas por la negociación colectiva *ex* artículo 88.2 de la LO 3/2018, lo cierto es que nada impide que el empleador se aparte de ellas, dada la falta de sanciones previstas por el legislador, y, por lo tanto, pudiendo desvirtuarse el diseño de la configuración del ejercicio de este derecho al ser el empleador uno de los sujetos implicados. No obstante, la exigencia de instrumentar una política interna supone una manifestación del poder de dirección empresarial que regulará una condición de trabajo (la desconexión digital) que blinda el contenido del citado instrumento, pues su modificación requerirá llevar a cabo un procedimiento de modificaciones sustanciales (artículo 41 del TRLET), e incluso habilitará la extinción indemnizada a instancia del trabajador como consecuencia de un incumplimiento empresarial (artículo 50 del TRLET), debido a la conexión de este derecho con la prevención de los riesgos laborales derivados del uso de las TIC, *ex* artículo 4.2.d del TRLET.

Bibliografía

ALEMÁN PÁEZ, F. (2017). «El derecho a la desconexión digital. Una aproximación conceptual, crítica y contextualizadora al hilo de la Loi Travail N.o 2016-1088». *Trabajo y Derecho,* vol. 30.

BAYLOS GRAU, A. (2019). «El derecho a la privacidad en el trabajo en la nueva Ley Orgánica de Protección de Datos: una mala regulación». *Ciudad del Trabajo,* vol. 14.

CIALTI, P. (2017). «El derecho a la desconexión en Francia: ¿más de lo que parece?». *Temas laborales: Revista andaluza de trabajo y bienestar social,* núm. 137.

GARCIA-PERROTE ESCARTÍN, I.; MERCADER UGUINA, J. R. (2016). «El permanente debate sobre la jornada laboral: una cuestión clásica (reducción del tiempo de trabajo) y otra reciente (el derecho a la desconexión del trabajo)». *Revista de información laboral*, vol. 10.

IGARTUA MIRÓ, M. 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, vol. 432.

MOLINA NAVARRETE, C. (2017). «Jornada laboral y tecnologías de la infocomunicación: "desconexión digital", garantía del derecho al descanso». *Temas laborales: Revista andaluza de trabajo y bienestar social*, vol. 138.

SERRANO ARGÜESO, M. (2019). «Always on. Propuestas para la efectividad del derecho a la desconexión digital en el marco de la economía 4.0». *Revista Internacional y Comparada de Relaciones Laborales y Derecho del Empleo*, vol. 7, núm. 2.

TALÉNS VISCONTI, E. E. (2018). «La desconexión digital en el ámbito laboral: un deber empresarial y una nueva oportunidad de cambio para la negociación colectiva». *Información Laboral*, vol. 4.

TASCÓN LÓPEZ, R. (2018). «El derecho de desconexión del trabajador (potencialidades en el ordenamiento español)». *Trabajo y Derecho*, núm. 41.

VALLECILLO GÁMEZ, M. R. (2018). «El derecho a la desconexión, ¿novedad digital o esnobismo del viejo derecho al descanso?». *Estudios financieros. Revista de Trabajo y Seguridad Social,* vol. 418.

Cita recomendada

GUTIÉRREZ, David (2020). «La desconexión digital de los trabajadores. Reflexiones a propósito de su calificación como derecho y su instrumentación». *IDP. Revista de Internet, Derecho y Política*, núm. 31, págs. 1-13. UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i31.3208

Sobre el autor

David Gutiérrez Colominas
david.gutierrez@uab.cat

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

www.uoc.edu/idp

ARTÍCULO

El proceso judicial electrónico y su encaje en el ordenamiento jurídico español: estudio comparado con el proceso electrónico británico

María José Catalán Chamorro
Universidad de Córdoba

Fecha de presentación: octubre de 2019
Fecha de aceptación: marzo de 2020
Fecha de publicación: junio de 2020

Resumen

España está capacitada para iniciar un proceso judicial electrónico automatizado, similar al implementado en el Reino Unido. En el presente trabajo se expone de manera paralela el análisis del proyecto británico y una propuesta de *lege ferenda* para la inclusión de esta modalidad en el ordenamiento jurídico español. Esta se iniciaría solamente para reclamaciones de cantidad y procesos monitorios y podría continuar con la resolución electrónica de los procesos por sanciones administrativas de tráfico, finalizando este primer estadio de su desarrollo con la resolución de algunos de los procesos civiles recogidos a través de la Ley de Jurisdicción Voluntaria, incluyendo una propuesta final para habilitar a la ciudadanía para introducir denuncias administrativas o penales en línea. De esta manera, acercaríamos definitivamente el acceso a la justicia a los ciudadanos y ciudadanas, pretendiendo una suerte de autodefensa regulada y garantizada por los jueces y tribunales a la par que cercana a la ciudadanía a través de una plataforma informática segura e intuitiva.

Palabras clave

justicia electrónica, proceso civil electrónico automatizado, jurisdicción voluntaria

Electronic process of law and its implementation in the Spanish legal system: a study of comparison with the British electronic process

Abstract

Spain is capable of launching an automated electronic judicial process, similar to the one implemented in the United Kingdom. In the present paper, we present in parallel the analysis of the British project and a proposal of lege ferenda for the inclusion of this modality in the Spanish legal system. The first stage of its development would conclude with the resolution of some of the civil proceedings under the Voluntary Jurisdiction Act, including a final proposal to enable citizens to file administrative or criminal complaints online. In this way, we would definitely bring access to justice closer to citizens, pretending a sort of self-defense regulated and guaranteed by judges and courts as well as close to citizens through a secure and intuitive computer platform.

Keywords

E-Justice, Automated Electronic Civil Procedure, Voluntary Jurisdiction

1. Introducción

El ritmo de la sociedad ha cambiado, casi todo está automatizado, ya no podemos vivir sin las compras, las gestiones administrativas o bancarias en línea, rechazamos cada vez más las colas en oficinas o comercios presenciales. Sin embargo, el Derecho –y sobre todo la Justicia– aún reniega del uso de las nuevas tecnologías. No obstante, en los últimos tiempos nos hemos visto acorralados hacia el uso de estos instrumentos. Ejemplo de ello son LexNET Justicia o los portales Adriano y Minerva, así como las importantes bases de datos o revistas digitales que consultamos los operadores del Derecho para estar al día de las novedades doctrinales y jurisprudenciales.

La evolución social avanza hacia los procedimientos de resolución alternativa de conflictos en línea que tienen cada vez más incidencia en nuestro día a día, principalmente en las reclamaciones de consumo[1]. Es decir, formas alternativas flexibles de justicia o de tutela efectiva de nuestros derechos que permiten a la ciudadanía acceder a la justicia de una manera sencilla y ágil, en ocasiones sin necesidad de desplazarse, desde su domicilio u oficina, y en cualquier momento del día o de la semana. De resultas, la justicia también se puede adaptar a las necesidades y tiempos de las personas.

Ciertamente, en España vemos como algo muy lejano el proceso electrónico automatizado; sin embargo, como iremos advirtiendo a lo largo del presente trabajo, este está cada vez más cerca, convirtiéndose poco a poco en un camino por el que irremediablemente tendremos que transitar. Por suerte, nuestra sociedad cuenta cada año con un nivel más alto de conocimientos informáticos y la brecha digital está disminuyendo año a año, tal y como muestran las encuestas que analizaremos más adelante[2]. Todo ello unido al esfuerzo legislativo que se está haciendo por parte de las Administraciones públicas para informatizar y facilitar el acceso a estos medios electrónicos a la ciudadanía a través de la firma digital.

2. Origen de la e-Justicia en España

Si tuviésemos que establecer un hito relevante en la legislación española a partir del cual arranca este proceso de automatización de la Administración de Justicia, sería la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia[3]. Este texto legislativo estableció las bases definitivas de la actual plataforma LexNET Justicia.

Sin embargo, esta plataforma se pondría en funcionamiento definitivamente con la entrada en vigor del Real Decreto 1065/2015, de 27 de noviembre, sobre comunicaciones electrónicas en la Administración de Justicia en el ámbito territorial del Ministerio de Justicia y por el que se regula el sistema LexNET[4], en vigor desde el 1 de enero de 2016, amén de las sucesivas actualizaciones. La última actualización del sistema LexNET 4.18 implementada el 2 de marzo de 2020 crea nuevas funcionalidades y mejoras, además de la actualización de septiembre de 2019 que reforzó su seguridad y agilidad en la gestión de los archivos, y donde se mejoraron los canales de comunicación a través de la puesta en marcha de una dirección de correo electrónico, una cuenta en la red social Twitter y un teléfono para la información y soporte de los usuarios. Estos canales de comunicación eran muy necesarios desde la entrada en funcionamiento de LexNET y llegan con cierto retraso.

Ese primer hito legislativo mencionado marcó definitivamente el futuro de la justicia electrónica en España, ya que dentro del anexo de definiciones de

1. Solo en la plataforma ODR de consumo creada por la Comisión Europea se han registrado más de 131.136 reclamaciones en su cuarto año de funcionamiento, de las que España ha realizado 11.959. Véase: https://ec.europa.eu/consumers/odr/main/?event=main.statistics.show [Fecha de consulta: 13 de marzo de 2020].
2. *Véase: Instituto Nacional de Estadística (2018). Población que usa Internet (en los últimos tres meses). Tipo de actividades realizadas por Internet:* https://www.ine.es/ss/Satellite?L=es_ES&c=INESeccion_C&cid=1259925528782&p=1254735110672&pagename=ProductosYServicios%2FPYSLayout [Fecha de consulta: 13 de marzo de 2020].
3. BOE núm.160, de 6 de julio de 2011.
4. BOE núm. 287, de 1 de diciembre de 2015.

la Ley 18/2011, de 5 de julio, se fue mucho más allá, estableciendo el significado del concepto «actuación judicial automatizada», del que se dice que es aquella actuación judicial producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular (Bueno de Mata, 2015, págs. 4-6). Además, en el artículo 42 del citado texto se decreta la necesidad de establecer, en los casos donde se ejecute la actuación judicial automatizada, un Comité técnico estatal de la Administración judicial electrónica, así como indicadores de gestión que se establezcan por la Comisión Nacional de Estadística Judicial y el Comité técnico estatal de la Administración judicial electrónica, cada uno en el ámbito de sus competencias (Palomar Olmeda, 2012, pág. 481).

Esta previsión legal incluye desde la producción de actos de trámite o resolutorios de procedimientos, hasta meros actos de comunicación. De este modo, muy acertadamente, el legislador establecía un marco amplio para las legislaciones venideras. Tanto es así que, acogiéndonos a este marco, podríamos implantar un sistema de iniciación electrónica de los procesos –sobre todo de los civiles– sin necesidad de modificar o crear un nuevo amparo legal.

3. El proyecto de tribunales digitales en el Reino Unido y su encaje en la jurisdicción española

En el presente apartado analizaremos el proyecto en el que el Reino Unido lleva trabajando muy activamente desde 2016. Hoy, cuatro años después, ya se están iniciando algunos procesos judiciales en varias jurisdicciones diferentes y sobre temáticas concretas íntegramente a través de internet. Este proyecto está basado en el caso de éxito del Tribunal de Resolución Civil de Canadá en línea –Canadian Civil Resolution Tribunal–[5], que lleva operando con total normalidad ocho años. En este país solo se ha visto incrementada la litigiosidad de este orden jurisdiccional en un 1% y se ha denotado que un 45% de sus usuarios utilizan esta plataforma fuera del horario habitual de los tribunales físicos (Slater, 2017). Así las cosas, lo que en un principio nació como un sistema ágil para dar respuesta a las reclamaciones de cantidad inferiores a las 10.000 libras esterlinas, hoy se extiende hasta divorcios, materia testamentaria o incluso denuncias penales.

De este modo, siguiendo un sistema comparado y conociendo la implantación de estos tribunales digitales en el Reino Unido, podemos esbozar algunas instituciones digitales que podríamos fácilmente implantar en España a fin de facilitar el acceso a la justicia de la ciudadanía a través del medio digital.

No obstante, tal y como indicábamos más arriba, el programa de modernización de la justicia británico va más allá de la justicia civil, incluyendo denuncias sobre presuntos delitos o asuntos sobre Derecho de familia, materias en definitiva a las que en principio no se aspiraría en el ordenamiento jurídico español debido a la especial protección que deben tener los menores en asuntos de familia y los denunciados en el ámbito penal, pues, a través del medio electrónico, se podrían infringir principios y garantías básicas del proceso. Aunque –a tenor de los vertiginosos avances tecnológicos– en algunos años probablemente no podremos renunciar a tramitar casi ningún tipo de controversia vía internet.

3.1. Identificación del actor

Una de las cuestiones que nos planteamos *a priori* en España, a la vista de la gran problemática existente con casos de suplantación de identidad a través de internet, es cómo estar seguros en la identificación de un actor o de un demandado si no se han personado en un juzgado para identificarse. Pues bien, en el caso británico, no es necesaria ni tan siquiera la identificación mediante firma digital para acreditarse e iniciar la solicitud de resolución por parte de un órgano judicial. La plataforma electrónica no solo permite efectuar la solicitud de tutela, sino también hacer un seguimiento de la gestión de los casos, todo en línea, además de la posibilidad de celebrar audiencias con el juez a través

5. Ver en: https://civilresolutionbc.ca/about-the-crt/ [Fecha de consulta: 4 de octubre de 2019].

de videoconferencia e incluso recibir la resolución judicial en el buzón electrónico particular[6]. Y todo ello sin necesidad de utilizar ningún tipo de identificación oficial ante la Administración de Justicia británica. Simplemente a partir de un registro a través de un email y de una contraseña, podemos iniciar, por ejemplo, nuestra reclamación de cantidad en el Reino Unido, donde se disuade la posible suplantación de identidad por la necesidad de pago de una tasa para dar entrada a las reclamaciones.

En España, para cualquier trámite con la Administración pública se requiere del sistema de firma o certificado digital para asegurar la identificación auténtica del ciudadano o ciudadana. Así las cosas, a fin de obtener dicho certificado es precisa la personación física e identificación por parte de un trabajador público para recibir este archivo electrónico que le permita este acceso. En la actualidad este sistema ya es utilizado en nuestro país para los procedimientos de resolución de reclamaciones de consumo en línea a través de la institución pública «Arbitraje de Consumo» en casi todas las comunidades autónomas[7].

3.2. Sin necesidad de abogado ni de procurador

El impulso de la Administración británica –al igual que el de la española– está implementándose en la dirección de la autorrepresentación y la autodefensa. Este servicio, como nuestra Ley 15/2015, de 2 de julio, de Jurisdicción Voluntaria[8], pretende fomentar los procesos sin necesidad de representación legal, lo que se ha denominado *litigants in person* –y reconocido a través de las siglas LIP– para las reclamaciones civiles de escasa y mediana cuantía (Cortés y Takagi, 2019). De esta manera, la justicia se viste de plataforma virtual, resultando así más accesible y amigable para la ciudadanía. Tal y como señaló a propósito de esta reforma el Lord Chief Justice, lo importante es que «la tecnología sea nuestra servidora, no nuestra ama, y ofrezca a nuestros tribunales la posibilidad de resolver las disputas más rápidamente y menos costosamente» (Burnett, 2018).

Esta tecnología puede venir a paliar los altos costes procesales existentes en nuestro sistema procesal civil, donde la *quota litis* supone un alto porcentaje dentro de las reclamaciones de cantidad o de los conflictos de escasa cuantía, obteniendo como resultado que la inmensa mayoría de estos asuntos quedan fuera del real y efectivo acceso a la justicia para el ciudadano medio de nuestro país, y, por ende, muestran una debilidad del sistema de justicia.

En este sentido se pronunciaba en su informe el británico lord Briggs, quien observó que: «La debilidad más omnipresente y de hecho más chocante de nuestra corte civil es que no proporcionan un acceso razonable a la justicia para los individuos ordinarios» (Briggs, 2016); y es que, ciertamente, para una mayoría de la población los tribunales de justicia quedan muy lejos de sus expectativas cuando lo que intentan reclamar son cantidades de escasa cuantía, debido al elevado porcentaje de *quota litis* que comportan los honorarios de los abogados y procuradores. En España, esta cuestión ha intentado ser paliada con normas como la reforma de la Ley de Enjuiciamiento Civil a través de la Ley 4/2011, de 24 de marzo[9], y de la Ley 42/2015, de 5 de octubre[10], por la que los litigantes podrán comparecer por sí mismos, es decir, sin necesidad de abogado ni procurador, en los juicios verbales cuya determinación se haya efectuado por razón de la cuantía y esta no exceda de 2.000 euros, así como en la petición inicial del procedimiento monitorio y hasta el momento en el que se plantee oposición. Aunque el espaldarazo definitivo ha venido dado por los diecinueve tipos de expedientes de jurisdicción voluntaria que la Ley 15/2015 permite realizar sin necesidad de abogado ni procurador. Sin embargo, nos encontramos con una problemática colateral como es el desconocimiento casi pleno que tiene la ciudadanía de estos instrumentos y de cómo obtener

6. Ver en: https://www.gov.uk/make-money-claim [Fecha de consulta: 4 de octubre de 2019].
7. Ejemplo de ello son: Andalucía https://ws231.juntadeandalucia.es/eadministracion/menu.do, Comunidad Madrid https://gestionesytramites.madrid.org/, Cataluña https://juntarbitral.bcn.cat/es/solicitud-de-arbitraje o Comunidad Valenciana https://www.gva.es/es/inicio/procedimientos?id_proc=2290&version=amp [Fecha de consulta: 4 de octubre de 2019].
8. BOE núm. 158, de 3 de julio de 2015.
9. BOE núm. 72, de 25 de marzo de 2011.
10. BOE núm. 239, de 6 de octubre de 2015.

una tutela judicial efectiva sin necesidad de acudir a profesionales del Derecho. Para la mayoría de ciudadanos y ciudadanas, los juzgados suelen ser instituciones lejanas en las que no creen poder actuar en su propio nombre. No obstante, es posible que, si establecemos una plataforma virtual suficientemente intuitiva para la ciudadanía, esta percepción pueda cambiar.

Si analizamos el conocimiento medio del ciudadano español para relacionarse telemáticamente con la Administración pública no es excesivamente alarmante, ya que un 47,2% de los encuestados afirma haber enviado formularios cumplimentados a alguna Administración o servicio público a través de la red en los últimos doce meses y un 65,4% asegura haber contactado o interactuado con las Administraciones o servicios públicos vía internet por motivos particulares también en el mismo período de tiempo. Estas cifras aumentan hasta un 49% y un 69,6% respectivamente si los encuestados tienen estudios terminados de segunda etapa de educación secundaria y siguen aumentando a mayor formación de la muestra consultada[11]. Así las cosas, podemos considerar que aproximadamente el 50% de la población española estaría capacitada para seguir un proceso judicial civil, de reclamación de cantidad sencillo a través del medio en línea y donde el ciudadano se represente y se defienda a sí mismo.

4. Inconvenientes en la digitalización de la justicia

A pesar de todos los beneficios ya expuestos en el presente trabajo, debemos ser realistas y contar con los diferentes inconvenientes que podrían surgir con la puesta en marcha de estos tribunales electrónicos.

En primer lugar, es cierto que podría suponer un hándicap para el Estado la inversión inicial que *a priori* necesita esta nueva tecnología para ponerse en marcha, sobre todo con las suficientes garantías que requiere la tutela judicial efectiva del artículo 24 de la Constitución, unido a los posibles problemas de seguridad e identificación de los individuos que se podrían plantear. No obstante, en nuestro país tenemos la experiencia positiva de las declaraciones de la renta, que se realizan mayoritariamente a través de internet y que no provocan, generalmente, ningún tipo de problemática acerca de las garantías, seguridad del sistema o identidad de los declarantes.

Y, en segundo lugar, también podría suponer un hándicap, en este caso para la ciudadanía española, la introducción de tasas para la utilización de estas plataformas telemáticas. Este sistema, a pesar de ser más económico que la *quota litis*, precisa de un sistema de tasas que de alguna manera sustente y dé seriedad a las acciones legales que se inicien en la plataforma.

Las tasas que plantea la plataforma británica son económicas: parten de 25 libras para reclamaciones de hasta 300 libras y llegan hasta un máximo de 410 libras de tasas si la reclamación es desde 5.000,01 hasta 10.000 libras[12]. En la propia plataforma también se introducen a modo comparativo la tasa del mismo tipo de reclamación en papel o por medio de la modalidad física. Con todo, estas tasas serán menos costosas, ya que a través de esta vía telemática no será necesaria la asistencia de ningún profesional del Derecho, debido a que la plataforma sería suficientemente intuitiva y, además, establecería un sistema de asistencia al reclamante o reclamado tanto vía telefónica como vía correo electrónico para ayudarle a resolver sus dudas.

No obstante, es necesario apuntar que esta tasa no es cerrada para todo el proceso, sino que en cada una de las instancias de este que se superen sin obtener la solución a la disputa se cobrará una tasa extra antes de acceder, por ejemplo, a la vista con el juez tras haberse intentado por este una solución amistosa en una audiencia previa o para recurrir la apelación de la decisión obtenida[13].

11. Fuente: Encuesta del INE sobre formas de contacto o interacción con las Administraciones o servicios públicos por Internet, por motivos particulares, en los últimos doce meses por características socioeconómicas y tipo de acción: https://www.ine.es/jaxi/Datos.htm?path=/t25/p450/base_2011/a2018/l0/&file=04014.px [Fecha de consulta: 13 de marzo de 2020].
12. Disponible en: https://www.gov.uk/make-court-claim-for-money/court-fees [Fecha de consulta: 13 de marzo de 2020].
13. Disponible en: https://www.gov.uk/make-court-claim-for-money/court-fees [Fecha de consulta: 18 de marzo de 2020.

Sin embargo, a pesar de los altos costes iniciales que tendría este sistema para el Estado y la adaptación de la ciudadanía a un nuevo sistema de tasas judiciales para la resolución de sus disputas, creemos que sigue siendo conveniente la implantación de este sistema de justicia civil electrónica en nuestro país.

5. Procesos judiciales afines para la digitalización

Vista la experiencia de otros países que ya llevan años desempeñando procesos electrónicos, debemos entender que esto ha sido un procedimiento adaptativo y evolutivo, iniciándose con algunos trámites electrónicos, continuando con algunos procesos e incluyendo paulatinamente una variedad mayor de materias enjuiciables electrónicamente con el paso de los años. Por ello, del gran abanico de tipos de procesos que tenemos en nuestro país para solventar los conflictos, podríamos comenzar con los procesos civiles de escasa cuantía y proseguir con la iniciación de procesos monitorios, reclamaciones por sanciones administrativas de tráfico y quizá la digitalización de algunos expedientes de jurisdicción voluntaria.

5.1. Reclamaciones de escasa cuantía

Las reclamaciones de escasa cuantía son fácilmente operables a través de la plataforma web[14] que el Gobierno británico ha puesto en marcha. Se trata de un sistema sencillo, que recuerda mucho a la plataforma web ODR[15] de reclamaciones de consumo europea implementada por la Comisión Europea en febrero de 2015. Para ello, el Reino Unido ha aprovechado los procesos monitorios de reclamación de cantidad –que ya se podían llevar a cabo sin asistencia letrada– y han abierto la posibilidad de efectuar estos procedimientos monitorios en línea para cantidades determinadas e inferiores a 10.000 libras. Este proyecto primigenio fue el Civil Money Claims Online (su acrónimo, CMCO) y, aunque su límite actual es de 10.000 libras esterlinas, se espera que pronto se incremente a 25.000, si bien excluye los casos más complejos, como pueden ser los de lesiones personales. La previsión estimada por el Ejecutivo británico ha sido que la inmensa mayoría de las demandas civiles por reclamación de cantidad corresponderán a este sistema, ya que solo el 10% de todas las demandas civiles superan las 25.000 libras esterlinas.

El proyecto piloto de la CMCO, que comenzó en marzo de 2018, ha registrado unos magníficos resultados, pues en junio de 2019 había tramitado más de 70.000 casos, con una tasa de satisfacción de los usuarios de estos tribunales del 90% (House of Commons Select Justice Committee, 2019).

5.2. Tribunales telemáticos para las sanciones de tráfico

Además de procesos civiles sencillos de reclamación de cantidades, existe otra institución británica que podríamos poner en marcha en nuestro país y que satisfará a la ciudadanía española: es la figura del Traffic Penalty Tribunal –Tribunal de Sanciones de Tráfico–, que se ocupa de las apelaciones contra las multas de tráfico impuestas por las autoridades locales y proporciona un servicio en línea que ofrece audiencias telefónicas y virtuales, además de permitir a las partes cargar las pruebas en la plataforma y contar con un equipo de asistencia digital (Sheppard, 2018).

Actualmente, en España, para recurrir cualquier multa de tráfico se puede interponer un escrito de alegaciones y, posteriormente, un recurso de reposición. Si ambos no han sido satisfactorios para el ciudadano, a este solo le queda acceder a la jurisdicción contencioso-administrativa. Este orden jurisdiccional es el encargado de llevar a cabo estos procesos, que, a pesar de ser relativamente sencillos y ágiles, suponen un alto coste tanto para la ciudadanía como para el Estado. El ciudadano recurrente deberá ser defendido y representado por abogado y procurador respectivamente, amén del riesgo al que se somete de ser condenado a pagar to-

14. Disponible en: https://www.gov.uk/make-money-claim [Fecha de consulta: 13 de marzo de 2020].
15. Disponible en: https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.home2.show&lng=ES [Fecha de consulta: 13 de marzo de 2020].

das las costas del proceso tras la entrada en vigor de la Ley 37/2011, de 10 de octubre, de medidas de agilización procesal[16]. Y, por otro lado, el Estado deberá soportar los costes que producen desde las vistas o audiencias que se han de celebrar de manera presencial, hasta la representación de los intereses del Estado a través de la Abogacía del Estado, también presencialmente. Razones de peso para dar la posibilidad al ciudadano de realizar este tipo de procedimientos a partir de una plataforma telemática, de manera eminentemente escrita, con la prueba en soporte documental y, si fuese precisa, la celebración de la vista por medio de videoconferencia, así como establecer como no preceptiva la asistencia de abogado ni de procurador para aquellas multas de tráfico administrativas inferiores a 2.000 euros, asimilando esta situación a las reclamaciones de cantidad entre privados recogidas en la Ley de Enjuiciamiento Civil. Y como es evidente quedarían fuera de estos tribunales virtuales aquellas sanciones penales derivadas de la conducción imprudente o dolosa de los ciudadanos.

5.3. Procesos recogidos en la Ley de Jurisdicción Voluntaria

Como indicábamos en apartados anteriores, para el ejercicio de los expedientes de jurisdicción voluntaria no es preceptiva la asistencia de abogado y procurador en expedientes relativos a la autorización o aprobación judicial del reconocimiento de la filiación no matrimonial; la habilitación para comparecer en juicio y el nombramiento de defensor judicial; la adopción; para la tutela, la curatela y la guarda de hecho, salvo para la remoción del tutor o curador; o la concesión judicial de la emancipación y del beneficio de la mayoría de edad, entre otros. Si bien es cierto que no todos los expedientes son aptos para la tramitación electrónica, porque, a pesar de que exista la posibilidad de celebrar vistas a través de videoconferencia, sobre todo en procesos donde intervenga el Ministerio Fiscal en defensa del interés superior de los menores o incapaces será necesario la presencia y examen de los mismos.

No obstante, existen otros muchos expedientes que son simples trámites administrativos que pueden ser perfectamente iniciados y tramitados a través de una plataforma electrónica desde el domicilio de los ciudadanos con la suficiente seguridad y credibilidad que otorga la firma digital para efectuar cualquier tipo de acto administrativo. Posteriormente se requerirá la actuación del juez o del letrado de la Administración de Justicia, según el caso, en atención a la autoridad que el titular de la potestad jurisdiccional merece como intérprete definitivo de la ley, imparcial, independiente y esencialmente desinteresado en los asuntos que ante ella se dilucidan. En estos casos de expedientes electrónicos sería recomendable retirar la potestad de estos expedientes a notarios y registradores de la propiedad y mercantiles[17] para, así, aumentar las garantías y la confianza en este sistema electrónico bidireccional exclusivo entre la Administración de Justicia y el conjunto de la ciudadanía.

6. El funcionamiento interno de la plataforma británica

6.1. Primera fase

En primer lugar, la plataforma web de reclamaciones de escasa cuantía británica realiza un test de idoneidad a fin de adaptar esta herramienta al usuario y comprobar la jurisdicción de los tribunales británicos, la capacidad de los participantes, los posibles litisconsorcios o la correcta representación de las partes. Sobre la base de este test, donde se preguntan cuestiones sencillas como si la persona reclamante y reclamada están domiciliadas en territorio británico y ambos son mayores de edad, o si la reclamación se dirige contra una o varias personas y si estas son personas físicas o jurídicas, así como si se realiza la reclamación en nombre propio o en representación de un cliente o una organización. Además, la plataforma requiere cerciorarse de que la reclamación cumple con el límite máximo monetario de

16. BOE núm. 245, de 11 de octubre de 2011, por el que se modificó el artículo 139 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa.
17. Preámbulo de la Ley de Jurisdicción Voluntaria: «Como regla general, los expedientes de jurisdicción voluntaria en materia de personas y de familia, y también alguno de los expedientes en materia mercantil y de Derecho de obligaciones y sucesorio que no se encomiendan a Secretarios judiciales, Notarios o Registradores».

las 10.000 libras, así como de si la persona reclamante tendrá problemas para pagar la tasa que comentábamos en apartados anteriores.

Una vez el ciudadano haya realizado con éxito el test de idoneidad, donde la tipología de la reclamación encaje con los supuestos que el sistema permite suscribir, se tendrá que identificar en una cuenta de usuario. A través de esta cuenta de usuario deberá aceptar un consentimiento informado donde se le indica al reclamante que debe haber intentado solucionar el conflicto en persona con su contraparte, así como considerar la opción de la mediación como posible y factible para este tipo de casuísticas. Asimismo, también tendrá que aceptar un consentimiento donde se le indica que si *a posteriori* quiere cambiar algún dato de la reclamación deberá pagar una tasa extra.

Aceptados estos consentimientos podrá iniciar la reclamación introduciendo los datos del reclamante y de su contraparte; la cantidad por la que desea reclamar, y el resto de detalles de la reclamación que el reclamante quiera que se tengan en cuenta. No obstante, para la remisión de esta reclamación al órgano competente será necesario efectuar con carácter previo el pago de la tasa a través de la plataforma web.

Actualmente, esta herramienta está siendo transferida al personal de la Administración de Justicia británica para la toma de decisiones en una primera instancia o fase. De esta manera se pone en valor la agilidad y la rapidez en las respuestas, aunque se pone en duda la transcendencia en sus decisiones, así como la idoneidad de estos profesionales para ejercer tal nivel de poder decisional. La Administración británica los ha denominado «officers case lawyers» para destacar sus conocimientos en el ámbito jurídico (Cortés y Takagi, 2019). No obstante, esta cuestión es perfectamente adaptable al sistema judicial español ya que en nuestro país es el letrado de la Administración de Justicia el encargado en primera instancia de realizar la mediación previa en los procesos, en virtud de la atribución competencial que les confiere el artículo 456.6.e de la LOPJ.

Una vez suscrita la reclamación y la contestación a la misma por parte de la contraparte podemos encontrarnos diferentes escenarios. Bien que la contraparte realice el pago de la cantidad reclamada y ahí finalizaría el proceso, o bien que la contraparte no esté de acuerdo con la reclamación por diferentes circunstancias, como por ejemplo que el reclamado responda que no debe ninguna cantidad al reclamante; que esta cantidad que le reclama no se ajusta a la realidad; que no está de acuerdo con la utilización de este procedimiento y requiere otro físico[18] y no en línea, siendo incluso posible que ni siquiera conteste a la reclamación.

En el caso de que la contraparte se persone se invitará a las partes a intercambiar información en línea y a buscar por sí mismas una solución anticipada mediante ofertas cruzadas elaboradas por el propio sistema electrónico.

Así las cosas, en este primer nivel o etapa se sitúa una autoevaluación efectuada a través de un test en línea y en el que la plataforma ya sugiere ofertas para proponer a la contraparte, seguida de una negociación entre ambas partes. Si en solitario no son capaces de llegar a un acuerdo, a esta negociación le seguirá una etapa de facilitación en la que un tercero neutral ayuda a los litigantes a resolver su litigio.

Este tercero neutral será encarnado por los antes comentados «officers case lawyers». Estos asesores jurídicos son personal judicial legalmente cualificado y capacitado que puede ayudar a las partes en la gestión de su caso y a llegar a un acuerdo a partir de un sistema de resolución alternativo de disputas vía internet o de una mediación telefónica. Es necesario apuntar que las decisiones tomadas por los «officers case lawyers» son siempre supervisadas por los jueces, de modo que lo que aquellos realizan no es más que la facilitación al entendimiento de las partes y promover propuestas, que legalmente son aceptables, para la resolución en cada uno de los conflictos.

18. No obstante, para intentar paliar la brecha digital y los diferentes problemas o dudas técnicas que puedan surgir, las partes disponen de apoyo a través de un chat electrónico y una línea telefónica, así como una nueva aplicación incluida dentro de la plataforma llamada Assisted Digital, diseñada para ayudar a los usuarios de los tribunales con poca competencia digital.

Las mediaciones que están autorizados a realizar el personal de la Administración de Justicia británica[19] es similar a las conciliaciones que en España pueden implementar los letrados de la Administración de Justicia de los juzgados de primera instancia o de lo mercantil para cuantías superiores a los 6.000 euros y los jueces de paz si es inferior a dicha cantidad. La competencia territorial en este caso será siempre la del domicilio del requerido en virtud del artículo 140 de la Ley 15/2015, de 2 de julio, de la Jurisdicción Voluntaria. En el caso español, la conciliación no tiene vertiente en línea, aunque podría tenerla sobre la base de una estructura similar a la británica. Si bien es cierto que nuestra Ley de Jurisdicción Voluntaria, con muy buen criterio, elimina la posibilidad de someter a este tipo de procedimientos a los interesados que sean menores o personas con capacidad modificada judicialmente para la libre administración de sus bienes, ya que en estos deberá ser parte también el Ministerio Fiscal, por existir intereses superiores necesitados de protección.

6.1.1. Inteligencia artificial y ODR: ¿ventaja o desventaja?

En esta primera fase, la plataforma británica trabaja activamente para evitar la imposición de la decisión por un tercero, ayudando a las partes en la búsqueda de una solución común y autocompositiva. De este modo, se apuesta, al igual que en otras experiencias previas de justicia en línea, por la resolución alternativa del conflicto –como la exitosa herramienta de eBay[20] para solventar desavenencias entre sus clientes–. Sin embargo, es posible que los creadores de esta plataforma estén almacenando todos los casos, sus parámetros, ofertas, contraofertas y modos de acuerdo en un sistema de *big data* (o macrodatos) para *a posteriori*, a través de la inteligencia artificial, mejorar los sistemas de oferta, de soluciones más adaptadas y casos de éxito para las partes, sin necesidad de que un tercero acabe imponiendo su voluntad.

En definitiva, se trataría de buscar una especie de programa especialista en crear un diagnóstico de cada problemática, basándose en las experiencias previas resueltas exitosamente en esta primera fase de resolución de los conflictos. Esta herramienta entraría dentro del ámbito de los Online Dispute Resolution (en adelante ODR), si bien no podemos aclarar la tipología de este ODR, es decir si funciona a través de mediación, conciliación o arbitraje, o forma parte de los llamados ODR híbridos, los cuales aprovechan las bondades de los métodos autocompositivos y adjudicativos para crear nuevas modalidades con personalidad propia, dando lugar a diferentes figuras como pueden ser los *med-arb*, *co-med-arb* o *multi-step-wise-men* (Vilalta Nicuesa, 2013, págs. 65-68).

Sin embargo, es cada vez más evidente que la alimentación de estas bases de datos de los sistemas de resolución alternativa de conflictos con objeto de que, a través de las experiencias previas, se creen algoritmos que nos den la respuesta más ajustada a nuestro conflicto particular, es a partes iguales tan beneficiosa, debido a la agilidad que nos proporciona, como contraproducente, a causa de la valiosa información personal que le regalamos con cada una de nuestras decisiones al propio sistema.

6.1.2. La especialización de los juzgadores

Este sistema de reconocimiento electrónico inteligente de conflictos podría asimismo derivar cada casuística o problemática a los jueces especialistas en las mismas (Cortés, 2018, págs. 103-121). No obstante, esto podría chocar con el principio de un juez ordinario predeterminado por la ley, a menos que se creen juzgados telemáticos especializados en cada tipo de problemática. El sistema podría determinar, según los datos introducidos y marcados por el reclamante, la competencia objetiva y territorial del conflicto, así como el juez que por turno se establezca competente, en atención a las normas de reparto del juzgado o tribunal competente –previamente introducidas en el sistema informático–.

19. Ver más en: Courts and Tribunals (Judiciary and Functions of Staff) Bill Factsheet: Authorised Court and Tribunal Staff-legal advice and judicial functions: https://www.gov.uk/government/publications/courts-and-tribunals-judiciary-and-functions-of-staff-bill [Fecha de consulta: 13 de marzo de 2020].
20. Podemos considerar el ODR iniciado por las empresas eBay y PayPal en 1999 como primer hito más importante de la historia del ODR de consumo. Ver más sobre el fenómeno ODR de eBay en: C. Rule (2008); y E. Katsh, J. Rifkin y A. Gaitenby (2000).

Al mismo tiempo el sistema podría efectuar un primer «cribado» relativo a la legitimación de este reclamante y determinar la competencia subjetiva del caso.

6.2 Segunda fase

Pasado el período de facilitación o conciliación, y no habiendo lugar a un acuerdo entre las partes, será el momento en que el «officer case lawyer» tome una decisión sobre la resolución del expediente. No obstante, es necesario referenciar que, si bien hasta el momento los «officers case lawyers» tienen potestad para imponer una respuesta final a las reclamaciones monetarias inferiores a 300 libras esterlinas, las partes siempre podrán requerir la revisión de la decisión por el juez. Como indicábamos anteriormente los casos asignados a los «officers» son los que le corresponden al juez con el que trabajan regularmente, lo que permite que ambos mantengan una comunicación fluida acerca de los expedientes que se están llevando a cabo. Sin embargo, estos «officers» no están autorizados para dar consejo jurídico a las partes y solo pueden asesorar en el ámbito procesal de la resolución del conflicto indicando o direccionando el mismo.

Finalmente, si la labor del «officer» no ha conseguido resolver el conflicto entre las partes y el valor de la reclamación es superior a 300 libras será entonces cuando un juez adjudique una decisión con respecto al conflicto. En esta etapa final, un juez decide sobre las reclamaciones basándose en los escritos presentados por las partes y en una audiencia que se espera se ofrezca a las partes a través de medios electrónicos y permita la inmediación necesaria por medio de teléfono o videoconferencia.

6.2.1. La vista

Así las cosas, la fase más en el aire de todo este proceso en línea británico para reclamaciones civiles es la vista. En este sistema está permitido que ambas partes comparezcan mediante videoconferencia, pero aún quedan incógnitas por resolver: por ejemplo, si las partes que asisten a la misma lo harán físicamente desde cualquier sede judicial o institucional habilitada por la Administración de Justicia –como es el caso actual de España–[21], o si será posible realizarla incluso desde el domicilio o lugar de trabajo de las partes con una simple autenticación del usuario. Sin lugar a dudas, España todavía necesitará que las partes asistan a estas vistas desde una sede judicial o policial para dar ese halo de oficialidad necesario en nuestros procesos judiciales, sin perjuicio de que en un futuro se permita a las partes asistir a estas vistas desde cualquier otro lugar físico a su elección.

6.2.2. La publicidad del proceso

Otra cuestión controvertida que surge a la luz de las vistas es el aseguramiento de la publicidad del proceso, es decir, cómo hacemos para que cualquier ciudadano o ciudadana pueda asistir a este tipo de vistas en línea donde cada parte se encuentra deslocalizada de la sede judicial en la que se celebra. Sin duda, la solución electrónica es factible, ya que se podrían habilitar pantallas en los juzgados para la visualización de estos procesos de una forma similar a como actúan los tablones edictales, tal y como ya se ha previsto para el caso británico.

7. La denuncia en línea ¿es posible?

Todo este sistema hasta aquí definido tiene total y absoluta cabida en el ordenamiento jurídico procesal español sin crear ningún conflicto importante entre sus normas. En el presente trabajo nos hemos centrado en las posibilidades que el proceso electrónico automatizado nos proporciona en el ámbito civil, aunque también es interesante esbozar las utilidades que nos puede ofrecer en el de las denuncias públicas para informar sobre posibles irregularidades o incluso delitos que los ciudadanos presencian a diario.

En ocasiones, la interposición de una denuncia ante cualquier cuerpo de seguridad del Estado o Adminis-

21. En virtud del artículo 229.3 de la LOPJ.

tración pública lleva aparejada para los denunciantes no agraviados un compromiso ético y social, además de una cesión importante de tiempo, ya que el desplazamiento hasta la comisaría o Administración pública y la declaración para la denuncia suele conllevar más tiempo del que en la vida cotidiana dispone la ciudadanía tras sus obligaciones laborales y familiares.

Por ello, del mismo modo que existe una aplicación informática para el aviso de la perpetración de determinados delitos y la personación de la policía en el lugar donde se esté cometiendo el mismo, igualmente sería posible que, a través del sistema de autenticación comentado con firma digital, se pudieran emprender denuncias en línea. Si bien, en caso de que la policía o Administración requiriese más datos o aclaraciones sobre lo dispuesto en la misma, estas instancias podrán entrevistar al denunciante vía telefónica o citarlo en sus dependencias con la finalidad de esclarecer los hechos denunciados. De resultas, se podría abrir línea directa con diversas Administraciones responsables de la inspección en diferentes sectores –laboral, sanitario, alimentario, educativo, de la hacienda pública, etc.– a fin de alertarlas de posibles irregularidades conocidas por los denunciantes. No obstante, estos últimos tendrán que marcar una declaración jurada y ser advertidos de las sanciones en caso de denuncia falsa.

Referencias bibliográficas

BRIGGS, L. J. (2016). *Civil Courts Structure Review: Final Report*, pág. 28 [en línea] https://www.judiciary.uk/wp-content/uploads/2016/07/civil-courts-structure-review-final-report-jul-16-final-1.pdf [Fecha de consulta: 13 de marzo de 2020].

BUENO DE MATA, F. (2015). «Mediación electrónica e inteligencia artificial». *Actualidad Civil*, núm. 1, págs. 4-6.

BURNETT, I. (Lord Chief Of Justice) (2018). *Keynote Speech at the First International Forum on Online Courts the Cutting Edge of Digital Reform* [en línea]. https://www.judiciary.uk/wp-content/uploads/2018/12/speech-lcj-online-court.pdf [Fecha de consulta: 13 de marzo de 2020].

CORTÉS, P.; TAKAGI, T. (2019). «The Civil Money Claim Online: The Flagship Project of Court Digitalization in England and Wales». *Computer and Telecommunications Law Review*, núm. 25(8).

CORTÉS, P. (2018). «Using Technology and ADR Methods to Enhance Access to Justice». *International Journal of Online Dispute Resolution*, núm. 1-2, págs. 103-121.

HOUSE OF COMMONS SELECT JUSTICE COMMITTEE (2019). Court and Tribunal Reforms [en línea]. https://www.parliamentlive.tv/Event/Index/9f5ba45a-e4f0-485d-9697-b60e9ae15576 [Fecha de consulta: 13 de marzo de 2020].

KATSH, E.; RIFKIN J.; GAITENBY, A. (2000). «E-Commerce, E-Disputes, and E-Dispute Resolution: In the Shadow of "eBay Law"». *Ohio State Journal on Dispute Resolution,* vol. 15(3), pág. 727.

PALOMAR OLMEDA, A. (2012). «La actuación judicial automatizada». En: E. GAMERO CASADO y J. VALERO TORRIJOS (coords.). *Las tecnologías de la información y la comunicación en la Administración de justicia: análisis sistemático de la Ley 18/2011, de 5 de julio*. Navarra: Thomson Reuters-Aranzadi. Cizur Menor, pág. 481.

RULE, C. (2008). «Making Peace on eBay» [en línea]. *ACResolution*. http://colinrule.com/writing/acr2008.pdf [Fecha de consulta: 13 de marzo de 2020].

SHEPPARD, C. (2018). *The Traffic Penalty Tribunal* [en línea]. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/762201/TECHNOLOGY_PLATFORMS_KEY_NOTE_PRESENTATION__CAROLINE_.pdf [Fecha de consulta: 13 de marzo de 2020].

SLATER, S. (2017). *Online dispute resolution and justice system integration. British Columbia's civil resolution tribun*al [en línea]. https://wyaj.uwindsor.ca/index.php/wyaj/article/view/5008/4272 [Fecha de consulta: 13 de marzo de 2020].

VILALTA NICUESA, A. E. (2013). *Mediación y arbitraje electrónicos*. Navarra: Aranzadi. Cizur Menor, págs. 65-68.

Cita recomendada

CATALÁN CHAMORRO, María José (2020). «El proceso judicial electrónico y su encaje en el ordenamiento jurídico español: estudio comparado con el proceso electrónico británico». *IDP. Revista de Internet, Derecho y Política*. N.º 31, págs. xx-xx. UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i31.3220

Sobre la autora

María José Catalán Chamorro
Universidad de Córdoba
maria.jose.catalan@uco.es

María José Catalán es doctora por la Universitat de València, donde realizó su tesis doctoral financiada por una ayuda predoctoral FPI-MINECO. Actualmente es profesora sustituta interina del área de Derecho Procesal de la Universidad de Córdoba y está acreditada como ayudante doctora por ANECA desde el año 2018. Se ha formado en las mejores universidades europeas, realizando diversas estancias de investigación en la Universidad de Dublín (Irlanda) o en la Universidad de Leicester (el Reino Unido), contando además con dos posgrados internacionales. Autora de un gran número de trabajos relacionados siempre con la protección del consumidor y su tutela judicial editados como capítulos de libros o artículos en revistas indexadas en numerosas bases de datos, ha publicado también un libro monográfico –*Acceso a la Justicia de los consumidores a través del ADR y del ODR*– del que ya se han vendido más de mil ejemplares. Asimismo, colabora con las Cortes Generales como experta para la redacción y modificación de leyes en materia de consumo y con la Generalitat de València en la redacción de la Ley de Mediación.

