CORTES GENERALES

DIARIO DE SESIONES DEL CONGRESO DE LOS DIPUTADOS

COMISIONES

Año 2025 | XV LEGISLATURA | Núm. 477 | Pág. 1

ECONOMÍA, COMERCIO Y TRANSFORMACIÓN DIGITAL

PRESIDENCIA DEL EXCMO. SR. D. PEDRO PUY FRAGA

Sesión núm. 28

celebrada el jueves 11 de diciembre de 2025

Página

ORDEN DEL DÍA:

Celebración de las siguientes comparecencias para informar en relación con el Proyecto de ley por la que se modifican diversas disposiciones legales para la mejora de la gobernanza democrática en servicios digitales y ordenación de los medios de comunicación (número de expediente 121/000068):

cve: DSCD-15-CO-477

Se abre la sesión a las cinco y cincuenta y seis minutos de la tarde.

CELEBRACIÓN DE LAS SIGUIENTES COMPARECENCIAS PARA INFORMAR EN RELACIÓN CON EL PROYECTO DE LEY POR LA QUE SE MODIFICAN DIVERSAS DISPOSICIONES LEGALES PARA LA MEJORA DE LA GOBERNANZA DEMOCRÁTICA EN SERVICIOS DIGITALES Y ORDENACIÓN DE LOS MEDIOS DE COMUNICACIÓN (número de expediente 121/000068):

— DE LA PRESIDENTA DE LA COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA, CNMC (FERNÁNDEZ VICIÉN). POR ACUERDO DE LA COMISIÓN DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL. (Número de expediente 212/000746).

El señor **PRESIDENTE:** Buenas tardes.

Se abre la sesión para tramitar el orden del día que sus señorías conocen.

Celebramos, en primer lugar, la comparecencia de la presidenta de la Comisión Nacional de los Mercados y la Competencia, Cani Fernández Vicién, para informar en relación con el Proyecto de Ley por la que se modifican diversas disposiciones legales para la mejora de la gobernanza democrática en servicios digitales y ordenación de los medios de comunicación.

Señora Fernández, tiene un tiempo aproximado de veinte minutos para exponer ante esta comisión cómo mejorar la ley objeto de la convocatoria.

La señora **PRESIDENTA DE LA COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA, CNMC** (Fernández Vicién): Gracias, presidente.

Señorías, comparezco ante esta Comisión de Economía, Comercio y Transformación Digital para informar, tal y como se me ha solicitado, sobre el Proyecto de Ley que modifica diversas disposiciones legales para la mejora de la gobernanza democrática en servicios digitales y ordenación de los medios de comunicación. Como saben, el proyecto de ley fue aprobado por el Consejo de Ministros el 29 de julio de 2025 y remitido al Congreso de los Diputados, donde se encuentra actualmente en tramitación.

La Comisión Nacional de los Mercados y la Competencia, la CNMC, ya evacuó el informe sobre este proyecto normativo el 2 de julio del 2025, a solicitud del ministerio, y hemos cumplido con eso nuestros trámites de opinión. Estoy encantada de poder comparecer ante ustedes hoy para abundar en su contenido.

El proyecto de ley tiene por objeto adaptar al ordenamiento jurídico español dos normas europeas: el reglamento relativo a un mercado único de servicios digitales, que se aprobó en 2022, conocido como Digital Service Act —DSA, en sus siglas en inglés—, y el reglamento por el que se establece un marco común europeo para los medios de comunicación, el Reglamento European Medium Freedom Act, —EMFA, en sus siglas en inglés—.

En relación con la DSA, el proyecto de ley propone, en esencia, la modificación de la Ley de Servicios de la Sociedad de la Información, mientras que EMFA supone, sobre todo, la modificación de la Ley General de la Comunicación Audiovisual. Por supuesto, el proyecto de ley propone en ambos casos la modificación de la ley de creación de la CNMC, por un lado, para poder atribuirnos legalmente las funciones y responsabilidades derivadas de la aplicación de estas normas europeas en cada caso, y, por otro lado —muy importante—, para adaptar la estructura orgánica de la CNMC y organizar su aplicación efectiva. En este sentido, el proyecto de ley prevé la creación de dos nuevas direcciones en el seno de la CNMC: una dirección para la supervisión de los servicios digitales y otra dirección para los medios de comunicación.

Por el contexto de esta comparecencia, y porque solo dispongo de veinte minutos, me centraré en la parte relativa a la DSA y a los cambios que esta normativa europea exige incorporar en nuestra propia normativa. No obstante, quedo a su disposición en el momento de las preguntas para cualquier cuestión que puedan precisar en relación con las previsiones que el proyecto de ley contempla respecto de la EMFA; incluso, pongo a disposición de sus señorías la posible comparecencia del miembro del consejo de la CNMC Carlos Aguilar, que en estos momentos ocupa precisamente la presidencia del *board* de EMFA, porque la CNMC la ostenta durante este primer año.

La DSA es una norma de carácter transversal, pionera en el ámbito europeo, que pretende regular y someter a supervisión —por primera vez, porque no existe una normativa en ese sentido— a los prestadores de servicios intermediarios digitales, muy especialmente a las plataformas, y su objetivo es crear un entorno en línea seguro, predecible y digno de confianza, en el que los ciudadanos puedan

cve: DSCD-15-CO-477

ejercer sus derechos fundamentales, en particular, libertad de expresión, de información, libertad de empresa, derecho a la no discriminación, así como el consumo *online* seguro. Conviene además recordar que la CNMC ya es la autoridad competente en España para aplicar el reglamento sobre mercados disputables y equitativos en el sector digital, es decir, el Reglamento de Mercados Digitales, la Digital Markets Act, la DMA, que viene a completar la supervisión que desde la CNMC se puede realizar de estos mercados digitales, tanto desde la perspectiva del destinatario del servicio —sería más bien la DSA— como de la competencia y la contestabilidad de estos mercados, que es tanto la DMA como también las normas de defensa de la competencia.

El Reglamento DSA se sustenta en un sistema de protección de derechos *online* articulado en torno a una gran red de vigilancia y actuación, en la que las competencias se reparten entre la Comisión Europea y los Estados miembros para garantizar una aplicación coordinada y coherente, como si fuera una malla de contención que está tejida entre la Comisión Europea y las autoridades designadas en cada uno de los Estados miembros, que se llaman coordinadores de servicios digitales o DSC, por sus siglas en inglés. Para que esta malla de contención funcione sin fisuras todos los Estados deben tener las competencias atribuidas para poder aplicar la DSA. Cuando uno de los Estados no tiene esas competencias, la red pierde eficacia, se generan desequilibrios y efectos negativos que comprometen tanto la aplicación uniforme del marco regulatorio