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

www.uoc.edu/idp

ARTÍCULO

Construyendo un *P2P accommodation* 4.0 frente al COVID-19: *Proptech*, autorregulación y Tokenización

Cristina Argelich Comelles
Universidad de Cádiz

Fecha de presentación: noviembre de 2019
Fecha de aceptación: mayo de 2020
Fecha de publicación: julio de 2020

Resumen

Este trabajo presenta diversas propuestas para la regulación del alojamiento colaborativo, considerando el necesario distanciamiento social del COVID-19 como una oportunidad. Para ello, se emplean soluciones existentes en el Derecho comparado europeo y de los Estados Unidos, junto con aplicaciones prácticas de las nuevas tecnologías. En este sentido, se examinará la desregulación en España y las propuestas novedosas surgidas en Andalucía y Cataluña, junto con una autorregulación mediante los mecanismos reputacionales de las plataformas P2P. Finalmente, se aplicarán diversas tecnologías emergentes en el alojamiento colaborativo, como la tecnología *blockchain*, la Tokenización y la *Proptech,* en particular el *Internet of Things*.

Palabras clave

Tecnología *blockchain*, Tokenización, *Internet of Things, Proptech, P2P accommodation,* turismo 4.0

Developing P2P accommodation 4.0 when faced with COVID-19: Proptech, self-regulation and Tokenization

Abstract

The work presented herein offers various proposals for the regulation of peer-to-peer accommodation, considering the required Covid-19 social distancing as an opportunity. For this, solutions existing in law are used by comparing European and US law, togeth-er with practical applications of the new technologies. In this sense, there will be an examination of deregulation in Spain and the new proposals which have arisen in An-dalusia and Catalonia, along with a self-regulation through the reputation systems of the P2P platforms. Finally, various emerging technologies in peer-to-peer accommodation will be applied, such as blockchain *technology, Tokenization and* Proptech*, and partic-ularly the* Internet of Things

Keywords

Blockchain *technology, Tokenization,* Internet of Things, Proptech, P2P accommoda-tion, *Tourism 4.0*

1. Retos de las plataformas P2P de alojamiento colaborativo por la crisis del COVID-19

Compartir o ceder el uso de una vivienda o habitación de forma autónoma a través de una plataforma *peer-to-peer*, en adelante plataforma P2P: esta es la idea, fruto de la economía colaborativa, que ha revolucionado el mercado de vivienda de uso turístico con el surgimiento del *peer-to-peer accommodation* o alojamiento colaborativo. Esta concepción del turismo y el alojamiento sostenible se ha visto sacudida recientemente por el COVID-19, con sucesos acontecidos desde que la OMS declaró la pandemia global el 11 de marzo de 2020, y que referimos[1] hasta el cierre del presente trabajo: la activación política de medidas de fuerza mayor tendentes a reembolsar las reservas abonadas; el destino de los alquileres turísticos a arrendamientos de vivienda tradicionales; el despido de trabajadores pertenecientes a las plataformas P2P; el ofrecimiento de estos alojamientos a personal sanitario; y procedimientos de higiene para la desescalada.

Lógicamente, el COVID-19 va a modificar las previsiones de crecimiento del alojamiento colaborativo. De conformidad con los datos proporcionados por el Banco Mundial en su informe *Tourism and the Sharing Economy: Policy & Potential of Sustainable Peer-to-Peer Accommodation*[2], este tipo de hospedaje se concretó en 8 millones de pernoctaciones en 2017, con una facturación de 75 millones de dólares. El alojamiento P2P representa un 7% del total y, según las previsiones referidas por el Banco Mundial, alcanzará un 17% en el año 2025. Por su parte, el Parlamento Europeo elaboró un estudio denominado *An economic review on the Collaborative Economy*[3], en el que señaló que la economía colaborativa facturó 26,5 millones de euros en 2016, empleando a 394.000 personas. Sus mercados principales se distribuían de la siguiente manera: Francia, con un 25% del total; el Reino Unido, con un 17%; Polonia, con un 10%; y España, con un 10%. Por lo que se refiere a España, según el informe *Los modelos colaborativos y bajo demanda en plataformas digitales*[4], elaborado por Sharing España y Adigital, la economía colaborativa representó un 1,4% del PIB nacional en 2016, y la previsión es que aumente hasta un 2 o 2,9% en el año 2025.

En este contexto, las plataformas P2P dedicadas al alojamiento colaborativo tienen un primer reto que abordar en materia de consumo: dar respuesta a la automatización contractual que se está produciendo por el surgimiento de los *smart contracts* –entendidos como *smart legal contracts*, en contraposición a las meras secuencias de código informático de los *smart code contracts*– y la tecnología *blockchain*, así como otorgar seguridad jurídica a los *adprosumers*[5], a pesar de su desregulación. Por otra parte, el control de la propiedad y uso del alojamiento colaborativo, que ni la plataforma P2P ni la vinculación del alojamiento al *Internet of Things* –en adelante IoT– pueden articular, pasará necesariamente por la Tokenización a fin de lograr un alojamiento colaborativo 4.0, como examinaremos en los siguientes apartados.

1. EUROPA PRESS (2020). Boletín informativo sobre Airbnb [en línea] https://www.europapress.es/temas/airbnb/.
2. BANCO MUNDIAL (2018). *Tourism and the Sharing Economy: Policy & Potential of Sustainable Peer-to-Peer Accommodation,* pág. 14 [en línea]. http://documents.worldbank.org/curated/en/161471537537641836/pdf/130054-REVISED-Tourism-and-the-Sharing-Economy-PDF.pdf [Fecha de consulta: 5 de junio de 2020].
3. PETROPOULOS, G. (2016). «An economic review on the collaborative economy». European Parliament, págs. 1-32 [en línea] http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/595358/IPOL_IDA(2016)595358_EN.pdf [Fecha de consulta: 5 de junio de 2020].
4. RODRÍGUEZ MARÍN, S. (2017). «Los modelos colaborativos y bajo demanda en plataformas digitales». Sharing España, Adigital, págs. 1-59 [en línea] https://www.fidefundacion.es/attachment/810605/ [Fecha de consulta: 5 de junio de 2020].
5. En relación con el turista 3.0 o *adprosumer*, véase BASTANTE GRANELL, V. (2018). «El turista 3.0 o *adprosumer*: un nuevo reto para el derecho y la economía». *Revista Internacional de Derecho del Turismo,* vol. 2, núm. 2, págs. 47-73.

2. Desregulación del alojamiento colaborativo y las plataformas P2P: a la espera de la *Digital Services Act* y la evolución del turismo colaborativo por la crisis del COVID-19

La economía colaborativa[6] –basada en que la relación entre el crecimiento económico y el bienestar no es lineal, pues resulta preferible favorecer el acceso a un bien o servicio que alcanzar su propiedad, así como en que los recursos naturales son limitados– ha cristalizado también en el *cohousing* o *vivienda colaborativa*[7], en donde tales principios se aplican a la financiación, acceso y organización de inmuebles. Este tipo de economía se asienta en tres tipos de actuación: el *Product Service System,* conforme al cual se proporciona a los consumidores el acceso a los bienes o servicios que requieren de forma concreta, sin adquirir su propiedad; el *Redistribution Market,* que permite redireccionar los bienes de segunda mano a quienes lo necesiten; y el *Collaborative Lifestyle*, que se materializa compartiendo activos inmateriales como la solidaridad, la colaboración y la comunidad.

En este marco, el alojamiento colaborativo busca singularizarse frente al arrendamiento de viviendas de uso turístico tradicional, sometido –en contraste– a una legislación especial y un régimen tributario restrictivo. El alojamiento colaborativo[8] reduce los costes de transacción y los impositivos, pues únicamente se grava dicha actividad indirectamente en el impuesto sobre la renta de las personas físicas (IRPF)[9] como rendimiento de actividades económicas, aunque podría articularse una imposición directa y municipal[10] al respecto. Asimismo, esta modalidad de alojamiento aumenta las redes de intercambio ilimitadamente mediante la compensación de oferta y demanda, ofrece precios más competitivos que otras modalidades de alojamiento turístico y proporciona una experiencia cercana a la convivencia vecinal. Sin embargo, también presenta externalidades negativas[11]: molestias vecinales; competencia desleal con el sector turístico y menor gravamen tributario; falta de exigencia de las condiciones de habitabilidad por la falta de regulación, en particular la seguridad, salubridad y privacidad; decrecimiento de la oferta de vivienda asequible a largo plazo; «gentrificación» de ciertas zonas urbanas; cambios en las actividades del sector comercial para atender el sector turístico; y presión en el mercado inmobiliario por el aumento del precio de la vivienda.

6. Los creadores del concepto de *economía colaborativa* fueron BOTSMAN, R.; ROGERS, R. (2010). *What's mine is yours: the rise of collaborative consumption.* Nueva York: Harpers Collins Publishers, págs. 16-17. Atiéndase también KASSAN, J.; ORSI, J. (2012). «The legal landscape of the sharing economy». *Journal of Environmental and Litigation,* núm. 27, págs. 1-20; y FELIU ÁLVAREZ DE SOTOMAYOR, S. (2018). «Modelos colaborativos en plataformas digitales: nuevos retos para los negocios internacionales y para el Derecho Internacional Privado». *Anuario Español de Derecho Internacional Privado,* vol. 18, págs. 399-424.
7. NASARRE AZNAR, S. (2018). «Collaborative housing and blockchain». *Administration,* vol. 66, núm. 2, págs. 59-82; y NASARRE AZNAR, S. (2018). «Ownership at stake (once again): housing, digital contents, animals and robots». *Journal of Property, Planning and Environmental Law,* vol. 1, págs. 69-86.
8. DE LA ENCARNACIÓN, A. M. (2016). «El alojamiento colaborativo: viviendas de uso turístico y plataformas virtuales». *Revista de Estudios de la Administración Local y Autonómica,* núm. 5, págs. 31-34.
9. GARCÍA CALVENTE, Y. (2007). *Aspectos tributarios del turismo residencial.* Barcelona: Bosch, págs. 10-170. BILBAO ESTRADA, I. (2018). «Imposición sobre la renta y alojamiento colaborativo». En: A. M. DE LA ENCARNACIÓN (dir.); A. BOIX PALOP (coord.). *La regulación del alojamiento colaborativo: viviendas de uso turístico y alquiler de corta estancia en el derecho español.* Cizur Menor: Thomson Reuters Aranzadi, págs. 475-502.
10. Sobre las imposiciones directa y municipal, atiéndase CALDERÓN CORREDOR, Z. (2018). «Claves para la praxis fiscal del alojamiento "colaborativo". Una perspectiva de Derecho comparado». En: A. M. DE LA ENCARNACIÓN (dir.); A. BOIX PALOP (coord.). *La regulación del alojamiento colaborativo: viviendas de uso turístico y alquiler de corta estancia en el derecho español.* Cizur Menor: Thomson Reuters Aranzadi, págs. 527-542.
11. PONCE SOLÉ, J. (2018). «Economía colaborativa, viviendas de uso turístico e impactos en el marco del desarrollo urbano sostenible, ¿hacia una futura regulación más innovadora y flexible?». En: A. M. DE LA ENCARNACIÓN (dir.); BOIX PALOP, A. (coord.). *La regulación del alojamiento colaborativo: viviendas de uso turístico y alquiler de corta estancia en el derecho español.* Cizur Menor: Thomson Reuters Aranzadi, págs. 41-42.

El alojamiento colaborativo carece de una legislación especial en nuestro Estado. La Comisión Nacional de los Mercados y la Competencia publicó el *Estudio sobre la regulación de las viviendas de uso turístico en España*[12], de 19 de julio de 2018, que contiene distintas recomendaciones[13]. En concreto, se muestra favorable a la regulación activa de la economía colaborativa, a fin de garantizar la competencia efectiva y la protección a los consumidores. Respecto del arrendamiento turístico por habitaciones, que permite el alojamiento colaborativo a diferencia del alojamiento turístico, señala que afecta a la competencia de los operadores existentes y los emergentes. Asimismo, desaconseja encomendarse a una regulación basada en los *mecanismos reputacionales*[14] proporcionados por las plataformas P2P y construidos a través de las opiniones de los *adprosumers*. Estos sistemas reputacionales[15] se concretan en los sellos de confianza, los sistemas de valoración o puntuación, que entendemos es el principal mecanismo reputacional al que se refiere, las *black lists* o listas negras, y la información de contacto y atención personalizada. En este sentido, debemos señalar que es posible la denominada *Regulation by Robot*[16] o la regulación algorítmica para la toma de decisiones administrativas mediante el uso del *Big Data,* aunque en la actualidad se encuentra en una fase muy primigenia.

Todo ello contrasta con lo dispuesto en el derecho comparado, que desarrollaremos cronológicamente a la luz de las regulaciones regionales y locales existentes en Europa y Estados Unidos. Algunas de estas experiencias, en particular las de Bruselas, Estocolmo y Budapest, han suscitado el interés de la Unión, como se contiene en el informe Home Sharing in the Digital Economy[17], elaborado para la Comisión Europea, relativo al *home sharing* o arrendamiento colaborativo, en el que el propietario habita en la vivienda al mismo tiempo que la arrienda parcialmente por habitaciones. Mientras esperamos una regulación especial[18] en España a modo de *better* o *smart regulation*[19] que dote de tratamiento legal al alojamiento colaborativo en la línea del derecho comparado examinado, el Parlamento Europeo aprobó la Resolución de 15 de junio de 2017 sobre una Agenda Europea para la economía colaborativa[20]. En ella, insta a la Comisión Europea a que

12. CNMC (2018). *Estudio sobre la regulación de las viviendas de uso turístico en España,* de 19 de julio de 2018, págs. 1-84 [en línea] https://www.cnmc.es/sites/default/files/2133063_2.pdf [Fecha de consulta: 5 de junio de 2020].
13. Estas recomendaciones consisten en revisar la regulación actual de los alojamientos turísticos para asegurar que sea necesaria y proporcionada y reducir su disparidad, y establecer restricciones graves y muy graves a evitar en la regulación de las viviendas de uso turístico.
14. En este sentido, PONCE SOLÉ, J. (2018). «Economía colaborativa...», *op. cit.*, pág. 51, expresa que los mecanismos reputacionales no tienen en cuenta aspectos como la seguridad, el riesgo de incendio, las afectaciones negativas a terceros, la fiabilidad de las opiniones ni una revisión de las mismas.
15. Para un examen exhaustivo de los mecanismos reputacionales, atiéndase VILALTA NICUESA, A. E. (2018). «Los sistemas reputacionales como mecanismos de compulsión privada». En: F. ESTEBAN DE LA ROSA (dir.). *La resolución de conflictos de consumo: la adaptación del Derecho español al marco europeo de resolución alternativa (ADR) y en línea (ODR).* Cizur Menor: Thomson Reuters Aranzadi, págs. 443-464.
16. COGLIANESE, C.; LEHR, D. (2017). «Regulating by robot: administrative decision making in the machine-learning era». *Georgetown Law Journal,* vol. 105, págs. 1.207-1.209. En materia administrativa, por la seguridad y garantías que ofrecen los procedimientos administrativos, PONCE SOLÉ, J. (2018). «Economía colaborativa...», *op. cit.*, pág. 67, lo califica con acierto de «falacia del nirvana», en el sentido de comparar cosas reales con alternativas no disponibles, suponiendo que existe una solución perfecta, e irreal, a un problema particular.
17. RANCHORDÁS, S.; ZUREK, K.; GEDEON, Z. (2016). «Home Sharing in the Digital Economy: The Cases of Brussels, Stockholm and Budapest». *Impulse Paper prepared for the European Commission* [en línea] https://www.rug.nl/research/portal/publications/homesharing-in-the-digital-economy-the-cases-of-brussels-stockholm-and-budapest-impulse-paper-prepared-for-the-european-commission(82c6123d-be1b-46b9-8b36-354632f7a673)/export.html [Fecha de consulta: 5 de junio de 2020].
18. Atiéndanse DOMÉNECH PASCUAL, G. (2015). «La regulación de la economía colaborativa (Uber contra el taxi)». *Revista CEFLegal,* núm. 175-176, págs. 61-104; y GUILLÉN NAVARRO, N. A.; ÍÑIGUEZ BERROZPE, T. (2015). «Las viviendas de uso turístico en el nuevo entorno p2p. Retos socio-jurídicos para el consumo colaborativo en el alojamiento turístico». *Estudios Turísticos,* núm. 205, págs. 9-34.
19. Término acuñado por PONCE SOLÉ, J. (2018). «Economía colaborativa...», *op. cit.*, págs. 61-62. Respecto de la regulación de las viviendas de uso turístico en el alojamiento colaborativo, véase GUILLÉN NAVARRO, N. A.; IÑIGUEZ-BERROZPE, T. (2016). «Acción pública y consumo colaborativo. Regulación de las viviendas de uso turístico en el contexto p2p». *Pasos. Revista de Turismo y Patrimonio Cultural,* vol. 14, núm. 3, págs. 751-768.
20. [En línea] http://www.europarl.europa.eu/doceo/document/TA-8-2017-0271_ES.html?redirect [Fecha de consulta: 5 de junio de 2020]. Para un análisis en profundidad de las propuestas de regulación europea de las plataformas P2P, así como de la legislación existente en distintos Estados miembros, atiéndase VILALTA NICUESA, A. E. (2018). «La regulación europea de las plataformas de intermediarios digitales en la era de la economía colaborativa». *Revista Crítica de Derecho Inmobiliario,* núm. 765, págs. 275-330.

preste su apoyo a las autoridades nacionales para regular la economía colaborativa, olvidando que nos encontramos en un mercado común que exige una regulación armonizada, en aras de garantizar la protección de los consumidores. Debemos señalar que el Tribunal de Justicia de la Unión Europea, en su Sentencia de 19 de diciembre de 2019[21], ha afirmado que las plataformas P2P de alojamiento colaborativo no deben regularse conforme a las normas relativas a los agentes inmobiliarios, calificándolas como «servicios de la sociedad de la información». Por todo ello, deberemos prestar una especial atención a la regulación que efectúe de las plataformas P2P la propuesta de directiva conocida como *Digital Services Act,* cuya aprobación se prevé para finales de 2020.

2.1. La regulación del alojamiento colaborativo en el derecho comparado

En el marco europeo, Ámsterdam[22] fue la primera ciudad donde se reguló el alojamiento colaborativo, al amparo de los arrendamientos de corta duración previstos en la *Wet van 4 juni 2014, houdende nieuwe regels met betrekking tot de verdeling van woonruimte en de samenstelling van de woonruimtevoorraad*[23]. Se estableció la *seven-day-rule,* es decir, que el alojamiento colaborativo debe pactarse por al menos siete días; en caso contrario, necesariamente deberá formalizarse en un hotel o un *Bed & Breakfast*. Las residencias habituales pueden cederse hasta un máximo de sesenta días al año y limitado a cuatro huéspedes.

En Alemania, existe una regulación regional del alojamiento colaborativo en el estado federado de Berlín y en la ciudad de Hamburgo. Así, la *Gesetz über das Verbot der Zweckentfremdung von Wohnraum*[24], del *Land* de Berlín, dispone que los arrendamientos de habitaciones y los arrendamientos de corta duración de viviendas completas sin licencia tendrán un plazo máximo de noventa días al año. Por su parte, la *Gesetz über das Schuldbuch der Freien und Hansestadt Hamburg*[25] dispone para dicha ciudad el alojamiento colaborativo sin licencia, siempre que se trate de la vivienda habitual y que al mismo tiempo los propietarios se encuentren temporalmente ausentes, lo que excluye al *home sharing*.

En Bélgica, la región de Bruselas-Capital reguló los arrendamientos de corta duración en la *Ordonnance relative à l'hébergement touristique*[26]. En ella dispuso que los propietarios de viviendas ofertadas en las plataformas P2P tienen el deber de registrarlas en la Administración local correspondiente, para su control.

En Grecia, la Ley 4446/2016, sobre el Código de insolvencia, justicia administrativa, deberes, honorarios y declaración voluntaria de ingresos no declarados, transacciones electrónicas y enmiendas a la Ley 4270/2014 y otras disposiciones[27] permite el alojamiento colaborativo de un máximo de dos viviendas, y limitado a noventa días al año.

En Italia, el *Decreto-legge 24 aprile 2017, Disposizioni urgenti in materia finanziaria, iniziative a favore degli enti territoriali, ulteriori interventi per le zone colpite da eventi sismici e misure per lo sviluppo*[28] dispone que las plataformas de alojamiento colaborativo deberán registrar los datos de las estancias en viviendas de uso turístico, así como tributar el 21% de los ingresos obtenidos. Por su parte, en la región de la Toscana, la *Legge regionale n. 86 del 20 dicembre 2016, Testo único del sistema turístico regionale*[29] permite el arren-

21. TJCE 2019\302.
22. HEIDE, J.; PETERS, K. B. M. (2015). «Airbnb als hulpmiddel voor spreading van toerisme in Amsterdam?». *Vrijetijdstudies,* núm. 2, págs. 9-22.
23. [En línea] https://wetten.overheid.nl/BWBR0035303/2019-07-01 [Fecha de consulta: 5 de junio de 2020].
24. [En línea] http://gesetze.berlin.de/jportal/portal/t/a5/page/bsbeprod.psml?pid=Dokumentanzeige&showdoccase=1&js_peid=Trefferliste&documentnumber=1&numberofresults=1&fromdoctodoc=yes&doc.id=jlr-WoZwEntfrGBErahmen&doc.part=X&doc.price=0.0 [Fecha de consulta: 5 de junio de 2020].
25. [En línea] http://www.landesrecht-hamburg.de/jportal/portal/page/bshaprod.psml?showdoccase=1&doc.id=jlr-SchuldBGHA2013rahmen&st=lr [Fecha de consulta: 5 de junio de 2020].
26. *Moniteur Belge* (17 de junio de 2014) [en línea] http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2014050850&table_name=loi [Fecha de consulta: 5 de junio de 2020].
27. *Government Gazette* de 22 de diciembre de 2016.
28. *Gazzetta Ufficiale* (23 de junio de 2017) [en línea] https://www.gazzettaufficiale.it/eli/id/2017/06/23/17A04320/sg [Fecha de consulta: 5 de junio de 2020].
29. *Bollettino Ufficiale della Regione Toscana* (28 de diciembre de 2016) [en línea] http://www.consiglio.regione.toscana.it/upload/pdl/2016/pdl135_burt.pdf [Fecha de consulta: 5 de junio de 2020].

damiento ilimitado de la vivienda si el propietario tiene hasta dos viviendas en propiedad, mientras que en caso contrario se limita a ochenta pernoctaciones.

En Francia[30], el *Décret nº 2017-678 du 28 avril 2017 relatif à la déclaration prévue au II de l'article L. 324-1-1 du code du tourisme et modifiant les articles D. 324-1 et D. 324-1-1 du même code*[31] establece la obligación de comunicar al ayuntamiento correspondiente el destino de una vivienda al alojamiento colaborativo. Asimismo, con la reforma de 2015 de la *Loi nº 2014-366 du 24 mars 2014 pour l'accès au logement et un urbanisme rénové*[32] se permite el *location saisonnière* o arrendamiento de temporada hasta un máximo de noventa días. Respecto de arrendamiento de habitaciones, denominado *chambres d'hôtes*, el L324-3 de la *Loi nº 2006-437 du 14 avril 2006 portant diverses dispositions relatives au tourisme*[33] prohíbe el arrendamiento de más de cinco habitaciones de la misma vivienda simultáneamente, limitando los ocupantes a quince personas, por un período máximo de cuatro meses al año y previa comunicación al ayuntamiento correspondiente.

En el Reino Unido[34], las secciones 44 y 45 de la *Deregulation Act 2015*[35] establecen para la ciudad de Londres la posibilidad de formalizar un alojamiento colaborativo por un máximo de noventa días al año. Por esta actividad, se impone al propietario un gravamen que deberá abonar en la *Council Tax*, equivalente a nuestro impuesto sobre bienes inmuebles (IBI).

Finalmente, en algunos estados y ciudades de Estados Unidos se ha regulado el alojamiento colaborativo[36], en particular en los estados de Portland, Washington DC, Nueva York y Chicago, así como en las ciudades de San José y San Francisco, en California. Fundamentalmente, la regulación tiene como objetivo legalizar el *home sharing* y que las plataformas P2P garanticen el cumplimiento de las obligaciones urbanísticas. A título ilustrativo, en el estado de Nueva York, la *New York State Multiple Dwelling Law*[37] impide el arrendamiento de viviendas turísticas por períodos inferiores a treinta días en edificios con tres o más viviendas turísticas, excepto en la modalidad de *home sharing*. Asimismo, la Ordenanza Municipal de San Francisco determina un mínimo de treinta días y un máximo de noventa al año para dicho alojamiento, salvo en el *home sharing*, y obliga al titular de la vivienda a registrarla en el *San Francisco Office of the Tresurer & Tax Collector*.

2.2. Una *smart regulation* del alojamiento colaborativo para España: regulación autonómica y mecanismos reputacionales para la autorregulación de las plataformas P2P

Las vías de regulación del alojamiento colaborativo en España, a la espera de una regulación europea, pasan o bien por una regulación estatal, basada en la competencia en derecho administrativo e igualdad *ex* artículo 149.1 de

30. LEFEBVRE, N. (2015). «Destination et expériences: l'adaptation de l'offre touristique de Paris aux novelles attentes». *Annales des Mines. Réalités industrielles,* núm. 3, págs. 58-62. FERRARY, N. (2015). «Les nouvelles formes de tourisme collaboratif: una demande en pleine expansion». *Annales des Mines. Réalités industrielles,* núm. 3, págs. 50-53. DEVAUX, C. (2015). *L'habitat participatif: De l'initiative habitante à l'action publique.* París: Presses Universitaires Rennes, págs. 10-262. PÉRINET-MARQUET, H. (2014). «Accès au logement et urbanisme renové. Loi ALUR du 24 mars 2014». *Semaine juridique,* núm. 15, págs. 709-712. Sobre la regulación francesa e inglesa, atiéndase DE LA ENCARNACIÓN, A. M. (2018). «Soluciones europeas en materia de regulación del alojamiento "colaborativo": París y Londres». En: A. M. DE LA ENCARNACIÓN (dir.); A. BOIX PALOP (coord.). *La regulación del alojamiento colaborativo: viviendas de uso turístico y alquiler de corta estancia en el Derecho español.* Cizur Menor: Thomson Reuters Aranzadi, págs. 189-210.
31. *Journal officiel de la République française* (30 de abril de 2017) [en línea] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=Journal officiel de la République françaiseTEXT000034517689&categorieLien=id [Fecha de consulta: 5 de junio de 2020].
32. *Journal officiel de la République française* (26 de marzo de 2014) [en línea] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=Journal officiel de la République françaiseTEXT000028772256&categorieLien=id [Fecha de consulta: 5 de junio de 2020].
33. *Journal officiel de la République française* (15 de abril de 2006) [en línea] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=Journal officiel de la République françaiseTEXT000000422900&categorieLien=id [Fecha de consulta: 5 de junio de 2020].
34. BOUAZZA ARIÑO, O. (2009). *La planificación territorial en Gran Bretaña. Especial referencia al sector turístico*. Cizur Menor: Civitas, págs. 57-65.
35. *UK Official Documents* (26 de marzo de 2015) [en línea] http://www.legislation.gov.uk/ukpga/2015/20/introduction/enacted [Fecha de consulta: 5 de junio de 2020].
36. JEFFERSON-JONES, J. (2015). «Airbnb and the Housing Segment of the Modern "Sharing Economy": Are Short-Term Rental Transactions an Unconstitutional Taking?». *Hastings Constitutional Law Quarterly,* vol. 42, núm. 3, págs. 557-575.
37. [En línea] https://www1.nyc.gov/assets/buildings/pdf/MultipleDwellingLaw.pdf [Fecha de consulta: 5 de junio de 2020].

la Constitución Española[38] –en adelante CE– apartados primero y decimoctavo, o bien por una adaptación de la regulación autonómica existente, fundamentada en las competencias en materia de turismo, urbanismo y vivienda. Ello seguiría la línea de la regulación estatal y autonómica en materia de vivienda –altamente mejorable–, por ejemplo, respecto de la distribución competencial en materia de arrendamientos urbanos –estatal– y las condiciones de habitabilidad, en virtud de la competencia autonómica en materia de urbanismo. Sin embargo, desaconsejamos esta opción porque, aunque sea posible desde un punto de vista competencial, consideramos que no garantiza una cierta uniformidad en el régimen legal, al igual que las propuestas[39] de regulación y de gravamen municipal por dicha actividad. Un tratamiento legal armonizado serviría para prevenir los abusos y garantizar el éxito y efectividad de la regulación, así como para evitar agravios comparativos.

El alojamiento colaborativo no encaja en la legislación arrendaticia debido a la necesaria vocación de destino de la vivienda al uso habitacional de manera habitual, que configura tanto los artículos 1542 y 1543 CC como el artículo 2 de la Ley 29/1994, de 24 de noviembre, de Arrendamientos Urbanos[40] –en adelante LAU 1994–, indicado en este último caso como necesidad permanente de vivienda. Es más, el artículo 5 e) LAU 1994 excluye, desde la reforma[41] operada por la Ley 4/2013, de 4 de junio, de medidas de flexibilización y fomento del mercado de alquiler de viviendas[42], la cesión temporal del uso de la totalidad de una vivienda amueblada que esté promocionada en canales de oferta turística, lo que en nuestra opinión incluye a las plataformas P2P de alojamiento colaborativo[43] por su finalidad turística. Negar que dicho arrendamiento esté excluido de la legislación de arrendamientos urbanos conlleva importantes problemas interpretativos respecto de determinadas prestaciones del contrato: su duración; la falta de regulación de la cesión parcial de vivienda, salvo en el caso del subarrendamiento parcial que sería equiparable al *home sharing,* al que atenderemos seguidamente; las condiciones de habitabilidad; y el ánimo de lucro de quien cede en alojamiento colaborativo una vivienda, aunque no se trate de un agente inmobiliario. En suma, debe reinterpretarse la exclusión con independencia del destinatario, para aplicarlo a las modalidades de alojamiento surgidas de las nuevas tecnologías.

Hechas estas consideraciones, la actividad económica de alojamiento colaborativo, sea total o parcial, debe calificarse como *turismo residencial*[44]. El alojamiento colaborativo constituye un arrendamiento complejo compuesto por el objeto del contrato –la vivienda completa o las habitaciones objeto de la cesión– y las prestaciones de las partes, que incluirán los servicios básicos y

38. *Boletín Oficial del Estado* (29 de diciembre de 1978), págs. 29.316-29.424.
39. PONCE SOLÉ, J. (2018). «Economía colaborativa...», *op. cit.*, págs. 61-62, considera además de las vías estatal y autonómica, una regulación municipal basada en las competencias en urbanismo y vivienda. CALDERÓN CORREDOR, Z. (2018). «Claves para la praxis fiscal», *op. cit.*, págs. 527-542, propone el establecimiento de un gravamen municipal.
40. *Boletín Oficial del Estado* (25 de noviembre de 1994), págs. 36.129-36.146.
41. Sobre la interpretación de las exclusiones de la LAU 1994 tras la reforma de la Ley 4/2013, atiéndanse NASARRE AZNAR, S. (2015). «La eficacia de la Ley 4/2013, de reforma de los arrendamientos urbanos, para aumentar la vivienda en alquiler en un contexto europeo». *Revista Crítica de Derecho Inmobiliario,* núm. 747, págs. 205-249, CAMPUZANO TOMÉ, H. (2015). «El alquiler de viviendas de uso turístico a partir de la Ley 4/2013: la necesaria interpretación conjunta de la LAU y de la legislación turística autonómica». *Revista Crítica de Derecho Inmobiliario,* núm. 749, págs. 1.199-1.246, y DE LA IGLESIA PRADOS, E. (2013). «La reforma en la regulación del contrato de arrendamiento urbano de vivienda de junio de 2013». *Actualidad Civil,* núm. 11, págs. 1-12.
42. *Boletín Oficial del Estado* (5 de junio de 2013), págs. 42.244-42.256.
43. Cfr. GONZÁLEZ CARRASCO, M. C. (2013). «El nuevo régimen de los arrendamientos de vivienda tras la ley de medidas de flexibilización y fomento del mercado del alquiler». *Revista CESCO de Derecho de Consumo,* núm. 6, págs. 170-190, CAMPUZANO TOMÉ, H. (2015). «El alquiler de viviendas», *op. cit.,* págs. 1.230-1.231, y NÚÑEZ IGLESIAS, A. (2010). «Tipología de los contratos de alojamiento extrahotelero (I)». *Actualidad Civil,* núm. 12, págs. 1-20.
44. El alojamiento colaborativo es calificado de *actividad turística* por CAMPUZANO TOMÉ, H. (2015). «El alquiler de viviendas», *op. cit.,* págs. 1.205-1.208. En el mismo sentido, VERDERA IZQUIERDO, B. (2009). «La problemática del turismo residencial». *Diario La Ley,* núm. 7.297, pág. 9, señala que debe calificarse de turismo residencial dicha actividad. MARTÍNEZ CAÑELLAS, A. (2014). «La cesión del uso de la vivienda a no residentes: contrato de alojamiento (de estancias turísticas) en viviendas y el contrato de arrendamiento de temporada, conforme a la Ley del Turismo de las Islas Baleares tras la reforma de la Ley de Arrendamientos Urbanos». *Boletín de la Academia de Jurisprudencia y Legislación de las Illes Balears,* núm. 15, págs. 151-176.

la cobertura de los gastos inherentes a la vivienda, así como la habilitación de uso de los espacios comunes en caso de arrendarse parcialmente. Debemos recordar que la mayor parte de la normativa sectorial no dispone el arrendamiento de habitaciones destinadas al uso turístico. Probablemente, el fundamento sea la insuficiencia de garantías para el cumplimiento efectivo de las condiciones de habitabilidad, a diferencia del artículo 26 LAU 1994 que habilita la suspensión del contrato por esta causa. Por todo ello, deberá atenderse a la legislación autonómica de carácter especial, en virtud del reparto competencial del artículo 148.1.18º CE, y supletoriamente al régimen de arrendamientos de temporada, regulado como arrendamientos para uso distinto de vivienda en los artículos 29-35 LAU 1994.

La dificultosa subsunción del alojamiento colaborativo en la normativa existente presenta otra disfunción, además del arrendamiento de habitaciones destinadas al uso turístico: la desregulación del llamado *home sharing*. Por *home sharing* entendemos el arrendamiento de economía colaborativa en virtud del cual el propietario de una vivienda continúa residiendo en ella, y arrienda de forma privativa una o varias habitaciones de la misma, con derecho al uso compartido de los espacios comunes y la cobertura completa de los gastos. Las comunidades autónomas[45] que han regulado las viviendas de uso turístico se refieren a viviendas amuebladas y equipadas para su uso inmediato, comercializadas o promocionadas mediante canales de oferta turística, para cederlas en su totalidad con fines de hospedaje a cambio de un precio. En la misma línea, se define el alojamiento turístico en el artículo 2 del Reglamento UE 692/2011 del Parlamento Europeo y del Consejo de 6 de julio de 2011, relativo a las estadísticas europeas sobre el turismo y por el que se deroga la Directiva 95/75/CE del Consejo[46], pues impide el arrendamiento con fines turísticos de la residencia habitual. Asimismo, el alojamiento turístico se caracteriza por la habitualidad en la prestación de este servicio y se trata de un establecimiento abierto al público, a diferencia del alojamiento colaborativo.

La mayor parte de la regulación autonómica dedicada al alojamiento turístico de viviendas completas no encaja en el alojamiento colaborativo, pues prohíbe de forma expresa su cesión en habitaciones. En sentido contrario,

45. Véanse cronológicamente las siguientes regulaciones de la Comunidad de Madrid, Comunidad Valenciana, Castilla y León, La Rioja, País Vasco, Andalucía, Aragón, Galicia, Islas Baleares, Extremadura, Asturias, Navarra, Cantabria, Murcia, Cataluña, Castilla-La Mancha y las Islas Canarias: Decreto 29/2019, de 9 de abril, del Consejo de Gobierno, por el que se modifica el Decreto 79/2014, de 10 de julio, por el que se regulan los Apartamentos Turísticos y las Viviendas de Uso Turístico de la Comunidad de Madrid, *Boletín Oficial de la Comunidad de Madrid* (12 de abril de 2019); Ley 15/2018, de 7 de junio, de turismo, ocio y hospitalidad de la Comunitat Valenciana, *Boletín Oficial del Estado* (29 de junio de 2018), págs. 65.200-65.258; Decreto 3/2017, de 16 de febrero, por el que se regulan los establecimientos de alojamiento en la modalidad de vivienda de uso turístico en la Comunidad de Castilla y León, *Boletín Oficial de Castilla y León* (17 de febrero de 2017); Decreto 10/2017, de 17 de marzo, por el que se aprueba el Reglamento General de Turismo de La Rioja en desarrollo de la Ley 2/2001, de 31 de mayo, de Turismo de La Rioja, *Boletín Oficial de La Rioja* (22 de marzo de 2017); Ley 13/2016, de 28 de julio, de Turismo, del País Vasco, *Boletín Oficial del País Vasco* (11 de agosto de 2016); Decreto 28/2016, de 2 de febrero, de las viviendas con fines turísticos y de modificación del Decreto 194/2010, de 20 de abril, de establecimientos de apartamentos turísticos, de Andalucía, *Boletín Oficial de la Junta de Andalucía* (11 de febrero de 2016); Decreto 80/2015, de 5 de mayo, del Gobierno de Aragón, por el que aprueba el Reglamento de las viviendas de uso turístico en Aragón, *Boletín Oficial de Aragón* (14 de mayo de 2015); Decreto 12/2017, de 26 de enero, por el que se establece la ordenación de apartamentos turísticos, viviendas turísticas y viviendas de uso turístico en la Comunidad Autónoma de Galicia, *Diario Oficial de Galicia* (20 de febrero de 2017); Ley 8/2012, de 19 de julio, del Turismo de las Illes Balears, *Boletín Oficial de las Islas Baleares* (21 de julio de 2012); Ley 2/2011, de 31 de enero, de desarrollo y modernización del turismo de Extremadura, *Boletín Oficial del Estado* (18 de febrero de 2011), págs. 18.739-18.790; Ley 7/2011, de 22 de junio, de Turismo, de Asturias, *Boletín Oficial del Principado de Asturias* (6 de julio de 2001); Decreto Foral 230/2011, de 26 de octubre, por el que se aprueba el reglamento de ordenación de los apartamentos turísticos en la Comunidad Foral de Navarra, *Boletín Oficial de Navarra* (14 de noviembre de 2011); Decreto 82/2010, de 25 de noviembre, por el que se regulan los establecimientos de alojamiento turístico extrahotelero en el ámbito de la Comunidad Autónoma de Cantabria, *Boletín Oficial de Cantabria* (9 de diciembre de 2010); Decreto 75/2005, de 24 de junio, por el que se regulan los apartamentos turísticos y alojamientos vacacionales, de Murcia, *Boletín Oficial de la Región de Murcia* (11 de julio de 2005); Ley 13/2002, de 21 de junio, de turismo de Cataluña, *Boletín Oficial del Estado* (16 de julio de 2002), págs. 25.810-25.829; Ley 8/1999, de 26 de mayo, de Ordenación del Turismo de Castilla-La Mancha, *Boletín Oficial del Estado* (28 de julio de 1999), págs. 28.074-28.086; Ley 7/1995, de 6 de abril, de Ordenación del Turismo de Canarias, *Boletín Oficial del Estado* (23 de mayo de 1995), págs. 15.038-15.055.

46. *Diario Oficial de la Unión Europea* (22 de julio de 2011).

se manifiestan las regulaciones indicadas anteriormente de Andalucía[47], Asturias, Canarias[48], Castilla y León[49], Comunidad Valenciana, Extremadura, Murcia, País Vasco, la proyectada en Cataluña, anulando recientemente el Tribunal Supremo la limitación a viviendas completas del Decreto 12/2017 de Galicia[50], indicado más arriba.

De estas regulaciones, las que contemplan expresamente el alojamiento colaborativo de viviendas completas y el *home sharing* son la de Andalucía y la proyectada en Cataluña. El Decreto 28/2016, de 2 de febrero, de las viviendas con fines turísticos y de modificación del Decreto 194/2010, de 20 de abril, de establecimientos de apartamentos turísticos[51], de Andalucía, dispone en el artículo 5.1 que las viviendas con fines turísticos pueden ser completas, cuando se cedan en su totalidad, o por habitaciones, debiendo la persona propietaria residir en ella. Por otra parte, se está tramitando el Decreto de reglamento de turismo de Cataluña desde el año 2015[52], cuya última versión[53] es de 23 de julio de 2019 y que previsiblemente se va a aprobar en el año 2020, con la finalidad de desarrollar el alojamiento colaborativo en virtud de la regulación sobre alojamiento turístico, contenida en el Decreto 159/2012[54], de 20 de noviembre, de establecimientos de alojamiento turístico y de viviendas de uso turístico. Debemos señalar que, como indica la Exposición de Motivos del Proyecto de Decreto, se ha integrado en esta normativa el alojamiento colaborativo, fruto del Acuerdo GOV/44/2016[55], de 5 de abril, para el desarrollo de la economía colaborativa en Cataluña y la creación de la Comisión Interdepartamental de la Economía Colaborativa. En los artículos 241-1 a 241-3 se van a regular las viviendas compartidas o *home sharing*, separadamente de las viviendas de uso turístico. El decreto califica el arrendamiento temporal de habitaciones como *viviendas de servicio turístico*, por considerar que las plataformas amplían el aprovechamiento de una oferta ya existente de espacios alternativos a los alojamientos tradicionales.

3. Tecnología *blockchain* y Tokenización para un alojamiento colaborativo 4.0: la gestión práctica del alojamiento colaborativo con el distanciamiento social del COVID-19

El alojamiento colaborativo, ampliamente extendido como alternativa al turismo tradicional, puede verse potenciado con el surgimiento de dos realidades: la aplicación de la tecnología *blockchain* y la Tokenización, especialmente útil para la gestión del alojamiento en el distanciamiento social impuesto por el COVID-19. La tecnología *blockchain* consiste en un código en cadena que emite registros descentralizados para evitar su manipulación. Las prin-

47. El decreto en vigor no prohíbe la cesión por habitaciones, pero obliga a que la vivienda en la que eventualmente se ceda la habitación constituya el domicilio habitual del titular.
48. En el supuesto de la regulación de Canarias, se eliminó la prohibición de la cesión por habitaciones que contenía el artículo 12.1 de la Ley 7/1995, mediante la STSJIC, 3.ª, de 21 de marzo de 2017, RJCA 2017\645.
49. Artículo 3 del decreto declarado nulo por la STSJCL de 2 de febrero de 2018, RJCA 2018\5.
50. Véase STS de 21 de octubre de 2019, Roj: 3261.
51. *Boletín Oficial de la Junta de Andalucía* (11 de febrero de 2016)
52. Sobre este decreto, véase CUSCÓ PUIGDELLÍVOL; E., FONT GAROLERA, J. (2013). «Nuevas formas de alojamiento turístico: comercialización, localización y regulación de las viviendas de uso turístico en Cataluña». *Biblio3W Revista Bibliográfica de Geografía y Ciencias Sociales,* núm. 1.134, págs. 1-17, y RODRÍGUEZ FONT, M. (2018). «Avances en el proceso de regulación normativa del alojamiento "colaborativo" en Cataluña». En: A. M. DE LA ENCARNACIÓN (dir.); A. BOIX PALOP (coord.). *La regulación del alojamiento colaborativo: viviendas de uso turístico y alquiler de corta estancia en el derecho español.* Cizur Menor: Thomson Reuters Aranzadi, págs. 295-324.
53. Versiones del Proyecto de Decreto de reglamento de turismo de Cataluña [en línea] http://empresa.gencat.cat/ca/departament/transparencia-i-bon-govern/normativa-i-organitzacio/normativa/normativa-en-tramit/projectes-normatius-en-tramit/projectes-de-decret/projecte-de-decret-de-reglament-de-turisme/ [Fecha de consulta: 5 de junio de 2020].
54. *Diario Oficial de la Generalitat de Cataluña (*5 de diciembre de 2012).
55. *Diario Oficial de la Generalitat de Cataluña* (7 de abril de 2016) [en línea] https://dogc.gencat.cat/es/pdogc_canals_interns/pdogc_resultats_fitxa/?action=fitxa&documentId=722189&language=es_ES [Fecha de consulta: 5 de junio de 2020].

cipales[56] plataformas de tecnología *blockchain* son Blockchain y Ethereum, aunque existen otras como Quorum. Blockchain[57], utilizada por más de 38 millones de usuarios, permite adherirse a un *smart contract* predispuesto y comprar criptomonedas, convertibles a saldo canjeable en *PayPal*, a cambio de una cesión de datos de carácter personal; dicha cesión no debemos equipararla al concepto jurídico de contraprestación, pues se trata únicamente del tratamiento de datos de carácter personal de cualquier usuario que utilice la plataforma.

Ethereum[58], utilizada por 12 millones de usuarios, es una *blockchain* programable por la que se pueden crear *smart contracts* personalizados y comprar la criptomoneda de la plataforma, que es el *Ether*. Por el momento, el hecho de que Ethereum funcione mediante unas tasas o *fees* está desincentivando su extensión, aunque tendrá externalidades positivas cuando los contratos tradicionales incorporen progresivamente algunas cláusulas que se autoejecuten, para pasar a un segundo estadio de programas ayudados de inteligencia artificial o IA que elaboren por sí mismos *smart contracts*, como un viaje combinado ejecutado mediante un *M2M contract*: es decir, de un consentimiento prestado para un contrato la *blockchain* –ayudada por la IA– obtiene la base para el consentimiento de un contrato posterior.

3.1. La *blockchain* REGTURI del Registro de la Propiedad para las viviendas turísticas

El Colegio de Registradores de España presentó el 4 de octubre de 2019 el Proyecto REGTURI[59], consistente en la implementación de la tecnología *blockchain* para el control en el Registro de la Propiedad de las viviendas turísticas inscritas. La plataforma REGTURI utilizará más de 1.100 nodos para conectar todas las oficinas, a efectos de verificar y validar el uso turístico de la vivienda y generar un *identificador* con nota marginal en el Registro de la Propiedad. Esta *blockchain* recogerá la oferta de arrendamiento vacacional disponible, que en la actualidad no está recopilada en una plataforma pública para su consulta. Asimismo, aportará un *certificado turístico* que acredite que la vivienda se encuentra en el mercado de arrendamiento turístico de forma regular, por lo que las oficinas del Registro de la Propiedad podrían comprobar su veracidad. Con el registro previo de una vivienda en REGTURI, las juntas de propietarios de viviendas en régimen de propiedad horizontal no podrán aprobar la prohibición estatutaria de destino al arrendamiento turístico de sus viviendas, contenido en el artículo 17 apartado 12 de la Ley 49/1960, de 21 de julio, sobre propiedad horizontal[60], apartado introducido por el Real Decreto-ley 7/2019, de 1 de marzo, de medidas urgentes en materia de vivienda y alquiler[61].

En definitiva, el Colegio de Registradores ha diseñado un ecosistema digital de seguridad preventiva para evitar el fraude en el arrendamiento turístico. Mediante la tecnología *blockchain* se van a interconectar las plataformas P2P, la Agencia Tributaria, las Fuerzas y Cuerpos de Seguridad del Estado, las Administraciones locales y las comunidades autónomas con el Registro de la Propiedad. De esta manera, se podrán gestionar adecuadamente las más de 185.000 viviendas turísticas existentes en España, según datos[62] de la Federación Española de Asociaciones de Viviendas y Apartamentos Turísticos (FEVITUR). Los datos registrados por REGTURI se incorporarán también al Instituto Nacional de Estadística, pues a día de hoy los operadores del mercado, principalmente las plataformas

56. Existen otras plataformas como Chainspace. Véase AL-BASSAM, M. (2017). «SCPKI: A Smart Contract-based PKI and Identity System». *BCC'17*, págs. 1-6.
57. Blockchain [en línea] https://www.blockchain.com/ [Fecha de consulta: 5 de junio de 2020].
58. Ethereum [en línea] https://www.ethereum.org/ [Fecha de consulta: 5 de junio de 2020].
59. COLEGIO DE REGISTRADORES DE ESPAÑA (2019). *Proyecto REGTURI: proyecto del Colegio de Registradores de España sobre apartamentos turísticos*. Nota de prensa de 4 de octubre de 2019 [en línea] https://www.registradores.org/-/la-decana-de-los-registradores-destaca-que-la-innovacion-esta-en-el-adn-de-los-registradores-y-senala-el-compromiso-con-el-medio-ambiente-y-con-la-igualdad/ [Fecha de consulta: 5 de junio de 2020].
60. *Boletín Oficial del Estado* (23 de julio de 1960), págs. 10.299-10.303.
61. *Boletín Oficial del Estado* (5 de marzo de 2019), págs. 21.007-21.024.
62. Federación Española de Asociaciones de Viviendas y Apartamentos Turísticos [en línea] https://www.fevitur.com/index.php?lang=es [Fecha de consulta: 5 de junio de 2020].

P2P, disponen de sistemas propios que no están interconectados con la Administración.

3.2. Una *smart property* para el control remoto del alojamiento colaborativo: *Proptech* y Tokenización

El término *Proptech* se refiere a la aplicación de las nuevas tecnologías al mercado inmobiliario de servicios de construcción, mantenimiento o administración de inmuebles. En el mercado *Proptech* se incluyen las *classfields* o plataformas de mercado, las plataformas P2P, el *Big Data,* el IoT y el *Property Management Software*, así como las plataformas de inversión e hipotecas de realidad virtual. Hasta 2018, se contabilizaron en España un total de 238 *startups* Proptech, unas empresas que poseen 150 millones de euros en recursos y 5.500 personas empleadas, según el *Informe*[63] *Proptech 2019*, siguiendo una progresión al alza desde 2013. Por todo ello, la presencia de las nuevas tecnologías –en particular la Tokenización–, la *blockchain* y el IoT posee cada vez más relevancia para la administración de las viviendas turísticas. A modo introductorio, indicamos que el IoT permitirá vincular la vivienda turística a un *smart contract* de alojamiento colaborativo, mientras que la Tokenización de dicho inmueble posibilitará un control remoto o mediato de su propiedad y uso.

Respecto de la Tokenización, profundizando en lo señalado al inicio de este trabajo, debemos indicar que, técnicamente, un *token* es un metadato o referencia criptográfica sobre un registro de tipo descentralizado, a modo de unidad de valor. De esta manera, la Tokenización es un método para convertir derechos en un activo digital que, operado en una *blockchain*, se vincule al control de un activo real. Estas fichas digitales tienen propiedad intelectual[64] y se someten a una programación informática que las hace susceptibles de ser objeto de *smart contracts*. Debemos indicar que también es posible la Tokenización de bienes muebles, con la finalidad de adquirir la propiedad u otro derecho real limitado mediante una aplicación móvil que vincule los *smart contracts* y la tecnología *blockchain* con la transmisión de los tokens correspondientes. FINMA[65], que es el regulador financiero de Suiza, ha distinguido tres clases de tokens, según su función: los *payment tokens,* destinados a utilizarse como criptomonedas; los *utility tokens*, que proporcionan acceso digital a una aplicación o servicio; y los *asset tokens*, que representan activos como acciones, participaciones e incluso el derecho al pago de dividendos o de intereses. FINMA advierte[66] de que pueden crearse tokens híbridos; ello sucederá, por ejemplo, en la criptomoneda *Ether*. En este caso, el *payment token* es utilizado como *utility token* a modo de *gas*, que es el coste de computación en la plataforma Ethereum para ejecutar *smart contracts*, a diferencia de la plataforma Blockchain, que no repercute el coste del *gas* al usuario.

Las empresas u otras organizaciones crean tokens para basar su modelo de negocio y que sus clientes los utilicen para interactuar con sus productos. La Tokenización posibilita la digitalización de la propiedad, de modo que su administración y disposición es programable, permitiendo su control mediato a tiempo real mediante la tecnología *blockchain*. En la actualidad, Blockchain y Ethereum permiten entre tres y seis transacciones por segundo, una cifra que Ethereum prevé incrementar hasta un millón por segundo, lo que facilitaría la Tokenización de inmuebles. La principal ventaja de la Tokenización es que hace factible transformar activos poco líquidos en instrumentos para obtener financiación, lo que proporciona liquidez inmediata al mercado inmobiliario en caso de transmisión, de forma similar al proceso de titulización hipotecaria. Por ejemplo, las plataformas P2P dedicadas al *crowdfunding inmobiliario* adquieren las propiedades y generan los tokens que se negocian en la plataforma *blockchain* correspondiente. Los tokens son divisibles y universales, de modo que si aumenta su demanda se reducirá el denominado *descuento de iliquidez*.

63. SHAMMA, H.; DE LA FUENTE, G.; BARROSO, P. (2019). *Informe PropTech 2019 en España*. Savills, Aguirre Newman, págs. 1-4 [en línea] http://inmuebles.savills-aguirrenewman.es/informes/proptech/informe-proptech.pdf [Fecha de consulta: 5 de junio de 2020].
64. Sobre los problemas de la propiedad intelectual en el ámbito de los tokens, véase KRUMHOLZ, J.; MAHONY, I. (2019). «Blockchain and intelectual property: A case study». En: J. DEWEY (dir.). *Blockchain Laws and Regulations 2019*. Londres: Global Legal Insights [en línea] https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/4-blockchain-and-intellectual-property-a-case-study [Fecha de consulta: 5 de junio de 2020].
65. [En línea] *https://www.finma.ch/en* [Fecha de consulta: 5 de junio de 2020].
66. FINMA (2018). *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs),* págs. 1-11 [en línea] https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/ [Fecha de consulta: 5 de junio de 2020].

Tanto en la Tokenización de bienes inmuebles como muebles, resulta esencial que el token permanezca vinculado al objeto del derecho real, es decir, que el activo digital tenga correspondencia posesoria con el activo real, una vinculación remota que resulta útil para la gestión ordinaria del alojamiento en tiempos de distanciamiento social por el COVID-19. Ello permite comprobar la existencia de los elementos de la adquisición derivativa y la extinción por pérdida o destrucción de la cosa. La comprobación material de la tradición en la adquisición derivativa realizada mediante la Tokenización se concreta en las siguientes clases de tradición: en primer lugar, mediante la representación de la propiedad en el token correspondiente, lo que se correspondería con la *traditio ficta*; en segundo lugar, puede articularse con la comprobación mediante oráculos o terceros de confianza para un correcto traspaso posesorio como *tradición real*; finalmente, el cambio del título posesorio en caso de constitución de un derecho real limitado puede realizarse mediante el *constitutum possessorium* que, aunque el artículo 1463 CC lo refiera a bienes muebles, también se aplica a bienes inmuebles, con la finalidad de ejecutar las prestaciones mediante la *blockchain* en el *smart contract* de que se trate. Otras opciones alternativas al uso de un tercero intermediario en una *blockchain* son las siguientes: *fábrica* y *harbor*. El concepto de *fábrica* consiste en introducir una capa intermedia entre la plataforma P2P que ofrece inmuebles y sus potenciales clientes para que esta capa actúe de tercero a modo de fideicomitente. La encomienda de *fábrica* es ser el receptor temporal de la propiedad para incluirla en un contrato operado en una *blockchain* y mediante unas APIS, que son unos protocolos informáticos para que las webs intercambien la información necesaria para formalizar un *smart contract*. Por su parte, *harbor* introduce la capa intermedia antes referida a modo de *regulated token*, con objeto de comprobar el cumplimiento normativo de la transacción correspondiente. El *regulated token* es un protocolo que verifica la información de los inversores que pretendan participar en la transacción, y comprueba su dirección y la aprobación comercial de la transacción.

Aplicando lo expuesto al alojamiento colaborativo, tokenizar una propiedad inmobiliaria permite generar un token en un *smart contract* para dar un valor a ese token correspondiente al activo real, mediante la división de la propiedad y la atribución parcial de tokens. Este control permanente del objeto y la facultad de exclusión materializan la *smart property* que Nick Szabo[67] concibió. Asimismo, el token, como representación de un objeto contractual, habilita *per se* a exigir una determinada prestación relacionada con la entrega de la cosa, porque extiende la tecnología *blockchain* a un objeto. La Tokenización de bienes inmuebles opera de la siguiente manera: con este método, se crean tokens o fichas virtuales que representan un derecho real sobre un bien inmueble. El valor del token corresponderá al valor inicial de su lanzamiento, sujeto a las variaciones del propio mercado inmobiliario. El inversor de una plataforma P2P de alojamiento colaborativo, además de poseer un token negociable, también podrá convertirlo en una criptomoneda susceptible de ser utilizada indirectamente como método de pago en otra plataforma vinculada; por ejemplo, Blockchain habilita la conversión de las criptomonedas en saldo canjeable en *PayPal*. Este mecanismo, aplicado al alojamiento colaborativo, posibilita el abono del precio o una eventual plusvalía por la venta del inmueble.

La Tokenización plantea dos retos[68] para el derecho civil en relación con el objeto contractual, en el sentido de incorporar un bien digital e inmaterial para la representación o control de un activo real. En primer lugar, la sustitución del objeto contractual del derecho civil y su regulación legal, por la regulación del token: en forma de mecanismo reputacional, a modo de aceptación de los términos y condiciones de uso[69] de la plataforma correspondiente; o, en el caso de tratarse de un modelo de acceso abierto, en forma de *core team*[70] o personas que controlan y desarrollan centralizadamente la plataforma. En segundo lugar, la determinación de la naturaleza real o personal de los derechos derivados de los tokens. Puede existir un token como derecho de crédito que obligue al deudor, por representar

67. SZABO, N. (1996). «Smart contracts: building blocks for digital markets». *Extropy: The Journal of Transhumanist Thought,* vol. 16 [en línea] http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html [Fecha de consulta: 5 de junio de 2020].
68. Estos retos son indicados por SAVELYEV, A. (2018). «Some risks of tokenization and blockchainizaition of private law». *Computer Law & Security Review,* núm. 34, págs. 863-869.
69. En este sentido, se expresa BYGRAVE, L. A. (2015). *Internet Governance by Contract.* Oxford: Oxford University Press, págs. 30-39.
70. PHILLIPS, D. E. (2009). *The Software License Unveiled: how legislation by License Controls Software Access.* Oxford: Oxford University Press, págs. 147-173.

el derecho de un inversor a participar en los beneficios sobre la explotación de un derecho real. El alojamiento colaborativo es, por tanto, un derecho de crédito con deudor, por tratarse de una actividad emitida y transferida sobre la base de los algoritmos del protocolo informático, lo cual es más ajustado aquí por su tendencia a la permanencia y reipersecutoriedad, permitiendo su control remoto. En este último caso, existe una persona obligada con base en el derecho que representa ese token.

Así, debemos distinguir[71] entre *the right to a token* o el derecho a un token, como en las criptomonedas, y *the rights certified by a token* o los derechos que represente, como el derecho de propiedad, pues ello hace que podamos diferenciar dos relaciones jurídicas: la del propietario del token respecto de terceros, y la del propietario del token y el emisor del token, como sucede en las criptomonedas. El *asset token* o token de activos tiene un emisor, que se convierte en deudor respecto del propietario del token en cuanto a las obligaciones que certifica para proveer un servicio *online*, por ejemplo, un alojamiento colaborativo. La relación entre el emisor del token y el propietario es un derecho de crédito, pero ello no convierte el derecho del token en un derecho real, como sucede en las criptomonedas, cuando se trata de relaciones con terceros.

En consecuencia, y para finalizar, resultan claves diversas cuestiones en aras de regular los tokens, por tratarse de un derecho real y un derecho de crédito según su ámbito material de aplicación: la pérdida de control sobre el token; la eventual alteración del token por un *hacker*; la protección *erga omnes,* de tratarse de un derecho real; la clase de posesión del token, que deberá ser mediata; y, finalmente, la imposibilidad de transmitir el token sin la intervención de mineros o terceros. La solución que debería adoptarse al respecto es una adaptación legislativa para que el objeto tokenizado tenga las mismas garantías en el tráfico jurídico que el que no lo esté, pues la Tokenización permite el control remoto o la representación de un activo real; por tanto, es instrumental al objeto al que se vincula digitalmente y, en consecuencia, el tratamiento legal debe ser parejo. Asimismo, debería disponerse de previsiones específicas para cada tipo de contrato, especialmente para los que tengan eficacia real, y en particular aquellos que, además, recaigan sobre un bien inmueble y cuyas prestaciones sean de tracto sucesivo, pues el transcurso del tiempo puede hacer variar el valor del objeto del contrato.

4. El *Internet of Things* para la facultad de exclusión con distanciamiento social en el alojamiento colaborativo 4.0

La Tokenización se encuentra muy vinculada al desarrollo tanto de la tecnología *blockchain* como del IoT[72], por lo que deberemos prestar atención a una evolución difícil de prever. Mientras que el IoT puede tener más utilidad cuando se refiere a la administración y la conexión de los bienes muebles que se contengan en el alojamiento colaborativo, la Tokenización permite el control mediato de la propiedad y los actos de administración y disposición que sean pertinentes, como hemos examinado.

El IoT posibilita integrar el objeto en un *smart contract*, una conexión que hace posible su control[73]. El *smart contract* no puede *per se* adaptar la codificación sin la vinculación del objeto mediante el IoT, pues este instrumento posibilita la recepción de los eventos externos que le afecten y la incorporación de sus consecuencias jurídicas al contrato. Por lo

71. SAVELYEV, A. (2018). «Some risks of tokenization», *op. cit*., pág. 867.
72. STARK, J. (2016). «Making sense of Blockchain Smart Contracts» [en línea] https://www.coindesk.com/making-sense-smart-contracts [Fecha de consulta: 5 de junio de 2020], indica que puede alterar la naturaleza de las transacciones comerciales. Sobre la vinculación del IoT y de *blockchain* para garantizar la seguridad de las transacciones, véase BISWAS, S.; SHAIF, K.; LI, F.; NOUR, B.; WANG, Y. (2018). «A Scalable Blockchain Framework for Secure Transactions in IoT». *IEEE Internet of Things Journal*, núm. 9, págs. 1-10.
73. Cfr. STARK, J. (2016). «How Close Are Smart Contracts to Impacting Real-World Law? CoinDesk» [en línea] https://www.coindesk.com/blockchain-smarts-contracts-real-world-law [Fecha de consulta: 5 de junio de 2020], quien alude como problema la inexistencia de un control físico sobre los activos reales por parte del *smart contract*; sin embargo, esta codificación no es necesaria porque mediante la vinculación del objeto contractual al IoT ya es posible dicho control: «First, smart contracts require a way for computer code to control real *assets*. By enabling fully digitized assets, blockchains make it possible for code to exercise control over property. On a blockchain, control over an asset means controlling a cryptographic key that corresponds to the asset in question, rather than any physical object».

que se refiere a la fase de ejecución del contrato, el IoT puede servir para evitar errores o fraudes[74] en el uso del alojamiento colaborativo, emitir permanentemente información de lo que suceda en el interior del alojamiento colaborativo, controlar un uso indebido, así como medir eventos externos mediante el uso de algoritmos conectados con el *Big Data*.

Las ventajas que plantea la aplicación del IoT son diversas. Por una parte, facilita la ejecución real del contrato, sin necesidad de un ordenador central en quien confiar la ejecución o de un acuerdo posterior de las partes. Además, la conexión del objeto contractual mediante el IoT desincentiva el incumplimiento, pues la principal prerrogativa para la contraparte es la posibilidad de inutilizar el objeto del contrato; por ejemplo, en caso de impago, se puede cambiar la clave de acceso para impedir el uso de la vivienda, sin considerar una eventual inconstitucionalidad por no tratarse de una vivienda habitual.

En concreto y respecto del alojamiento colaborativo, el uso del IoT permite calificarlo de un verdadero *P2P accommodation 4.0*, como producto del turismo 4.0[75]. Una de las aplicaciones más comunes del alojamiento colaborativo 4.0 la encontramos en el uso de *cerraduras inteligentes,* programables por días concretos y claves ilimitadas para ejercer la facultad de exclusión. Estas se concretan en forma de códigos de acceso, como en el Reino Unido, o la programación de distintos códigos para el acceso a llaves tradicionales, como se realiza en Francia o Alemania. Encontramos otros métodos de acceso al alojamiento, como el reconocimiento facial –frecuente en el *home sharing*–, las pulseras inteligentes y los códigos PIN o códigos QR programables desde una aplicación móvil; esta *app*, por su conexión con el IoT, permitiría además avisar al usuario de un cierre incorrecto en caso de que se ausente de la vivienda. Asimismo, respecto de los bienes muebles del alojamiento colaborativo, es posible que los que sean de uso cotidiano se conecten a la red mediante el IoT, para que nos aconsejen o se activen mediante órdenes, sin intervención del propietario. Ello sucede con los altavoces inteligentes, la iluminación inteligente, e incluso pulseras inteligentes que gestionan determinados consumos programables. También existen aplicaciones, ejecutables con tabletas o *smartphones*, para personalizar cualquier elemento, incluyendo un asistente virtual para contratar servicios externos. Finalmente, también podremos ser atendidos, como sucede en algunos hoteles 4.0, por *smart robots*[76] o robots programados al efecto.

5. Reflexiones finales

El alojamiento colaborativo se encuentra fuertemente influenciado por el devenir que tenga *blockchain,* el IoT y la Tokenización para la gestión remota de dicho alojamiento, especialmente útil en el distanciamiento social impuesto por el COVID-19. La expansión de la tecnología *blockchain* y la Tokenización del alojamiento colaborativo, así como el IoT para el control del acceso al mismo o de los bienes muebles que se encuentren en él, va a permitir hablar de un verdadero alojamiento colaborativo 4.0, en la línea de la evolución que ha experimentado el turismo 4.0.

De esta manera, deberemos atender a un panorama cambiante en esta materia, a la regulación de las plataformas que efectúe la *Digital Services Act* y el reequilibrio de la asimetría negocial para el consumidor 2.0 y el turista 3.0, así como a la afectación de la pandemia en el turismo a nivel mundial. Por ello, resultaría oportuno abordar una regulación específica de la economía colaborativa en general, y de las plataformas P2P y del alojamiento colaborativo en particular, a pesar de ser consideradas por el Tribunal de Justicia de la Unión como servicios de la sociedad de la información. Por todo ello, podemos concluir que la evolución de las nuevas tecnologías en el alojamiento colaborativo deberá perseguir un objetivo final: que la transparencia programada de las prestaciones proteja al consumidor de alojamiento colaborativo frente a la abusividad.

74. JOHNSON, G. L. (2017). «Planning the future: blockchain Technology and the Insurance Industry». *In-House Defense Quarterly*, núm. 73, págs. 73-78 [en línea] https://www.rbmn.com/wp-content/uploads/2017/10/16J1065-GLJ-BLOCKCHAIN-TECHNOLOGY_.pdf [Fecha de consulta: 5 de junio de 2020].
75. Sobre el turismo 4.0, véase RODRÍGUEZ BAUTISTA, F. (2018). *Del hospitium al turismo 4.0*. Madrid: Libros.com, págs. 11-56.
76. NAVAS NAVARRO, S. (2016). Smart robots y otras máquinas inteligentes en nuestra vida cotidiana. Revista CESCO de *Derecho de Consumo*, 20, págs. 82-109.

Referencias bibliográficas

ABADI, J.; BRUNNERMEIER, M. (2019). «Blockchain Economics». *CEPR Discussion Paper.* 13420, pág. 2-6 [en línea] https://ssrn.com/abstract=3310346 [Fecha de consulta: 5 de junio de 2020].

AL-BASSAM, M. (2017). «SCPKI: A Smart Contract-based PKI and Identity System». *BCC'17,* págs. 1-6.

BANCO MUNDIAL (2018). *Tourism and the Sharing Economy: Policy & Potential of Sustainable Peer-to-Peer Accommodation* [en línea] http://documents.worldbank.org/curated/en/161471537537641836/pdf/130054-REVISED-Tourism-and-the-Sharing-Economy-PDF.pdf [Fecha de consulta: 5 de junio de 2020].

BASTANTE GRANELL, V. (2018). «El turista 3.0 o *adprosumer*: un nuevo reto para el derecho y la economía». *Revista Internacional de Derecho del Turismo*, vol. 2, núm. 2, págs. 47-73.

BILBAO ESTRADA, I. (2018). «Imposición sobre la renta y alojamiento colaborativo». En: A. M. DE LA ENCARNACIÓN (dir.); A. BOIX PALOP (coord.). *La regulación del alojamiento colaborativo: viviendas de uso turístico y alquiler de corta estancia en el derecho español.* Cizur Menor: Thomson Reuters Aranzadi, págs. 475-502.

BISWAS, S.; SHAIF, K.; LI, F.; NOUR, B.; WANG, Y. (2018). «A Scalable Blockchain Framework for Secure Transactions in IoT». *IEEE Internet of Things Journal,* núm. 9, págs. 1-10.

BOTSMAN, R.; ROGERS, R. (2010). *What's mine is yours: the rise of collaborative consumption.* Nueva York: Harpers Collins Publishers.

BOUAZZA ARIÑO, O. (2009). *La planificación territorial en Gran Bretaña. Especial referencia al sector turístico.* Cizur Menor: Civitas.

BYGRAVE, L. A. (2015). *Internet Governance by Contract.* Oxford: Oxford University Press.

CALDERÓN CORREDOR, Z. (2018). «Claves para la praxis fiscal del alojamiento "colaborativo". Una perspectiva de Derecho comparado». En: A. M. DE LA ENCARNACIÓN (dir.); A. BOIX PALOP (coord.). *La regulación del alojamiento colaborativo: viviendas de uso turístico y alquiler de corta estancia en el derecho español.* Cizur Menor: Thomson Reuters Aranzadi, págs. 527-542.

CAMPUZANO TOMÉ, H. (2015). «El alquiler de viviendas de uso turístico a partir de la Ley 4/2013: la necesaria interpretación conjunta de la LAU y de la legislación turística autonómica». *Revista Crítica de Derecho Inmobiliario,* núm. 749, págs. 1.199-1.246.

CNMC (2018). *Estudio sobre la regulación de las viviendas de uso turístico en España,* de 19 de julio de 2018, págs. 1-84 [en línea] https://www.cnmc.es/sites/default/files/2133063_2.pdf [Fecha de consulta: 5 de junio de 2020].

CNMC (2018). *Criterios en relación con las ICOs,* págs. 1-4 [en línea] http://cnmv.es/DocPortal/Fintech/CriteriosICOs.pdf [Fecha de consulta: 5 de junio de 2020].

COGLIANESE, C.; LEHR, D. (2017). «Regulating by robot: administrative decision making in the machine-learning era». *Georgetown Law Journal,* vol. 105, págs. 1.207-1.209.

COLEGIO DE REGISTRADORES DE ESPAÑA (2019). *Proyecto REGTURI: proyecto del Colegio de Registradores de España sobre apartamentos turísticos,* Nota de prensa de 4 de octubre de 2019 [en línea] https://www.registradores.org/-/la-decana-de-los-registradores-destaca-que-la-innovacion-esta-en-el-adn-de-los-registradores-y-senala-el-compromiso-con-el-medio-ambiente-y-con-la-igualdad/ [Fecha de consulta: 5 de junio de 2020].

CUSCÓ PUIGDELLÍVOL, E.; FONT GAROLERA, J. (2013). «Nuevas formas de alojamiento turístico: comercialización, localización y regulación de las viviendas de uso turístico en Cataluña». *Biblio3W Revista Bibliográfica de Geografía y Ciencias Sociales,* 1.134, págs. 1-17.

DE LA ENCARNACIÓN, A. M. (2016). «El alojamiento colaborativo: viviendas de uso turístico y plataformas virtuales». *Revista de Estudios de la Administración Local y Autonómica,* núm. 5, págs. 31-34.

DE LA ENCARNACIÓN, A. M. (2018). «Soluciones europeas en materia de regulación del alojamiento "colaborativo": París y Londres». En: A. M. DE LA ENCARNACIÓN (dir.); A. BOIX PALOP (coord.). *La regulación del alojamiento colaborativo: viviendas de uso turístico y alquiler de corta estancia en el Derecho español.* Cizur Menor: Thomson Reuters Aranzadi, págs. 189-210.

DE LA IGLESIA PRADOS, E. (2013). «La reforma en la regulación del contrato de arrendamiento urbano de vivienda de junio de 2013». *Actualidad Civil,* núm. 11, págs. 1-12.

DEVAUX, C. (2015). *L'habitat participatif: De l'initiative habitante à l'action publique.* París: Presses Universitaires Rennes, 394 pág.

DOMÉNECH PASCUAL, G. (2015). «La regulación de la economía colaborativa (Uber contra el taxi)». *Revista CEFLegal,* núm. 175-176, págs. 61-104.

EUROPA PRESS (2020). Boletín informativo sobre Airbnb [en línea] https://www.europapress.es/temas/airbnb/.

FELIU ÁLVAREZ DE SOTOMAYOR, S. (2018). «Modelos colaborativos en plataformas digitales: nuevos retos para los negocios internacionales y para el Derecho Internacional Privado». *Anuario Español de Derecho Internacional Privado,* vol. 18, págs. 399-424.

FERRARY, N. (2015). «Les nouvelles formes de tourisme collaboratif: una demande en pleine expansion». *Annales des Mines. Réalités industrielles,* núm. 3, págs. 50-53.

FINMA (2018). *Guidelines for enquiries regarding the regulatory framework for initial coin offerings (ICOs),* págs. 1-11 [en línea] https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/ [Fecha de consulta: 5 de junio de 2020].

GARCÍA CALVENTE, Y. (2007). *Aspectos tributarios del turismo residencial.* Barcelona: Bosch.

GONZÁLEZ CARRASCO, M. C. (2013). «El nuevo régimen de los arrendamientos de vivienda tras la ley de medidas de flexibilización y fomento del mercado del alquiler». *Revista CESCO de Derecho de Consumo,* núm. 6, págs. 170-190.

GUILLÉN NAVARRO, N. A.; ÍÑIGUEZ BERROZPE, T. (2015). «Las viviendas de uso turístico en el nuevo entorno p2p. Retos socio-jurídicos para el consumo colaborativo en el alojamiento turístico». *Estudios Turísticos,* núm. 205, págs. 9-34.

GUILLÉN NAVARRO, N. A., IÑIGUEZ-BERROZPE, T. (2016). «Acción pública y consumo colaborativo. Regulación de las viviendas de uso turístico en el contexto p2p». *Pasos. Revista de Turismo y Patrimonio Cultural,* vol. 14, núm. 3, págs. 751-768.

HEIDE, J.; PETERS, K. B. M. (2015). «Airbnb als hulpmiddel voor spreading van toerisme in Amsterdam?». *Vrijetijdstudies,* núm. 2, págs. 9-22.

JEFFERSON-JONES, J. (2015). «Airbnb and the Housing Segment of the Modern "Sharing Economy": Are Short-Term Rental Transactions an Unconstitutional Taking?». *Hastings Constitutional Law Quarterly,* vol. 42, 3, págs. 557-575.

JOHNSON, G. L. (2017). «Planning the future: blockchain Technology and the Insurance Industry». *In-House Defense Quarterly,* núm. 73, págs. 73-78 [en línea] https://www.rbmn.com/wp-content/uploads/2017/10/16J1065-GLJ-BLOCKCHAIN-TECHNOLOGY_.pdf [Fecha de consulta: 5 de junio de 2020].

KASSAN, J.; ORSI, J. (2012). «The legal landscape of the sharing economy». *Journal of Environmental and Litigation,* núm. 27, págs. 1-20.

KRUMHOLZ, J.; MAHONY, I. (2019). «Blockchain and intelectual property: A case study». En: DEWEY, J. (dir.). *Blockchain Laws and Regulations 2019.* Londres: Global Legal Insights [en línea] https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/4-blockchain-and-intellectual-property-a-case-study [Fecha de consulta: 5 de junio de 2020].

LEFEBVRE, N. (2015). «Destination et expériences: l'adaptation de l'offre touristique de Paris aux nouvelles attentes». *Annales des Mines. Réalités industrielles,* núm. 3, págs. 58-62.

MARTÍNEZ CAÑELLAS, A. (2014). «La cesión del uso de la vivienda a no residentes: contrato de alojamiento (de estancias turísticas) en viviendas y el contrato de arrendamiento de temporada, conforme a la Ley del Turismo de las Islas Baleares tras la reforma de la Ley de Arrendamientos Urbanos». *Boletín de la Academia de Jurisprudencia y Legislación de las Illes Balears,* núm. 15, págs. 151-176.

NASARRE AZNAR, S. (2015). «La eficacia de la Ley 4/2013, de reforma de los arrendamientos urbanos, para aumentar la vivienda en alquiler en un contexto europeo». *Revista Crítica de Derecho Inmobiliario,* núm. 747, págs. 205-249.

NASARRE AZNAR, S. (2018). «Collaborative housing and blockchain». *Administration,* vol. 66, 2, págs. 59-82.

NASARRE AZNAR, S. (2018). «Ownership at stake (once again): housing, digital contents, animals and robots». *Journal of Property, Planning and Environmental Law,* vol. 1, págs. 69-86.

NAVAS NAVARRO, S. (2016). «Smart robots y otras máquinas inteligentes en nuestra vida cotidiana». *Revista CESCO de Derecho de Consumo,* núm. 20, págs. 82-109.

NÚÑEZ IGLESIAS, A. (2010). «Tipología de los contratos de alojamiento extrahotelero (I)». *Actualidad Civil,* núm. 12, págs. 1-20.

PÉRINET-MARQUET, H. (2014). «Accès au logement et urbanisme renové. Loi ALUR du 24 mars 2014». *Semaine juridique,* núm. 15, págs. 709-712.

PETROPOULOS, G. (2016). «An economic review on the Collaborative Economy». *European Parliament,* págs. 1-32 [en línea] http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/595358/IPOL_IDA(2016)595358_EN.pdf [Fecha de consulta: 5 de junio de 2020].

PHILLIPS, D. E. (2009). *The Software License Unveiled: how legislation by License Controls Software Access.* Oxford: Oxford University Press.

PONCE SOLÉ, J. (2018). «Economía colaborativa, viviendas de uso turístico e impactos en el marco del desarrollo urbano sostenible, ¿hacia una futura regulación más innovadora y flexible?». En: A. M. DE LA ENCARNACIÓN (dir.); A. BOIX PALOP (coord.). *La regulación del alojamiento colaborativo: viviendas de uso turístico y alquiler de corta estancia en el derecho español.* Cizur Menor: Thomson Reuters Aranzadi, págs. 39-70.

RANCHORDÁS, S.; ZUREK, K.; GEDEON, Z. (2016). «Home Sharing in the Digital Economy: The Cases of Brussels, Stockholm and Budapest». *Impulse Paper prepared for the European Commission* [en línea] https://www.rug.nl/research/portal/publications/homesharing-in-the-digital-economy-the-cases-of-brussels-stockholm-and-budapest-impulse-paper-prepared-for-the-european-commission(82c6123d-be1b-46b9-8b36-354632f7a673)/export.html [Fecha de consulta: 5 de junio de 2020].

RODRÍGUEZ BAUTISTA, F. (2018). *Del hospitium al turismo 4.0.* Madrid: Libros.com.

RODRÍGUEZ FONT, M. (2018). «Avances en el proceso de regulación normativa del alojamiento "colaborativo" en Cataluña». En: A. M. DE LA ENCARNACIÓN (dir.); A. BOIX PALOP (coord.). *La regulación del alojamiento colaborativo: viviendas de uso turístico y alquiler de corta estancia en el derecho español.* Cizur Menor: Thomson Reuters Aranzadi, págs. 295-324.

RODRÍGUEZ MARÍN, S. (2017). «Los modelos colaborativos y bajo demanda en plataformas digitales». *Sharing España, Adigital,* págs. 1-59 [en línea] https://www.fidefundacion.es/attachment/810605/ [Fecha de consulta: 5 de junio de 2020].

SAVELYEV, A. (2018). «Some risks of tokenization and blockchainizaition of private law». *Computer Law & Security Review,* núm. 34, págs. 863-869.

SHAMMA, H.; DE LA FUENTE, G.; BARROSO, P. (2019). *Informe PropTech 2019 en España.* Savills, Aguirre Newman, págs. 1-4 [en línea] http://inmuebles.savills-aguirrenewman.es/informes/proptech/informe-proptech.pdf [Fecha de consulta: 5 de junio de 2020].

STARK, J. (2016). «How Close Are Smart Contracts to Impacting Real-World Law?». *CoinDesk* [en línea] https://www.coindesk.com/blockchain-smarts-contracts-real-world-law [Fecha de consulta: 5 de junio de 2020].

STARK, J. (2016). «Making sense of Blockchain Smart Contracts» [en línea] https://www.coindesk.com/making-sense-smart-contracts [Fecha de consulta: 5 de junio de 2020].

SZABO, N. (1996). «Smart contracts: building blocks for digital markets». *Extropy: The Journal of Transhumanist Thought,* vol. 16 [en línea] http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html [Fecha de consulta: 5 de junio de 2020].

VERDERA IZQUIERDO, B. (2009). «La problemática del turismo residencial». *Diario La Ley,* 7.297, págs. 9-11.

VILALTA NICUESA, A. E. (2018). «La regulación europea de las plataformas de intermediarios digitales en la era de la economía colaborativa». *Revista Crítica de Derecho Inmobiliario,* núm. 765, págs. 275-330.

VILALTA NICUESA, A. E. (2018). «Los sistemas reputacionales como mecanismos de compulsión privada». En: F. ESTEBAN DE LA ROSA (dir.). *La resolución de conflictos de consumo: la adaptación del Derecho español al marco europeo de resolución alternativa (ADR) y en línea (ODR).* Cizur Menor: Thomson Reuters Aranzadi, págs. 443-464.

Cita recomendada

ARGELICH COMELLES, Cristina (2020). «Construyendo un P2P *accommodation 4.0* frente al COVID-19: *Proptech*, autorregulación y Tokenización». *IDP. Revista de Internet, Derecho y Política*, núm. 31, págs. 1-20. UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i31.3225

Sobre la autora

Cristina Argelich Comelles
cristina.argelich@uca.es

Profesora Doctora de Derecho civil de la Universidad de Cádiz (2017-), acreditada por ANECA a Profesor Contratado Doctor (2019) y Profesor de Universidad Privada (2018), y por AQU a Profesor Lector (2019). Coordinadora del Módulo de Mediación Familiar del Máster Universitario en Mediación (2018-). Doctora en Derecho con sobresaliente *cum laude* por la Universidad de Lleida (2017), obtuvo el IX Premio de la Revista Crítica de Derecho Inmobiliario (2020) y el Primer Premio del XII Certamen Universitario Arquímedes del Ministerio de Educación (2013), en el área de ciencias sociales y humanidades. Anteriormente, fue investigadora predoctoral de la Generalitat de Cataluña (2014-2017), investigadora predoctoral de la Universidad de Lleida (2013-2014), asistente de docencia de la Generalitat de Cataluña (2012-2014), becaria de Introducción a la Investigación de la Universidad de Lleida (2012-2013), y becaria de colaboración del Ministerio de Educación (2011-2012). El derecho inmobiliario constituye su principal línea de investigación, donde destaca su monografía *La expropiación temporal del uso de viviendas* (Marcial Pons, 2017), junto con otras publicaciones. Cuenta con la realización de diversas ponencias en congresos académicos, así como una estancia posdoctoral en The University of Manchester (2017).

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

www.uoc.edu/idp

ARTÍCULO

Inteligencia artificial, *big data* y aplicaciones contra la COVID-19: privacidad y protección de datos

Lorenzo Cotino Hueso
Universidad de Valencia

Fecha de presentación: abril de 2020
Fecha de aceptación: julio de 2020
Fecha de publicación: julio de 2020

Resumen

El *big data* y la IA han fracasado en la prevención, pero pueden ser muy útiles frente a la COVID-19 e incluso para evitar confinamientos y otras restricciones de derechos que provoca. La IA puede ser extremadamente eficaz para integrar, estructurar y extraer información y conocimiento de ingente cantidad y variedad de *big data* para la investigación biomédica. También es útil para mejorar la atención e información ciudadana y de salud, la telemedicina y la mejor asignación de los recursos humanos y materiales. Más amenazante para la privacidad puede ser el desarrollo de *apps,* pasaportes biológicos electrónicos o sistemas de geolocalización, trazabilidad y monitoreo de personas implementados para hacer frente a la COVID-19, en especial si se sigue el caso asiático. No obstante, de momento no es el que parece seguirse en la UE. Se analiza el régimen jurídico aplicable, la legitimación legal de los diferentes tratamientos de datos, la necesidad de una base legal de calidad, especialmente para el caso de *apps* y rastreos. Y más allá de la base legal y legitimación se tienen en cuenta las necesarias garantías de estos tratamientos masivos, especialmente de las *apps*. El Consejo Constitucional francés y especialmente las instituciones europeas han marcado el camino a seguir, con una acción más discreta en España, que en junio ha regulado con fuerza de ley algunos aspectos del tratamiento de datos de manera muy insuficiente. Existen dos grandes modelos europeos (PEPP-PT y el DP-3T por el que se ha decantado España) más o menos centralizados y más o menos seguros, así como desarrollos propios. Y al parecer para su utilidad deben integrarse bajo las APIs y desarrollos conjuntos de Apple y Google, lo que genera suspicacias. Se sostiene que el Derecho impulsa que tecnológicamente sí sea posible maximizar tanto la eficacia de la lucha contra la COVID-19 como todos nuestros derechos. El tema, sin duda, exigirá un análisis continuo de expertos, sociedad civil y autoridades de datos.

Palabras clave

COVID-19, protección de datos, inteligencia artificial, geolocalización, privacidad

Artificial intelligence, big data and applications against Covid-19, and privacy and data protection

Abstract

Big data and AI did not succeed in preventing Covid-19, but they can be very useful in the fight against it and even for avoiding confinements and other restrictions on rights which it brings about. AI can be extremely useful for integrating, structuring and extracting an enormous quantity and variety of big data information and knowledge for biomedical research. It is also useful for improving civic and health assistance and information, telemedicine and the best assignment of human resources and materials. Even more threatening for privacy could be the development of apps, electronic biological passports, geolocation systems, and the traceability and monitoring of people in the fight against Covid-19, particularly if the Asian model is followed. However, it seems that this not being followed in the EU. There is an analysis of the applicable legal set of rules, the legal legitimation of the various data processing systems, and the need for a legal basis of quality, especially in the case of apps and searches. And besides the legal basis and legitimation, the necessary guarantees of these mass processing systems are considered, particularly of the apps. The impetus of law means that it is indeed technologically possible to maximise the efficiency of the fight against Covid-19 and to maximise all our rights.

Keywords

Covid-19, data protection, artificial intelligence, geolocation, privacy

1. Introducción. El virus de la amenaza

El coronavirus SARS-CoV-2 no se ve ni se aprecia en el momento, sino tarde y cuando se dan sus consecuencias, pudiendo estar atacando de modo silente los derechos COVID-19 y, en particular, la privacidad. El coronavirus se expandió de China a todo el mundo y esperemos que, en una segunda oleada, no exporte también el control social y la vigilancia totalitaria de la mano del *big data*, la IA, las *apps* covid y los pasaportes biológicos electrónicos. Entre los peligros de la IA (Cotino, 2019a), Han nos ha venido alertando desde hace años de la *psicopolítica digital data*; ahora lo hace con respecto a la *biopolítica digital*, en la que se controlan todos nuestros biodatos (Han, 2020). Al parecer, frente al coronavirus, la *d* de la *d*isciplina asiática ha sido mucho más eficaz que la *d*escoordinación europea o el *d*arwinismo norteamericano (Ferràs, 2020). Han nos recuerda que la mentalidad autoritaria asiática –procedente del confucionismo– conduce a la obediencia, donde impera el colectivismo y no hay conciencia crítica ante la vigilancia digital. La infraestructura de control social de la IA china parece ser sumamente eficaz contra la pandemia y ahora genera incluso admiración. Ello puede llevarnos a la *biopolítica*, o en términos de Harari (2020), a una «vigilancia hipodérmica». Hasta hace poco, imperaba una «vigilancia epidérmica»: «el Gobierno quería saber sobre qué clicaba exactamente nuestro dedo». Ahora quiere conocer nuestra temperatura, nuestra presión arterial y muchos otros datos relativos a nuestra salud para saber si estamos enfermos antes que nosotros, dónde hemos estado y con quién nos hemos reunido.

No solo los Gobiernos han fallado. La IA y el *big data*, las plataformas o redes sociales no han servido para predecir y alertar sobre la magnitud y propagación del coronavirus: ha habido un «fallo colosal del capitalismo de vigilancia» (Ortega, Balsa-Barreiro y Cebrián, 2020), que no lidia bien con las sorpresas, y tampoco la IA ha sabido integrar información de calidad de modo coherente. La competencia económica entre inteligencias artificiales parece que ha ido en contra de la inteligencia colectiva. Sin embargo, la IA y el *big data* pueden ser unas herramientas formidables contra la COVID-19, pero como toda herramienta dependerá del uso acertado de la misma.

Señala Harari (2020) que, «cuando a la gente se le da a elegir entre la intimidad y la salud, suele elegir la salud». También se ha afirmado que «anteponer el derecho a la privacidad al derecho a la vida o al de libertad de movimientos no tiene sentido, [y] es un dislate» (Pedreño, 2020). Plantear este tipo de debates en términos binarios es peligroso e incluso demagógico. El sistema constitucional política y jurídicamente tiene la virtud de saber deliberar, ponderar y armonizar derechos fundamentales entre sí y con otros bienes constitucionales. Como se verá, hay soluciones de carácter tecnológico que, guiadas por el Derecho, permiten una maximización de la eficacia contra el coronavirus minimizando los impactos en la privacidad, la libertad de circulación y otros derechos. Se trata de una cuestión cambiante, como lo ha sido desde el momento de entrega del presente estudio en abril hasta su revisión final dos meses después.

2. Usos esenciales de la IA y el big data frente a la COVID-19

2.1. IA y *big data* para estructurar y extraer información y conocimiento en la investigación biomédica

En el área de la sanidad, cada vez es más importante «el procesamiento de datos personales relacionados con la salud en los sectores público y privado mediante herramientas digitales» (apdo. 2.1)[1]. Y cada vez son más variadas las fuentes y su naturaleza. Se tratan datos estructurados, semiestructurados y, mayoritariamente, no estructurados[2] y brutos, procedentes de sensores, de grandes transacciones de datos, de registros médicos electrónicos y de datos biométricos (huellas dactilares, información genética, escáneres de retina, rayos X y otras imágenes médicas,

1. Recomendación CM / Rec (2019) 2 del Comité de Ministros a los Estados miembros sobre la protección de datos relacionados con la salud, de 27 de marzo de 2019.
2. Ortega, 2019, págs. 176-178; Alcalde y Alfonso, 2019, págs. 60 y sigs.

la presión arterial, el pulso y lecturas de oximetría de pulso y otros tipos similares de datos), pero también de historias clínicas, imágenes, pruebas, publicaciones, webs y redes sociales. Asimismo, también pueden ser de especial importancia los datos de tráfico, la geolocalización, los metadatos y la información procedente de aplicaciones COVID-19 y operadores de telecomunicación.

Algunos son datos primarios propiamente relativos a la salud, con un régimen jurídico relativamente nítido, pero cada vez se barajan más datos secundarios muy heterogéneos, en sus fuentes y tipología (German Ethics Council, 2017, núm. 99). Esta variedad de orígenes y usos primarios y secundarios genera cada vez más problemas e incertidumbres jurídicas (núm. 19). Estos datos se canalizan, integran o vierten en *datahubs* con fuente central, lagos de datos o de modo centralizado en *data warehouse*. La IA es esencial para que estos datos de usos secundarios y especialmente desestructurados puedan ser datos útiles para la investigación y los usos médicos (Montalvo, 2019, págs. 47-48).

En las acciones frente a la COVID-19 se ha de facilitar el flujo de estos datos entre los sectores público y privado de los distintos países –dentro y fuera de la UE– a fines de salud pública. Para extraer información y conocimiento se precisan tratamientos de ingentes cantidades de datos –principalmente secundarios y desestructurados– a los que aplicar esquemas de lectura y escritura y otros sistemas de IA. Esta se emplea asimismo para llevar a cabo un profundo análisis de datos clínicos de pacientes infectados, hospitalizados, en cuarentena o sospechosos (Martínez, 2020a). De especial interés con redes neuronales para el reconocimiento inteligente y la lectura natural de imágenes relativas o para el apoyo a la asignación selectiva e individualizada de fármacos.

2.2. IA para la atención e información ciudadana y de salud, la telemedicina y la asignación de recursos

La Comisión Europea (2020 c) ha subrayado los tres ejes o "funcionalidades" del tratamiento de datos frente al COVID-19: funcionalidad de información, de comprobación de síntomas y de telemedicina y de rastreo de contactos y de alerta. La IA puede jugar un papel importante a la hora de facilitar atención e información ciudadana y de salud. Puede canalizar las muchas consultas de la ciudadanía, generar datos y extraer conocimiento de las mismas. Es de interés gestionar el origen y localización de llamadas para la gestión de los riesgos granularizada por territorios y otros factores. Al respecto, hoy en día es posible gestionar datos de las conversaciones a través de la analítica de las emociones, una técnica habitualmente utilizada en el *neuromarketing*. La IA también es capaz de facilitar los mensajes perfilados e individualizados para cada tipología de consulta. Permite también el uso de *chatbots* que descongestionen las líneas de atención e incluso que proporcionen información de calidad y perfilada. Al respecto, el ICO (Information Commissioner's Office) ha señalado que es posible el envío de mensajes de salud pública, «ya que estos mensajes no son *marketing* directo» (ICO, 2020). Otra cuestión es, obviamente, cómo se efectúa el perfilado y selección de los destinatarios.

La IA y el *big data* también pueden ser muy útiles para proponer una farmacología adecuada y para implementar una asignación estratégica de recursos médicos humanos y materiales, así como para distribuir o derivar a los pacientes, según necesidades concretas derivadas de la COVID-19, maximizando así la eficiencia de los sistemas sanitarios. Esta trazabilidad, por supuesto, también podría potenciar la eficacia de nuestro hospitales y centros de salud.

Asimismo, la telemedicina (la seria) puede facilitar la prestación de servicios sanitarios, descongestionar la atención presencial y reutilizar al personal médico infectado y en cuarentena que siga estando operativo, pudiendo generar un estimable *big data* luego utilizable. El ICO (2020) ha recordado que la normativa «tampoco les impide utilizar la última tecnología para facilitar consultas y diagnósticos seguros y rápidos». Esencialmente, lo que hay que asegurar es la seguridad informática.

3. El régimen jurídico aplicable, legitimación legal y cumplimiento normativo en España y Europa. La constitucionalidad de la regulación francesa

La IA atrae casi por defecto la aplicación del régimen de protección de datos, el cual, en ocasiones, es casi el único régimen jurídico hoy día claramente aplicable. Y esto es así porque la IA implica el perfilado y activación de decisiones automatizadas que afectan a las personas (Grupo de trabajo del artículo 29, 2018, págs. 7-8). Para que el régimen de protección de datos pueda ser aplicado debe darse la premisa de que los variados macrodatos que *alimentan* la IA sean datos de personas identificadas, identificables o reidentificables. Como se ha recordado con ocasión de la crisis de la COVID-19, no se aplicará la normativa si existe una anonimización que garantice que los datos no vuelvan a ser personales[3]. Pero ello es realmente difícil puesto que, como ha recordado el Libro blanco de la IA (Comisión Europea, 2020, págs. 21 y sigs.), estas mismas tecnologías se utilizan para «rastrear y desanonimizar datos relativos a personas (...) con relación a conjuntos de datos que, en sí mismos, no contienen datos personales».

En cuanto a la legitimación del tratamiento de datos en razón de la pandemia, tanto las autoridades comunitarias[4] como españolas (AEPD y APDCAT) de protección de datos han señalado que «las reglas (...) actualmente vigentes en Europa son lo suficientemente flexibles» (SEPD, 2020a). En concreto, hay que seguir el considerando 46 y los artículos 6.2 párrafos c, d y e y el artículo 9.2, párrafos c, g, h e i) 6 y 9 del RGPD. Así, el EDPB (2020a) afirma que el RGPD «permite a las autoridades de salud pública competentes y a los empleadores procesar datos personales en el contexto de una epidemia, de conformidad con la legislación nacional y en las condiciones establecidas en ella por parte de las autoridades públicas competentes». Ello es aplicado «estrictamente a la duración de la emergencia» (EDPB, 2020a), pues las restricciones «no están aquí para quedarse después de la crisis» (SEPD, 2020a). La Comisión Europea ha ido en la misma línea (2020 b y c), pero con acierto señala que «cuanto mayor sea la repercusión de cara a las libertades de la persona, mayores deben ser las correspondientes salvaguardias previstas en la legislación pertinente». Es más, la Comisión concreta la necesaria previsión legal del detalle del tratamiento y la finalidad, excluyendo expresamente otros fines, determinación del responsable, así como las garantías específicas (2020 c 3.3). Algo que ni por asomo se da en la legislación española al momento de cerrar estas páginas.

En consecuencia, para el Derecho de la UE y en general es relativamente fácil legitimar legalmente los tratamientos de datos ordinarios y especialmente protegidos como los de salud, entre otros, con el fin de prevenir, atender y gestionar los servicios sanitarios, así como para la investigación médica. Hay que advertir que por lo general se requiere que haya una ley nacional, salvo en caso de la concreta excepción por la protección de intereses vitales del interesado u otras personas físicas (artículo 6.1.d) o por tratarse de datos sensibles (artículo 9, 2.º c, del RGDP).

Como ha recordado el EDPD, el papel del legislador nacional es muy importante, al punto que «las condiciones y el alcance de dicho tratamiento [de datos frente al COVID-19] varían en función de las disposiciones legislativas promulgadas en cada Estado miembro» (2020 b) 69. 2º). Pues bien, por cuanto a la regulación en España, la AEPD (2020b) y la APDCAT (2020) no han dudado en acudir al genérico artículo 3 de la Ley Orgánica 3/1986, de 14 de abril. Asimismo, los artículos 5, 9 y 84 de la Ley 33/2011, de 4 de octubre, General de Salud Pública contienen genéricas habilitaciones para el control de pacientes, la comunicación de datos y otras afectaciones de derechos que pueden valer también para la protección de datos. De modo más concreto, el artículo 16, 3.º de la Ley 41/2002 de autonomía del paciente regula el acceso concreto y motivado por profesional sanitario en caso de riesgos graves de salud. Asimismo, la legislación ordinaria excepcional de protección civil puede en su caso ser igualmente proyectable. En la última revisión cabe destacar, de un lado, la Orden SND/404/2020, de 11 de mayo, de medidas de

3. Alberto Sáiz, 2017, págs. 40 y sigs.; Grupo de trabajo del artículo 29, Dictamen 5/2014.
4. EDPB en un documento más informal al inicio y más concreto después, Supervisor Europeo de Protección de datos SEPD, Comisión Europea en sus dos documentos, posiblemente los más definidos y concretos. También en Reino Unido en primer lugar el ICO y luego sucesivas autoridades nacionales.

vigilancia epidemiológica dirigida a la adecuación de sistemas informáticos y los tratamientos y comunicaciones de datos, que se legitiman por «interés público esencial en el ámbito específico de la salud pública [...] y para la protección de intereses vitales» (art. 9). No parece que dicha norma infralegal fuera la más adecuada. En este sentido, y con mayor importancia a inicios de junio, destaca el Real Decreto-ley 21/2020, de 9 de junio de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por la COVID-19. Esta norma con fuerza de ley dedica un capítulo a la detección, control y vigilancia. Por lo que aquí interesa, se impone la obligación de facilitar al sector de salud información y datos de contacto para la trazabilidad a «establecimientos, medios de transporte o cualquier otro lugar, centro o entidad pública o privada en los que las autoridades sanitarias identifiquen la necesidad de realizar trazabilidad de contactos». Todo ello bajo la legitimación del «interés público esencial en el ámbito específico de la salud pública, y para la protección de intereses vitales de los afectados y de otras personas físicas». No hay delimitación concreta de datos, finalidades muy específicas, previsión de reutilización, ni siquiera para la investigación. Tampoco hay previsiones específicas respecto de las garantías o medidas de seguridad. No se da cobertura alguna a pasaportes biológicos y, especialmente, a aplicaciones de rastreo. Aunque se brinda cierta cobertura legal, ciertamente no es la respuesta legal que sería precisa en España y a buen seguro no pasaría el tamiz del Consejo Constitucional francés, por ejemplo, ni las especificaciones europeas. Más preocupante si cabe es para Cataluña su Decreto Ley 27/2020, de 13 de julio, que en su *escondido* Anexo III permite obligar a "registrar a los asistentes" a lugares de culto y "todas las reuniones tienen que registrar a los asistentes", para su posible cesión. Todo ello sin mayor concreción o garantía.

Además de la referida legitimación del RGPD y la base legal nacional, en el caso del uso de IA y *big data* para la investigación y lucha contra la COVID-19 hay que tener en cuenta el régimen claramente favorable a la investigación biomédica (artículos 5, 9 y 89 del RGPD) y prestar especial atención a la LO 3/2018 en el artículo 9 y especialmente su disposición adicional 17.ª[5]. Este régimen facilita la investigación de la COVID-19 por parte del sector público y privado con legitimación sin consentimiento directo, así como las cesiones de datos de fuentes variadas para usos secundarios y reutilización en «líneas» o «áreas» de investigación afines en lucha contra la COVID-19. Ello, no obstante, bajo garantías de minimización, seudonimización, confidencialidad, separación funcional e incluso de participación de comités de ética e informes particulares del DPD. Aunque no solo, hay que tener sobre todo en cuenta su apartado c 2.º, que permite únicamente a autoridades e instituciones públicas sanitarias estudios de salud sin consentimiento «en situaciones de excepcional relevancia y gravedad para la salud pública», como es el caso[6].

Más allá de la necesidad del consentimiento, hay que centrarse en el cumplimiento normativo y sus garantías. El EDPB recuerda que, «incluso en estos tiempos excepcionales, el responsable y el encargado de datos deben garantizar la protección de los datos personales de los interesados» con el cumplimiento de los principios de proporcionalidad, limitación al período de emergencia y a los fines específicos y explícitos e información transparente –incluyendo el tiempo de retención–, así como implementar las medidas de seguridad y políticas de confidencialidad adecuadas, que deben documentarse apropiadamente (EDPB, 2020). En la misma dirección, la AEPD (2020a) insiste en que hay que controlar solo aquellos datos que sean verdaderamente necesarios para la finalidad, «sin que pueda confundirse conveniencia con necesidad». Asimismo, hay que evitar innecesarias comunicaciones a terceros, «como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines» (considerando 54) (AEPD, 2020b, pág. 7). Sin perjuicio de la base legal y la no necesidad de consentimiento, se ha de seguir el régimen general de protección –principios, legitimación del tratamiento, transparencia, derechos, responsabilidad proactiva y privacidad– en el diseño o el régimen de las transferencias internacionales de datos. Igualmente, y por defecto, se exigirá el estudio de impacto. Será necesaria la articulación de un buen entramado jurídico entre responsables, corresponsables, encargados y todos aquellos sujetos que participan en la compleja cadena de valor de la IA que garantice el cumplimiento normativo y las distintas responsabilidades.

5. Sobre el tema cabe seguir los estudios de A. Troncoso o R. Martínez y, en especial, el ya citado monográfico de Revista de derecho y genoma humano, núm. extra 1, 2019.
6. Entre otros, Dictamen Autoridad Catalana de Protección de Datos CNS 15 y el 18/2019 y el «Informe 073667/2018», de la AEPD.

Además, el uso de la IA respecto de los humanos es el ámbito potencial de proyección del «derecho» a no ser sometido a decisiones automatizadas reconocido en el artículo 22 del RGPD de la UE con las garantías añadidas que implica (Cotino, 2019b). Tanto el Grupo de trabajo del artículo 29-UE (2018, págs. 35, 37-38) como la AEPD (2020a) van detallando las garantías del cumplimiento normativo respecto de la IA y las decisiones automatizadas, que no solo son relativas al derecho a expresar e impugnar decisión o las reforzadas garantías de transparencia (artículos 13. 2.º f, 14. 2.º g y 15. 1.º h del RGPD). En cuanto al ámbito de salud, este «derecho» emanado del artículo 22 también supone una prohibición más intensa de tratamientos automatizados si estos se basan en datos especialmente protegidos. No obstante, el consentimiento explícito o una legislación específica en razón de un «interés público fundamental» pueden levantar esta prohibición (artículo 9. 2 a y g del RGPD).

Igualmente, el empleo sanitario de la IA es sin duda un uso de alto riesgo para el Libro blanco de la IA de la Comisión Europea (2020, págs. 21 y sigs.). En estos casos se deben cumplir más severamente las garantías; y tanto es así que se prevé un sistema de control previo.

Además, si se trata del uso público de la IA por parte de los poderes públicos, habrá que modular y, por lo general, intensificar muchas garantías, tal y como hemos perfilado desde 2019 en la Red de Derecho Administrativo e IA (DAIA)[7] y en diferentes monografías[8], así como en otros estudios de Cerrillo (2019), Boix (2020) o Sierra (2020).

La reciente sentencia de 5 de febrero de 2020 del Tribunal de Distrito de la Haya (C / 09/550982 / HA ZA 18-388) es un buen recordatorio de que sí que se puede utilizar la IA para finalidades públicas, si bien bajo fuertes garantías de transparencia y caja blanca frente a la opacidad (Cotino, 2020b). De igual modo, deben darse garantías de separación funcional, control y auditorías independientes, seudonimización o confidencialidad.

En la revisión de este estudio, hay que destacar la regulación del tratamiento de datos frente a la COVID-19 en Francia de 9 de mayo[9] y su admisibilidad por el Consejo Constitucional (2020) el 11 de mayo. El extenso artículo 11 (1.500 palabras) regula los tratamientos de datos determinando claramente cuatro finalidades: identificación de personas infectadas y en riesgo de infección, orientación y apoyo, y vigilancia epidemiológica e investigación). Expresamente «Se excluye de estos propósitos el desarrollo o despliegue de una aplicación informática destinada al público y disponible en equipos móviles que permita informar a las personas que han estado cerca de personas diagnosticadas con COVID-19». Los tratamientos serán por el tiempo estrictamente necesario o como máximo seis meses para tratar y comunicar datos sin consentimiento por el sistema de información de salud y distintas entidades. Se señala un plazo de conservación de tres meses, hasta seis. Hay remisiones al desarrollo reglamentario, pero no en blanco, así como prescripciones de información y control parlamentario. El Consejo Constitucional da una amplia respuesta (núm. 59-82) a las diversas alegaciones de inconstitucionalidad y es prácticamente favorable a toda la regulación. Se pone de manifiesto del valor de la salud, señala que expresamente se excluye el desarrollo de *app* de este precepto (por lo que no hace valoración alguna sobre el tema), considera bien delimitados los datos a recabar, comunicar y utilizar y todos acordes a cada finalidad. Se admite igualmente como adecuado quiénes serán los cesionarios de los datos y se aceptan las remisiones reglamentarias. También se reputan como suficientes las garantías para la subcontratación y, especialmente de interés, se recuerda que esta regulación especial no exime del régimen jurídico general europeo y francés respecto de garantías, seguridad, derechos, transferencias, etc. Asimismo, se reafirman las competencias de la CNIL (autoridad francesa de datos), así como las atribuciones de las distintas autoridades, sin perjuicio del control parlamentario. Es más, para dicho control parlamentario no procede la remisión de datos personales sensibles. Se trata de un referente importante tanto la regulación legal, como la constitucionalidad de las diversas medidas a adoptar.

7. Ver las conclusiones de Toledo de 1 de abril (http://links.uv.es/PHAPt3l) y la declaración final de Valencia de 24 de octubre (http://links.uv.es/e2w7MCR).
8. Monográficos de la Revista general de Derecho Administrativo, núm. 50 (febrero de 2019) y de la Revista catalana de derecho público, núm. 58 (2019).
9. Ley que extiende el estado de emergencia de salud hasta el 10 de julio y complementa sus disposiciones, http://www.assemblee-nationale.fr/dyn/15/textes/l15t0418_texte-adopte-seance

4. *Apps*, pasaportes biológicos electrónicos, sistemas de geolocalización, trazabilidad y monitoreo de personas frente a la COVID-19

Preocupa sobre todo la captación y tratamiento masivo de datos especialmente protegidos (incluso *hipodérmicos*, en términos de Harari), así como de metadatos, datos de geolocalización y de tráfico a través de webs, plataformas y aplicaciones, principalmente aplicaciones creadas como medida frente al coronavirus. Siguiendo el caso de China, se especula con pasaportes biológicos electrónicos en razón de estas aplicaciones. Tales herramientas pueden resultar muy útiles para gestionar las relaciones, contactos y movilidad de los afectados o para controlar el cumplimiento de confinamientos generales y particulares, así como la ubicación de enfermos y contagiados. Además de para el control sanitario, y en su caso de seguridad, también puede ser esencial para la previsión y asignación de servicios de salud, sociales y de cualquier otro tipo. De igual modo, los sistemas y aplicaciones informáticas podrían posibilitar el autodiagnóstico a través de la introducción de datos o a partir de los datos captados directamente de los terminales y aplicaciones, implementar evaluaciones para saber si procede hacer test, aconsejar la permanencia en casa o acudir al ambulatorio o al hospital, entre muchos otros servicios. Estas herramientas también pueden servir para liberar servicios de atención.

Además de las finalidades anteriores, estos tratamientos y aplicaciones pueden ser una fuente de *big data* muy variada de la que extraer información y conocimiento para la investigación frente a las consecuencias de la COVID-19.

Como señalamos al inicio, según cómo estén configuradas, estas aplicaciones son capaces de extraer información *hipodérmica*, al tiempo que efectuar tratamientos profundos de datos. Es esencial fijar lo que se pretende de modo concreto, ya se trate de tratamientos informativos, asesoramiento, autodiagnóstico, diagnóstico médico y farmacológico, prestación de servicios sociales y médicos, o medidas de control (barreras de acceso a servicios de transporte, establecimientos o actividades económicas y laborales), incluidas posibles medidas de control administrativo, policial e incluso penal. Obviamente ello puede ser muy relevante para determinar el impacto y graduar las garantías, medidas de seguridad y deberes de transparencia.

Entre las *apps* vinculadas con la COVID-19 destacó Corea del Sur (*app* pública *self-quarantine safety protection*, o privadas: *Corona 100m, Corona map* o *Corona Alert*). Y, por supuesto, el control social chino previo y especialmente posterior a la pandemia. Además de aplicaciones, Google ha facilitado alguna información de movilidad comunitaria[10] y muy posiblemente las grandes plataformas cuenten con datos muy profundos que podrían ser de total interés para hacer frente a la presente pandemia. En España, desde los poderes públicos, también ha habido tempranas iniciativas autonómicas en cascada: *CoronaMadrid*; *Stop COVID-19 CAT* en Cataluña; *Salud Responde* en Andalucía; *Test COVID-19* en Castilla y León; *CoronaTest* en Navarra; *COVID-19.EUS* en Euskadi; web Coronavirus Sergas en Galicia, o *coronavirusautotest.san.gva.es* en la Comunidad Valenciana, entre otras. Aunque pueden haber implicado una captación de datos, se trata de iniciativas básicamente informativas. En todo caso, el Estado, a finales de marzo, inició sus pasos con la Orden SND/297/2020, de 27 de marzo, que encomendó a la Secretaría de Estado de Digitalización e Inteligencia Artificial (SGAD) «el desarrollo de soluciones tecnológicas y aplicaciones móviles para la recopilación de datos». Sus finalidades parecen bastante limitadas a la «autoevaluación», «ofrecer información» y dar «consejos» y «recomendaciones», en ningún caso «diagnóstico» o «prescripción». Así, el Gobierno lanzó en abril *AsistenciaCOVID-19* para el autodiagnóstico, se encomendó una web informativa y el desarrollo de *chatbot* para ser utilizado por aplicaciones de mensajería tipo WhatsApp (apartado 1.º)[11] y se dispuso *Hispabot-Covid19*[12]. En cuanto al más sensible tema de la geolocalización se pretende «contar con información real sobre la movilidad de las personas en los días previos y durante el confinamiento» para «ver cómo de dimensionadas están las capacidades sanitarias en cada provincia» y «a los solos

10. https://www.google.com/Covid19/mobility/
11. https://asistencia.Covid19.gob.es/; https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/asuntos-economicos/Paginas/2020/060420-asistencia-Covid19.aspx
12. https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/asuntos-economicos/Paginas/2020/080420-consulta.aspx

efectos de verificar que se encuentra en la comunidad autónoma en que declara estar» (apartado 1.º). También a través del INE se pretende, junto con los operadores, «el análisis de la movilidad de las personas en los días previos y durante el confinamiento» (apartado 2.º).

Está bien claro que con aquella orden no está «vaciándose de contenido» el derecho de protección de datos (Piñar, 2020) y que estábamos «muy lejos del apocalipsis orwelliano» (Martínez, 2020b). Era sólo un primer paso que debía haber venido acompañado de una cobertura legal. Y en la ley es donde han de recogerse usos y finalidades de esta u otras herramientas, incluso para el control de la salud, de la seguridad, laboral, etc. Además, y de especial importancia, hay que hacer un seguimiento de los datos que se están introduciendo y su posible comunicación y reutilización con las garantías oportunas.

En abril de 2020 el SEPD (2020b) abogó por un «European model *COVID-19 mobile application*». En la misma dirección y con mayor concreción, el 8 de abril la Comisión Europea (2020 b) recomendó la rápida adopción de tecnologías, la implicación de los estados y las autoridades europeas de protección de datos. Con una visión claramente garantista se insiste (núm. 10) en limitar estrictamente los tratamientos y datos empleados, revisar continuamente lo que se haga garantizando su terminación con la evolución de la pandemia y la destrucción irreversible de los datos salvo «su valor científico» a criterio de los consejos de ética y autoridades de datos. El núm. 16 concreta diversas garantías de la privacidad y opciones técnicas (*bluetooth*, cifrado, seguridad, ciberseguridad, finalización de las medidas cuando la pandemia esté bajo control, anonimato, transparencia). En esta línea ya destacaban iniciativas cooperativa y abiertas, como la *Pan-European Privacy-Preserving Proximity Tracing Project* (www.pepp-pt.org) centralizada, con sede en Alemania (aunque no empleada por ese país) y, en paralelo, iniciativa descentralizada y con sede en Suiza, el protocolo DP3T. Ambos protocolos confieren muchas garantías y normalización técnica interoperable. A la iniciativa PEPP-PT se sumó inicialmente la SGAD desde el 13 de abril[13], si bien finalmente parece haber apostado por el protocolo DP3T integrado con APIs Apple y Google. Esta línea es la seguida por Suiza, Austria, Estonia, Finlandia o Alemania. La mala experiencia de desarrollos propios no fácilmente integrables, como Reino Unido, pueden haber influido esta opción. Francia, aunque expresamente no ha regulado específicamente el desarrollo de una *covapp*, en mayo lanzó su app propia con el aval de su autoridad de datos (CNIL)[14]. Todo hay que decir que ya en julio, el desarrollo español parece ser un fiasco[15] (Radar Covid se puede descargar desde el 14 de julio) en contraste con aplicaciones masivamente descargadas como la alemana.

El 17 de abril de nuevo la Comisión (2020 c) concretó sus «orientaciones sobre las aplicaciones móviles» posiblemente en el documento más concreto desde las instituciones. Terminado este estudio, la AEPD (2020 d) en mayo de 2020 ha analizado el uso de apps, discerniendo entre las Apps para autotest o cita previa, las de información voluntaria de contagios (COVapps). Por lo general se aprecian positivamente si no se aprovechan para acumular y acceder a datos. Mayor atención implican las *apps* de seguimiento de contactos por *bluetooth* (*Contact trace apps*) por la realización de mapas de relaciones entre personas, reidentificación por localización implícita y la posible fragilidad de los protocolos que emplean. Se muestra escéptica sobre la eficacia de estos sistemas en general.

Finalizado este estudio, a fines de mayo, el Estado español anunció la puesta en marcha de app *Asistencia COVID-19* en junio[16]. Esta *app* (finalmente llamada Radar Covid) se integra bajo las APIs desarrolladas por Apple y Google y bajo el protocolo D3PT y no el inicialmente indicado PEPP-PT. Ello ha generado preocupación, al punto que la AEPD ha afirmado el inicio de «actuaciones de investigación su valor científico» de la *app*[17] y ha realizado actividades para conocer de cerca el protocolo D3PT[18].

13. https://twitter.com/SEDIAgob/status/1249610155408449537
14. https://www.cnil.fr/fr/lapplication-mobile-stopcovid-en-questions
15. De especial interés, MÉNDEZ, M. A. "El fiasco de España con la 'app' de rastreo del covid nos deja tres amargas lecciones" https://blogs.elconfidencial.com/tecnologia/homepage/2020-06-21/app-rastreo-contactos-covid-canarias-carme-artigas-sedia-sanidad-fernando-simon_2644739/
16. https://asistencia.covid19.gob.es/
17. https://twitter.com/AEPD_es/status/1263475663887044609
18. Así, cabe seguir la exposición del protocolo para la AEPD por Carmela Troncoso en mayo https://t.co/IKFON9jjfG?amp=1

Hay que esperar la coordinación y supervisión permanente de las autoridades de protección de datos y el EDPB. Sin perjuicio de las iniciativas públicas, el 10 de abril Google y Apple anunciaron que integrarán sus sistemas operativos con los dispositivos para que los usuarios no tengan que buscarlas, aunque sí consentir en su descarga y uso. Y lo que es mucho más importante, que van a «habilitar una plataforma más amplia de rastreo de contactos basada en Bluetooth», preferidas a las que usan GPS (Islandia, Canadá, China o Corea del Sur). No obstante, se prevé en todo caso su integración en «un ecosistema más amplio de aplicaciones y autoridades sanitarias gubernamentales», bajo «privacidad, la transparencia y el consentimiento»[19]. Pues bien, a fines de abril ya pusieron a disposición su tecnología. Como era previsible, no pocos países, incluido España desde inicio de mayo han confirmado la adopción e integración en las API de la *app* desarrollada.

5. Cuestiones específicas que suscitan legitimación, regulación legal de calidad y la dudosa voluntariedad de estas aplicaciones

Estas aplicaciones generan interrogantes jurídicos más allá de los generales, especialmente por los datos de geolocalización y la trazabilidad de los individuos. Además del RGDP converge la particular normativa de telecomunicaciones. El SEPD afirma que hay que «usar solo datos anónimos para mapear movimientos de personas». El EDPB (2020a) parte de que los datos de localización solo pueden ser utilizados por el operador cuando se hacen anónimos o con el consentimiento de las personas. No obstante, admite que, si no son útiles los datos anónimos o no se cuenta con el consentimiento, cabe aplicar la excepción de seguridad del artículo 15 de la Directiva 2002/58/CE de privacidad y comunicaciones, que permite a los Estados comunitarios adoptar disposiciones legales como «medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional». El EDPB (2020a, apartado 1.º) admite incluso medidas invasivas –como el «rastreo»– en circunstancias excepcionales y en función de las modalidades concretas del procesamiento. En todo caso, insiste en la obligación de «establecer las salvaguardias adecuadas»: minimización y proporcionalidad, el menor impacto posible con relación a la finalidad, garantías, recursos ante autoridades y recursos judiciales, medidas todas restringidas «estrictamente a la duración de la emergencia». En la misma línea el SEPD (2020b) insiste en que «la legalidad, la transparencia y la proporcionalidad son esenciales» y recuerda que «los grandes datos significan una gran responsabilidad».

Hay que tener en cuenta los límites y garantías de la excepción del artículo 15 de la Directiva 2002/58/CE y especialmente hay que seguir el análisis del Grupo de trabajo del artículo 29 (2016, págs. 7-12), en el que se destilaron las «garantías esenciales europeas» frente a medidas de vigilancia en transferencias electrónicas de datos, en síntesis: a) «que el procesamiento se base en normas claras, precisas y accesibles»; b) «demostración de la necesidad y la proporcionalidad con respecto a los objetivos legítimos que se persiguen»; c) «existencia de un mecanismo de supervisión independiente», así como d) «disponibilidad de recursos efectivos para el individuo». A ello hay que añadir que la excepción del artículo 15 no permite (en la lucha contra la delincuencia) «la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización de todos los abonados y usuarios registrados en relación con todos los medios de comunicación electrónica» (STJUE, Gran Sala, de 21 de diciembre de 2016, asuntos C 203/15 y C 698/15).

Es preciso dotar de base legal de calidad y con garantías a estas futuras aplicaciones. El referido artículo 15 permite a los Estados «adoptar medidas legales» adecuadas. Según vimos más arriba, los artículos 6.2 c y 9 apartado 2.º del RGPD también abren la puerta a regulaciones legales. Así pues, hay que acudir de nuevo al muy genérico artículo 3 de la Ley Orgánica 3/1986 (que menciona expresamente la Orden SND/297/2020, de 27 de marzo) y a otra legislación relativa a salud y protección civil. Pero en este caso es mucho más problemático. Con ocasión de la crisis de la COVID-19, he tenido ocasión de analizar detenidamente el Derecho excepcional ordinario tanto de salud como de protección civil, que desarrolla el deber constitucional fundamental del artículo 30, apartado 4.º, de la CE y ha-

19. https://www.apple.com/es/newsroom/2020/04/apple-and-google-partner-on-Covid-19-contact-tracing-technology/

bilita para adoptar medidas restrictivas de derechos, en ocasiones muy indefinidas (Cotino, 2020a). Se dan insuficiencias constitucionales en esta legislación por cuanto pueden implicar severas restricciones de derechos muy genéricas. Hay que considerar que, para la adopción de medidas colectivas y generalizadas de impacto e intromisión en derechos –como es el lanzamiento de aplicaciones y herramientas para el tratamiento masivo de datos personales que afectan a las personas y que han de permanecer en el tiempo– es imprescindible una acción legislativa que legitime democráticamente la restricción, a ser posible con el correspondiente debate y deliberación social. No sería oportuna –ni bastaría– una legitimación con la intervención judicial inmediata *expost* que regula el artículo 8 apartado 6.º de la Ley 29/1998, de 13 de julio (Salamero, 2020), que se mantiene en general bajo el Decreto de alarma 463/2020, de 14 de marzo (disposición final 1.ª). No está pensada para ejecutar medidas no urgentes y de afectación de derechos no individualizados.

Para la regulación, valdrían las normas con valor de ley de derecho constitucional de excepción (artículo 116 de la CE: declaración de alarma, excepción y sitio (ATC 7/2012, FJ 9.º). Como no cabe suspensión del artículo 18 apartados 1.º y 4.º de la CE en ningún caso estas normas excepcionales podrían afectar al contenido esencial de estos derechos. Según el contenido a regular, puede dudarse si bastaría una ley ordinaria o un decreto ley. La excepcionalidad de la pandemia y la clara tolerancia por parte del TC (Cotino, 2020c) pueden justificar el uso del decreto ley. En todo caso, la ley (y no el reglamento) debe contener los elementos básicos, los requisitos de la restricción de derechos y, principalmente, las garantías. Además de las exigencias del artículo 23 del RGPD, precisamente respecto de restricciones en el ámbito de datos sensibles, la reciente STC 76/2019, de 22 de mayo (FJ apartado 8.º) sobre perfilado de datos por partidos políticos ha sido especialmente exigente en cuanto a las garantías y calidad de la ley limitadora de derechos fundamentales y las posibilidades de apoderar a un poder público para restringir derechos. El mandato de calidad «no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares». Asimismo, en el caso de ser aplicable, deben tenerse en cuenta los mínimos del artículo 41 apartado 2.º de la Ley 40/2015.

Pero, más allá de la base legal, hay que prestar atención a la voluntariedad y consentimiento del interesado en estos sistemas.

En España y en la UE desde el inicio se habla de aplicaciones voluntarias, por ejemplo, la Comisión Europea insiste en «garantizar que la persona siga teniendo el control», acompañado de garantías de transparencia y derechos (2020 c) 3.2). Se afirma que para la legitimación «el consentimiento [...] sería la justificación más adecuada». La eficacia de estas herramientas dependerá de su uso masivo y, si no lo hay voluntariamente, no hay que descartar su obligatoriedad sobre la base de una clara legalidad. Asimismo, hay que ser cautos respecto de esta «voluntariedad». En razón del artículo 7 apartado 4.º del RGPD y la doctrina continuada del Grupo de trabajo del artículo 29 –y como ha señalado la AGPD– salvo excepciones «la base jurídica del tratamiento en las relaciones con la Administración (...) no sería el consentimiento del interesado», siendo además que no cabe el interés legítimo (AEPD, 2018, I. Conclusión). No obstante, la voluntariedad real de los interesados en el uso de aplicaciones puede ser un elemento de importancia en cuanto al impacto y las garantías compensatorias precisas. Viendo el pasaporte biológico que utilizó China, en ningún caso sería válida la legitimación por consentimiento si la instalación de la aplicación, su uso y transmisión de datos es condición para la prestación de servicios sociales, de salud, transporte, acceso a actividades y establecimientos. La Comisión señala que «no debería haber ninguna consecuencia negativa para el usuario» (2020 c) 3.3). Para eludir el consentimiento sería precisa una legitimación legal especialmente intensa. Con respecto a las aplicaciones privadas, Google y Apple parten del consentimiento, que legitima tanto el tratamiento de datos sensibles (artículo 9 apartado 2.º a) del RGPD) como los perfilados y tratamientos automatizados (artículo 22 apartado 4.º del RGPD). No obstante, habrá que estar vigilantes. Si este tipo de *apps* privadas se consideran peligrosas cabría incluso una prohibición por ley (artículo 9 apartado 2.º de la LO 3/2018). Especialmente respecto de webs y *apps* privadas la AEPD (2020b) advirtió pronto de los riesgos de facilitar datos sensibles a estas plataformas y herramientas, «incluso en aquellos casos en los que aparentemente esos datos no se asocian a la identidad del usuario que utiliza la aplicación», pues podrían producirse importantes carencias de transparencia y delimitación de finalidades.

6. El diablo está en los detalles: garantías específicas exigibles en el diseño de estas aplicaciones

Según hemos visto, más allá de considerar si en principio se pueden utilizar aplicaciones y rastreos frente al COVID-19, hay que determinar exactamente *para qué* se quieren emplear. A partir de ello, la clave es *cómo* se hace. Desde la finalización y entrega de este estudio no han sido pocos los documentos que han ido concretando estos aspectos por instituciones y organizaciones, con más precisión por parte de la Comisión Europea (2020 b y c) o el SEPD (2020 c) y no tanto por la AEPD (2020 d).

La anonimización es esencial, pero, como esta no será completa, resultará ineludible el cumplimiento del régimen de protección de datos con sus principios y garantías, la privacidad y, por defecto, la evaluación de su impacto. Reforzar la transparencia de los perfilados y tratamientos automatizados es clave para la confianza social. Y lo mismo podría decirse para el sector público con respecto al inventario de actividades (artículo 31.2 de la LO 3/2018).

Anonimizar no es «simplemente eliminar identificadores obvios como números de teléfono y números IMEI». En este sentido, «el uso de identificadores temporales de radiodifusión y de la tecnología *Bluetooth* para el rastreo de contactos parece ser una vía útil para lograr la protección efectiva de la intimidad y de los datos personales» (SEPD, 2020a). No obstante, como veremos, sí que es muy posible la minimización, principalmente a través de la seudonimización y la separación de acceso a datos de los distintos sujetos participantes en la cadena de valor (responsables de las *apps*, sistemas operativos, terminales, operadores, etc.). La minimización es, sin duda, un elemento de garantía esencial como se ha subrayado desde el inicio y que ha especialmente en conexión para el rastreo de contactos y de alertas sobre la base de la distancia y duración de los contactos, señalando que la tecnología *Bluetooth* de baja energía (BLE) parece ser la más precisa y no permite el rastreo, a diferencia de la geolocalización, por lo que la recomienda, además de que no se almacene «ni el momento exacto ni el lugar del contacto», pero sí el día del contacto para determinar síntomas y medidas a adoptar (Comisión Europea 2020 c) 3.4).

Habrá que ser extremadamente cautos respecto de las cesiones de los datos que se *absorban* a través de estas *apps*. Para que estas aplicaciones o sistemas informáticos puedan nutrir de *big data* a la investigación biomédica contra la COVID-19, como prevé el sistema PEPP-PT, será de especial interés prever cesiones de datos para la investigación biomédica y los detalles de seudonimización. Así se complementaría o reforzaría la cobertura legal que para ello puede brindar la Disposición adicional 17.ª apartado 2.º de la LO 3/2018.

El SEPD (2020a) señala que incluso si se trata de datos anónimos hay obligaciones de seguridad relativas a la información y la confidencialidad que deben mantenerse si se acude a terceros encargados (operadores, desarrolladores, etc.). La Comisión Europea es más concreta si cabe (2020 c) 3.8) exigiendo «las técnicas criptográficas más avanzadas» y si hay un servidor central, el acceso al mismo bajo registro previo. El almacenamiento de los datos «cifrado y pseudonimizado» y que «todas las transmisiones desde el dispositivo personal a las autoridades sanitarias nacionales deberían cifrarse».

Si se trata de iniciativas del sector público será plenamente aplicable el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad y su Anexo. A falta de definir y concretar la aplicación, finalidades, funcionamiento e impacto, es muy posible que haya que exigir un nivel de seguridad alto en las dimensiones de confidencialidad y trazabilidad y un nivel medio en las restantes (disponibilidad, autenticidad e integridad). Asimismo, es probable que haya que concretar la excepción de la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica 3/2018 a fin de permitir la posibilidad de utilizar datos y metadatos para otras finalidades.

Apple y Google (2020) desde inicio de abril anunciaron las especificaciones técnicas de su propuesta, inicialmente inspirado en el protocolo DP-3T, al que finalmente se ha sumado el Gobierno español y no como inicialmente en abril a la también sólida iniciativa europea PEPP-PT. Estas iniciativas suponen un sistema de aplicaciones que detectan proximidad con otros posibles infectados con Bluetooth y calcula riesgos individuales de contagio por exposición a personas infectadas, pero manteniendo la información anónima. La diferencia de los protocolos es que PEPP-PT carga registros de los contactos en un servidor central de informes y con DP-3T el servidor central no accede a

los datos ni es quien los trata e informa a los usuarios del contacto. Hay debate sobre la eficacia de un sistema más o menos centralizado. Expertos han concluido que los ataques contra sistemas descentralizados son indetectables y, por el contrario, los sistemas centralizados permiten medidas de seguridad y auditoría más fuertes, aunque al parecer tampoco del todo seguros (Vaudenay, 2020).

Los detalles recogidos en el Libro blanco (AA.VV., 2020, págs. 2-3 y 29) no se pueden aquí más que abreviar en lo esencial: se certifica la seguridad y cumplimiento normativo bajo código abierto auditable y transparente. El sistema está preparado para implementarse en cada país y para su interoperabilidad. Se «insta firmemente» a adoptar un sistema descentralizado y a que se almacenen datos anonimizados con identificaciones efímeras y seudoaleatorias. Estos datos se utilizan para la investigación. Cuando hay una declaración de infección, entonces se recaban los datos almacenados para las alertas. En todo caso, los «datos siempre permanecen en los teléfonos de los usuarios y el cálculo del riesgo se realiza localmente». No hay un *backend* centralizado a la asiática, que facilitaría el control social: el servidor central solo tiene los identificadores anónimos de los no infectados. Además de eliminar datos en catorce días, el sistema se desmantelaría a sí mismo elegantemente (*graceful dismantling*) conforme se dejara de usar. Cabe apuntar que ante las dudas de seguridad y suspicacias que puedan generarse (como en Noruega), en Francia se acudió a una comunidad de *hackers* éticos (*Yeswehack*) que han examinado la *app* antes que su lanzamiento. El tema, sin duda, exigirá un análisis continuo de expertos, sociedad civil y autoridades de datos.

Referencias bibliográficas

AA.VV. (2020). *Decentralized Privacy-Preserving Proximity Tracing. White Paper* (versión del 25 de mayo de 2020), págs. 2-3 y 29. https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf

AEPD (2018). «Informe 175/2018, noviembre, sobre investigación biomédica».

AEPD (2020a). «Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial» (febrero). https://www.aepd.es/media/guias/adecuacion-rgpd-ia.pdf

AEPD (2020b). «Informe 20/2020, de 12 de marzo, en relación con los tratamientos de datos resultantes de la actual situación derivada de la extensión del virus COVID-19» https://www.aepd.es/es/documento/2020-0017.pdf

AEPD (2020c). «Comunicado de la AEPD en relación con webs y apps que ofrecen autoevaluaciones y consejos sobre el coronavirus» (16 de febrero). https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-de-la-aepd-en-relacion-con-webs-y-apps-que-ofrecen

AEPD (2020 d). «El uso de las tecnologías en la lucha contra el Covid19. Un análisis de costes y beneficios». Mayo de 2020, https://www.aepd.es/sites/default/files/2020-05/analisis-tecnologias-COVID19.pdf

ALBERTO SÁIZ, C. (coord.) (2017). *Código de buenas prácticas en protección de datos para proyectos de* Big Data. AEPD e ISMS Forum, págs. 40 y sigs. y especialmente Grupo de trabajo del artículo 29: *Dictamen 5/2014, de 10 de abril*, sobre anonimización.

ALCALDE BEZHOLD, G.; ALFONSO FARNÓS, I. (2019). «Utilización de tecnología *Big Data* en investigación clínica». *Revista de derecho y genoma humano*, núm. extra 1, págs. 55-83.

APDCAT (2020). «Nota en relación a los tratamientos de datos personales relacionados con las medidas para hacer frente al COVID-19» (15 de marzo). https://apdcat.gencat.cat/es/actualitat/noticies/noticia/Nota-en-relacio-amb-els-tractaments-de-dades-personals-relacionats-amb-les-mesures-per-fer-front-al-COVID-19

APPLE-GOOGLE (2020). «Privacy-Preserving Contact Tracing» (abril). https://www.apple.com/Covid19/contacttracing/

BOIX, A. (2020). «Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la administración para la adopción de decisiones». *Revista de Derecho Público: Teoría y Método*, vol. 1, págs. 223-270. https://doi.org/10.37417/RPD/vol_1_2020_33

CERRILLO I MARTÍNEZ, A. (2019). «El impacto de la inteligencia artificial en el derecho administrativo, ¿nuevos conceptos para nuevas realidades técnicas?». *Revista general de Derecho Administrativo*, núm. 50.

COMISIÓN EUROPEA (2020a). *Libro blanco sobre la inteligencia artificial* (19 de febrero). Bruselas: UE, págs. 21 y sigs. https://op.europa.eu/es/publication-detail/-/publication/aace9398-594d-11ea-8b81-01aa75ed71a1

COMISIÓN EUROPEA (2020b). Recomendación (UE) 2020/518 de la Comisión de 8 de abril de https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2020.114.01.0007.01.SPA&toc=OJ:L:2020:114:TOC

COMISIÓN EUROPEA (2020c). Comunicación Comisión UE, de 17 de abril (2020/C 124 I/01) orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de covid-19 en lo

referente a la protección de datos (2020/C 124 I/01). https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52020XC0417%2808%29

CONSEJO CONSTITUCIONAL (2020). Decisión núm. 2020-800 DC del 11 de mayo de 2020, https://www.conseil-constitutionnel.fr/decision/2020/2020800DC.htm

COTINO HUESO, L. (2019a). «Riesgos e impactos del *big data*, la inteligencia artificial y la robótica y enfoques, modelos y principios de la respuesta del Derecho». *Revista General de Derecho Administrativo*, núm. 50. https://bit.ly/37RifyJ

COTINO HUESO, L. (2019b). «Derecho y garantías ante el uso público y privado de inteligencia artificial, robótica y *big data*». En: BAUZÁ, M. (dir.). *El Derecho de las TIC en Iberoamérica*. Montevideo: FIADI-Thompson-Reuters, págs. 917-952, http://links.uv.es/BmO8AU7

COTINO HUESO, L. (2020a). «Los derechos fundamentales en tiempos del coronavirus. Régimen general y garantías y especial atención a las restricciones de excepcionalidad ordinaria». *IUSTEL* (monográfico «Coronavirus... y otros problemas»), págs. 88-101. www.elcronista.es

COTINO HUESO, L. (2020b). «SyRI, ¿a quién sanciono? Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020». *La Ley Privacidad, Wolters Kluwer,* núm. 2. www.academia.edu.

COTINO HUESO, L. (2020c). «La (in)constitucionalidad de la "intervención", "mordaza" o "apagón" de las telecomunicaciones e internet por el Gobierno en virtud del Real Decreto-Ley 14/2019», de próxima publicación.

EDPB (2020a). «Statement of the EDPB Chair on the processing of personal data in the context of the COVID-19 outbreak» (20 de marzo). https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-Covid-19-outbreak_en

EDPB (2020 b). Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19 (Abril) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032020-processing-data-concerning-health-purpose_es

FERRÀS, X. (2020). «Las tres D». *La Vanguardia* (4 de abril). https://www.lavanguardia.com/economia/20200404/48311997448/las-tres-d.html

GERMAN ETHICS COUNCIL (2017). «Big Data and Health: Data Sovereignty as the Shaping of Informational Freedom. Opinion». Berlín: Deutscher Ethikrat. https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/englisch/opinion-big-data-and-health-summary.pdf

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2016). «Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees)». WP 237, págs. 7-12. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp237_en.pdf

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2018). «Directrices sobre decisiones automatizadas» (6 de febrero), págs. 7-8. https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf

HAN, B. CHUL (2020). «La emergencia viral y el mundo de mañana». *El País* (22 de marzo). https://elpais.com/ideas/2020-03-21/la-emergencia-viral-y-el-mundo-de-manana-byung-chul-han-el-filosofo-surcoreano-que-piensa-desde-berlin.html

HARARI, Y. (2020). «El mundo después del coronavirus». *La Vanguardia* (6 de abril). https://www.lavanguardia.com/internacional/20200405/48285133216/yuval-harari-mundo-despues-coronavirus.html

ICO (2020). «Data protection and coronavirus» (12 de marzo). https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/03/data-protection-and-coronavirus

MARTÍNEZ, R. (2020a). «Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública». *Diario La Ley*, núm. 9.604 (30 de marzo). Wolters Kluwer. https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAmMDc2NjM7Wy1KLizPw8WyMDI6CYoSVIIDOt0iU_OaSyINU2LTGnOBUAZxgvATUAAAA=WKE

MARTÍNEZ, R. (2020b). «Protección de datos y geolocalización en la Orden SND/297/2020». *Expansión* (blog Hay Derecho) (31 de marzo). https://hayderecho.expansion.com/2020/03/31/proteccion-de-datos-y-localizacion-en-la-orden-snd-297-2020/

MONTALVO JÄÄSKELÄINEN, F. (2019). «Una reflexión desde la teoría de los derechos fundamentales sobre el uso secundario de los datos de salud en el marco del *Big Data*». *Revista de Derecho Político*, núm. 106, págs. 43-75. https://doi.org/10.5944/rdp.106.2019.26147

ORTEGA GIMÉNEZ, A. (2019). «Implicaciones jurídicas de la internalización de la tecnología del *Big Data* y Derecho Internacional Privado». *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada*, núm. extra 1, págs. 169-204.

ORTEGA, A.; BALSA-BARREIRO, J.; CEBRIÁN, M. (2020). «Los límites del capitalismo de vigilancia». *El País* (8 de abril). https://elpais.com/elpais/2020/04/07/opinion/1586252351_094192.html

PEDREÑO, A. (2020). «La pandemia constata la hegemonía de Asia frente a Europa en Inteligencia Artificial». *El Independiente* (6 de abril). https://www.elindependiente.com/opinion/2020/04/06/la-pandemia-constata-la-hegemonia-de-asia-frente-a-europa-en-inteligencia-artificial/

PIÑAR MAÑAS, J. L. (2020). «Privacidad en estado de alarma y normal aplicación de la Ley». *Expansión* (blog Hay Derecho) (9 de abril). https://hayderecho.expansion.com/2020/04/09/privacidad-en-estado-de-alarma-y-normal-aplicacion-de-la-ley/

SALAMERO, L. (2020). «COVID-19 y jurisdicción contencioso-administrativa». www.academia.edu.

SEPD (2020a). «Comments to DG CONNECT of the European Commission on monitoring of COVID-19 spread» (25 de marzo). https://edps.europa.eu/sites/edp/files/publication/20-03-25_edps_comments_concerning_Covid-19_monitoring_of_spread_en.pdf

SEPD (2020b). «EU Digital Solidarity: a call for a pan-European approach against the pandemic» (6 de abril). https://edps.europa.eu/sites/edp/files/publication/2020-04-06_eu_digital_solidarity_Covid19_en.pdf

SEPD (2020c). TechDispatch on Contact Tracing with Mobile Applications, 7 de mayo, https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12020-contact-tracing-mobile_en

SIERRA, S. (2020). «Inteligencia artificial y justicia administrativa: una aproximación desde la teoría del control de la Administración Pública». *Revista General de Derecho Administrativo*, núm. 53.

VAUDENAY, S. (2020). «Centralized or Decentralized? The Contact Tracing Dilemma». *IACR*, mayo https://eprint.iacr.org/2020/531.

Cita recomendada

COTINO HUESO, Lorenzo (2020). «Inteligencia artificial, *big data* y aplicaciones contra la COVID-19: privacidad y protección de datos», *IDP. Internet, Derecho y Política*, núm. 31, págs. 1-17. UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i31.3244

Sobre el autor

Lorenzo Cotino Hueso
cotino@uv.es
Catedrático de la Universidad de Valencia

Lorenzo Cotino Hueso (www.cotino.es) es Catedrático de la Universidad de Valencia, Investigador de la Universidad Católica de Colombia (Proyecto "Derecho y Big Data", Grupo de Investigación en Derecho Público y TIC). IP Proyecto I+D+i Retos MICINN "Derechos y garantías frente a las decisiones automatizadas en entornos de inteligencia artificial, IoT, big data y robótica" (PID2019-108710RB-I00, 2020-2022). Ha sido magistrado suplente del TSJ Comunidad Valenciana desde el año 2000 hasta 2019. Doctor y licenciado en Derecho (UVEG), máster en la especialidad de derechos fundamentales en Barcelona (ESADE), licenciado y diplomado de Estudios Avanzados de Ciencias políticas (UNED). Premio Extraordinario de Doctorado, Ministerio Defensa, Ejército, INAP, CAC. Profesor invitado en Konstanz (Alemania) desde 2004 honorario en la Universidad Nacional de Colombia y en la Universidad Católica Cuenca, en Ecuador; con estancias de investigación en Utrech (Países Bajos) y Virginia (Estados Unidos). Investigador principal de quince proyectos de investigación, miembro de otros veintiuno, autor de diez libros y coordinador de catorce, así como de ciento cuarenta artículos o capítulos científicos. Ha impartido más de trescientas ponencias y conferencias. Dirige la red www.derechotics.com desde 2004 y desde 2019 es cofundador de la Red DAIA (Derecho Administrativo de la Inteligencia artificial). Profesor en la Universidad de Alcalá (2005-), en la UOC (2012-) y en la UNIR (2014-). ORCID 0000-0003-2661-0010. http://www.researcherid.com/rid/H-3256-2015.

Universitat Oberta de Catalunya

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

www.uoc.edu/idp

ARTÍCULO

Uber, Airbnb y la llamada "influencia decisiva" de las plataformas digitales

Ricardo Pazos Castro
Universidad Autónoma de Madrid*

Fecha de presentación: noviembre de 2019
Fecha de aceptación: julio de 2020
Fecha de publicación: octubre de 2020

Resumen

En este artículo se analiza el criterio de la llamada «influencia decisiva»: un parámetro que determina la naturaleza de los servicios prestados por las plataformas intermediarias y sus correspondientes implicaciones jurídicas. Tales plataformas intentan generar confianza, algo esencial para que la actividad económica se desarrolle satisfactoriamente, mediante diferentes mecanismos. Entre ellos, el establecimiento de algunas de las condiciones de la prestación de los servicios subyacentes, como el transporte o el alojamiento. La influencia de una plataforma como Uber sobre el servicio de transporte ulterior ha sido calificada como «decisiva» por el Tribunal de Justicia de la Unión Europea (TJUE). Por ello, su actividad no constituye un servicio de intermediación en la sociedad de la información, sino un servicio en el ámbito de los transportes. Por el contrario, la actividad de otra plataforma como Airbnb ha sido considerada por el TJUE como un servicio de la sociedad de la información, ya que su influencia sobre el servicio de alojamiento es menor. Tras exponer todas estas cuestiones, se articula una reflexión en torno a la configuración y consecuencias del criterio de la influencia decisiva. En este sentido, presenta algunas opiniones divergentes con la jurisprudencia europea, proporcionándose algunos ejemplos de cómo el mencionado

* Tanto la investigación previa como la redacción de este trabajo fueron llevadas a cabo cuando el autor era investigador posdoctoral en la Universidad de Santiago de Compostela, disfrutando de una beca del Programa de axudas á etapa posdoutoral da Xunta de Galicia (Consellería de Cultura, Educación e Ordenación Universitaria). El artículo se enmarca en el Proyecto de Investigación «Soluciones jurídicas y económicas al problema inmobiliario turístico» (DER 2017-82705-R) del Programa Estatal de I+D+i Orientada a los Retos de la Sociedad del Ministerio de Economía, Industria y Competitividad.

criterio afecta al derecho del trabajo y al derecho civil, y plantea varios debates: la adecuación de la influencia decisiva a la economía de las plataformas; la necesidad de revisar la regulación de los servicios subyacentes relacionados con las plataformas intermediarias, y la conveniencia de establecer una regulación específica en materia de plataformas, adaptando las normas aplicables al grado de influencia ejercido.

Palabras clave

plataformas digitales, economía colaborativa, intermediarios, influencia decisiva, servicios de transporte, servicios de alojamiento

Uber, Airbnb and the So-Called "Decisive Influence" of Digital Platforms

Abstract

This article analyses the criterion of the so-called "decisive influence", a benchmark that determines the nature of the services provided by intermediary platforms, and its corresponding legal implications. Such platforms try to generate trust, something essential for the economic activity to successfully move forward, by several means. Among them, by setting some of the conditions of the underlying services, such as transportation and accommodation. The influence of a platform like Uber on the subsequent transportation service has been regarded "decisive" by the Court of Justice of the European Union. Because of that, its activity does not amount to an information society service of intermediation, but to a service in the field of transport. On the contrary, the activity of another platform like Airbnb has been qualified by the CJEU as an information society service, because the platform operator has a lesser influence on the accommodation service. After explaining all these issues, the paper reflects on the concept and consequences of the decisive influence criterion. In this regard, the paper presents some views diverging from the EU case-law, offers some examples of how the referenced benchmark affects labour law and private law, and poses some debates. These are the appropriateness of the decisive influence within the platform economy, the need to review the regulation of the underlying services related to intermediary platforms, and the convenience of passing specific regulation on platforms, adapting the applicable rules to the degree of influence exercised.

Keywords

Online platforms, sharing economy, intermediaries, decisive influence, transportation services, accommodation services

Introducción

Las plataformas digitales han permitido acceder a un número mayor de bienes y servicios, siendo evidente que las opciones de consumo han crecido exponencialmente en los últimos años. A las mayores posibilidades de elección de los consumidores debería (en teoría) corresponder un mayor fomento de su autorresponsabilidad. Pero, en la medida en que esas opciones crecientes son el resultado de innovaciones y modelos de negocio desarrollados por empresas, también a estas podrá exigírseles un nivel de responsabilidad superior, al menos en determinados contextos.

El presente trabajo se centra en la llamada «influencia decisiva», un criterio que probablemente determinará qué operadores de la economía digital se verán sometidos a una responsabilidad especial. Se trata de dilucidar qué plataformas son simples intermediarias entre la oferta y la demanda, y cuáles ejercen un papel mayor en relación con el servicio subyacente. Si la influencia ejercida por la plataforma es escasa, su rol será neutral o pasivo, podrá decirse que tiene un menor poder, y en consecuencia recaerán sobre ella menores obligaciones. Por el contrario, si la influencia del operador de la plataforma es relevante, podrá considerarse que no es un simple intermediario y habrá que imponerle ciertas obligaciones o una mayor responsabilidad.

Para desarrollar este tema, el apartado 1 parte del problema de la confianza en el ámbito digital, cuya resolución es imprescindible para que el comercio en línea pueda desarrollarse. Existen muchas maneras de infundir la seguridad necesaria, algunas más «invasivas» que otras, lo que determina la existencia de plataformas activas y pasivas. En el apartado 2 se analiza la noción de «influencia decisiva» tomando como referencia el caso relacionado con la empresa Uber, abordado por el TJUE. En el apartado 3 se examina otra transacción típica de la economía colaborativa como es el alojamiento turístico, en particular el realizado a través de la plataforma Airbnb, sobre la que también se ha pronunciado el Tribunal Europeo. Finalmente, en el apartado 4 se articulan algunas reflexiones en torno a la aplicación del criterio de la influencia decisiva a los nuevos modelos de negocio. Quizá el mundo digital nos obligue a reinterpretar ciertos conceptos, o, al menos, a adoptar perspectivas distintas de las mantenidas hasta ahora.

1. El comercio digital y los problemas de confianza

El comercio digital no puede desarrollarse si los participantes no tienen confianza en la buena marcha del sistema. En realidad, la confianza es un requisito necesario para cualquier actividad económica. Pero la cuestión resulta más evidente en contextos digitales porque las personas están más dispersas y su interrelación tiene un carácter más esporádico (Busch, 2016, págs. 224-226). En este contexto, los nuevos operadores digitales reducen tanto las barreras físicas y técnicas como el obstáculo consistente en la inseguridad (Hira y Reilly, 2017, pág. 176; Rodríguez Marín, 2018, págs. 52-54). Desde el punto de vista de la parte de la relación económica que se pretende que infunda confianza, puede hablarse de instrumentos que la generan «entre pares», por un lado, y «centralizados», por otro (Thierer *et al*., 2016, págs. 858-869).

El primer grupo engloba los encaminados a que las dos partes de la eventual transacción confíen entre sí, siendo el ejemplo paradigmático reunir, clasificar y publicar experiencias de consumo. A través de puntuaciones numéricas y opiniones escritas, los usuarios manifiestan sus impresiones con relación a bienes, servicios, contenidos digitales, empresarios, otros usuarios, etc.[1]. Esto ayuda a tomar decisiones sobre si contratar o no, con quién, en relación con qué productos y en qué condiciones (Thierer *et al*., 2016, págs. 855-857). Otro recurso representativo es el sistema de seguimiento por GPS que utilizan las aplicaciones relacionadas con el transporte de corta distancia (Koopman, Mitchell y Thierer, 2015, págs. 541-542; Edelman y Geradin, 2016, pág. 297). Por su parte, mediante el segundo tipo de instrumentos, las partes confían en un tercero, el intermediario, porque este asumirá ciertas responsabilidades. La garantía de devolución del precio paga-

1. Cfr. artículo 2(k) del *Discussion draft of a Directive on online intermediary platforms* (RGLDS, 2016), artículo 2(k) de las *Model rules on online platforms* (ELI, 2020), y artículos 3.1 y 3.13 de la norma ISO 20488:2018, de junio de 2018, sobre opiniones en línea de los consumidores y los principios y requisitos para su recopilación, moderación y publicación.

do y los seguros son dos de las herramientas a través de las cuales los operadores de las plataformas se ganan la confianza de sus usuarios. También resulta especialmente interesante mencionar los mecanismos de resolución de conflictos surgidos durante la transacción (Mak, 2018, págs. 92 y 98).

En definitiva, existe una amplia gama de herramientas que reducen los problemas de incertidumbre en el marco de la economía digital. Los diferentes operadores pueden servirse de algunas o de muchas de ellas, afectando a una o a varias fases del proceso. En consecuencia, tales operadores adoptan posiciones que oscilan entre una relativa pasividad y un marcado carácter activo, según sus necesidades e intereses respectivos (Thierer *et al*., 2016, pág. 859). De este modo, aparece la distinción entre plataformas activas y pasivas, en función de su grado de influencia o control en el proceso contractual y, sobre todo, en la transacción subyacente. Algunas plataformas no incorporan únicamente servicios adicionales y accesorios, sino que determinan las condiciones en las que deben ser prestados los servicios sustantivos latentes. Y cuando esta última hipótesis gana en importancia, surge el debate sobre la responsabilidad que debería asumir la plataforma por estos últimos servicios (Twigg-Flesner, 2016, págs. 36-37; Busch, 2018, págs. 39-40). El grado de control puede determinar otras muchas consecuencias jurídicas, como, por ejemplo, la sujeción o no a autorizaciones previas y licencias (Comisión Europea, 2016, pág. 6).

Por último, conviene destacar que la idea de vincular la responsabilidad al control dista de ser algo novedoso en el ámbito digital. Piénsese en la Directiva sobre el comercio electrónico[2]. Sus artículos 12 y siguientes establecen la exención de responsabilidad de las plataformas proveedoras de servicios intermediarios de la sociedad de la información con respecto a la información transmitida o almacenada, sometida a una condición descrita como la falta de cualquier control y conocimiento sobre dicha información: su actividad debe ser meramente técnica, automática y pasiva (Comisión Europea, 2016, págs. 8-9).

En el próximo apartado abordaremos la denominada «influencia decisiva», un criterio que posiblemente juegue un papel central a la hora de establecer el marco jurídico de las plataformas intermediarias en la economía digital.

2. El criterio de la «influencia decisiva» en relación con Uber

Para estudiar el criterio de la influencia decisiva, conviene partir de la sentencia del TJUE *Asociación Profesional Élite Taxi*[3]. En este asunto se trataba de dilucidar si la actividad de intermediación realizada por la empresa Uber debía considerarse un servicio de la sociedad de la información, o, por el contrario, un servicio «en materia de transportes» en el sentido del artículo 58 del Tratado de Funcionamiento de la Unión Europea (TFUE)[4].

Para el TJUE, la actividad de esta plataforma no se limita a la intermediación entre el conductor y la persona que desea realizar un desplazamiento, existiendo dos aspectos que lo reflejan. Primero, la creación de una oferta de servicios de transporte urbano que, sin la aplicación, no podrían prestarse. Segundo, el ejercicio de una influencia decisiva sobre las condiciones de prestación de servicios de transporte por los conductores. En este sentido, la plataforma desarrolla una labor de verificación de los conductores –pudiendo excluirles– y de los vehículos, establece el precio máximo de la carrera, y recibe el precio pagado para luego transmitir una parte al conductor. De ello resulta que la actividad de intermediación integra y está indisociablemente vinculada a «un servicio global cuyo elemento principal es un servicio de transporte». En consecuencia, la actividad de la plataforma debe ser calificada como un servicio en el ámbito de los transportes (STJUE *Asociación Profesional Élite Taxi,* apartados 37-40, 48). El Tribunal se reafirmó en estas observaciones en una sentencia posterior[5], perfilando los contornos del criterio de la influencia decisiva (Finck, 2018, págs. 1.630-1.634).

2. Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (DO L 178, de 17 de julio de 2000, pág. 1).
3. Sentencia del TJUE de 20 de diciembre de 2017, *Asociación Profesional Élite Taxi*, C-434/15, ECLI:EU:C:2017:981.
4. DO C 202, de 7 de junio de 2016, pág. 47 (versión consolidada).
5. Sentencia del TJUE de 10 de abril de 2018, *Uber France*, C-320/16, ECLI:EU:C:2018:221.

En resumen, cuando una plataforma ofrece una combinación de servicios, su actividad es considerada un único servicio global si aquella ejerce una influencia decisiva sobre varios componentes de ese conjunto entre los que hay una relación inherente. Las normas aplicables a ese servicio global se determinan en función de su componente principal. Y si la actividad principal no se desarrolla en línea, el servicio global no puede ser considerado un servicio de intermediación en la sociedad de la información (Hacker, 2018, págs. 84, 87-88)[6].

La determinación de si una plataforma ejerce una influencia decisiva gira en torno a algunos factores que ya habían sido mencionados por la Comisión Europea. La Comisión destacaba la fijación por la plataforma del precio del servicio subyacente y de otras condiciones contractuales esenciales, así como la propiedad por parte de la plataforma de activos clave para que el servicio subyacente pueda ser prestado. El cumplimiento de estos criterios constituiría un indicio claro de una influencia significativa. Por el contrario, otros elementos accesorios o servicios auxiliares, como los relacionados con las modalidades de pago, no implicarían necesariamente que se estuviese ejerciendo tal influencia. En todo caso, cuanto mayor fuese la gestión y organización de la plataforma con respecto a los servicios subyacentes –en particular, seleccionando a los proveedores y determinando la manera en que se prestan tales servicios–, más probable sería que debiera ser considerada (también) el prestador del servicio subyacente (Comisión Europea, 2016, págs. 6-9). El hecho de que el TJUE no aludiese en ningún momento a la propiedad de los activos fue aplaudido por la doctrina (De Franceschi, 2018, pág. 2)[7]. Por el contrario, se ha criticado la referencia a la creación de un servicio que sin la aplicación no existiría, pues esto es una característica inherente a cualquier servicio de intermediación que tenga éxito (Hacker, 2018, pág. 85).

La jurisprudencia europea solo implica de manera directa que la actividad de Uber está sometida a las normativas nacionales en materia de transporte urbano no colectivo y a los servicios indisociablemente vinculados a ellos (STJUE *Asociación Profesional Élite Taxi*, apartados 46-47), tales como las eventuales autorizaciones previas necesarias[8]. Esto no quiere decir que Uber preste un servicio de transporte. Podría tratarse de un servicio «de intermediación en el transporte», ciertamente englobado en el ámbito de los transportes en el sentido del artículo 58 del TFUE, pero no *necesariamente* sometido a las mismas normas que la actividad de transporte en sí misma[9]. Sea como fuere, el pronunciamiento del TJUE afecta indirectamente a muchas otras cuestiones jurídicas. Desde el momento en que la plataforma integra un servicio global cuyo elemento principal es el transporte, es razonable pensar que deberá asumir ciertas responsabilidades: por retrasos, por eventuales hurtos, en caso de accidente, etc. (Huet, 2018, pág. 211).

La respuesta del TJUE en el asunto relativo a Uber no puede aplicarse automáticamente a otras plataformas digitales, ya que debe realizarse un examen caso por caso. Pero la influencia decisiva se convierte en el parámetro de referencia para llevar a cabo ese examen circunstanciado (Renders y De Valkeneer, 2018, pág. 48). A continuación, trataremos el servicio relacionado con el alojamiento turístico prestado por la empresa Airbnb.

3. El caso de Airbnb

La plataforma Airbnb también ha puesto en marcha diferentes mecanismos que incrementan el nivel de influencia sobre el servicio de alojamiento latente, a pesar de proclamarse un simple intermediario o «facilitador» (Mak, 2018, págs. 90-98). Examinada esta plataforma bajo el prisma de la sentencia *Asociación Profesional Élite Taxi,* algún autor reconocía que podían existir dudas sobre la naturaleza de su actividad; concluyendo, sin embargo, que la respuesta probablemente debía ser análoga a la recaída en relación con Uber. El motivo es que Airbnb crea una oferta de alojamiento que sin la plataforma no existiría,

6. Cfr. considerandos núm. 18 y 21, y artículos 2.a) y 2.h).ii), de la Directiva sobre el comercio electrónico.
7. Cfr. conclusiones del Abogado General en el asunto *Asociación Profesional Élite Taxi*, presentadas el 11 de mayo de 2017, punto 55 (ECLI:EU:C:2017:364).
8. Cfr. STS (Sala 3.ª) de 25 de enero de 2018 (ECLI:ES:TS:2018:120), Fundamento de Derecho quinto.
9. Cfr. SJMer núm. 3 de Barcelona de 10 de abril de 2018 (ECLI:ES:JMB:2018:38), Fundamento de Derecho tercero, puntos 11 y 14.

gestiona los pagos, realiza un *screening* de los participantes y puede excluir de la plataforma aquellos perfiles que no alcancen una determinada puntuación media, ofrece a los propietarios de los inmuebles una garantía por los daños causados por los huéspedes, y cuenta con un sistema de resolución de conflictos. En suma, aunque no establece el precio del alojamiento, su grado de control sobre este servicio –el cual, obviamente, no se desarrolla a distancia y por vía electrónica– es significativo (Hacker, 2018, págs. 88 y 93).

Sin embargo, la Comisión Europea manifestó en su momento que, si el proveedor del servicio de alojamiento gozaba de libertad para fijar el precio y la plataforma no poseía ninguno de los activos para la prestación del servicio, el operador de dicha plataforma estaría prestando únicamente un servicio de la sociedad de la información, aun cuando se sirviese de mecanismos como el seguro y la calificación a través de opiniones de los usuarios (2016, pág. 7).

El TJUE ha tenido que pronunciarse recientemente sobre la naturaleza de la actividad de la plataforma Airbnb, debiendo determinar si constituye o no un servicio de la sociedad de la información, lo que conlleva beneficiarse de la libertad de prestación de servicios establecida en el artículo 3 de la Directiva sobre el comercio electrónico[10].

Según el Abogado General, cuyas conclusiones fueron presentadas el 30 de abril de 2019[11], la respuesta era afirmativa. En su opinión, Airbnb no crea una oferta de servicios nueva, por lo que el servicio de alojamiento no está indisociablemente vinculado al prestado por Airbnb, conservando ambos su autonomía e independencia económica (conclusiones del Abogado General en el asunto *Airbnb Ireland,* puntos 55-59). La plataforma tampoco ejerce un control significativo sobre aspectos esenciales del alojamiento, tales como la ubicación del inmueble, el precio y las condiciones; aunque proporcione diversos servicios auxiliares. Por lo tanto, Airbnb sí presta un servicio de la sociedad de la información (conclusiones del Abogado General en el asunto *Airbnb Ireland*, puntos 69-91)[12].

El TJUE coincidió con el Abogado General, concluyendo que la actividad de la plataforma Airbnb constituye un servicio de la sociedad de la información[13]. Considera que el servicio que presta Airbnb es disociable de la transacción inmobiliaria propiamente dicha, diciendo que consiste en proporcionar un instrumento –la plataforma– que facilita la conclusión de contratos de alojamiento. La presentación organizada de las ofertas y el suministro de herramientas que permiten su búsqueda y comparación no puede considerarse un servicio accesorio del alojamiento, sino que mantiene su autonomía y es independiente desde el punto de vista económico (STJUE *Airbnb Ireland*, apartados 51-54).

El servicio prestado por Airbnb no es imprescindible para que se preste el servicio de alojamiento, pues tanto arrendadores –que pueden ser profesionales o particulares– como arrendatarios disponen de otras vías para alcanzar el mismo resultado. Además, el precio del alojamiento no es determinado ni limitado por la plataforma, que no hace más que ofrecer una herramienta opcional para su estimación. Tampoco el hecho de recibir el pago del arrendatario, para luego transmitir el importe del alojamiento al arrendador, hace que la intermediación se convierta en parte integrante de un servicio global cuyo elemento principal sea el alojamiento. No es más que un mecanismo que proporciona seguridad a las partes. Ofrecer a los arrendadores una garantía por daños y un seguro de responsabilidad civil opcional tampoco hace que la actividad de Airbnb deje de consistir en una labor de intermediación. La acumulación de todos estos servicios no debe conllevar la alteración de esta calificación jurídica (STJUE *Airbnb Ireland,* apartados 55-64).

El criterio de la influencia decisiva, en su configuración resultante de la jurisprudencia europea, se adapta mejor a las características de la intermediación en el transporte urbano que en el alojamiento turístico. La contratación del servicio de transporte se hace con agilidad, e incluso con un cierto grado de urgencia. Esto no sucede con el alojamiento turístico, ya que los usuarios se toman su tiempo para comparar opciones. La necesidad de «control» en la primera hipótesis es mayor, pues el problema de asimetría

10. Sentencia del TJUE de 19 de diciembre de 2019, *Airbnb Ireland,* C-390/18, ECLI:EU:C:2019:1112.
11. ECLI:EU:C:2019:336.
12. Cfr. Dyal-Chand (2015, págs. 297-299).
13. Para un análisis de las implicaciones directas de la sentencia en el ordenamiento español, cfr. González Carrasco (2020, págs. 8-12).

informativa y confianza debe solventarse con rapidez. Además, la heterogeneidad es más alta en materia de alojamiento turístico. Por supuesto, en el transporte hay diferencias de calidad, en particular en función de la gama del vehículo. Uber, de hecho, ofrece varias tarifas teniendo en cuenta este factor. Pero tales diferencias son marginales si se comparan con las que pueden darse entre los inmuebles: situación, superficie, número de habitaciones, equipamiento de la cocina, decoración, velocidad de la conexión a Internet, canales de televisión disponibles, etc. Por todo ello, la influencia de Airbnb –en particular, sobre el precio– puede ser inferior a la que necesita ejercer Uber.

Expuesto el criterio de la influencia decisiva, procede ahora efectuar diversas observaciones con respecto al mismo, a sus implicaciones jurídicas en la economía digital, y a los debates que merecen ser abiertos.

4. Reflexiones sobre el criterio de la influencia decisiva y su incidencia en la economía de las plataformas

Hay argumentos para respaldar tanto la utilización del criterio de la influencia decisiva como la conclusión de que la plataforma Uber presta un servicio en materia de transportes, e incluso que su actividad constituye un servicio de transporte en sí mismo. El grado de control ostentado permitiría afirmar que los conductores son meros instrumentos de la plataforma. Y, si es la plataforma quien determina una serie de parámetros relevantes desde el punto de vista de la competencia con los prestadores de servicios clásicos, parece lógico someter a todos ellos a un mismo régimen jurídico (Finck, 2018, págs. 1.632-1.633; Hacker, 2018, págs. 85-86, 94).

Sin embargo, no deberíamos obviar la existencia de opiniones contrarias al Tribunal que también ofrecen argumentos interesantes. En este sentido, algún comentarista ha manifestado con rotundidad que «Uber no es una empresa de transporte por mucho que el TJUE sea incapaz de entender su modelo de negocio», aseverando que el hecho de que «el TJUE haya concluido que sí lo es solo demuestra su escaso conocimiento sobre esta materia» (Rallo, 2017). No niega que Uber ejerza una influencia decisiva, pero sostiene que esta es imprescindible para que conductores y usuarios puedan cooperar. La fijación de determinadas condiciones del servicio de transporte por parte de la plataforma no es más que un mecanismo de coordinación de oferta y demanda, pues simplemente genera la confianza necesaria para que el mercado se desarrolle con éxito. En resumen, el control del servicio subyacente es clave para prestar exitosamente el servicio de intermediación, que no por ello se convierte en un servicio en materia de transportes.

Este enfoque crítico parece sólido. Determinadas plataformas no pueden operar con expectativas de éxito si no ejercen un control más o menos detallado sobre algunos aspectos de la transacción subyacente (Epstein, 2019). Y, si la intermediación solo llegará a buen término ejerciendo ese control, cabe sostener que este último no es más que un medio para desarrollar aquella. En la descripción –desde un punto de vista puramente fáctico– que suele hacerse de la actividad de la plataforma Uber, por ejemplo, abundan conceptos propios de una función de intermediación como «facilitar», «organizar», «conectar», «contacto» y «dar acceso» a un servicio mediante la aplicación correspondiente[14]. A la vista de lo expuesto, no sería irrazonable pensar que la influencia ejercida tiene por objeto, en todo caso, desempeñar (satisfactoriamente y con expectativas de mantenerse en el tiempo) una labor de *matchmaking*[15]. Siguiendo este razonamiento, y puesto que el proceso de *conectar* oferta y demanda se articula exclusivamente en línea, estaríamos ante un servicio de intermediación de la sociedad de la información. En otras palabras, la plataforma intermediaria que influye decisivamente sobre el servicio subyacente produce un (exigente) «sello de calidad» privado, ofreciendo los recursos técnicos que permiten a los usuarios encontrar proveedores que quieran prestar sus servicios beneficiándose de dicho sello.

Algún autor ha mantenido que, en el caso de Uber, debería haberse separado la labor de intermediación del servicio de transporte. El servicio prestado mediante la primera

14. Cfr. auto del Juzgado de lo Mercantil núm. 3 de Barcelona, de 16 de julio de 2015 (ECLI:ES:JMB:2015:1359A), Fundamentos de Derecho tercero y sexto; Ruda González (2018, pág. 426).
15. Cfr. Dyal-Chand (2015, págs. 279-283, 289).

consiste en hacer posible la contratación a distancia del segundo, y la conexión entre ambos no impide apreciar el valor generado separadamente por cada uno, haciéndolos económicamente independientes[16]. Según esta opinión, el operador de la plataforma podría ser considerado al mismo tiempo el prestador de un servicio de la sociedad de la información y el prestador de un servicio en el ámbito de los transportes, de tal forma que debería cumplir con ambos marcos normativos simultáneamente, cada uno en su ámbito de actividad respectivo (Schaub, 2018, págs. 112-113)[17].

Por consiguiente, creo que el debate en torno a la configuración y aplicación del criterio de la influencia decisiva no está cerrado. Las dudas sobre su adecuación surgirán a medida que aparezcan nuevos modelos de negocio en el ámbito digital. Esto parece aún más plausible a la vista de las numerosas implicaciones jurídicas indirectas que tiene la jurisprudencia europea.

La influencia decisiva –u otros criterios cercanos– constituye un parámetro al que recurrir con el fin de determinar la condición de los prestadores del servicio subyacente a los efectos de la normativa laboral (Hernández Bejarano, 2016, apartado III; Schaub, 2018, pág. 112)[18]. En efecto, hay decisiones judiciales sobre el carácter dependiente o autónomo del trabajo de las personas que prestan servicios en el marco de la economía colaborativa que han resuelto la cuestión atendiendo a criterios que podrían reconducirse sin demasiadas dificultades a aquella noción[19]. El ejercicio de una influencia decisiva en el sentido de la jurisprudencia europea no implica automáticamente que tales proveedores sean trabajadores por cuenta ajena de la plataforma, pero si esta última fuese considerada un simple intermediario, esa calificación a efectos laborales quedaría vedada (Sánchez-Urán Azaña, 2018, apartado IV.2). El laboral es sin duda uno de los ámbitos más importantes en el debate sobre la economía de las plataformas: el modelo de negocio de algunas de ellas depende en buena medida de que los prestadores de servicios no sean considerados subordinados –lo que a veces no se corresponde con la realidad, pero en otras ocasiones sí– (Rodríguez-Piñero Royo, 2019, pág. 5).

En el ámbito civil, considerar a la plataforma empleadora de los proveedores directos del servicio *offline* implicaría hacer responsable a la primera por los hechos de los segundos (Østergaard y Jakobsen, 2019, págs. 35-36). Ahora bien, aun cuando no se tenga a las plataformas por prestadoras del servicio subyacente, ni a los proveedores de este servicio por trabajadores por cuenta ajena, el ejercicio de una influencia decisiva puede implicar la existencia de una relación de subordinación entre ellos. Y esto quizá haga que la plataforma deba responder por hechos ajenos (Ruda González, 2018, págs. 430-437).

La relación que determina la responsabilidad civil de los empresarios por hechos de sus dependientes (artículo 1903 del Código Civil) se interpreta de manera flexible en nuestro derecho, tendencia que se aprecia en numerosos ordenamientos jurídicos. No es preciso que exista una relación laboral, y ni siquiera contractual. Lo fundamental es identificar a un auxiliar con un cierto grado de dependencia o subordinación, en el sentido de que su actividad está sometida a una –siquiera mínima– dirección, vigilancia o control por medio de directrices e instrucciones dadas por un principal que ejerce, en consecuencia, un mínimo rol de supervisión (Solé Feliu, 2012, págs. 50-72). Pues bien, si una plataforma es considerada una simple intermediaria, la responsabilidad civil descrita posiblemente debería descartarse. Por el contrario, si no recibe tal condición porque ejerce una influencia decisiva sobre el servicio offline subyacente, resulta difícil excluir esa responsabilidad. El motivo es que tal influencia podría describirse como la organización del funcionamiento general de ese servicio (conclusiones del Abogado General en el asunto *Airbnb Ireland*, puntos 52-53), y esto necesariamente conllevará la existencia de instrucciones o directrices.

Desde el punto de vista de la responsabilidad contractual del operador de la plataforma por incumplimientos de los proveedores en la transacción subyacente, debe traerse a colación el artículo 18 del borrador preliminar de la Directiva sobre plataformas intermediarias, elaborado por el *Research Group on the Law of Digital Services* (RGLDS, 2016). Según este precepto, la plataforma es responsable,

16. En contra, cfr. conclusiones del Abogado General en el asunto *Asociación Profesional Élite Taxi*, puntos 33 a 65.
17. Cfr. Comisión Europea (2016, págs. 6-7).
18. Cfr. Dyal-Chand (2015, págs. 293-294, 296, 298-299, 301-302).
19. Cfr. sentencia del Juzgado de lo Social núm. 6 de Valencia de 1 de junio de 2018 (ECLI:ES:JSO:2018:1482), y sentencia del Juzgado de lo Social núm. 39 de Madrid de 3 de septiembre de 2018 (ECLI:ES:JSO:2018:3042).

solidariamente con el proveedor del servicio subyacente, si el cliente puede razonablemente esperar que el operador de aquella ejerza una influencia «predominante» sobre el segundo. Para determinar si esta influencia se produce, deberá atenderse a aspectos como los siguientes: si el contrato entre proveedor y consumidor se celebra únicamente a través de la plataforma; si esta puede retener pagos hechos por los clientes; si las condiciones contractuales del servicio subyacente son fijadas por el operador de la plataforma; si este establece el precio a pagar por el cliente; si la plataforma genera una imagen uniforme de los proveedores o una imagen de marca; si las labores de *marketing* se concentran en la plataforma y no en los proveedores, y si la plataforma se compromete a monitorizar la conducta de estos. Para atribuir la responsabilidad a la plataforma no sería imprescindible que se cumpliesen todos estos requisitos, aunque tampoco sería siempre suficiente con responder a solo uno de ellos (Busch, 2018, pág. 49).

El contenido esencial del artículo 18 del borrador preliminar ha sido mantenido, con algún cambio para conseguir una mayor claridad y perfilar mejor los criterios que revelan la influencia de la plataforma, en el artículo 20 de las reglas modelo sobre plataformas en línea publicadas por el *European Law Institute* (ELI, 2020), que asumió y continuó el proyecto de investigación que había dado lugar a aquel borrador.

Quizá el principio de relatividad de los contratos deba ser objeto de algunos matices en la economía de las plataformas. De manera similar a lo que sucede en la compraventa de inmuebles o de automóviles[20], podría decirse que una plataforma intermediaria que ejerce una influencia decisiva, aun cuando no sea parte del contrato de prestación del servicio subyacente, tampoco es un tercero ajeno a él. Dicho de otro modo: si bien en la economía de las plataformas suele identificarse una estructura triangular entre la plataforma, el proveedor y el usuario (Rodríguez Marín, 2018, págs. 49-50), cuando la primera ejerce una influencia decisiva sobre el segundo también habría una cierta verticalidad, de tal modo que la plataforma sería responsable por el servicio –o por algunos de sus elementos– derivado del contrato entre proveedor y usuario.

El criterio de la influencia decisiva también puede suscitar debates desde ópticas ideológicas y de política jurídica. No resulta difícil constatar que la opinión crítica presentada al inicio de este apartado promueve una visión más favorable al libre mercado. Como tampoco resulta excesivamente difícil darse cuenta de que el criterio de la influencia decisiva, de la forma que ha sido articulado por el TJUE, favorece una mayor intervención en la actividad económica.

El prestador de un servicio de la sociedad de la información recibe un trato más benévolo por el Derecho de la Unión –en forma de ciertas exenciones de responsabilidad y de una mayor libertad para prestar sus servicios–, mientras que algunos servicios subyacentes –como el transporte– están fuertemente regulados en los Estados miembros (Hacker, 2018, págs. 82 y 87). Esto no quiere decir que los servicios de la sociedad de la información carezcan de regulación, existiendo, en particular, un régimen normativo derivado de la Directiva sobre el comercio electrónico que encuadra la responsabilidad de los prestadores de tales servicios (Touriño, 2018, págs. 79-92). De hecho, hay quien subraya que, negando a Uber ese carácter –en lugar de acumular esa condición a la de prestador de un servicio en materia de transporte–, algunas normas que benefician a los consumidores no son aplicables (Schaub, 2018, págs. 110, 113-114). Tampoco puede obviarse el Reglamento europeo 2019/1150, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea[21]. Pero resulta evidente que servicios como el alojamiento y el transporte están sometidos a un gran volumen regulatorio que los intermediarios en la economía colaborativa intentan evitar (Cao, 2017, págs. 1.089-1.096; Finck, 2018, págs. 1.621-1.622).

Además, los denominados «fallos de mercado» son el principal argumento con el que se justifica la intervención pública en la economía. Pues bien, si las plataformas no ejercen un control con respecto a las relaciones subyacentes, no tendrán éxito y el mercado no se desarrollará. Esto servirá como pretexto para la aprobación de numerosas normas, también a nivel de la Unión Europea. Y si las plataformas ejercen un control sobre las transacciones subyacentes para corregir asimetrías informativas, se exponen

20. Cfr. STS (Sala 1.ª) de 11 de marzo de 2020 (ECLI:ES:TS:2020:735), Fundamento de Derecho cuarto.
21. DO L 186, de 11 de julio de 2019, pág. 57.

a la regulación que afecta a tales transacciones. Esto es, a través del criterio de la influencia decisiva, cuantos más fallos del mercado resuelva el empresario por sí mismo, más expuesto está al riesgo de verse sometido a una carga regulatoria superior (Hacker, 2018, pág. 94).

Ciertamente, este resultado no es del todo ilógico. Sin ir más lejos, la responsabilidad extracontractual por riesgo se basa en la idea de que quien domina en interés propio una fuente de peligros, controlando las características de los riesgos inherentes, debe asumir las consecuencias derivadas de su materialización (Santos Briz, 1984, págs. 413-414). Ya se ha planteado la posibilidad de una responsabilidad por riesgo a cargo de las plataformas, derivada de su cercanía y control sobre el servicio subyacente (Østergaard y Jakobsen, 2019, págs. 36-37). Ahora bien, aplicar semejante razonamiento a las plataformas intermediarias puede ser un obstáculo para la economía digital. Estas plataformas tendrán que evaluar si les compensa asumir los mayores riesgos y costes regulatorios derivados de una mayor influencia, o renunciar a controlar en gran medida el servicio ulterior, con la consiguiente reducción de su expectativa de éxito (Hacker, 2018, pág. 94). A todo ello se añade el hecho de que un aumento de la carga regulatoria supone la creación de barreras de entrada al mercado y mayores costes operativos. Esto favorece a las empresas ya implantadas, y sobre todo a las más fuertes, con más recursos para hacer frente a la normativa (Koopman, Mitchell y Thierer, 2015, págs. 534, 537-538).

Lo mismo puede decirse de la eventual atribución de responsabilidad contractual por el servicio subyacente a las plataformas que ejercen una influencia decisiva. Aunque esto parezca beneficioso para los usuarios finales, lo cierto es que no es necesariamente así. Probablemente, los grandes beneficiados de generalizar esa responsabilidad contractual serían, de nuevo, las grandes empresas que cuentan con recursos para afrontar mayores costes operativos. Por este motivo, es posible argumentar que la asunción de la citada responsabilidad debería ser voluntaria para las plataformas, como un aspecto más del proceso competitivo. En definitiva, el criterio de la influencia decisiva comporta un riesgo de concentración del mercado y de desincentivar la innovación.

Las consecuencias del criterio de la influencia decisiva también fomentan el debate sobre la regulación de los servicios subyacentes. Un sector entiende que las normas tradicionales no se adaptan bien a los nuevos modelos de negocio, y que, de hecho, muchas de ellas deberían derogarse incluso con relación a los prestadores clásicos *offline*; mientras que otro sector mantiene una opinión diferente u opuesta (Edelman y Geradin, 2016, pág. 294). Es razonable pensar que algunas normas que estaban justificadas en su momento no lo estarán ya en la sociedad digital, procediendo su derogación o modificación. El mantenimiento de otras normas seguirá estando justificado, pero solo con respecto a los operadores clásicos, porque las causas o fallos del mercado que motivaron su adopción no concurren respecto de los operadores en línea. Y, por supuesto, también puede suceder que la necesidad o conveniencia de las normas vigentes se vea inalterada, debiendo ser aplicadas, sin más, también en la economía digital. La reflexión en este sentido resulta obligada[22].

Se habla, por ejemplo, de una desprotección de los usuarios de servicios de alojamiento turístico en viviendas particulares a través de plataformas con respecto a quienes recurren a los establecimientos de hospedaje tradicionales, que ofrecen una serie de garantías de calidad, higiene, seguridad y responsabilidad (De la Encarnación, 2016, págs. 46-47). Hay numerosas voces que proclaman la necesidad de que los modelos de negocio de la economía digital se equiparen, en cuanto a seguridad, garantías y estatuto protector, a los *offline* (Sánchez-Urán Azaña, 2018, apartados III y IV.2). El criterio de la influencia decisiva probablemente responda mejor a estas observaciones. Pero las inquietudes reflejadas, sin duda legítimas, deberán contrarrestar algunos argumentos que conducen a opiniones muy distintas.

Debe subrayarse que la naturaleza de los nuevos servicios no coincide con la de los servicios tradicionales por el mero hecho de que ambos operen en el mismo mercado. En consecuencia, someter a todos ellos a un mismo marco regulador puede no estar justificado (Rodríguez Marín, 2018, pág. 67). Además, si todo comercio requiere confianza, el ámbito digital permite la cooperación de personas cada vez más alejadas entre sí, y es un hecho que la economía de las plataformas se está desarrollando cada vez

22. Cfr. Edelman y Geradin (2016, págs. 305-326); Hacker (2018, págs. 94-96).

más; una conclusión lógica es que los usuarios no están tan desprotegidos como pudiera parecer. Quizá los actores privados ofrezcan un nivel de calidad, seguridad y responsabilidad satisfactorio para sus usuarios. De ser así, habría que plantearse la posibilidad de que ciertas normas sirvan más bien a los intereses de las empresas reguladas, con efectos «proteccionistas» (Edelman y Geradin, 2016, págs. 306-309). No obstante, también hay que reconocer que los intentos de autorregulación por parte de las plataformas podrían no ser suficientes, de modo que la regulación por una autoridad resulte imprescindible (Dyal-Chand, 2015, págs. 303-304; Cao, 2017, págs. 1.097-1.110).

En relación con lo anterior, puede cuestionarse la eficiencia del marco legal que obliga a ofrecer las «garantías de calidad» referidas por la doctrina. Si hay personas que se decantan por opciones de consumo que no las ofrecen, conviene preguntarse si el legislador se ha olvidado de las preferencias de parte de los ciudadanos, y si los costes y beneficios que implican aquellos estándares arrojan un beneficio neto. Quizá los operadores digitales hayan solucionado problemas de asimetría informativa de manera más eficiente que los reguladores en su momento, de manera que algunas normas deban relajarse (Koopman, Mitchell y Thierer, 2015, págs. 539-544). Claro que tampoco debe excluirse una incorrecta evaluación de los riesgos por parte de los usuarios, derivada de sesgos cognitivos, cuya corrección recomiende una actividad regulatoria (Edelman y Geradin, 2016, págs. 317-318).

Tampoco cabe descartar la necesidad de establecer nuevas categorías de operadores con un régimen jurídico diferenciado, para una mejor adaptación del ordenamiento a la economía de las plataformas, como ya se ha planteado en relación con el derecho del trabajo (Hernández Bejarano, 2016, apartado III.2). En efecto, en este ámbito se ha puesto de relieve la dificultad de identificar en las nuevas relaciones las categorías tradicionales de trabajo autónomo y subordinado; lo que lleva a plantear perspectivas en las que el foco no se sitúa en el grado de dependencia funcional, sino en el tipo de mercado en el que se desarrolla la actividad profesional (Rodríguez-Piñero Royo, 2019, págs. 4-10). Así pues, la heterogeneidad de los nuevos modelos de negocio quizá requiera una clasificación más detallada que la bipartita entre plataformas activas y plataformas pasivas. Por supuesto, definir diferentes grados de influencia y adaptar la normativa a cada uno no es una tarea sencilla, pero no por ello debe rechazarse. Las plataformas constituyen actores de funciones híbridas y en constante evolución que encajan difícilmente en conceptos tradicionales (Finck, 2018, pág. 1.638). Cómo regularlas es, en consecuencia, una cuestión que permanece abierta, exigiendo un gran esfuerzo teórico para comprender la economía colaborativa (Dyal-Chand, 2015; Rodríguez Marín, 2018, págs. 62-67).

5. Conclusiones

El éxito de la economía digital depende de solucionar problemas de confianza, algo que las plataformas intermediarias intentan conseguir mediante diferentes mecanismos, algunos más invasivos con respecto al servicio subyacente que otros. El grado de influencia o control sobre dicho servicio permite distinguir las plataformas activas de aquellas cuya actividad es neutral o pasiva.

En el caso de Uber, el TJUE ha considerado que su influencia es decisiva. La plataforma no desarrolla una simple actividad de intermediación en la sociedad de la información, sino un servicio en el ámbito de los transportes. En el caso de Airbnb, la respuesta del Tribunal ha sido distinta: la actividad de intermediación es disociable del servicio de alojamiento y el operador de la plataforma no ejerce una influencia decisiva sobre este, por lo que su actividad sí constituye un servicio de la sociedad de la información.

El criterio de la influencia decisiva se revela un elemento clave en la economía digital, desde una perspectiva jurídica. De él pueden derivarse consecuencias importantes en ámbitos como el derecho del trabajo y las responsabilidades contractual y extracontractual, entre otros. En este contexto, conviene abrir varias líneas de debate. En primer lugar, parece oportuno verificar si el referido criterio ofrece una respuesta adecuada. Es posible que ejercer un importante grado de control no deba significar que las plataformas correspondientes dejen de tener la condición de intermediarios prestadores de servicios de la sociedad de la información. Ya sea como condición exclusiva, ya sea como condición cumulativa a la de prestadores de servicios en la materia propia de la actividad subyacente. En segundo lugar, es preciso revisar la regulación de los servicios subyacentes que se relacionan con la actividad de las plataformas intermediarias. Y, en tercer lugar, quizá sea necesario establecer un marco regulatorio para las plataformas intermediarias adaptado a varios niveles de influencia sobre aquellos servicios.

Referencias bibliográficas

BUSCH, C. (2016). «Crowdsourcing consumer confidence. How to regulate online rating and review systems in the collaborative economy». En: DE FRANCESCHI, A. (ed.). *European contract law and the digital single market*. Cambridge-Antwerp- Portland: Intersentia, págs. 223-243. https://doi.org/10.1017/9781780685212.013 [Fecha de consulta: 24 de julio de 2020].

BUSCH, C. (2018). «European model rules for online intermediary platforms». En: BLAUROCK, U.; SCHMIDT-KESSEL, M.; ERLER, K. (eds.). *Plattformen: Geschäftsmodell und Verträge*. Baden-Baden: Nomos, págs. 37-57. https://doi.org/10.5771/9783845292298-37 [Fecha de consulta: 24 de julio de 2020].

CAO, D. (2017). «Regulation through deregulation: sharing economy companies gaining legitimacy by circumventing traditional frameworks». *Hastings Law Journal*, vol. 68, núm. 5, págs. 1.085-1.110.

COMISIÓN EUROPEA (2016). *Una Agenda Europea para la economía colaborativa* [Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones]. COM(2016) 356 final.

DE FRANCESCHI, A. (2018). «*Uber Spain* and the "identity crisis" of online platforms». *Journal of European Consumer and Market Law*, vol. 7, núm. 1, págs. 1-4.

DE LA ENCARNACIÓN, A. M. (2016). «El alojamiento colaborativo: Viviendas de uso turístico y plataformas virtuales». *Revista de Estudios de la Administración Local y Autonómica*, núm. 5, págs 30-55 [en línea] https://doi.org/10.24965/reala.v0i5.10350 [Fecha de consulta: 6 de julio de 2020].

DYAL-CHAND, R. (2015). «Regulating sharing: the sharing economy as an alternative capitalist system». *Tulane Law Review*, vol. 90, núm. 2, págs. 241-309.

EDELMAN, B. G.; GERADIN, D. (2016). «Efficiencies and regulatory shortcuts: how should we regulate companies like Airbnb and Uber?». *Stanford Technology Law Review,* vol. 19, núm. 2, págs. 293-328.

ELI (European Law Institute) (2020). *Model rules on online platforms* [en línea] https://www.europeanlawinstitute.eu/fileadmin/user_upload/p_eli/Publications/ELI_Model_Rules_on_Online_Platforms.pdf [Fecha de consulta: 6 de julio de 2020].

EPSTEIN, R. A. (2019). «California knifes the gig economy» [en línea] https://www.hoover.org/research/california-knifes-gig-economy [Fecha de consulta: 6 de julio de 2020].

FINCK, M. (2018). «Distinguishing internet platforms from transport services: *Elite Taxi* v. *Uber Spain*». *Common Market Law Review*, vol. 55, núm. 5, págs. 1.619-1.640.

GONZÁLEZ CARRASCO, C. (2020). «Airbnb es un prestador de servicios de la sociedad de la información. Consecuencias de la STJUE 19.12.2019 (C-390/18) para el alquiler vacacional español» [en línea] http://centrodeestudiosdeconsumo.com/images/Airbnb_es_un_prestador_de_servicios_de_la_sociedad_de_la_informacion_-_consecuencias.pdf [Fecha de consulta: 6 de julio de 2020].

HACKER, P. (2018). «UberPop, UberBlack, and the regulation of digital platforms after the *Asociación Profesional Elite Taxi* judgment of the CJEU». *European Review of Contract Law,* vol. 14, núm. 1, págs. 80-96 [en línea] https://doi.org/10.1515/ercl-2018-1005 [Fecha de consulta: 6 de julio de 2020].

HERNÁNDEZ BEJARANO, M. (2016). «El apoyo europeo al modelo de economía colaborativa: algunas cuestiones y propuestas para afrontar una regulación laboral y de seguridad social». *Revista Española de Derecho del Trabajo,* núm. 192 (BIB 2016\85594).

HIRA, A.; REILLY, K. (2017). «The emergence of the sharing economy: implications for development». *Journal of Developing Societies*, vol. 33, núm. 2, págs. 175-190 [en línea] https://doi.org/10.1177/0169796X17710071 [Fecha de consulta: 6 de julio de 2020].

HUET, J. (2018). «Est un "service dans le domaine des transports" l'intermédiation numérique mettant en relation des chauffeurs non professionnels utilisant leur propre véhicule avec des personnes qui souhaitent effectuer un déplacement urbain (arrêt Uber)». *Revue des contrats,* núm. 2, págs. 210-211.

KOOPMAN, C.; MITCHELL, M.; THIERER, A. (2015). «The sharing economy and consumer protection regulation: the case for policy change». *Journal of Business, Entrepreneurship & the Law,* vol. 8, núm. 2, págs. 529-545.

MAK, V. (2018). «Regulating online platforms: the case of Airbnb». En: GRUNDMANN, S. (ed.). *European contract law in the digital age.* Cambridge-Antwerp-Portland: Intersentia, págs. 87-102.

ØSTERGAARD, K.; JAKOBSEN, S. S. (2019). «Platform intermediaries in the sharing economy: questions of liability and remedy». *Nordic Journal of Commercial Law,* núm. 1, págs. 21-41.

RALLO, J. R. (2017). «Con o sin sentencia, acabemos con las licencias de taxi». *El Confidencial* [en línea] https://blogs.elconfidencial.com/economia/laissez-faire/2017-12-20/sentencia-tjue-taxi-uber-licencias_1496098/ [Fecha de consulta: 6 de julio de 2020].

RENDERS, D.; DE VALKENEER, D. (2018). «Arrêt "Asociación Profesional Elite Taxi": Uber, un service de transport freiné dans sa course?». *Journal de droit européen,* núm. 246, págs. 47-48.

RGLDS (Research group on the Law of Digital Services) (2016). «Discussion draft of a Directive on online intermediary platforms». *Journal of European Consumer and Market Law,* vol. 5, núm. 4, págs. 164-169.

RODRÍGUEZ MARÍN, S. (2018). «Aspectos jurídicos de la economía colaborativa y bajo demanda en plataformas digitales». En: RODRÍGUEZ MARÍN, S.; MUÑOZ GARCÍA, A. (coords.). *Aspectos legales de la economía colaborativa y bajo demanda en plataformas digitales*. Las Rozas (Madrid): Bosch, págs. 43-76.

RODRÍGUEZ-PIÑERO ROYO, M. (2019). «Trabajo en plataformas: innovaciones jurídicas para unos desafíos crecientes». *IDP. Revista de Internet, Derecho y Política,* núm. 28, págs. 3-16 [en línea] http://dx.doi.org/10.7238/idp.v0i28.3180 [Fecha de consulta: 6 de julio de 2020].

RUDA GONZÁLEZ, A. (2018). «Responsabilidad por hechos ajenos en la economía colaborativa. El caso de UBER». En: BALCELLS, J. *et al*. (coords.). *Collaborative Economy*. Challenges & Opportunities. Barcelona: Huygens Editorial, págs. 424-440.

SÁNCHEZ-URÁN AZAÑA, M.ª Y. (2018). «Economía de plataformas digitales y servicios compuestos. El impacto en el Derecho, en especial, en el Derecho del Trabajo. Estudio a partir de la STJUE de 20 de diciembre de 2017, C-434/15, Asunto Asociación Profesional Élite Taxi y Uber Systems Spain S.L.». *La Ley Unión Europea,* núm. 57 (LA LEY 2492/2018). https://doi.org/10.5209/FORO.57538 [Fecha de consulta: 24 de julio de 2020].

SANTOS BRIZ, J. (1984). «Artículo 1902». En: ALBALADEJO, M. (dir.). *Comentarios al Código Civil y Compilaciones Forales,* tomo XXIV. Madrid: EDERSA, págs. 99-560.

SCHAUB, M. Y. (2018). «Why Uber is an information society service. Case note to CJEU 20 December 2017 C-434/15 (Asociación profesional Élite Taxi)». *Journal of European Consumer and Market Law,* vol. 7, núm. 3, págs. 109-115.

SOLÉ FELIU, J. (2012). *La responsabilidad extracontractual del principal por hechos de sus auxiliares: Principios y tendencias.* Madrid: Reus.

THIERER, A. *et al*. (2016). «How the Internet, the sharing economy, and reputational feedback mechanisms solve the "lemons problem"». *University of Miami Law Review,* vol. 70, núm. 3, págs. 830-878 [en línea] https://repository.law.miami.edu/umlr/vol70/iss3/6 [Fecha de consulta: 6 de julio de 2020].

TOURIÑO, A. (2018). «Régimen de responsabilidad de las plataformas que operan en el ámbito de la economía colaborativa». En: RODRÍGUEZ MARÍN, S.; MUÑOZ GARCÍA, A. (coords.). *Aspectos legales de la economía colaborativa y bajo demanda en plataformas digitales*. Las Rozas (Madrid): Bosch, págs. 77-101.

TWIGG-FLESNER, C. (2016). «Disruptive technology-disrupted law? How the digital revolution affects (contract) law». En: DE FRANCESCHI, A. (ed.). *European contract law and the digital single market*. Cambridge-Antwerp-Portland: Intersentia, págs. 21-48. https://doi.org/10.1515/ercl-2018-1005 [Fecha de consulta: 24 de julio de 2020].

Cita recomendada

PAZOS CASTRO, Ricardo (2020). «Uber, Airbnb y la llamada "influencia decisiva" de las plataformas digitales», *IDP. Revista de Internet, Derecho y Política,* núm. 31, págs. 1-14. UOC [Fecha de consulta: dd/mm/aa]. http://dx.doi.org/10.7238/idp.v0i31.3224

Sobre el autor

Ricardo Pazos Castro
ricardo.pazos@uam.es
Profesor ayudante doctor de Derecho Civil

Ricardo Pazos Castro es profesor ayudante doctor de Derecho Civil en la Universidad Autónoma de Madrid. Ha sido becario posdoctoral del Programa de axudas á etapa posdoutoral da Xunta de Galicia (Consellería de Cultura, Educación e Ordenación Universitaria), etapa durante la cual se llevó a cabo este trabajo. Tras realizar una tesis sobre el control de contenido de las condiciones generales de la contratación, ampliada posteriormente para su publicación en la editorial Aranzadi bajo el título "El control de las cláusulas abusivas en los contratos con consumidores", publicó una monografía en la editorial Bosch acerca de la protección de los consumidores en el transporte aéreo de pasajeros. También cuenta con publicaciones en materias como la protección de datos, la responsabilidad civil y la contratación bancaria, entre otros asuntos. Es miembro del grupo de trabajo en el Proyecto de Investigación «Soluciones jurídicas y económicas al problema inmobiliario turístico» (DER 2017-82705-R), del Programa Estatal de I+D+i Orientada a los Retos de la Sociedad del Ministerio de Economía, Industria y Competitividad. El presente trabajo se enmarca dentro de este proyecto de investigación.

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

www.uoc.edu/idp

ARTÍCULO

Redes sociales y discurso del odio: perspectiva internacional[1]

Göran Rollnert Liern
Universidad de Valencia

Fecha de presentación: febrero de 2020
Fecha de aceptación: junio de 2020
Fecha de publicación: septiembre de 2020

Resumen

El presente trabajo analiza las medidas legislativas que se obligan a adoptar los Estados parte en el Protocolo adicional al Convenio sobre la Ciberdelincuencia de 2003 para homogeneizar la legislación penal sobre la difusión de «material racista y xenófobo» en internet tipificando como delito determinadas conductas contra personas o grupos por razón de su raza, color, ascendencia, origen nacional o étnico o religión, tratando en primer lugar las cuestiones interpretativas que plantea su redacción y que han sido abordadas por el Informe explicativo. A continuación se estudian los problemas que plantea la aplicación de los criterios que resultan del Protocolo al llamado «discurso del odio» en las redes sociales: la intencionalidad de la conducta y de los efectos de la difusión teniendo en cuenta las especificidades de las redes sociales; la publicidad intencional de la conducta, que se deslinda de las comunicaciones privadas no penalizables por la predeterminación del destinatario, con los problemas que se plantean cuando el destinatario es un grupo de personas; y la definición del material racista y xenófobo que propugna, promueve o incita al odio, la discriminación y la violencia, por remisión a los instrumentos internacionales en los que la incitación es un elemento clave de forma que se incorpora como requisito implícito adicional el «riesgo inminente» según el conocido estándar norteamericano. Finalmente, se examina cómo algunos de estos criterios –en particular, la doctrina del «riesgo inminente»– han sido aplicados en una reciente sentencia del Tribunal Europeo de Derechos Humanos de 2018 sobre el discurso del odio en internet.

Palabras clave

ciberdelincuencia, discurso de odio, libertad de expresión, incitación, Tribunal Europeo de Derechos Humanos

1. Trabajo realizado en el marco del proyecto de I+D+i Retos MICINN "Derechos y garantías frente a las decisiones automatizadas en entornos de inteligencia artificial, IoT, big data y robótica" (PID2019-108710RB-I00, 2020-2022).

Social networks and hate speech: an international perspective

Abstract

The work analyses the legislative measures which the Party States in the Additional Protocol at the 2003 Convention on Cybercrime are obliged to adopt in order to harmonise the criminal legislation on the dissemination of "racist and xenophobic material" on the Internet, classifying as criminal certain conduct against individuals or groups for reasons of their race, colour, descent, national or ethnic origin or religion, addressing firstly the interpretative issues which its composition brings forward and which were addressed by the Explanatory Report. Next, there is a study of the problems posed by the application of the criteria resulting from the Protocol to that which is termed "hate speech" in social networks: the intentionality of both the conduct and the effects brought about by the dissemination, taking into account the specifities of the social networks; intentional dissemination to the public in relation to the conduct, which is separate from private communications that are unpunishable due to the predetermination of the recipient, with the problems which arise when the recipient is a group of people; and the definition of the racist and xenophobic material which advocates, promotes or incites hatred, discrimination and violence, by reference to the international instruments in which incitement is a key element so that "imminent danger" is incorporated as an additional implicit requirement in accordance with the recognised North American standard. Finally, there is an examination of how some of these criteria –in particular, the doctrine of "imminent danger"– have been applied in a recent judgement by the European Court of Human Rights in 2018 on Internet hate speech.

Keywords

cybercrime, hate speech, freedom of expression, incitement, European Court of Human Rights

Introducción

La proliferación del discurso del odio en internet y, en particular, en las redes sociales[2] es un fenómeno constatado hasta el punto de que con la introducción de los denominados «delitos de odio» en nuestro Código Penal en 2015 se ha pretendido hacerle frente mediante la agravación de las penas «cuando los hechos se hubieran llevado a cabo a través de un medio de comunicación social, por medio de internet o mediante el uso de tecnologías de la información» (artículo 510.3).

El Preámbulo de la Ley Orgánica 1/2015, de 30 de marzo, de reforma del Código Penal, ha justificado la nueva regulación de la incitación al odio y a la violencia «por la necesidad de atender compromisos internacionales» (apartado I). Ahora bien, esta remisión a la normativa internacional no es una novedad. La jurisprudencia constitucional relativa al discurso del odio[3] viene incorporando a su argumentación los textos internacionales sobre esta materia desde el primer momento, tendencia que ha ido *in crescendo* en los pronunciamientos más recientes[4]. Asimismo, a partir de la STC 112/2016, de 20 de junio, el Tribunal Supremo se ha sumado también a esta progresiva recepción del marco internacional sobre el discurso del odio, en especial en lo que se refiere al enaltecimiento del terrorismo.

En consecuencia, cualquier análisis jurídico del discurso del odio resultaría incompleto si no atendiera al vector interpretativo de la normatividad internacional[5], siendo esta última el objeto del presente trabajo, que adopta un enfoque muy concreto, centrado en las peculiaridades de las redes sociales por ser este el entorno en el que las expresiones de odio han incrementado exponencialmente su presencia en detrimento del espacio físico.

1. El Protocolo Adicional al Convenio sobre Ciberdelincuencia y la interpretación de sus términos

El único instrumento internacional sobre el discurso del odio que contempla específicamente las expresiones de odio en internet es el Protocolo Adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos[6], de 28 de enero de 2003, en vigor desde el 1 de marzo de 2006 (en España desde el 1 de abril de 2015), cuyo objetivo es armonizar la legislación penal sustantiva referente a la lucha contra la propaganda racista y xenófoba, completando así las provisiones del Convenio.

En su virtud, los Estados parte se obligan a tipificar como delito en su derecho interno determinadas conductas cometidas «por medio de un sistema informático» sobre personas o grupos por razón de su raza, color, ascendencia, origen nacional o étnico o religión. Entre estas conductas se encuentran las amenazas de comisión de delitos graves, los insultos, la difusión o puesta a disposición del público de material negacionista o justificador de genocidios o crímenes contra la humanidad y, especialmente, la difusión o puesta a disposición del público de «material racista y xenófobo» (artículos 3-6).

Los términos del Protocolo plantean al menos tres cuestiones interpretativas que han sido abordadas por el Informe explicativo[7] (el Informe en adelante) que, aunque no proporciona una «interpretación autorizada del Protocolo» (pág. 1) –como él mismo reconoce–, sí facilita la aplicación de sus disposiciones:

a) ¿Qué se entiende por «material racista y xenófobo»? Según el Protocolo, «todo material escrito, toda imagen o cualquier otra representación de ideas o teorías, que

2. Miró-Llinares y Gómez-Bellvís (2020), págs. 13-15.
3. SSTC 214/1991, de 11 de noviembre, FJ 3; 176/1995, de 11 de diciembre, FJ 5; 235/2007, de 7 de noviembre, FJ 5; y 177/2015, de 22 de julio, FFJJ 2, c) y 5, y voto particular de A. Asúa Batarrita, apartados 1 y 4.
4. SSTC 112/2016, de 20 de junio, FFJJ 4 y 6; y 35/2020, de 25 de febrero, FJ 2, b) y c), por remisión a la anterior.
5. Rollnert Liern (2019).
6. Para una visión general del Protocolo y una valoración crítica del mismo, Akdeniz (2008).
7. Council of Europe (2003). Todos los entrecomillados posteriores de este apartado hacen referencia a este documento, salvo indicación en contrario.

propugne, promueva o incite al odio, la discriminación o la violencia» (artículo 2.1). Afirma el Informe que se penaliza la difusión de «ideas y teorías» en cualquier formato (escrito, imágenes o cualquier otra representación de «ideas o teorías» almacenable, procesable y trasmisible por medios informáticos), no tanto porque sea «expresión de sentimientos/creencias/aversión» sino porque puede llevar a «cierta conducta» (pág. 3) en la medida que «propugne, promueva o incite al odio, la discriminación o la violencia». Dicho de otra forma, la relevancia penal del material radica, más que en lo que expresa, en las acciones que podría provocar en terceras personas, en su efecto perlocutivo.

b) Con carácter general, el Protocolo anuda la responsabilidad penal a que las conductas sean cometidas «intencionalmente», si bien, como señala el Informe, en ciertos casos se exige una intención específica adicional; así, en la negación o justificación del genocidio o de crímenes contra la humanidad, cabe condicionar la penalización a la presencia de la «intención de incitar» al odio, discriminación o violencia; y en la cooperación y la complicidad (artículo 7), el cooperante o cómplice debe tener también la intención de que el delito sea cometido. Los redactores del Protocolo acordaron que «el significado exacto de "intencionalmente" debería dejarse a la interpretación nacional», añadiendo que no se puede castigar penalmente a nadie por los delitos descritos en el Protocolo si no tienen la intención requerida. El Informe se refiere como ejemplo a los proveedores de servicios de internet afirmando que no serán criminalmente responsables por alojar una web con material racista y xenófobo si no han tenido la intención exigida por el derecho interno en el caso particular, no siéndoles exigible que supervisen o controlen activamente la conducta y los contenidos de sus clientes (págs. 5-7).

c) Respecto a la publicidad de la conducta, exigida por la propia naturaleza de los delitos de «difundir o poner a disposición del público» material racista y xenófobo o material negacionista o justificador de genocidios o crímenes contra la humanidad, el Informe define la difusión como la «divulgación (*dissemination*) activa» y la puesta a disposición como la acción de subir material a internet para uso de terceros, incluyendo la creación o compilación de hiperenlaces que faciliten acceso al mismo.

La referencia al «público» deja claro que las comunicaciones o expresiones privadas transmitidas informáticamente quedan fuera del ámbito del delito y están protegidas por el derecho al respeto de la vida privada y familiar y de su correspondencia (artículo 8.1 CEDH).

La exigencia de publicidad se incorpora también al delito de insultos[8] racistas o xenófobos que serían penalmente atípicos en comunicaciones privadas. Por contra, en las amenazas racistas o xenófobas, el tipo delictivo se extiende también a las realizadas en comunicaciones privadas.

2. La problemática aplicación de los criterios del Protocolo al discurso del odio en las redes sociales

2.1. La intencionalidad de la conducta (y de los efectos de la difusión)

La intencionalidad es uno de los «principios centrales» que, según el Tribunal Penal Internacional para Ruanda, emergen de la jurisprudencia internacional sobre incitación a la discriminación y la violencia[9]. Este principio ha resultado relativizado, no obstante, por la Comisión Europea contra el Racismo y la Intolerancia (2016) en su Recomendación de política general núm. 15 de 2015 que recomienda penalizar el discurso del odio no solo cuando exista «intención de incitar» sino, alternativamente, cuando «pueda razonablemente esperarse que incite a actos de violencia, intimidación, hostilidad o discriminación» por existir «riesgo inminente» de violencia, hostilidad, intimidación o discriminación. Sin embargo, la generalización de la exigencia de intencionalidad en los instrumentos internacionales sobre discurso del odio –con matices en

8. McGonagle, comentando la definición de insulto postulada en el Informe (pág. 7), señala la dificultad para deslindar los insultos de las ideas que «ofenden» o «chocan», que la STEDH *Handyside* (7 de diciembre de 1976) considera amparadas por la libertad de expresión en su apartado 49 (2012, pág. 472).
9. *Sentencia Prosecutor v. Ferdinand Nahimana, Jean-Bosco Barayagwiza, Hassan Ngeze. Case No. ICTR-99-51-T (3 de diciembre de 2003)*, conocida como «*Media case*», apartados 980-1007.

algunos casos[10]– y, sobre todo, su asunción expresa en el Protocolo al describir las conductas típicas no dejan lugar a dudas acerca de su aplicabilidad al discurso del odio en internet.

La intencionalidad es un requisito subjetivo definitorio del discurso del odio, más determinante incluso, para algunos autores, que las características del individuo o grupo destinatario del mensaje[11] y que el propio contenido de la expresión, que no es en sí mismo el factor decisivo[12]. La valoración de esta intención en el discurso del odio *online* presenta dos singularidades a considerar:

a) La intención del sujeto no se limita, en el caso de la difusión de material, a la propia conducta de distribuirlo, hacerlo circular, diseminarlo o ponerlo a disposición de terceros, sino que se extiende a su propia naturaleza incitadora o promocional del odio, la discriminación y la violencia. Dicho de otra forma, el autor debe querer difundir ese material y tener «conocimiento efectivo del contenido del material»[13], compartiendo así el propósito de que el efecto de su difusión sea propugnar, promover o incitar al odio, la discriminación o la violencia. A decir del Informe, «el acto de difundir o poner a disposición es solo criminal si la intención está también dirigida al carácter racista y xenófobo del material» (Council of Europe, 2003, pág. 6). En este sentido debe interpretarse la exigencia expresa de que la conducta sancionable se lleve a cabo «intencionadamente y sin derecho», de tal manera que no será sancionable cuando la difusión esté justificada por principios o intereses legítimos que, conforme a la legislación interna de cada Estado, excluyan la responsabilidad criminal (finalidades de aplicación de la ley o investigación de delitos, motivos académicos o de investigación, u otros, Council of Europe, 2003, pág. 5).

b) La valoración de la intención debe tener en cuenta las especificidades del medio en el que se produce la conducta, internet, y en particular de las redes sociales. La desinhibición y libertad de tono propia de las redes sociales, reforzada por la sensación de anonimato[14] son aspectos significativos para calificar la intención del sujeto. La valoración de la intención de los mensajes tiene que tener en cuenta los «códigos expresivos de las redes sociales» (Boix Palop, 2016, pág. 82) que no siempre están claros y son conocidos por los emisores de los mensajes[15]. La difusión de un mensaje de odio en redes sociales, retuiteando por ejemplo o enlazando o poniendo en circulación determinado material, no siempre implica adhesión al contenido del mismo con intención de incitar o fomentar, sino que puede buscar informar sobre dichos mensajes por considerarlos un asunto de interés público, denunciarlos o criticarlos abiertamente o con expresiones o imágenes de carácter cómico, irónico o satírico (memes), siendo por tanto necesario evaluar el propósito del emisor «a partir del conjunto de sus mensajes y no aisladamente»[16].

2.2. La publicidad (intencional) de la conducta

La publicidad requerida por el Protocolo para definir las conductas penalizables (salvo las amenazas) es objeto de consideración en el Informe, que, por una parte, excluye las comunicaciones o expresiones privadas del ámbito de aplicación del Protocolo y, por otra, para deslindar casuísticamente las comunicaciones privadas de aquellas que deben considerarse difusión de material racista y xenófobo penamente perseguible, identifica como criterio principal «la intención del emisor de que el mensaje en cuestión será recibido solo por el destinatario predeterminado», intención subjetiva que puede establecerse a partir de «factores objetivos» como «el contenido del mensaje, la tecnología usada, las medidas de seguridad aplicadas y el contexto en el que el mensaje es enviado» (Council of Europe, 2003, pág. 6).

Sin embargo, también afirma que, si hay más de un destinatario simultáneo del mensaje, el carácter público o privado dependerá del número de receptores y de la naturaleza de la relación entre emisor y receptor. Según el Informe, el acceso abierto del material a cualquier persona (en un

10. Rollnert Liern (2019), págs. 95-98.
11. Reed (2009), pág. 81.
12. Titley, Keen y Földi (2015), pág. 28.
13. Teruel Lozano (2015), pág. 93.
14. Falxa (2015), págs. 3-4. Véase García González sobre la sensación de usuario anónimo como factor de riesgo (2015, págs. 10-13).
15. Díez Bueso (2018), pág. 10.
16. Ídem.

chat, en un grupo de noticias o en un foro, son los ejemplos que pone el Informe) encajará en la conducta típica de «poner a disposición del público», incluso cuando se requiera contraseña, siempre que la misma se proporcione a cualquiera o al que cumpla ciertos criterios; no obstante, la naturaleza de la relación entre los participantes en la comunicación deberá tenerse en cuenta para determinar si hubo difusión pública o puesta a disposición del público o si, por el contrario, se trató de una comunicación privada penalmente atípica (Council of Europe, 2003, pág. 6).

La aplicación de este criterio no plantea problemas en mensajes accesibles para cualquier usuario indeterminado al tratarse de un ámbito público, y tampoco en comunicaciones privadas con destinario único determinado. La dificultad radica en delimitar lo público y lo privado en mensajes dirigidos a grupos de destinatarios que, por el número de sus integrantes y las relaciones que mantienen entre ellos (desde amistad en el mundo real hasta la simple condición de «amigo de un amigo» en las redes sociales), ya no pueden considerarse estrictamente cerrados sino semipúblicos o semiprivados –como los grupos amplios de WhatsApp o Telegram con muchos participantes[17]– difuminándose así los límites entre la privacidad y la esfera pública. La combinación de los criterios del número de destinatarios y sus relaciones con el emisor será aquí lo decisivo, pero no deja de ser conflictiva. ¿A partir de qué número de destinatarios la comunicación es pública, aunque sea un grupo cerrado? ¿Hay publicidad cuando la comunicación en un grupo cerrado se dirige a pocos destinatarios, pero no hay criterios selectivos de admisión en el círculo privado o, si los hay, no se aplican en la práctica?

Otro aspecto a considerar es si en la valoración de la relevancia penal de la difusión debe atenderse a la publicidad potencial del mensaje en las redes sociales (al difundirse en abierto o a grupos numerosos de destinatarios no determinados selectivamente) o, por el contrario, a la publicidad «efectiva», de manera que no por publicarse un contenido en una red social debe considerarse, por definición, público[18]. Para Tamarit Sumalla, la publicidad no solo se produce cuando el acceso es libre sino «también a través de las redes sociales con acceso restringido a usuarios registrados, siempre que el mensaje pueda ser transmitido a un amplio y relativamente indeterminado número de personas» (2018, págs. 20-21). Por su parte, Teruel Lozano propone tener en cuenta «por un lado, el canal o espacio de difusión (si se trata de un canal o espacio privado o abierto a un público indeterminado), y, por otro, la audiencia potencial que haya podido tener el mensaje», de modo que, cuando la difusión se haya producido en un canal público, lo determinante serán los destinatarios potenciales, mientras que en los canales privados con un grupo numeroso de destinatarios habría que tener en cuenta los destinatarios efectivos de la comunicación (2018, pág. 25).

Finalmente, si el criterio fundamental para diferenciar las comunicaciones privadas no punibles de la difusión pública tipificada penalmente es, según el Informe, la intención subjetiva del emisor de limitar el mensaje a un determinado destinatario, la difusión pública solo será sancionable cuando sea intencional y voluntaria. Por tanto, si la publicidad no ha sido buscada intencionadamente por el emisor porque es el destinatario quien ha difundido un mensaje privado, será este último el responsable penalmente de la difusión (si ha tenido intención de incitar, promover o fomentar el odio, la violencia o la discriminación); y si no lo ha difundido con esta intención, sino para denunciar o criticar las expresiones del emisor, ni uno ni otro podrán ser incriminados por faltar la intencionalidad en el destinatario que lo difunde y la intención de darle publicidad en el emisor originario del mensaje. Otro tanto cabe decir si la publicidad es imputable al emisor pero no es deliberada, sino consecuencia de una configuración errónea de la privacidad de la cuenta o de cualquier otro factor ajeno a su voluntad consciente.

La falta de plena conciencia de la publicidad de la conducta es otro elemento a ponderar para apreciar la intencionalidad de la publicidad, influyendo en ello la inmaterialidad del medio de difusión o, dicho de otra manera, la desconexión entre la emisión del mensaje en un entorno físico privado y su repercusión en la esfera pública virtual en la que despliega sus consecuencias. Como dice Rodríguez-Izquierdo Serrano, «al poder hacerlo sin salir físicamente del ámbito privado desde el que escribe, donde tenga su terminal, el receptor-emisor no adquiere una conciencia nítida de estar actuando en un espacio público de comu-

17. Boix Palop (2016), pág. 58.
18. Ídem, pág. 89.

nicación» (2017, pág. 140); de la misma forma, esa desconexión «desvirtúa (...) la percepción clara de los límites a la expresión en internet» y del «carácter lesivo» de las conductas que se realizan en el ciberespacio[19].

Ello nos lleva a la cuestión de la repercusión de las características de la comunicación en redes sociales sobre los elementos típicos de las conductas penalizables según el Protocolo, dificultando y complicando la valoración de la intencionalidad y la publicidad. Así, la facilidad de la expresión espontánea en las redes sociales ofrece a personalidades con rasgos de impulsividad y precipitación una forma rápida y sencilla de comunicar mensajes negativos que, en ocasiones, puede tener más que ver con la construcción de una identidad digital propia ante el círculo de contactos o seguidores que con la intención consciente de provocar en los posibles destinatarios la voluntad de realizar actos de odio, violencia o discriminación. Sin embargo, esta facilidad es un arma de doble filo dado que un tribunal puede deducir la intencionalidad de la conducta del hecho de que, teniendo la posibilidad de corregir, rectificar o aclarar el mensaje fácilmente en la misma red, no se haya hecho uso de esa posibilidad.

Por otra parte, la sensación de anonimato e impunidad[20] maximiza la posibilidad de dar rienda suelta a discursos destructivos sin tener que afrontar las consecuencias que tendrían idénticas acciones en la vida real[21] y, al mismo tiempo, sin ser plenamente conscientes de la difusión y trascendencia de sus mensajes.

La propia percepción del entorno de la red social por los usuarios afecta a la publicidad intencional de la conducta. ¿Hasta qué punto los usuarios tienen conciencia de la posible repercusión pública de sus mensajes en las redes o las perciben como prolongación virtual de un espacio de comunicación informal y desenfadado con un círculo limitado de amistades en el que son permisibles expresiones que no harían en un ámbito público?[22] Las redes sociales convierten inmediatamente en públicos actos y comportamientos individuales antes limitados a ambientes y redes personales, existiendo por ello entre los usuarios jóvenes mayor tolerancia a mensajes de odio y violentos en internet que en el entorno real[23]. La falta de conciencia de actuar en un espacio público de comunicación hace que expresiones exaltadas y de odio «que en principio solo se permitiría a sí mismo en un entorno reducido (...) saltan al debate público digital sin que se haya reflexionado sobre la diferencia cuantitativa y cualitativa que le da su difusión en la red»[24].

2.3. El material que propugne, promueva o incite al odio, la discriminación o la violencia y la doctrina del «riesgo inminente»

La definición del material racista y xenófobo como aquel «que propugne, promueva o incite al odio, la discriminación o la violencia» (artículo 2.1) cuya difusión obliga a sancionar penalmente el Protocolo (artículo 3) requiere ser comentada. El Informe parece establecer una escala entre las tres acciones por su menor o mayor efecto sobre la audiencia destinataria: propugnar sería hacer un alegato justificando en abstracto el odio, la discriminación o la violencia; promover implicaría estimularlo o fomentarlo, buscando una influencia más incisiva en la audiencia; e incitar supondría instar o llamar al público al odio, la discriminación o la violencia (Council of Europe, 2003, pág. 3).

El Informe afirma que esta definición «se basa en las definiciones y documentos existentes nacionales e internacionales (ONU, UE) en la medida de lo posible» (pág. 3) por lo que la determinación del alcance y extensión de las acciones sancionables requiere ser contextualizada en el marco de la regulación internacional sobre el «discurso del odio». El Pacto Internacional de Derechos Civiles y Políticos, de 16 de diciembre de 1966 (en vigor desde el 23 de marzo de 1976), es referencia obligada al disponer su artículo 20.2 que «toda apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia estará prohibida por la ley».

19. Falxa (2015), pág. 3.
20. Jubany y Malin (2015), pág. 16.
21. Gagliardone, I. *et al.* (2015), pág. 8.
22. En este sentido, Boix Palop (2016), pág. 61.
23. Jubany y Malin (2015), págs. 16 y 28.
24. Rodríguez-Izquierdo Serrano (2017), pág. 40.

La noción de incitación constituye así un elemento clave del que no existe interpretación auténtica en el propio Pacto ni en las Observaciones generales y jurisprudencia del Comité de Derechos Humanos. Puede considerarse una interpretación relativamente autorizada[25] la contenida en el Principio 12.1.iii de Camden de 2009 sobre la libertad de expresión y la igualdad: «declaraciones sobre grupos nacionales, raciales o religiosos que puedan crear un riesgo inminente de discriminación, hostilidad o violencia contra las personas que pertenecen a dichos grupos»[26]. Lo decisivo de la incitación es, por tanto, la generación de un riesgo inminente de discriminación, hostilidad o violencia.

Esta definición de la acción de incitar por remisión al estándar de los Principios de Camden incorpora pues el «riesgo inminente» de odio, discriminación o violencia como requisito adicional implícito en la definición del Protocolo. Ello supone asumir el estándar Brandenburg[27] sobre incitación proveniente de Estados Unidos, siendo difícil de aplicar a los mensajes difundidos en redes sociales al implicar una cierta proximidad temporal entre la incitación y el daño producido por el mensaje.

Por este motivo se ha discutido la utilidad del estándar Brandenburg para la incitación en internet[28]: la exigencia del «riesgo inminente» podría cumplirse en el caso de llamadas inmediatas a la acción en redes como Instagram o Snapchat, pero no cuando los efectos se producen a largo plazo[29]. Se ha señalado así la mayor adecuación de la doctrina de las «amenazas verdaderas» (*true threats*[30]) para inspirar la legislación restrictiva del discurso del odio en internet por cuanto no requiere la inminencia del riesgo sino la intención del emisor de provocar temor en el destinatario sin necesidad de producción de un resultado peligroso: «no hay necesidad de demostrar si una persona razonable habría entendido las declaraciones como intimidantes ni de aportar evidencias de la respuesta de la audiencia, sino solamente la intención de amenazar»[31].

Efectivamente, la relación de causalidad entre un mensaje difundido en las redes sociales y la probabilidad de impacto en forma de actos de odio, discriminación o violencia en pocas ocasiones podrá considerarse que cumple con la exigencia de inminencia del riesgo, en particular dada la fugacidad característica de la comunicación en las redes sociales[32]. Pero por muy fugaz que sea un mensaje o un comentario en las redes, sus efectos potenciales pueden desplegarse mucho más allá del momento en que desaparezcan a consecuencia de su permanencia en la red al margen de la voluntad del emisor, en diversos formatos y a través de la itinerancia de los contenidos mediante los hiperenlaces[33], lo que permite hablar de una potencial «indelebilidad» de los mensajes[34]. La arquitectura de las distintas plataformas influye, no obstante, en la probabilidad de que el mensaje en cuestión haga surgir el riesgo de reacciones de hostilidad, discriminación o violencia; así, se ha señalado que mientras Twitter facilita la rápida y potencialmente extensa difusión del mensaje ofreciendo al mismo tiempo la posibilidad de réplicas inmediatas por interlocutores influyentes que pueden neutralizarlo, Facebook permite la coexistencia paralela de múltiples hilos que pueden pasar más inadvertidos pero, al mismo tiempo, permanecer de forma más duradera[35].

25. Rollnert Liern (2019), págs. 84-91.
26. Article 19 (2009).
27. Por referencia a la conocida sentencia *Brandenburg v. Ohio* 395 U.S. 444, 447 (1969), según la cual «las garantías constitucionales de la libertad de expresión y de la libertad de prensa no permiten a un Estado prohibir o proscribir la defensa del uso de la fuerza excepto cuando tal defensa esté dirigida a incitar o producir una inminente ilegalidad y sea probable que incite o produzca tal acción». Al respecto, Rollnert Liern (2014), págs. 253-255.
28. Tsesis (2017), págs. 667-670; y Ring, 2013, págs. 18-19 y 46.
29. Tsesis, ídem.
30. Formulada en las sentencias *Watts v. United States*, 394 U.S. 705 (1969); *Virginia v. Black*, 538 U.S. 343 (2003); y *Elonis v. United States* 135 S. Ct. 2001 (2015).
31. Tsesis (201), pág. 669.
32. Falxa (2014), pág. 6.
33. Titley *et al.* (2015), págs. 13-14.
34. Díez Bueso (2018), págs. 7 y 13; y Boix Palop (2016), pág. 60.
35. Titley *et al.* (2015), págs. 13-14.

Para finalizar con este punto, las especificidades de las dinámicas comunicativas en las redes sociales parecen coexistir mejor con una definición de la incitación elaborada sustancialmente en torno a la intención subjetiva del emisor de provocar una acción en la audiencia que con el requisito de la inminencia temporal del riesgo, sin perjuicio de que no deba prescindirse de parámetros que permitan estimar el impacto de la expresión al menos en términos de probabilidad razonable.

3. El discurso del odio en internet ante el Tribunal Europeo de Derechos Humanos

Aunque el Protocolo solo ha sido utilizado en una ocasión por el TEDH como Derecho europeo e internacional relevante[36], el Tribunal se ha pronunciado recientemente sobre un caso de discurso del odio en internet en el que, a diferencia de tres casos previos sin doctrina significativa a efectos del presente trabajo[37], aplica los criterios tratados en los apartados anteriores.

Se trata de la sentencia de 28 de agosto de 2018 (caso *Savva Terentyev* c. Rusia) que estimó que violaba la libertad de expresión la condena de un ciudadano ruso por incitación al odio por un comentario contra la policía en un blog que, en términos muy insultantes, decía que «sería genial si en el centro de cada ciudad rusa, en la plaza principal (...) hubiera un horno, como en Auschwitz, en el que ceremonialmente todos los días, y mejor aún, dos veces al día (...) policías infieles fueran quemados. La gente los estaría quemando. Este sería el primer paso para limpiar a la sociedad de esta basura policial» (apartado 13).

El criterio de la intencionalidad de la conducta[38] no es aplicado directamente por el Tribunal, aunque sí implícitamente al señalar que los comentarios del recurrente, realizados durante una discusión, mostraban «desaprobación y rechazo emocional» hacia lo que consideraba abusos policiales y que pueden entenderse como una crítica feroz de la situación de la policía en Rusia (apartado 71); dice el Tribunal no estar convencido de que la referencia a la incineración ceremonial de los policías infieles pueda ser interpretada como «una llamada a la exterminación física de los policías por los ciudadanos ordinarios» siendo más bien «una metáfora provocativa que reafirmó frenéticamente el deseo de que la policía se "purificase" de oficiales corruptos y abusadores ("policías infieles") y fue su llamada emocional a tomar medidas para mejorar la situación» (apartado 72), añadiendo que «la destrucción por el fuego en sí misma no puede ser considerada tampoco como una incitación a una acción ilegal, incluida la violencia», puesto que «actos simbólicos de esta clase pueden ser entendidos como una expresión de insatisfacción y protesta más que como una llamada a la violencia» (apartado 74).

Tampoco la intención es mencionada previamente entre los «factores» a tener en cuenta para valorar las injerencias en la libertad de expresión en casos relativos a expresiones incitadoras o justificadoras del odio, la violencia o la intolerancia (resumidos en el caso *Perinçek*), a cuya luz afirma que va a resolver el caso con particular consideración a «la naturaleza y la redacción de las declaraciones impugnadas, el contexto en el que fueron publicadas, su potencial para llevar a consecuencias dañinas y las razones aducidas por los tribunales rusos para justificar la injerencia en cuestión» (apartado 66).

Para valorar el «impacto potencial», el Tribunal parte de la alta publicidad potencial de las publicaciones en internet, señalando que los comentarios enjuiciados fueron publicados en un blog públicamente accesible y que es verdad que el riesgo de daño planteado por los contenidos y comunicaciones en internet para el ejercicio y disfrute de los derechos y libertades es ciertamente mayor que el que supone la prensa, dado que el discurso ilegal, incluyendo el discurso del odio y las llamadas a la violencia, puede ser difundido como nunca antes, por todo el mundo, en

36. En la sentencia *Perinçek* (15 de octubre de 2015), apartado «Instrumentos y materiales relevantes del Consejo de Europa» (apartados 74-76).
37. SSTEDH *Delfi AS* (16 de junio de 2015), apartados 110, 115, 117, 140, 151, 153, 154, 156-159 y 162; *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt* (2 de febrero de 2016), apartado 91; y la Decisión de inadmisibilidad *Pihl* (9 de marzo de 2017), apartados 25 y 37.
38. El recurrente afirmó no haber tenido intención de hacer público el comentario –por ser una respuesta a un comentario anterior– y mucho menos de llamar a ninguna acción contra la policía, por cuanto había usado la exageración provocativa solamente para expresar la idea de que los policías «infieles» debían ser severamente castigados (apartado 17).

cuestión de segundos y en ocasiones permanece de forma persistente disponible en línea (apartado 79).

Afirmación que matiza seguidamente al señalar que, siendo claro que el alcance y potencial impacto de una afirmación lanzada en línea con unos pocos lectores no es ciertamente el mismo que si hubiera sido publicada en páginas web populares y muy visitadas, «es esencial para la valoración de la influencia potencial de una publicación *online* determinar el ámbito de su alcance entre el público» (apartado 79).

Así, después de reprochar a los tribunales rusos que no hayan valorado siquiera si el blog era generalmente muy visitado o el número de usuarios que accedieron, la Corte valora:

1. la publicidad efectiva que tuvo el comentario, publicado en línea durante un mes hasta que el recurrente lo retiró al conocer la existencia del procedimiento penal;

2. aunque el acceso no había estado restringido había atraído muy poca atención pública: algunos de los conocidos del recurrente lo desconocían y fue solo el procedimiento penal lo que suscitó el interés del público;

3. el recurrente no parece ser un bloguero conocido ni un usuario popular de las redes sociales y menos aún un personaje público o influyente cuya condición pudiera haber aumentado el impacto potencial de sus declaraciones.

A partir de estas consideraciones, el Tribunal llega finalmente a la conclusión de que «el potencial del comentario del recurrente para llegar al público y, por ello, para influir en su opinión fue muy limitado» (apartados 80 y 81).

Pero quizá lo más relevante de la sentencia es que aplica el criterio del «riesgo inminente» acogiendo el estándar Brandenburg sobre el «peligro claro e inminente», utilizado con anterioridad en las sentencias *Gül and others* (8 de junio de 2010), apartado 42, y *Kiliç and Eren* (29 de febrero de 2012), apartado 29, pero que por primera vez se proyecta sobre la incitación *online*. Así, señala que las declaraciones no atacaban personalmente a policías identificables sino más bien a la institución (apartado 75), que debería tener un grado particularmente alto de tolerancia al discurso ofensivo «a menos que tal discurso provocativo pueda provocar *inminentes acciones ilegales* con respecto a su personal y exponerlos a un *verdadero riesgo de violencia física*» (cursivas mías), añadiendo que solo en un «contexto muy sensible» de tensión, conflicto armado, lucha contra el terrorismo o disturbios letales en las prisiones, el Tribunal ha entendido que las declaraciones «pudieron alentar una violencia susceptible de poner en riesgo a los miembros de las fuerzas de seguridad» (apartado 77). Considera el Tribunal que ni en las sentencias de los tribunales nacionales ni en las alegaciones del Gobierno se reseñan circunstancias particulares por las que las afirmaciones en cuestión fueran «responsables de producir acciones ilegales inminentes respecto a los policías y de exponerlos a una amenaza real de violencia física»; los tribunales no explicaron por qué la policía, como grupo social, necesitaba protección reforzada ni se refirieron a ningún factor o contexto que pudiera demostrar que los comentarios del recurrente hubieran animado de hecho a la violencia y puesto a la policía en riesgo.

Para los jueces de Estrasburgo, los tribunales rusos se focalizaron en la naturaleza y redacción del comentario, limitándose a la forma y tenor del discurso, sin analizar las declaraciones en el contexto de la discusión y las ideas que trataban de transmitir, sin intentar valorar su potencial para provocar consecuencias lesivas en atención al ambiente social y político, y su alcance, por lo que fallaron en considerar todos los hechos y factores relevantes (apartado 82); así, afirma en el apartado 84 que a pesar de que la redacción de las declaraciones impugnadas era, de hecho, ofensiva, insultante y virulenta (por lo que el solicitante finalmente se disculpó), no puede considerarse que susciten emociones primarias o prejuicios arraigados en un intento de incitar al odio o la violencia contra los policías rusos; (..) fue más bien la reacción emocional del solicitante a lo que vio como un caso de conducta abusiva de las fuerzas de policía.

Finaliza el Tribunal afirmando que no se puede concluir que el comentario en cuestión tuviera capacidad para provocar violencia sobre la policía rusa generando de este modo «un peligro claro e inminente» que exigiese perseguir y condenar al recurrente (apartado 84), dando así carta de naturaleza a la aplicación del estándar norteamericano del peligro inminente al discurso del odio *online*. Habrá que esperar a ver si se consolida

esta doctrina[39] de la inminencia del peligro con la consiguiente dificultad de su aplicación a las redes sociales.

4. Conclusión

La aplicación de los criterios establecidos en el Protocolo a la penalización del discurso del odio en el ciberespacio resulta problemática en las redes sociales por las singularidades de este entorno.

Así, la valoración de la intencionalidad, que en el caso de la difusión de material debe abarcar su carácter racista o xenófobo y su efecto incitador, tiene que tener en cuenta los códigos propios de las redes sociales (espontaneidad, desinhibición, significado del retuiteo) considerando el conjunto de los mensajes.

La publicidad de la conducta excluye la relevancia penal de las comunicaciones privadas (salvo las amenazas) pero, si lo que determina la naturaleza privada o pública de un mensaje es la predeterminación selectiva del destinatario o la indeterminación del mismo, esta distinción se dificulta cuando los destinatarios integran un grupo numeroso y el acceso al grupo es relativamente abierto. Asimismo, se discute si basta la publicidad potencial de los contenidos o se requiere, en entornos semiprivados con numerosos participantes, una publicidad efectiva.

Por otra parte, el emisor solo responderá penalmente si buscó intencionadamente la difusión pública y al valorar esta intencionalidad de la publicidad deben ponderarse elementos como la plena conciencia de la potencial repercusión pública de sus mensajes allende su círculo de contactos o seguidores, y que no respondan a la construcción de un perfil digital sino a la voluntad de provocar la acción de la audiencia.

La remisión del Protocolo a los documentos internacionales para definir el material racista y xenófobo conduce a la noción de incitación presente en el artículo 20.2 PIDCP. La interpretación más extendida de la incitación incorpora un resultado de «riesgo inminente» asumiendo el estándar norteamericano del caso Brandenburg. Siendo este estándar difícilmente aplicable a las redes sociales, por requerir inmediatez temporal entre las declaraciones y el peligro sin tener en cuenta la permanencia y la itinerancia de los mensajes, resulta más apropiada la doctrina de las «amenazas verdaderas», que solo requiere intención intimidatoria.

Reciente jurisprudencia del TEDH, aun sin citar el Protocolo, ha proyectado estos criterios a comentarios ofensivos en un blog, valorando la intencionalidad del autor, su impacto –potencialmente alto al hacerse en internet, pero muy limitado en el caso concreto– y, lo más relevante, aplicando por primera vez el estándar del «peligro claro e inminente» al discurso del odio *online*.

39. En este sentido, Fathaigh y Voorhoof (2019) critican que en la reciente sentencia *Gürbüz and Bayar* (23 de julio de 2019) el TEDH no ha tomado en consideración el «peligro inminente de violencia» como parte del test de incitación a la violencia que sí aplicó en el caso *Savva Terentyev* que comentamos.

Referencias bibliográficas[40]

ARTICLE 19 (2009). *Los Principios de Camden sobre la Libertad de expresión y la Igualdad* [en línea] https://www.article19.org/data/files/pdfs/standards/los-principios-de-camden-sobre-la-libertad-de-expresion-y-la-igualdad.pdf [Fecha de consulta: 11 de junio de 2020].

AKDENIZ, Y. (2008). *An Advocacy Handbook for the Non Governmental Organisations The Council of Europe's Cyber-Crime Convention 2001 and the additional protocol on the criminalisation of acts of a racist or xenophobic nature committed through computer systems* [en línea] https://www.cyber-rights.org/cybercrime/coe_handbook_crcl.pdf [Fecha de consulta: 11 de junio de 2020].

BOIX PALOP, A. (2016). «La construcción de los límites a la libertad de expresión en las redes sociales». *Revista de Estudios Políticos,* núm. 173, págs. 55-112 [en línea] https://doi.org/10.18042/cepc/rep.173.02 [Fecha de consulta: 11 de junio de 2020].

COMISIÓN EUROPEA CONTRA EL RACISMO Y LA INTOLERANCIA (2016). *Recomendación núm. 15 de política general de la ECRI relativa a la lucha contra el discurso del odio y Memorándum explicativo* (8 de diciembre de 2015), CRI (2016) 15 [en línea] https://rm.coe.int/ecri-general-policy-recommendation-n-15-on-combating-hate-speech-adopt/16808b7904 [Fecha de consulta: 11 de junio de 2020].

COUNCIL OF EUROPE (2003). *Explanatory Report to the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*. Estrasburgo, 28-1-2003 [en línea] https://rm.coe.int/16800d37ae [Fecha de consulta: 11 de junio de 2020].

DÍEZ BUESO, L. (2018). La libertad de expresión en las redes sociales. En: GONZÁLEZ JIMÉNEZ, A. (coord.). *Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes. IDP. Revista de Internet, Derecho y Política*, núm. 27 [en línea] http://dx.doi.org/10.7238/idp.v0i27.3146 [Fecha de consulta: 11 de junio de 2020].

FALXA, J. (2015). «Redes sociales y discursos de odio: Un enfoque europeo». En: *Moderno discurso penal y nuevas tecnologías: Memorias [del] III Congreso Internacional de Jóvenes Investigadores en Ciencias Penales* [en línea] https://www.academia.edu/8703187/Redes_sociales_y_discursos_de_odio._Un_enfoque_europeo [Fecha de consulta: 11 de junio de 2020].

FATHAIGH, R.; VOORHOOF, D. (2019). «ECtHR engages in dangerous "triple pirouette" to find criminal prosecution for media coverage of PKK statements did not violate Article 10». En: *Strasbourg Observers* [blog] [en línea] https://biblio.ugent.be/publication/8638098 [Fecha de consulta: 11 de junio de 2020].

GAGLIARDONE, I.; GAL, D.; ALVES, T.; MARTÍNEZ, G. (2015). *Countering online hate speech.* UNESCO [en línea] http://egalitecontreracisme.fr/sites/default/files/atoms/files/countering_online_hate_speech_3.pdf [Fecha de consulta: 11 de junio de 2020].

40.En todas las referencias a bibliografía en inglés debe entenderse que la cita es al original siendo la traducción del autor.

GARCÍA GONZÁLEZ, J. (2015). «Oportunidad criminal, internet y redes sociales: Especial referencia a los menores de edad como usuarios más vulnerables» [en línea]. *Indret: Revista para el Análisis del Derecho,* núm. 4 [en línea] https://indret.com/oportunidad-criminal-internet-y-redes-sociales/ [Fecha de consulta: 11 de junio de 2020].

JUBANY, O.; ROIHA, M. (2015). *Backgrounds, Experiences and Responses to Online Hate Speech: A Comparative Cross-Country Analysis*. PRISM [en línea] https://doi.org/10.2991/sschd-16.2016.143 [Fecha de consulta: 11 de junio de 2020].

MCGONAGLE, T. (2012). «A survey and critical analysis of Council of Europe strategies for countering "hate speech"». En: HERZ, M.; MOLNAR, P. (eds.). *The content and context of hate speech: rethinking regulation and responses.* Cambridge: Cambridge University Press, págs. 456-498.

MIRÓ-LLINARES, F.; GÓMEZ-BELLVÍS, A. B. (2020). «Freedom of expression in social media and criminalization of hate speech in Spain: Evolution, impact and empirical analysis of normative compliance and selfcensorship». *Spanish Journal of Legislative Studies,* núm. 1, págs. 1-42 [en línea] https://doi.org/10.21134/sjls.v0i1.1837 [Fecha de consulta: 11 de junio de 2020].

REED, C. (2009). «The challenge of hate speech online». *Information & Communications Technology Law Routledge*, 18 (2), págs. 79-82 [en línea] https://doi.org/10.1080/13600830902812202 [Fecha de consulta: 11 de junio de 2020].

RING, C. E. (2015). «Hate speech in social media: an exploration of the problem and its proposed solutions», *Journalism & Mass Communication Graduate Theses & Dissertations,* núm. 15 [en línea] file:///C:/Users/Usuario/Downloads/hateSpeechInSocialMediaAnExplorationOfTheProblemAndIt.pdf [Fecha de consulta: 11 de junio de 2020].

RODRÍGUEZ-IZQUIERDO SERRANO, M. (2017). «Hate speech y sociedad de la información: La difusión del odio en Internet y las redes sociales». En: ALONSO, L.; VÁZQUEZ, V. J.; CORTINA, A. *Sobre la libertad de expresión y el discurso del odio: Textos críticos.* Sevilla: Athenaica, págs. 129-143.

ROLLNERT LIERN, G. (2014). «Incitación al terrorismo y libertad de expresión: el marco internacional de una relación problemática». *Revista de Derecho Político*, núm. 91, págs. 231-262 [en línea] https://doi.org/10.5944/rdp.91.2014.13675 [Fecha de consulta: 11 de junio de 2020].

ROLLNERT LIERN, G. (2019). «El discurso del odio: una lectura crítica de la regulación internacional». *Revista Española de Derecho Constitucional,* núm. 115, págs. 81-109 [en línea] https://doi.org/10.18042/cepc/redc.115.03 [Fecha de consulta: 11 de junio de 2020].

TAMARIT SUMALLA, J. M. (2018). «Los delitos de odio en las redes sociales». En: GONZÁLEZ JIMÉNEZ, A. (coord.). *Implicaciones jurídicas de los usos y comentarios efectuados a través de las redes. IDP. Revista de Internet, Derecho y Política,* núm. 27 [en línea] https://doi.org/10.7238/idp.v0i27.3151 [Fecha de consulta: 11 de junio de 2020].

TERUEL LOZANO, G. M. (2015). *La lucha del derecho contra el negacionismo: una peligrosa frontera. Estudio constitucional de los límites penales a la libertad de expresión en un ordenamiento abierto y personalista*. Madrid: Centro de Estudios Políticos y Constitucionales.

TERUEL LOZANO, G. M. (2018). «Internet, incitación al terrorismo y libertad de expresión en el marco europeo». *Indret. Revista para el Análisis del Derecho,* núm. 3 [en línea] https://indret.com/internet-incitacion-al-terrorismo-y-libertad-de-expresion-en-el-marco-europeo/ [Fecha de consulta: 11 de junio de 2020].

TITLEY, G.; KEEN, E.; FÖLDI, L. (2014). *Starting points for combating hate speech online. Three studies about online hate speech and ways to address it*. Council of Europe [en línea] https://rm.coe.int/starting-points-for-combating-hate-speech-online/16809c85ea [Fecha de consulta: 11 de junio de 2020].

TSESIS, A. (2017). «Terrorist speech on social media». *Vanderbilt Law Review,* núm. 70 (2), págs. 651-708 [en línea] https://ssrn.com/abstract=2782050 [Fecha de consulta: 11 de junio de 2020].

Cita recomendada

ROLLNERT LIERN, Göran (2020). «Redes sociales y discurso del odio: perspectiva internacional», *IDP. Internet, Derecho y Política,* N.º 31, págs. 1-14. UOC [Fecha de consulta: dd/mm/aa]. http://dx.doi.org/10.7238/idp.v0i31.3233

Sobre el autor

Göran Rollnert Liern
goran.rollnert@gmail.com
Universidad de Valencia

Doctor en Derecho y licenciado en Ciencias Políticas, profesor titular de Derecho Constitucional en la Universidad de Valencia. Miembro de la Red DerechoTICS (www.derechotics.com), ha participado en varios proyectos de investigación sobre libertades informativas, gobierno abierto y redes sociales. Autor de tres monografías, 29 capítulos de libro, 24 artículos en revistas académicas y director de un libro colectivo. Sus líneas de investigación principales son la jefatura del Estado en la monarquía parlamentaria y las libertades ideológicas y de expresión en relación con la incitación al terrorismo y el discurso del odio.

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

www.uoc.edu/idp

ARTÍCULO

La modernización y transformación digital de la Administración de Justicia: el papel del Consejo General del Poder Judicial

Juan Ignacio Cerdá Meseguer
Universidad de Murcia

Fecha de presentación: marzo de 2020
Fecha de aceptación: julio de 2020
Fecha de publicación: octubre de 2020

Resumen

Hace aproximadamente una década se inició una ambiciosa reforma en la Administración de Justicia que afectaba a todos los ámbitos de la misma: estructural, funcional, personal y tecnológico. A tal fin, se acometió la promulgación de las normas reguladoras de la Nueva Oficina Judicial (NOJ); se aprobaron las necesarias reformas legales para adaptar las distintas funciones y competencias del personal al servicio de la Administración de Justicia; se promulgó la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia (LUTICAJ); y, finalmente, se han impulsado importantes reformas en normas procesales con el fin de adaptarlas a un nuevo paradigma: la Justicia electrónica o e-Justicia, que se pretende más moderna, eficiente, eficaz y capaz de dar respuestas a los requerimientos que la sociedad demanda de este servicio público en el siglo XXI. Sin embargo, el resultado no ha sido, en muchos aspectos, el que se esperaba de tan relevante reforma. En este trabajo nos proponemos analizar las acciones del CGPJ, los indudables logros alcanzados, pero también los problemas pendientes de resolver y que impiden, en definitiva, la culminación de este proceso de modernización.

Palabras clave

e-Justicia, Administración de Justicia, modernización, transformación digital

Tema

Derecho Administrativo, Administración electrónica, Justicia electrónica

The modernisation and digital transformation of the administration of justice: the role of the General Council of the Judiciary

Abstract

About a decade ago an ambitious reform in the administration of justice began that affected all its areas: structural, functional, personal and technological. To this end, the promulgation of the regulatory norms of the New Judicial Office (NJO) was undertaken; the necessary legal reforms were approved to adapt the different functions and competences of the personnel to the service of the administration of justice; Law 18/2011, of July 5, regulating the use of information and communication technologies in the administration of justice was promulgated; and, finally, important reforms in procedural norms have been promoted in order to adapt them to a new paradigm: electronic Justice or e-Justice, which aims to be more modern, efficient, effective and capable of responding to the requirements that society demands for this public service in the 21st century. However, the result has not been, in many respects, what was expected of such a relevant reform. In this work we will analyse the actions of CGPJ (General Council of the Judiciary), the undoubted achievements, but also the problems that are pending to be resolved and that ultimately prevent the culmination of this modernisation process.

Keywords

e-Justice, Administration of justice, modernisation, digital transformation.

Topic

Administrative law, electronic Administration, electronic justice.

1. Introducción

Administrar justicia es una de las más complejas funciones que actualmente desarrolla el Estado concebido como poder público, sobre todo desde un punto de vista técnico. La Administración de Justicia se presenta como la garante, en última instancia, de los derechos y libertades. Para cumplir con este cometido la Justicia debe ser capaz de dar respuesta a las demandas y necesidades de la sociedad con agilidad y eficiencia. En última instancia, su correcto funcionamiento es esencial en un Estado de derecho.

Históricamente la Administración de Justicia en España estaba residenciada en un modelo con una estructura arcaica, tecnológicamente muy limitada y lastrada por un endémico problema de este servicio público: la falta de jueces y magistrados, lo que se concretaba en la incapacidad de dar respuesta a la alta litigiosidad en tiempos razonables. Consecuentemente, la percepción social de este servicio público era en general negativa, reflejo de una Administración obsoleta que era, además, la peor valorada[1], percepción que no se ha conseguido revertir. La Administración de Justicia sigue siendo demasiado lenta, adolece de agilidad para ofrecer respuestas eficaces, sigue siendo oscura, poco comprensible para los profanos en la

1. Un análisis de la imagen de la Justicia entre los años 1985 a 2015 puede verse en CERDÁ MESEGUER, J. I. (2018). *El uso de medios electrónicos en la Administración de Justicia. Del expediente en papel al expediente electrónico.* Valencia: Tirant Lo Blanch, págs. 87-97.

materia y alejada, en muchas ocasiones, de la realidad que vive la sociedad a quien tiene la obligación de servir[2]. En este contexto, otro factor que resulta determinante cuando se trata de analizar la evolución y el estado actual de la Administración de Justicia es el retraso con el que se ha acometido su modernización e incorporación a la sociedad de la información, en particular para adaptar y utilizar las tecnologías de la información y la comunicación en el desarrollo de su actividad[3]. Este retraso se debe, además, a la fragmentación competencial que, unida a la falta de una efectiva coordinación entre las distintas Administraciones con competencias en la materia y el propio Consejo General del Poder Judicial (CGPJ), supone que la modernización estructural, funcional y tecnológica se produzca de manera desigual y termine por afectar al diseño y funcionamiento conjunto del sistema, en particular si tenemos en cuenta las exigencias de interoperabilidad que plantea la implantación de la tecnología.

De la misma forma, las inercias contrarias a una modernización radical por parte de muchos de los colectivos implicados –personal funcionario, jueces y magistrados, y profesionales– y del propio Ejecutivo –que puede ver en una Justicia ágil, moderna y dotada de medios un elemento de control de sus actuaciones[4]– suponen una limitación importante para que esos avances sean todo lo efectivos que se preveían. Por otra parte, no ha habido un auténtico impulso a la incorporación de las tecnologías de la información y la comunicación hasta hace pocos años, y es aún reciente la implantación de un sistema que pueda llegar a ser efectivo pero que, en nuestra opinión, se ha visto negativamente afectado por una deficiente previsión tanto por lo que se refiere a la formación como a los medios disponibles.

Así pues, la Administración de Justicia sigue pendiente de culminar la reforma iniciada para poder obtener los beneficios y ventajas que el uso de la tecnología puede reportar de inmediatez –por el ahorro en tiempo y la consiguiente agilización en la tramitación de expedientes– y de reducción de costes y necesidades de espacio, mejoras que se han podido apreciar desde hace años en otros ámbitos como el tributario o la Seguridad Social[5].

Se trata en definitiva de poner los medios para «prestar servicios públicos de mejor calidad, reducir los tiempos de espera, mejorar la eficacia en el uso de los fondos públicos, aumentar la productividad y mejorar la transparencia y la rendición de cuentas»[6]. Todo ello sin que se retroceda en el respeto a los derechos de los ciudadanos y ciudadanas, quienes no deben ver mermadas sus garantías jurídicas ante la mayor eficacia que se presume de la innovación tecnológica[7], uno de los pilares en los que se asienta el proceso de modernización.

2. La reforma de la Administración de Justicia diez años después

La reforma de la Oficina Judicial se inicia con un doble objetivo. Por una parte, su rediseño estructural, funcional, espacial y de personal y, por otra, la incorporación de la tecnología con el objetivo de optimizar la actividad del personal y los recursos. Una especial atención se ha prestado a la implantación del expediente judicial electrónico, con el que se pretendía reducir los tiempos de tramitación y la excesiva burocratización eliminando el uso del papel

2. En este sentido, CERDÁ MESEGUER, J. I. (2018), *op. cit.*, pág. 22; y BUENO DE MATA, F. (2014). *Prueba electrónica y Proceso 2.0.* Valencia: Tirant Lo Blanch, pág. 23. También JIMÉNEZ GÓMEZ, C. E. (2014). «Desafíos de la modernización de la Justicia en tiempos del Gobierno Abierto». Revista Digital de Derecho Administrativo, núm. 12, págs. 225-239.
3. Véase DELGADO GARCÍA, A. M.ª; OLIVER CUELLO, R. (2007). «Administración de Justicia y tec-nologías de la información y la comunicación: aspectos jurídicos». *Revista Aranzadi de Derecho y Nuevas Tecnologías,* núm. 13, pág. 1. También JIMÉNEZ GÓMEZ, C. E. (2014), *op. cit.,* pág. 226.
4. SUÁREZ-QUIÑONES Y FERNÁNDEZ, J. C. (2010). «Administración de Justicia y Nuevas Tecnologías: presente y futuro». *Diario La Ley*, núm. 7.421. Véase también ORTUÑO MUÑOZ, P. (2011). «Del arancel al expediente electrónico (Notas históricas sobre el modelo de oficina judicial español)». *Revista Jurídica Fundación Mariano Ruiz-Funes, núm.* 45, pág. 105.
5. GAMERO CASADO, E.; MARTÍNEZ GUTIÉRREZ, R. (2010). «El Derecho Administrativo ante la Era de la Información». En: GAMERO CASADO, E.; VALERO TORRIJOS, J. (coords.). *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.* Navarra: Aranzadi-Thomson-Reuters, págs. 64 a 68.
6. DELGADO GARCÍA, A. M.ª; OLIVER CUELLO, R. (2006). *Las tecnologías de la información y la comunicación en la Administración de Justicia.* Oñati (Bilbao): Instituto Vasco de Administración Pública, pág. 10.
7. VALERO TORRIJOS, J. (2013). *Derecho, Innovación y Administración Electrónica.* Sevilla: Derecho Global, pág. 18.

en todos sus trámites, en búsqueda de una mayor agilidad y eficacia que, en definitiva, supondría también una reducción de costes[8].

2.1. El punto de partida

Ha sido fundamentalmente en los últimos diez años cuando ha tenido lugar la aprobación de diversas normas jurídicas con las que se ha pretendido modificar el funcionamiento de la Administración de Justicia[9].

En el plano estructural, las modificaciones legales operadas en los artículos 435 y sigs. de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial (LOPJ) han tratado de incorporar un nuevo modelo de oficina judicial (NOJ). Hasta entonces, su estructura se basaba en un «modelo diseñado en el siglo XIX para una sociedad eminentemente rural y con un muy diferente sistema de comunicaciones»[10], en el que cada juzgado y tribunal funcionaba de forma independiente, diseño que resultaba poco operativo y que algún sector de la doctrina ha calificado como «islas»[11]. La NOJ pasará a estar integrada por dos unidades: los Servicios Comunes Procesales (SCP) y las Unidades Procesales de Apoyo Directo (UPAD)[12]. Esta nueva estructura está diseñada para una Administración de Justicia totalmente informatizada en la que el expediente judicial electrónico es el elemento fundamental de trabajo. En este contexto incipiente se producen las primeras implantaciones a modo de prueba y como experiencia piloto del modelo de NOJ en el año 2010, únicamente en algunas comunidades autónomas, en determinadas ciudades, y solo inicialmente en la jurisdicción social y civil[13].

En el plano tecnológico se diseña la plataforma LexNET, se promulga la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia (LUTICAJ), que regula la incorporación de las TIC a la Administración de Justicia, y se procede a la progresiva implantación de los tres elementos clave: la NOJ, LexNET, regulado hoy por el Real Decreto 1065/2015, y el expediente judicial electrónico, cuya regulación básica se encuentra en la mencionada LUTICAJ. Asimismo, se acometen diversas reformas en leyes procesales para adaptar los procesos al nuevo expediente judicial electrónico. Básicamente, su regulación más detallada se encuentra en la Ley de Enjuiciamiento Civil como normativa procesal de referencia. En particular es necesario destacar la reforma operada por la Ley 42/2015, de 5 de octubre, en la que se estableció la obligación de utilizar medios electrónicos –y en concreto el sistema LexNET– en un intento de que la Administración de Justicia abandonara el soporte papel tanto en la gestión documental como en las presentaciones de escritos, notificaciones y comunicaciones. Sin embargo, dicha implantación fue a nuestro juicio precipitada, pues ni la Administración de Justicia estaba preparada tecnológicamente ni se apostó decididamente por la formación del personal y de los diversos colectivos profesionales implicados. Además, las carencias en cuanto a falta de interoperabilidad entre los distintos sistemas de gestión procesal, el retraso en la dotación a jueces y magistrados de la firma electrónica, la falta de cumplimiento de los requerimientos establecidos en el Esquema Nacional de Seguridad y, en definitiva, la ausencia de actuaciones coordinadas entre Administraciones han complicado la plena implantación del expediente judicial electrónico.

8. En este sentido, DELGADO GARCÍA, A. M.ª; OLIVER CUELLO, R. (2006), *op. cit.*, pág. 94.
9. Al respecto, PÉREZ-LUÑO ROBLEDO, E. C. (2019). «La informatización de la Administración de Justicia en España». En: CONDE FUENTES, J.; SERRANO HOYO, G. (dir.). *La Justicia Digital en España y la Unión Europea: situación actual y perspectivas de futuro*. Barcelona: Atelier, págs. 51 y 52.
10. 1PARRA GARCÍA, J. I. (2019). «La Oficina Judicial en España: un balance de diez años». Actividad formativa del curso «Estatuto orgánico LAJ» (8.ª ed.). Madrid: Centro de Estudios Jurídicos, 25 y 26 de noviembre de 2019.
11. ARNAIZ SERRANO, A.; TOMÁS PORTER, J. J. (2010). «La nueva oficina judicial y el nuevo modelo procesal: un estudio sobre la organización y funciones en la oficina judicial y los procesos judiciales tras la reforma de la legislación procesal operada por la Ley 13/2009». *Revista jurídica de la Comunidad Valenciana: jurisprudencia seleccionada de la Comunidad Valenciana,* núm. 33, págs. 69-93. También JIMÉNEZ ASENSIO, R. (2010). «El encaje constitucional de la NOJ». Ponencia presentada en el curso «La Nueva Oficina Judicial». Madrid: CENDOJ. Así como CERRILLO MARTÍNEZ, A. (2010). «Cooperación entre Administraciones públicas para el impulso de la administración electrónica». En: GAMERO CASADO, E.; VALERO TORRIJOS, J. *La Ley de Administración Electrónica. Comentarios a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*. Navarra: Aranzadi-Thomson Reuters (Cizur Menor), pág. 780.
12. Sobre la nueva estructura de la NOJ, véase CLÈRIES I NERÍN, N. (2007). «Administración electrónica en el Área de Justicia». *IDP. Revista de Internet, Derecho y Política*, núm. 4, págs. 14 y 15. Monográfico e-Justicia [en línea] https://idp.uoc.edu/42/volume/0/issue/4/ [Fecha de consulta: 3 de septiembre].
13. Inicialmente se implanta en Zaragoza, Avilés, Palma de Mallorca, Santander, Ciudad Real, Burgos, Cáceres, Murcia, Logroño, Ceuta y Melilla.

En el plano funcional, la transición de un modelo a otro se ha apoyado fundamentalmente en la figura del Letrado de la Administración de Justicia (LAJ), quien ha asumido no solo las tradicionales funciones de gestión, personal y fe pública judicial, sino que a estas se han sumado –no sin ciertas desavenencias y resistencias doctrinales[14]–, funciones decisorias en determinadas fases del procedimiento e incluso la asunción total de la facultad de decidir en determinados tipos de procedimiento[15]. En puridad lo que se ha pretendido con la reforma es descargar al titular del órgano judicial de cualquier otra tarea que no sea la de juzgar y hacer ejecutar lo juzgado, reservando al LAJ y demás personal funcionario el resto de funciones[16].

También en el ámbito espacial se preveían importantes cambios en el diseño de las nuevas oficinas judiciales. Frente al tradicional juzgado se pretende la implantación de grandes espacios comunes cuyo personal se adscribe a servicios comunes procesales especializados (de ordenación del procedimiento, de ejecución, de notificaciones y embargos, etc.), al frente de los cuales hay varios LAJ. Por otra parte, las UPAD están servidas por un reducido número de funcionarios que realizan las labores de asistencia al titular del órgano judicial, y que despachan los procedimientos que llegan desde los SCP para un determinado trámite que requiere decisión judicial, al frente de las cuales también se encuentra un LAJ que puede servir a uno o más órganos judiciales.

Así pues, este diseño institucional habría requerido una efectiva interconexión de los sistemas de información pues, como puede comprobarse, supone pasar de un modelo de gestión basado en cada órgano judicial a otro sustentado en la gestión común de espacios, herramientas y aplicaciones informáticas, lo cual supone en, definitiva, además de un cambio organizativo, un cambio cultural[17], es decir, la aceptación plena por parte de todos los sectores implicados de que los avances, si bien lentos y costosos, se van a reflejar en mejoras en el servicio que presta la Justicia, en su gestión y en su eficiencia y eficacia. Sin embargo, las inercias contrarias existentes tanto a nivel político como a nivel de operadores jurídicos –tanto externos como internos– indican que falta por consolidarse ese cambio cultural y de mentalidad necesario para que se aborden las multiples tareas que aún quedan pendientes de realizar, como analizamos seguidamente.

2.2. El estado actual de la Administración de Justicia

De haberse seguido las previsiones normativas en cuanto a plazos y acciones programadas, en la actualidad la NOJ y el expediente judicial electrónico debieran estar plenamente implantados y funcionando con normalidad. No obstante, como hemos venido exponiendo, tales previsiones no solo no se han cumplido, sino que la dotación, situación e imagen de la Administración de Justicia sigue, prácticamente, en los mismos parámetros que al inicio de la reforma.

Estas acciones normativas referidas deben ir acompañadas de otras sinérgicas y proactivas de carácter económico y tecnológico. En este sentido, la insuficiente inversión presupuestaria, la fragmentación competencial unida a la ausencia de una efectiva coordinación, la falta de interoperabilidad entre los distintos sistemas de gestión procesal –también inicialmente con el sistema Fortuny de la Fiscalía General del Estado[18]–, han lastrado el proceso de modernización. Así, a nivel estructural, en la actualidad las

14. Acerca de esta disputa doctrinal véase SEOANE CHACARRÓN, J. (2011). «El Secretario Judicial ante la Ley 13/2009, de 3 de noviembre, de Reforma de la Legislación Procesal (civil y penal) para la implantación de la Nueva Oficina Judicial». *Diario La Ley,* núm. 7.561, pág. 1. También PARRA GARCÍA, J. L. (2010). «El año uno en la Oficina Judicial: nueva organización, nuevas formas de hacer Justicia». *Derecho y Jueces, EL DERECHO*, núm. 55, pág. 3. En sentido contrario, BANACLOCHE PALAO, J. (2009). «El proyecto de Nueva Oficina Judicial: ¿hacia un nuevo proceso administrativizado?». *Diario La Ley*, núm. 14.035. También en BANACLOCHE PALAO, J. (coord.) (2010). *Guía Práctica de la Nueva Oficina Judicial*. Madrid: Editorial LA LEY.
15. Ejemplos de lo afirmado son el Decreto de admisión a tramite de las demandas; que en los procesos de juras de cuentas el LAJ decide en todo momento; o que en las ejecuciones las primeras medidas contra el ejecutado las adopta el LAJ.
16. En este sentido, PARRA GARCÍA, J. L.; PASQUAL DEL RIQUELME HERRERO, M. (2009). «Oficina Judicial integrada o hacia una Justicia inteligente en España». *Boletín del Ministerio de Justicia,* año 63, núm. 2094, págs. 2.333-2.345; págs. 8-9 del trabajo.
17. Como ha señalado CLÈRIES I NERÍN, N. (2007). «Administración electrónica en el Área de Justicia», *op. cit*., pág. 13.
18. Para un análisis al respecto CERDÁ MESEGUER, J. I. (2018), *op. cit*., caps. I, II, III y VI.

sedes de la NOJ con plena implantación están en las ciudades de Murcia, Cuenca, Ciudad Real, Cáceres, Badajoz, León, Burgos, Ceuta y Melilla[19], sin que se haya implantado en el resto del Estado. En cuanto a la Oficina Fiscal solo se está implantando en el territorio donde ejerce sus competencias el Ministerio de Justicia y, dentro de este, está plenamente implantada en Murcia, Ceuta, Melilla, Cuenca y Cáceres[20]. Tan escaso índice de cumplimiento de las previsiones legales iniciales es indicativo de que, además de las causas indicadas, hay una importante falta de asunción y empatía con el nuevo modelo por parte de todos los sectores implicados.

En el plano tecnológico no pueden negarse evidentes avances, además de que hemos de poner en valor las decididas acciones del CGPJ para avanzar en la dotación de herramientas a los juzgados y tribunales que faciliten y economicen múltiples gestiones de las que han de realizarse en la tramitación de los procedimienrttos judiciales, contribuyendo a la agilización, eficacia y ahorro de tiempo en la resolución de los expedientes. En este sentido ha sido determinante el Punto Neutro Judicial y la aplicación Inter-Ius[21]. Sin embargo, la falta de interoperabilidad entre los distintos sistemas de gestión procesal es el principal obstáculo para una Justicia plenamente electrónica al no haber cumplido el CGPJ el mandato contenido en el artículo 230 de la LOPJ de exigir su efectiva compatibilidad, tal y como establecía el apartado 5 del artículo en su anterior redacción, competencia que en la redacción actual el apartado 6 atribuye al Comité Técnico Estatal de la Administración de Justicia Electrónica (CTEAJE).

En este contexto no es posible trabajar con el expediente judicial electrónico y que este despliegue todas las funcionalidades y ventajas que de su implantación y utilización se pueden obtener y que se definen y regulan en la LUTICAJ. También en el plano tecnológico resulta determinante la incompatibilidad de varios de los sistemas de gestión procesal de algunas comunidades autónomas con la plataforma LexNET[22]. Más allá de que revertir esta situación resulta especialmente costoso tanto económica como técnicamente –hacer los sistemas compatibles requiere un volcado de documentación que precisa de fuertes inversiones de dinero y tiempo, además de superar otras complicaciones tecnológicas–, situación que podría haberse evitado si, desde el primer momento, el CGPJ hubiera autorizado solo sistemas compatibles que cumplieran los requerimientos técnicos determinados por el propio CGPJ. Dicha previsión por parte del órgano de gobierno de los jueces cobraba si cabe más sentido precisamente por la fragmentación competencial a que hemos aludido, pues podían presumirse las dificultades que se presentarían en el futuro para hacer compatibles los distintos SGP creados por las Aministraciones autonómicas con competencias en la materia, como efectivamente está sucediendo.

Finalmente, el diseño de mejoras en las herramientas que hagan más útil y facilite el uso para la gestión de los expedientes resulta fundamental cuando se trata de abandonar un modelo de trabajo para empezar a utilizar otro. El usuario o usuaria debe encontrar ventajas en el nuevo modelo para que no desarrolle resistencias e inercias contrarias a su uso. De la misma forma es preciso efectuar las inversiones necesarias para que las salas de vistas estén dotadas

19. Información obtenida de la página web del Ministerio de Justicia: https://www.mjusticia.gob.es/cs/Satellite/Portal/es/justicia-espana/proyectos-transformacion/oficina-judicial/mapa-sedes-oficina-judicial [Fecha de consulta: 3 de septiembre de 2020].
20. *Ibid.*: https://www.mjusticia.gob.es/cs/Satellite/Portal/es/justicia-espana/proyectos-transformacion/oficina-fiscal#id_1288784209469 [Fecha de consulta: 3 de septiembre de 2020].
21. Una detallada descripción de las utilidades del Punto Neutro Judicial y de la aplicación Inter-Ius puede consultarse en DELGADO GARCÍA, A. Mª; OLIVER CUELLO, R. (2007). «Iniciativas recientes de la e-Justicia en España». *IDP. Revista de Internet, Derecho y Política*, núm. 4, págs. 24 y 25. Monográfico e-Justicia [en línea] https://idp.uoc.edu/42/volume/0/issue/4/ [Fecha de consulta: 3 de septiembre de 2020].
22. La fragmentación competencial vuelve a presentarse como un hecho diferencial del grado de implantación, siendo distinto en función de la comunidad autónoma de que se trate. En Navarra, País Vasco y Cantabria tanto la presentación de escritos como la recepción de notificaciones se hace a través de sus SGP (Navarra-Avatius; País Vasco-Justizia.Sip; y Cantabria-Vereda). En Cataluña, la presentación se hace con su sistema de gestión procesal (Justicia.Cat), pero las notificaciones sí se reciben por LexNET. En Aragón, excepto en Zaragoza, se utiliza Avantius para la recepción de notificaciones y la presentación de escritos está temporalmente fuera de servicio. Con respecto a la Fiscalía General del Estado, su SGP Fortuny ya es compatible con LexNET en la actualidad. Para un detallado estudio sobre la cuestión, CERNADA BADÍA, R. (2019). «LexNET o la selección natural en el foro del siglo XXI». En: GÓMEZ MANRESA, M. F.; FERNÁNDEZ SALMERÓN, M. (coords.). *Modernización digital e innovación en la Admnistración de Justicia.* Navarra: Aranzadi-Thomson Reuters (Cizur Menor), págs. 401 a 429.

de los equipos informáticos necesarios para poder realizar y seguir un juicio de modo totalmente electrónico.

Según se ha advertido con acierto, la situación actual deriva de una «falta de continuidad en las políticas integradas de gestión del cambio»[23]. Los objetivos establecidos en las normas reguladoras que no se han cumplido son relevantes, tal y como sucede con el relativo al «papel cero», de imposible cumplimiento en estos momentos[24]; o la definitiva incorporación de los medios tecnológicos necesarios y adecuados para hacer de la Justicia un servicio público más cercano a la ciudadanía y más transparente[25], permitiendo el acceso a los expedientes judiciales. De la misma forma el problema de la insuficiente dotación de órganos judiciales sigue sin resolverse[26], así como la falta de eficacia y la dilación en la resolución de los procedimientos, que sigue siendo apreciado como otro grave y endémico problema[27].

Ante esta situación el CGPJ ha aprobado la Instrucción 1/2018, relativa a la obligatoriedad para jueces y magistrados del empleo de medios informáticos a que se refiere el artículo 230 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, en la que establecen las condiciones y requerimientos técnicos que deben cumplir los medios tecnológicos al servicio de la Administración de Justicia para que su uso se pueda imponer como obligatorio a los jueces y magistrados, que analizamos seguidamente. La pregunta a plantear resulta elemental: la citada Instrucción, ¿ha servido para impulsar este proceso?

3. La Instrucción 1/2018, del CGPJ: ¿un freno o un avance para la definitiva modernización tecnológica de la Administración de Justicia?

A partir del 1 de enero de 2016, en aplicación de lo dispuesto en el artículo 230 de la LOPJ, la LEC obliga a todos los profesionales de la Justicia y órganos judiciales y fiscalías a la utilización de los sistemas telemáticos existentes en la Administración de Justicia para la presentación de escritos y documentos y la realización de actos de comunicación procesal, debiendo la Administración competente, las demás Administraciones, profesionales y organismos que agrupan a los colectivos establecer los medios necesarios para que ello sea una realidad. La obligatoriedad y exclusividad del uso de medios electrónicos y la prohibición de transcripción y empleo del papel en la tramitación de los procedimientos[28] que impone el mencionado artículo 230 de la LOPJ y el 147 de la LEC conlleva la necesaria puesta a disposición de los jueces y magistrados de los

23. PARRA GARCÍA, J .L. (2019), *op. cit.*, pág. 20. El autor identifica una serie de dificultades que han lastrado el proceso de modernización.
24. Véase CERDÁ MESEGUER. J. I. (2016). «El objetivo "papel cero" en la Administración de Justicia española: ¿una realidad procesalmente imposible?». En: BUENO DE MATA, F. (dir.). *Hacia una Justicia 2.0.* Salamanca: Actas del XX Congreso Iberoamericano de Derecho e Informática, vol. II, págs. 35-48.
25. CERRILLO I MARTÍNEZ, A. (2012). «La dotación suficiente de medios e instrumentos electrónicos y el marco general de la cooperación interadministrativa en materia de Administración de Justicia». En: GAMERO CASADO, E.; VALERO TORRIJOS, J. (coords). *Las Tecnologías de la Información y la Comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio.* Navarra: Aranzadi-Thomson Reuters. También CERRILLO I MARTÍNEZ, A. (2007). «E-justicia: las tecnologías de la información y el conocimiento al servicio de la Justicia Iberoamericana en el siglo XXI». *IDP. Revista de Internet, Derecho y Política*, núm. 4, pág. 5. Monográfico e-Justicia [en línea] https://idp.uoc.edu/42/volume/0/issue/4/ [Fecha de consulta: 3 de septiembre de 2020]. En este sentido véase también DELGADO GARCÍA, A. M.ª; OLIVER CUELLO, R. (2006), *op. cit.*, pág. 10.
26. Según el Cuadro de Indicadores de la Justicia en la UE de 2019, de la Comisión Europea, COM 2019, la media de jueces en España por cada cien mil habitantes es de doce, mientras que la media europea se sitúa en veintidós. El Eurobarómetro de la Justicia de la UE indica la mala imagen de la Justicia para los ciudadanos, de los cuales un 55% no confía en la independencia judicial.
27. En este sentido, Mora-Sanguinetti, J. S.; MartÍnez-Matute, M. (2020). «Los impactos económicos del funcionamiento de la Justicia en la Región de Murcia». Murcia: Consejo Económico y Social de la Región de Murcia, febrero 2020. Se afirma que la lentitud en la resolución de las causas judiciales puede ser causa de la paralización de proyectos de inversión, o de una menor tasa de emprendimiento de nuevos negocios. Según sostiene el informe, un leve incremento del colapso judicial podría elevar los niveles de paro en la Región de Murcia al 20% en un solo año [en línea] https://www.cesmurcia.es/cesmurcia/paginas/publicaciones/UltimasPublicaciones.seam?pubId=2241 [Fecha de consulta: 3 de septiembre de 2020].
28. Salvo algunas excepciones como se advierte en CERDÁ MESEGUER, J. I. (2019). «Hacia una Administración de Justicia plenamente electrónica: disfunciones normativas y jurisprudenciales». En: GÓMEZ MANRESA, M. F.; FERNÁNDEZ SALMERÓN, M. (coords.). *Modernización digital e innovación en la Administración de Justicia.* Navarra: Aranzadi-Thomson Reuters (Cizur Menor), págs. 369 a 397.

medios adecuados para poder desarrollar su trabajo con plenas garantías y sin que el mismo les suponga duplicar esfuerzos y trabajo. Ante tales obligaciones legales, la falta de la correlativa dotación de los medios tecnológicos necesarios y adecuados provocó una inercia contraria a asumir tales obligaciones por parte de los titulares de los órganos judiciales, quienes han constatado que la incabada transformación digital de la Administración de Justicia complica en muchas ocasiones su tarea y no ha contribuido a subsanar los problemas que intentaban afrontarse.

En este contexto se promulga la Instrucción 1/2018, cuya justificación queda expuesta en su Exposición de Motivos, donde se evidencia que el CGPJ, después de muchos y reiterados incumplimientos en la normativa general y específica en materia de implantación de las TIC en la Administración de Justicia, ha tomado la decisión de ejercer sus competencias de coordinación en la materia que le atribuyen tanto la LUTICAJ como la LOPJ[29].

La Instrucción trae causa en las modificaciones que el artículo 230.1 y 2 de la LOPJ ha sufrido, y en cuya redacción actual se establece la obligatoriedad del uso por los jueces y tribunales de los «medios técnicos, electrónicos, informáticos y telemáticos, puestos a su disposición para el desarrollo de su actividad y el ejercicio de sus funciones». Ante tal previsión legal y la consecuencia jurídica derivada de un posible incumplimiento por parte de los jueces y magistrados, que podría llevar aparejadas sanciones disciplinarias por desatención e incumplimientos de los deberes del cargo, el CGPJ acuerda establecer los requisitos que deben satisfacer los medios técnicos para que la obligatoriedad de su uso sea exigible. Los motivos que sustentan tal decisión, más allá de ser absolutamente razonables, impiden que se traslade a jueces y magistrados la carga de soportar las consecuencias que se derivan de las decisiones de las Administraciones competentes en materia de Administración de Justicia. En concreto, en el sentido de que, de no ejercer ese control previo, se correría el riesgo de que, bajo la apariencia del suministro de medios técnicos –un simple programa informático de gestión procesal–, se alteren las condiciones del puesto de trabajo del juez o magistrado.

Conforme a lo dispuesto en el artículo 1 de la Instrucción, los ejes de actuación del CGPJ se centran en tres cuestiones relacionadas entre sí. En primer lugar, las especificaciones y requerimientos técnicos que deben reunir los programas y SGP para trabajar en un entorno de expediente judicial electrónico, tanto integrado en el SGP o externo al mismo, como herramienta especializada para trabajar con él, a lo cual dedica la norma el artículo 2, en el que se establecen los requisitos técnicos para que la obligatoriedad de su uso sea exigible a jueces y magistrados. En relación directa con este eje está el artículo cuarto de la norma, que regula el procedimiento para la verificación de que los programas reúnen las condiciones que permiten al CGPJ imponer su obligatoriedad para jueces y magistrados.

El segundo eje de actuación es el referido a la formación en la utilización de los programas[30], artículo tercero de la norma, estableciéndose la obligatoriedad de que las Administraciones que implanten los programas de gestión procesal deberán facilitar a los jueces y magistrados la formación necesaria para el uso de los mismos. Dicha formación será validada por la Comisión Permanente del CGPJ antes de imponer a los jueces y tribunales la obligatoriedad de su uso, que ponderará si la misma es adecuada por tiempo, contenidos y calidad, previo informe del Servicio de Formación Continua y de la Sección de Informática Judicial. Se añade además que el uso de programas y SGP o de los instrumentos informáticos no será obligatorio mientras no se imparta la formación necesaria en los términos indicados. Asímismo, por primera vez se introduce por parte del CGPJ una nueva variable dirigida a las Administraciones con competencias en materia de Justicia consistente en el establecimiento de políticas de prevención de salud profesional con relación al uso de pantallas de visualización de datos conforme a la normativa del Plan de Prevención de Riesgos Laborales de la Carrera Judicial[31].

29. MARTÍNEZ GUTIÉRREZ, R. (2019). «Los retos de la innnovación tecnológica en la Jurisdicción Contencioso-Administrativa». Ponencia presentada en el XIV Congreso Nacional de Profesores de Derecho Administrativo, celebrado en Murcia, los días 8 y 9 de febrero de 2019, pág. 20. Véase también MARTÍNEZ GUTIÉRREZ, R. (2019). «La e-Justicia contencioso-administrativa después de la Instrucción 1/2018 del CGPJ». *Revista General de Derecho Administrativo,* núm. 51.
30. Parte de las quejas y demandas formuladas por los colectivos de operadores judiciales implicados (jueces, fiscales, jueces, fiscales, letrados de la Administración de Justicia y funcionarios) han sido por la escasa formación recibida para el uso de programas y herramientas que se les imponía como obligatorios, por ejemplo LexNET. Véase CERDÁ MESEGUER, J. I. (2018), *op. cit.*, págs. 270 a 277.
31. La Comisión Permanente del CGPJ aprobó el 27 de enero de 2015 el primer Plan de Prevención de Riesgos Laborales para la Carrera Judicial. Información obtenida de la web oficial del CGPJ.

El tercer eje se concreta en las consecuencias derivadas de la no superación del test de requisitos técnicos, de gestión y de formación mínimos para que el programa pueda imponerse como obligatorio. Para estos casos, la Instrucción prevé que se deberá garantizar el acceso a los expedientes en papel, así como su conservación en dicho formato en tanto subsista la situación descrita.

La Instrucción incorpora un anexo técnico en el que se regulan especificaciones técnicas para el expediente judicial electrónico, que impone a las Administraciones Públicas con competencias en la materia que cualquier desarrollo de sistemas o herramientas deberá cumplir con las especificaciones señaladas por el CTEAJE.

4. Conclusiones

Conforme a lo expuesto, la valoración que hemos de hacer de las acciones desarrolladas por el CGPJ y de la Instrucción 1/2018 del CGPJ debe ser positiva, sin que en ningún caso pueda ser esta considerada un freno para la culminación de la modernización tecnológica de la Justicia[32]. Aunque es la primera vez que el CGPJ está ejerciendo de forma decidida sus competencias en la materia a fin de aprobar que los SGP sean compatibles y superen las especificaciones técnicas mínimas, debe considerarse una iniciativa que ayuda a superar las dificultades sobre interoperabilidad, lo que conllevará que el uso de tecnologías comunes –LexNET, por ejemplo– pueda ser una realidad en todo el territorio nacional.

Por otra parte, asegura que jueces y magistrados de todo el país tengan acceso a una formación adecuada sobre los medios técnicos de que dispongan y deban utilizar obligatoriamente, lo cual puede suponer que se esté más cerca de conseguir el objetivo de la plena implantación del expediente judicial electrónico. Resulta también positiva porque resuelve, sin invadir competencias del resto de Administraciones implicadas, los problemas que podrían derivarse en el futuro respecto a cambios en los SGP o en los programas por parte de estas, pues tendrán que ser previamente aprobados por el propio CGPJ, lo que implica mayor garantía para jueces y magistrados, a quienes solo podrá imponerse su uso después de superar ese control previo.

Se puede concluir que el CGPJ ha adoptado una actitud proactiva en el plano tecnológico. Esta debe ser acompañada de otras acciones coordinadas, que corresponde efectuar a las otras Administraciones competentes, con la finalidad de subsanar el problema de la falta de jueces y magistrados; de realizar las inversiones precisas para dotar de medios humanos, materiales y espaciales a la Administración de Justicia; y de culminar definitivamente la implantación de la NOJ y del expediente judicial electrónico. De esta forma se estará en condiciones de empezar a revertir la situación actual de la Administración de Justicia, de corregir sus defectos y de subsanar sus deficiencias.

32. No obstante, es llamativa la falta de preocupación del CGPJ por las implicaciones que tiene este proceso desde la perspectiva de la protección de datos, sobre todo a la vista de las importantes novedades que plantea la nueva regulación europea. Acerca de la importancia de este requerimiento, en particular por lo que respecta al expediente judicial, véase ARENAS RAMIRO, M. (2019). «La modernización de la tutela judicial efectiva y el expediente judicial electrónico». En: GÓMEZ MANRESA, M. F.; FERNÁNDEZ SALMERÓN, M. (coords.). *Modernización digital e innovación en la Admnistración de Justicia*. Navarra: Aranzadi-Thomson Reuters (Cizur Menor), págs. 285 y 286.

Referencias bibliográficas

ARENAS RAMIRO, M. (2019). «La modernización de la tutela judicial efectiva y el expediente judicial electrónico». En: GÓMEZ MANRESA, M. F.; FERNÁNDEZ SALMERÓN, M. (coords.). *Modernización digital e innovación en la Administración de Justicia*. Navarra: Thomson Reuters Aranzadi (Cizur Menor).

ARNAIZ SERRANO, A.; TOMÁS PORTER, J. J. (2010). «La nueva oficina judicial y el nuevo modelo procesal: un estudio sobre la organización y funciones en la oficina judicial y los procesos judiciales tras la reforma de la legislación procesal operada por la Ley 13/2009». *Revista jurídica de la Comunidad Valenciana: jurisprudencia seleccionada de la Comunidad Valenciana,* núm. 33.

BUENO DE MATA, F. (2014). P*rueba electrónica y Proceso 2.0.* Valencia: Tirant Lo Blanch.

CLÈRIES I NERÍN, N. (2007). «Administración electrónica en el Área de Justicia». *IDP. Revista de Internet, Derecho y Política,* núm. 4. Monográfico e-Justicia [en línea] https://idp.uoc.edu/42/volume/0/issue/4/ [Fecha de consulta: 3 de septiembre de 2020].

CERDÁ MESEGUER. J. I. (2016). «El objetivo "papel cero" en la Administración de Justicia española: ¿una realidad procesalmente imposible?». En: BUENO DE MATA, F. (dir.). *Hacia una Justicia 2.0.* Salamanca: Actas del XX Congreso Iberoamericano de Derecho e Informática, vol. II, págs. 35-48.

CERDÁ MESEGUER, J. I. (2018). *El uso de medios electrónicos en la Administración de Justicia. Del expediente en papel al expediente electrónico.* Valencia: Tirant Lo Blanch.

CERDÁ MESEGUER, J. I. (2019). «Hacia una Administración de Justicia plenamente electrónica: disfunciones normativas y jurisprudenciales». En: GÓMEZ MANRESA, M. F.; FERNÁNDEZ SALMERÓN, M. (coords.). *Modernización digital e innovación en la Admnistración de Justicia*. Navarra: Aranzadi-Thomson Reuters (Cizur Menor).

CERNADA BADÍA, R. (2019). «LexNET o la selección natural en el foro del siglo xxi». En: GÓMEZ MANRESA, M. F.; FERNÁNDEZ SALMERÓN, M. (coords.). *Modernización digital e innovación en la Admnistración de Justicia* (Navarra): Aranzadi-Thomson Reuters (Cizur Menor).

CERRILLO I MARTÍNEZ, A. (2007). «E-justicia: las tecnologías de la información y el conocimiento al servicio de la Justicia Iberoamericana en el siglo XXI». I*DP. Revista de Internet, Derecho y Política,* núm. 4. Monográfico e-Justicia [en línea] https://idp.uoc.edu/42/volume/0/issue/4/ [Fecha de consulta: 3 de septiembre de 2020].

CERRILLO I MARTÍNEZ, A. (2010). «Cooperación entre Administraciones públicas para el impulso de la administración electrónica». En: GAMERO CASADO, E.; VALERO TORRIJOS, J. *La Ley de Administración Electrónica. Comentarios a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos.* Navarra: Aranzadi-Thomson Reuters (Cizur Menor).

CERRILLO I MARTÍNEZ, A. (2012). «La dotación suficiente de medios e instrumentos electrónicos y el marco general de la cooperación interadministrativa en materia de Administración de Justicia». En: GAMERO CASADO, E.; VALERO TORRIJOS, J. (coords.). *Las tecnologías de la información y la comunicación en la Administración de Justicia. Análisis sistemático de la Ley 18/2011, de 5 de julio.* Navarra: Aranzadi-Thomson Reuters.

DELGADO GARCÍA, A. M.ª; OLIVER CUELLO, R. (2006). *Las tecnologías de la información y la comunicación en la Administración de Justicia.* Oñati (Bilbao): Instituto Vasco de Administración Pública.

DELGADO GARCÍA, A. M.ª; OLIVER CUELLO, R. (2007). «Administración de Justicia y tecnologías de la información y la comunicación: aspectos jurídicos». *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 13.

DELGADO GARCÍA, A. M.ª; OLIVER CUELLO, R. (2007). «Iniciativas recientes de la e-Justicia en España». *IDP. Revista de Internet, Derecho y Política,* núm. 4. Monográfico e-Justicia [en línea] https://idp.uoc.edu/42/volume/0/issue/4/ [Fecha de consulta: 3 de septiembre de 2020].

GAMERO CASADO, E.; MARTÍNEZ GUTIÉRREZ, R. (2010). «El Derecho Administrativo ante la Era de la Información». En: GAMERO CASADO, E.; VALERO TORRIJOS, J. (coords.). *La Ley de Administración Electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos*. Navarra: Aranzadi-Thomson Reuters.

JIMÉNEZ ASENSIO, R. (2010). «El encaje constitucional de la NOJ». Ponencia presentada en el curso «La Nueva Oficina Judicial». Madrid: CENDOJ.

JIMÉNEZ GÓMEZ, C. E. (2014). «Desafíos de la modernización de la Justicia en tiempos del Gobierno Abierto». *Revista Digital de Derecho Administrativo*, núm. 12.

MARTÍNEZ GUTIÉRREZ, R. (2019). «Los retos de la innnovación tecnológica en la Jurisdicción Contencioso-Administrativa». Ponencia presentada en el XIV Congreso Nacional de Profesores de Derecho Administrativo, celebrado en Murcia, los días 8 y 9 de febrero de 2019.

MARTÍNEZ GUTIÉRREZ, R. (2019). «La e-Justicia contecioso-administrativa después de la Instrucción 1/2018 del CGPJ». *Revista General de Derecho Administrativo,* núm. 51.

MORA-SANGUINETTI, J. S.; MARTÍNEZ-MATUTE, M. (2020). «Los impactos económicos del funcionamiento de la Justicia en la Región de Murcia». Murcia: Consejo Económico y Social de la Región de Murcia, febrero de 2020. [en línea] https://www.cesmurcia.es/cesmurcia/paginas/publicaciones/UltimasPublicaciones.seam?pubId=2241 [Fecha de consulta: 3 de septiembre de 2020].

ORTUÑO MUÑOZ, P. (2011). «Del arancel al expediente electrónico (Notas históricas sobre el modelo de oficina judicial español)». *Revista Jurídica Fundación Mariano Ruiz-Funes,* núm. 45.

PARRA GARCÍA, J. L.; PASQUAL DEL RIQUELME HERRERO, M. (2009). «Oficina Judicial integrada o hacia una Justicia inteligente en España». *Boletín del Ministerio de Justicia,* año 63, núm. 2.094.

PARRA GARCÍA, J. L. (2010). «El año uno en la Oficina Judicial: nueva organización, nuevas formas de hacer Justicia». *Derecho y Jueces, EL DERECHO*, núm. 55.

PARRA GARCÍA, J. L. (2019). «La Oficina Judicial en España: un balance de diez años». Actividad formativa del curso «Estatuto orgánico LAJ» (8.ª ed.) en el Centro de Estudios Jurídicos, 25 y 26 de noviembre de 2019.

SEOANE CHACARRÓN, J. (2011). «El Secretario Judicial ante la Ley 13/2009, de 3 de noviembre, de Reforma de la Legislación Procesal (civil y penal) para la implantación de la Nueva Oficina Judicial». *Diario La Ley,* núm. 7.561.

SUÁREZ-QUIÑONES Y FERNÁNDEZ, J. C. (2010). «Administración de Justicia y Nuevas Tecnologías: presente y futuro». *Diario La Ley,* núm. 7.421.

VALERO TORRIJOS, J. (2013). *Derecho, innovación y Administración electrónica.* Sevilla: Derecho Global.

Cita recomendada

CERDÁ MESEGUER, Juan Ignacio (2020). «La modernización y transformación digital de la Administración de Justicia: el papel del Consejo General del Poder Judicial». *IDP. Revista de Internet, Derecho y Política*,núm. 31, págs. 1-12. UOC [Fecha de consulta: dd/mm/aa]. http://dx.doi.org/10.7238/idp.v0i31.3239

Sobre la autor

Juan Ignacio Cerdá Meseguer
jignaciocm@um.es
Universidad de Murcia

Licenciado en Derecho y doctor por la Universidad de Murcia con la tesis *El expediente judicial electrónico*, ha participado como ponente y comunicante en diversos congresos nacionales e internacionales y es autor de una monografía y varias publicaciones en obras colectivas y revistas especializadas. Sus líneas de investigación se han centrado principalmente en las implicaciones jurídicas del uso de medios electrónicos en la Administración de Justicia y en el marco normativo de la protección de los datos de carácter personal. Abogado en ejercicio con despacho propio durante veintisiete años, actividad profesional compaginada con la docencia universitaria, actualmente es profesor del Departamento de Derecho Administrativo e investigador en iDerTec a tiempo completo, participando en varios proyectos de investigación sobre dichos temas.

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

www.uoc.edu/idp

RESEÑA

Una nueva edición del congreso IDP en formato virtual dedicada al cibercrimen

Marc Balcells Magrans
Universitat Oberta de Catalunya

Fecha de publicación: octubre de 2020

Durante los días 1 y 2 de julio se ha celebrado la decimoquinta edición del congreso internacional Internet, Derecho y Política (IDP), organizado por los Estudios de Derecho y Ciencia Política de la Universitat Oberta de Catalunya. El congreso, titulado «Cybercrime: new threats, new responses», se ha dedicado a analizar los nuevos retos que presenta la ciberdelincuencia, celebrando a su vez la primera edición del máster universitario en esta materia impartido en nuestros estudios.

Esta es la primera vez que el congreso se ha celebrado de forma virtual, consecuencia de la pandemia causada por el virus SARS-CoV-2. Poco nos podíamos imaginar desde el Comité científico, al empezar a organizar el congreso en el año 2018, que en el momento de su celebración estaríamos inmersos en una crisis sanitaria mundial que afectaría a tantos aspectos en nuestras vidas. Uno de ellos ha sido la delincuencia: a falta de un análisis criminológico más profundo que solamente se podrá llevar a cabo con el estudio detenido y cuidadoso de las estadísticas oficiales, parece ser que a medida que la delincuencia callejera disminuía, aumentaba la ciberdelincuencia. Nuestras vidas confinadas, en las que gran parte del tiempo ha transcurrido en el mundo virtual, han dejado un rastro de vulnerabilidades que los ciberdelincuentes han podido explotar. Si algo ha dejado claro esta edición del congreso IDP es que este tipo de delincuencia sigue adaptándose y evolucionando con ataques hechos a la medida de los tiempos vividos.

En esta edición virtual del congreso, se ha contado con la presencia de tres expertos de renombre en el campo del estudio de la ciberdelincuencia, tanto desde la óptica del derecho penal como de la criminología, como son los profesores Alfonso Galán, de la Universidad Pablo Olavide; Fernando Miró, de la Universidad Miguel Hernández; y David Wall, de la Universidad de Leeds.

Alfonso Galán impartió la primera de las tres conferencias, relativa a la *compliance* en los delitos informáticos. En palabras suyas, «no es difícil imaginar que muchas compañías podrían optar por establecer algunas medidas, como el monitoreo permanente de todas las actividades de internet de sus trabajadores o el borrado automático de cualquier información publicada desde sus servidores que pueda parecer ilegal, para mantenerse a salvo de cualquier castigo. El uso de este tipo de medidas preventivas, sin duda, puede evitar muchos comportamientos criminales posibles, pero también, y de forma indiscutible, tensionará el debido respeto de algunos derechos y garantías fundamentales de la ciudadanía, como los del secreto de las comunicaciones de los trabajadores o el de la libertad de expresión de los emisores de los mensajes bloqueados o borrados».

Por su parte, los profesores Miró y Wall impartieron, respectivamente, la segunda de las conferencias y la clausura del congreso. Ambos incidieron en el impacto de la covid-19 en la ciberdelincuencia. El primero, tras recopilar todos los indicios existentes respecto al supuesto aumento del cibercrimen derivado del confinamiento y constatar la falta de información, reflexionó en torno a los marcos teóricos, premisas y exigencias analíticas con que debemos afrontar el estudio científico del impacto de la covid-19 en el crimen y muy en particular en el delito perpetrado en el ciberespacio. La tesis del profesor Miró es que la crisis del coronavirus no es tanto la causante como la aceleradora de una tendencia de desplazamiento de actividades diarias del espacio físico al ciberespacio que puede haber incidido directamente, y lo hará aún más en el futuro, tanto en la reducción de la delincuencia en las calles como en el aumento de la cometida en el ciberespacio.

David Wall, en la conferencia de clausura del congreso, argumentó que los delitos cibernéticos evolucionan continuamente con el desarrollo de las TIC, por lo que ya no se puede decir que son un fenómeno nuevo. Después de tres décadas de observar su progresión, poco a poco hemos llegado a comprender sus cualidades y factores concomitantes, como por ejemplo si las instituciones tardan más tiempo en adaptarse a los desafíos que este tipo de delincuencia genera. Así, el profesor Wall describió los desarrollos clave en el cibercrimen durante la última década, para pasar a analizar a continuación los retos que presentan para el legislador y las fuerzas del orden. Finalmente, presentó algunos hallazgos de su investigación reciente sobre *ransomware* para ilustrar los cambios sufridos en este campo.

El profesor Alfonso Galán no solamente abrió con su ponencia la primera de las jornadas, sino que participó en la primera de las mesas redondas, dedicada a aspectos jurídicos de la ciberdelincuencia, en la que participaron la profesora Paz Lloria, de la Universidad de Valencia; el magistrado Alberto Varona, de la Audiencia Provincial de Barcelona y profesor del Área Penal de la Escuela Judicial; y el letrado Ramon Miralles, socio de Elix Group. A lo largo de esta primera jornada quedó ampliamente demostrado el gran abanico de temas penales derivados de la ciberdelincuencia, como las intervenciones de los ponentes relativas a la aplicación de la *compliance* ante el discurso terrorista en la red; el concepto y las características del delito tecnológico; la obtención y el aseguramiento de evidencias digitales o el impacto de la ciberdelincuencia en los derechos fundamentales. A su vez, el profesor Fernando Miró fue el encargado de abrir la segunda de las jornadas, dedicada a los aspectos criminológicos de la ciberdelincuencia. En esta mesa participaron también, además del propio Miró, el profesor Josep Ramon Agustina, de la Universitat Internacional de Catalunya, y el subinspector y jefe de la Unidad Central de Delitos Informáticos del cuerpo de los Mossos d'Esquadra Albert Álvarez, donde se trataron, entre otros temas, la problemática con las estadísticas policiales o la cooperación internacional. Todas estas intervenciones pueden seguir siendo visionadas en la página web del congreso, al igual que el libro de actas (en http://symposium.uoc.edu/30247/videos/xv-congreso-idp_-cybercrime_-new-threats-new-responses-1-2-de-julio.html).

La adopción de un formato virtual en esta edición del congreso IDP no significaba que se obviaran las comunicaciones presentadas por profesionales de todo el mundo sobre esta materia en los meses anteriores a la pandemia. Por ello, sus comunicaciones han sido recogidas en un libro de actas digital no solo por su calidad sino también, más que nunca, como un homenaje a su participación truncada por la pandemia. Al igual que con las sesiones en línea, los capítulos del libro de actas reflejan la variedad de temas alrededor del fenómeno de la ciberdelincuencia, como por ejemplo el discurso de odio y el racismo en internet; los problemas derivados de la regulación relativa a la protección de datos; o la problemática causada por el cibercrimen en Nigeria, entre otros.

La conferencia destacó la necesidad de seguir promoviendo la investigación y la cooperación en un campo en constante evolución como es la ciberdelincuencia. Desde los Estudios de Derecho y Ciencia Política de la Universitat Oberta de Catalunya apostamos por la formación de futuros profesionales en el campo de la ciberdelincuencia a través de nuestro máster universitario, donde los alumnos y alumnas reciben una formación multidisciplinar en materias criminológicas, jurídicas e informáticas que les permitirá operar en uno de los campos más dinámicos, relevantes e internacionales de la criminalidad actual.

Cita recomendada

BALCELLS MAGRANS, Marc (2021). «Una nueva edición del congreso IDP en formato virtual dedicada al cibercrimen». *IDP. Revista de Internet, Derecho y Política*, núm. 31. UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i31.3264

Sobre el autor

Marc Balcells i Magrans
Ph.D., City University of New York/John Jay College of Criminal Justice
Profesor lector de Criminologiía y Derecho Penal
Grado de Criminología/Máster Universitario Advocacía/Mster Universitario Ciberdelincuencia
Estudios de Derecho y Ciencia Política de la Universitat Oberta de Catalunya

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

www.uoc.edu/idp

RESEÑA

Webinar sobre la docencia en línea con RStudio Cloud

Jordi Mas Elias
Universitat Oberta de Catalunya

Fecha de publicación: octubre de 2020

La docencia a distancia en metodología y estadística presenta dificultades añadidas a las de otras asignaturas en línea, debido a que normalmente se requiere el uso de software de datos. El docente y el alumnado dedican buena parte del inicio del curso a la familiarización con un determinado programa estadístico y se destinan una gran cantidad de horas a resolver dudas y problemas de instalación, así como a comprender el lenguaje y las dinámicas del programa. Estos obstáculos se amplifican con la distancia física entre docente y alumnado, por lo que se ralentiza el aprendizaje.

Con el objetivo de facilitar la docencia en línea de asignaturas relacionadas con la metodología en ciencias sociales, el profesor de los Estudios de Derecho y Ciencia Política de la UOC Jordi Mas presentó el 20 de mayo el webinar titulado «RStudio Cloud en la docencia *online* en asignaturas de metodología y estadística» en el marco del ciclo *Docencia no presencial de emergencia* organizado por la universidad. La sesión se orientó a explicar el uso de la herramienta RStudio Cloud, diseñada por los creadores de RStudio, que ayuda en buena medida a solucionar estos problemas. Principalmente, se reducen las horas dedicadas a la instalación y familiarización, se eliminan los problemas particulares de cada alumno o alumna con el software y se incrementa el control del profesor sobre el escritorio de datos del alumnado. A principios de agosto de este año RStudio Cloud dejó de estar en versión beta. Con la primera versión algunas de sus ventajas han pasado a ser de pago.

Cita recomendada

MAS ELIAS, Jordi (2020). «Webinar sobre la docencia en línea con RStudio Cloud». *IDP. Revista de Internet, Derecho y Política,* núm. 31. UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i31.3268

Sobre el autor

Jordi Mas Elias
Universitat Oberta de Catalunya

Es profesor de política internacional en la Universitat Oberta de Catalunya (UOC). En su etapa predoctoral ha estudiado en el Instituto de Barcelona de Estudios Internacionales, la London School of Economics y la Universidad Autónoma de Barcelona. Su investigación incluye regionalismo y economía política internacional. En docencia, imparte clases en el grado de Relaciones Internacionales y el máster de Conflict, Peace, and Security de la UOC en los ámbitos de análisis de datos, métodos de investigación y economía política internacional.

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

www.uoc.edu/idp

RESEÑA

XI Jornada de Docencia del Derecho y Tecnologías de la Información y la Comunicación

Ana María Delgado García
Catedrática de Derecho Financiero y Tributario
Directora del Máster Universitario de Fiscalidad

Fecha de publicación: marzo de 2020

En las circunstancias actuales, se ha evidenciado la necesidad de aplicar formas alternativas de aprender y de enseñar. Por ello, la tecnología va a estar más presente que nunca, no solo en modalidades de enseñanza no presencial o semipresencial, sino como una pieza inherente de la enseñanza presencial. Ser un profesor es un reto y ahora más que nunca; de manera que es el momento de crear valor a partir de nuevas posibilidades y oportunidades.

En este contexto, no se trata solo de tecnología ni es suficiente con que nuestros estudiantes sean nativos digitales para que la docencia online funcione, sino que hay que poner la tecnología al servicio de la docencia. El docente debe reformular los objetivos de aprendizaje, adaptar las metodologías y estrategias docentes, diseñar y seleccionar los recursos de aprendizaje más adecuados para alcanzar dichos objetivos. Por consiguiente, hay que realizar un rediseño pedagógico, que va más allá del uso de herramientas digitales.

Todos estos aspectos han sido objeto de reflexión en la XI Jornada de Docencia del Derecho y Tecnologías de la Información y la Comunicación, organizada, de manera virtual, por los Estudios de Derecho y Ciencia Política de la Universitat Oberta de Catalunya el día 10 de julio de 2020 (http://symposium.uoc.edu/38228/section/20457/xi-jornada-sobre-docencia-del-derecho-y-tecnologias-de-la-informacion-y-la-comunicacion.html). El Comité organizador de esta actividad ha estado formado por los directores de la misma, la Dra. Ana María Delgado García y el Dr. Ignasi Beltran de Heredia, y por los siguientes profesores: la Dra. Irene Rovira Ferrer, el Dr. Benjamí Anglès Juanpere y Jordi García Albero.

Esta jornada se ha consolidado como punto de encuentro de profesores de asignaturas jurídicas de numerosas universidades para el intercambio de ideas y buenas prácticas en el uso de las TIC en el proceso de enseñanza/aprendizaje del Derecho, con el fin de mejorar la calidad de la educación superior. Los ejes temáticos abordados han sido: la planificación docente, los sistemas de evaluación, la formación práctica del Derecho y las herramientas de trabajo colaborativo.

En esta ocasión, nuevamente ha habido una importante participación, plasmada en las 33 comunicaciones aceptadas y que se recogen en el libro colectivo, coordinado por los directores de la jornada, La docencia del Derecho en línea: cuando la innovación se convierte en necesidad, publicado por la Editorial Huygens.

Cita recomendada

DELGADO GARCÍA, Ana María (2020). «XI Jornada de Docencia del Derecho y Tecnologías de la Información y la Comunicación». *IDP. Revista de Internet, Derecho y Política*. núm. 31. UOC [Fecha de consulta: dd/mm/aa] https://doi.org/10.7238/idp.v0i31.374685

Sobre la autora

Ana María Delgado García
Catedrática de Derecho Financiero y Tributario
Directora del Máster Universitario de Fiscalidad

Universitat Oberta de Catalunya

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

www.uoc.edu/idp

ACTUALIDAD NORMATIVA

Novedades legislativas

Jordi Garcia Albero
Profesor de los Estudios de Derecho y Ciencia Política (UOC)

Fecha de publicación: octubre de 2020

Boletín Oficial del Estado (BOE)

Real Decreto-ley 8/2020, de 17 de marzo, de **medidas urgentes extraordinarias** para hacer frente al **impacto económico y social** del COVID-19.
BOE núm. 73, 18 de marzo de 2020.
https://www.boe.es/boe/dias/2020/03/18/pdfs/BOE-A-2020-3824.pdf

Real Decreto-ley 11/2020, de 31 de marzo, por el que se adoptan **medidas urgentes complementarias** en el **ámbito social y económico** para hacer frente al **COVID-19.**
BOE núm. 91, 1 de abril de 2020.
https://www.boe.es/boe/dias/2020/04/01/pdfs/BOE-A-2020-4208.pdf

Resolución de 15 de abril de 2020, de la Dirección General de la **Agencia Estatal de Administración Tributaria**, por la que se **modifica la de 11 de marzo de 2020**, sobre **asistencia** a los obligados tributarios y ciudadanos en su **identificación telemática** ante las entidades colaboradoras, con ocasión del pago de deudas con tarjetas de crédito y de débito, **mediante el sistema de firma no avanzada con clave de acceso en un registro previo (sistema CI@VE PIN).**
BOE núm. 111, 21 de abril de 2020.
https://www.boe.es/boe/dias/2020/04/21/pdfs/BOE-A-2020-4538.pdf

Real Decreto-ley 15/2020, de 21 de abril, de **medidas urgentes complementarias** para **apoyar la economía y el empleo.**
BOE núm. 112, 22 de abril de 2020.
https://www.boe.es/boe/dias/2020/04/22/pdfs/BOE-A-2020-4554.pdf

Real Decreto-ley 16/2020, de 28 de abril, de **medidas procesales y organizativas** para hacer frente al **COVID-19** en el ámbito de la **Administración de Justicia.**
BOE núm. 119, 29 de abril de 2020.
https://www.boe.es/boe/dias/2020/04/29/pdfs/BOE-A-2020-4705.pdf

Resolución de 29 de abril de 2020, de la Secretaría General de Administración Digital, por la que se acuerda la **continuación de los procedimientos administrativos de autorización de nuevos sistemas de identificación y firma electrónica mediante clave concertada y cualquier otro sistema** que las Administraciones consideren válido a que se refieren los artículos 9.2 c) y 10.2 c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, **en aplicación de la disposición adicional tercera del Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19.**
BOE núm. 120, 30 de abril de 2020.
https://www.boe.es/boe/dias/2020/04/30/pdfs/BOE-A-2020-4733.pdf

Instrucción de 22 de junio de 2020, de la Dirección General de Seguridad Jurídica y Fe Pública (Ministerio de Justicia), sobre la **remisión telemática al Registro de Bienes Muebles de contratos privados de financiación** suscritos mediante un sistema de identificación y prestación del consentimiento basado en firmas no criptográficas.
BOE núm. 184, 4 de julio de 2020.
https://www.boe.es/boe/dias/2020/07/04/pdfs/BOE-A-2020-7296.pdf

Resolución de 15 de julio de 2020, de la Dirección General de la **Agencia Estatal de Administración Tributaria**, por la que se modifica la de 19 de marzo de 2020, por la que se establecen las **condiciones para la tramitación y contestación en la Sede Electrónica** de la Agencia Estatal de Administración Tributaria de los requerimientos de información a que se refiere el artículo 97.5 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, **dirigidos a entidades de crédito y referidos a bienes inmuebles.**
BOE núm. 201, 24 de julio de 2020.
https://www.boe.es/boe/dias/2020/07/24/pdfs/BOE-A-2020-8520.pdf

Diario Oficial de la Unión Europea (DOUE)
Legislación, comunicaciones e informaciones comunitarias

Reglamento interno de Eurojust relativo al tratamiento y a la protección de datos personales.
DOUE L 50, 24 de febrero de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020Q0224(02)&from=ES

Reglamento (UE) 2020/261 del Consejo de 19 de diciembre de 2019 por el que se **modifica el Reglamento (UE) 389/2012** sobre **cooperación administrativa** en el ámbito de los **impuestos especiales** por lo que se refiere al **contenido de los registros electrónicos** (ST/14108/2019/INIT).
DOUE L 58, 27 de febrero de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020R0261&from=ES

Reglamento (UE) 2020/283 del Consejo de 18 de febrero de 2020 por el que se **modifica** el **Reglamento (UE) 904/2010** en lo que respecta a las medidas para **reforzar la cooperación administrativa a fin de combatir el fraude en el ámbito del IVA** (ST/14128/2019/INIT).
DOUE L 62, 2 de marzo de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020R0283&from=ES

Directiva (UE) 2020/284 del Consejo de 18 de febrero de 2020 por la que se **modifica la Directiva 2006/112/CE** en lo que respecta a la introducción de determinados **requisitos para los proveedores de servicios de pago** (ST/14127/2019/INIT).
DOUE L 62, 2 de marzo de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020L0284&from=ES

Dictamen del Comité Europeo de las Regiones-Trabajo en plataformas digitales: retos normativos en las esferas local y regional.
DOUE C 79, 10 de marzo de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52019IR2655&from=ES

Decisión del Consejo de Administración del Centro Europeo para la Prevención y el Control de las Enfermedades de 9 de septiembre de 2019 relativa a las normas internas sobre las **limitaciones** de determinados **derechos de los interesados en relación con el tratamiento de datos personales** en el marco del funcionamiento del Centro Europeo para la Prevención y el Control de las Enfermedades.
DOUE L 98, 31 de marzo de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020Q0331(01)&from=ES

Recomendación (UE) 2020/518 de la Comisión de 8 de abril de 2020 relativa a un conjunto de **instrumentos comunes** de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar **la crisis de la COVID-19,** en particular por lo que respecta a las **aplicaciones móviles y a la utilización de datos de movilidad anonimizados** (C/2020/3300).
DOUE L 114, 14 de abril 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020H0518&from=ES

Comunicación de la Comisión orientaciones sobre las **aplicaciones móviles** de apoyo a la **lucha contra la pandemia de covid-19** en lo referente a la protección de datos (C/2020/2523).
DOUE C 124 I, 17 de abril de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020XC0417(08)&from=ES

Conclusiones del Consejo sobre la configuración del **futuro digital de Europa** (ST/8711/2020/INIT).
DOUE C 202 I, 16 de junio de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020XG0616(01)&from=ES

Decisión (UE) 2020/969 de la Comisión de 3 de julio de 2020 por el que se establecen **disposiciones de aplicación** relativas al **responsable de la protección de datos,** a las **restricciones de los derechos de los interesados** y a la **aplicación del Reglamento (UE) 2018/1725** del Parlamento Europeo y del Consejo, **y por la que se deroga la Decisión 2008/597/CE de la Comisión** (C/2020/4183).
DOUE L 213, 6 de julio de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020D0969&from=ES

Reglamento de Ejecución (UE) 2020/1030 de la Comisión de 15 de julio de 2020 por el que se establecen las **especificaciones técnicas de los requisitos de datos aplicables al tema «uso de las TIC y comercio electrónico» para el año de referencia 2021,** de conformidad con el Reglamento (UE) 2019/2152 del Parlamento Europeo y del Consejo (Texto pertinente a efectos del EEE) (C/2020/4700).
DOUE L 227, 16 de julio de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020R1030&from=ES

Comunicación de la Comisión sobre la **protección de la información confidencial por los órganos jurisdiccionales nacionales** en los procedimientos de aplicación privada del **Derecho de la competencia de la UE** (C/2020/4829).
DOUE C 242, 22 de julio de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52020XC0722(01)&from=ES

Reglamento de Ejecución (UE) 2020/1121 de la Comisión de 29 de julio de 2020 relativo a la **recogida y el intercambio de estadísticas y observaciones de los usuarios** sobre los servicios de la **pasarela digital única** de conformidad con el Reglamento (UE) 2018/1724 del Parlamento Europeo y del Consejo (Texto pertinente a efectos del EEE) (C/2020/5075).
DOUE L 245, 30 de julio de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020R1121&from=ES

Decisión 2020-04 del Colegio de Comisarios de 15 de julio de 2020 relativa a las **normas internas** sobre las limitaciones de determinados derechos de los titulares de datos en relación con el **tratamiento de datos personales en el marco de las actividades llevadas a cabo por Eurojust.**
DOUE L 287, 2 de septiembre de 2020.
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020Q0902(01)&from=ES

Jordi Garcia Albero
Profesor de los Estudios de Derecho y Ciencia Política (UOC)

‹https://dx.doi.org/10.7238/idp.v0i31.3263›

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

www.uoc.edu/idp

ACTUALIDAD JURÍDICA

Jurisprudencia

Patricia Escribano
Profesora ayudante doctora
Universitat Jaume I

Fecha de publicación: octubre de 2020

Sentencia del Tribunal Supremo (Sala de lo Penal, Sección 1.ª), núm. 70/2020 de 24 de febrero

En la presente sentencia se analiza si la conducta realizada por el acusado se circunscribe al delito de descubrimiento de revelación de secretos del art. 197.7 del Código Penal. Este precepto dispone que: «Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquélla que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. La pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa».

En el presente supuesto se condena a un hombre a la pena de seis meses de multa con una cuota diaria de seis euros, ya que envió una fotografía que le había enviado su amiga, en la que aparecía desnuda y sin su consentimiento, a la pareja sentimental de esta. El condenado interpone recurso de apelación que también es desestimado.

Los argumentos que esgrime la defensa son: a) el acusado no obtuvo la fotografía en su domicilio o en otro lugar «fuera del alcance de la mirada de terceros», sino que fue ella quien se la envió; b) la imagen no se difundió tal y como exige el artículo, sino que se envió solamente a una persona; y c) no hubo «grave menoscabo de la intimidad» de la afectada, ya que la ruptura con la persona que recibió la imagen «no fue la causa de la ruptura, sino su consecuencia».

El TS analiza de forma pormenorizada el art. 197.7 CP haciendo referencia en primer término que se considera un precepto controvertido. Posteriormente, hace hincapié en las dos tendencias que existen respecto al artículo. De este modo determina que «su valoración enfrenta a quienes consideran que se trata de un tipo penal indispensable para evitar clamorosos vacíos de impunidad –*sexting* o *revenge porn*– y aquellos otros que entienden, por el contrario, que la descripción del tipo vulnera algunos de los principios informadores del derecho penal».

La Sala entiende que la esfera sexual es una de las manifestaciones del núcleo duro de la intimidad, aunque no sea la única. Por otro lado, el eje central consiste en difundir imágenes que se han obtenido con el consentimiento de la víctima en un domicilio u otro lugar fuera del alcance de terceros. El TS –después de traer a colación el significado de «obtener» según el diccionario de la RAE– establece que «resulta muy difícil sostener que cuando esas imágenes se remiten por la propia víctima y se alojan en el móvil del destinatario, en realidad, no se *consiguen*, no se *logran*, no se *tienen*, no se *conservan* o no se *mantienen*». Por otro lado, matiza que la obtención de imágenes o vídeos puede realizarse captando la imagen o grabando el vídeo, o bien remitirse de forma voluntaria por la víctima «valiéndose para ello de cualquier medio convencional o de un programa de mensajería instantánea que opere por redes telemáticas». Y que el núcleo duro de la acción típica es difundir las imágenes que se han obtenido con consentimiento de la víctima y que afecten de forma grave a su intimidad. Además, el TS considera que el sujeto activo, según el fiscal, es a quien que se le remite de forma voluntaria la fotografía o el vídeo y, posteriormente, sin el consentimiento de la persona que la ha remitido, «quebrantando la confianza en él depositada, la reenvía a terceros, habitualmente con fines sexistas, discriminatorios o de venganza».

En relación con el argumento que alegó el acusado de que la víctima fue quien creó el riesgo de difusión, la Sala mantiene que quien envía una foto de este tipo no está renunciando de forma anticipada a esta ni «tampoco está sacrificando de forma irremediable su privacidad. Su gesto de confiada entrega y selectiva exposición a una persona cuya lealtad no cuestiona, no merece el castigo de la exposición al fisgoneo colectivo». Tampoco puede aceptarse que, para que pueda aplicarse el 197.7 CP, sea necesario la difusión a una colectividad, sino que puede darse en caso de que se envíe a una sola persona. Básicamente, por estos motivos (obviamente, de forma resumida), se desestima el recurso de casación.

Sentencia del Tribunal Supremo (Sala de lo Civil, Sección 1.ª), núm. 235/2020 de 2 de junio

Esta resolución judicial versa sobre una cuestión muy debatida, hasta que el TS, en 2009, pronunció diversas sentencias en relación con la materia tratada: la responsabilidad de las entidades prestadoras de servicios de la información.

Los hechos que dan lugar al recurso de casación son los siguientes: la entidad demandada es titular de un dominio que fue condenada en segunda instancia, ya que tuvo conocimiento efectivo de varios comentarios vejatorios que constaban en la página hacia un político, como consecuencia de una noticia que se publicó en noviembre de 2015. En concreto, la resolución se centra en los insultos «ladrón» e «hijo de puta». Queda acreditado que la persona afectada solicitó hasta en dos ocasiones que se eliminaran los comentarios ofensivos (no la noticia en sí). Casi un año después de la publicación de esta envío un correo electrónico exigiendo su retirada, a través de un despacho de abogados. A falta de respuesta, cinco días después envió un burofax, el cual tampoco tuvo los efectos deseados, motivo por

el cual un mes después interpone demanda sobre intromisión ilegítima en su derecho al honor contra la página web, exigiendo el pago de 30.000 euros de indemnización, que se publique la sentencia o, en su defecto, el fallo y al pago de las costas.

La sentencia de primera instancia desestimó la petición del demandante, la cual fue estimada en parte por la Audiencia Provincial, aunque se redujo la cuantía de la indemnización, se mandó publicar el fallo de la sentencia y no se le impusieron costas a la demandada. Esta interpuso recurso de casación fundándose en la infracción de los arts. 18 y 20 de la Constitución y en la infracción del art. 16 de la Ley de Servicios de la Sociedad de la Información en relación con los arts. 14 y 15 de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.

Pues bien, trayendo a colación varias sentencias el TS señala que «para que no se revierta en el caso en concreto la preeminencia de la que goza en abstracto la libertad de expresión sobre el derecho al honor es preciso que concurran dos presupuestos, consistentes en el interés general o la relevancia pública de la opinión expresada, sea por la materia, por razón de las personas o por las dos cosas y, en la necesaria proporcionalidad en la difusión de las opiniones, pues se proscribe el empleo de manifiestamente injuriosas, vejatorias o que no guarden relación o no resulten necesarias para transmitir la idea crítica» (FJ 3.º). Por otro lado, precisa que, aunque el personaje de la crítica sea público, la libertad de expresión no ampara ni las expresiones vejatorias ni los insultos hacia su persona y, menos aún, «hijo de puta».

En consecuencia, desestima el recurso por varias razones:

- *En el caso de la colisión del derecho al honor del demandante y la libertad de expresión de los usuarios, el TS considera que el término «ladrón» podría admitirse, pero no «hijo de puta», comentario que no puede tener amparo en la libertad de expresión, aunque sea una palabra que se usa de forma coloquial, como menciona el recurrente.*

- *La parte demandada es proveedora de servicios de la información que está actuando como intermediaria, tal y como establece la jurisprudencia que los cataloga entre otros como «el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros, y a provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet».*

- *En este caso, quedó acreditado que el demandante solicitó dos veces la retirada de los comentarios insultantes (recordemos, no la noticia) al titular de la página, el cual no respondió, matizando que no la condena por no controlar la publicación, sino que el Tribunal la hace responsable porque, tras conocer la existencia de insultos, no hizo nada por retirarlos ni para impedir su acceso, incluso al haberle proporcionado a la página todos los datos necesarios. Por este motivo, el TS considera que «tuvo conocimiento efectivo de los comentarios y de su ilicitud, no desde la notificación de la demanda (...), sino al menos desde la primera comunicación dirigida por medio de correo electrónico, sin que la demandada obrara con la diligencia que le era exigible a la hora de retirar esos contenidos ilícitos o de impedir que se pudiera seguir accediendo a ellos» (FJ 4.º).*

Cita recomendada

ESCRIBANO, Patricia (2020). «Jurisprudencia». IDP. Revista de Internet, Derecho y Política, núm. 31. UOC [Fecha de consulta: dd/mm/aa] http://dx.doi.org/10.7238/idp.v0i31.3265

Sobre la autora

Patricia Escribano
Profesora ayudante doctora
Universitat Jaume I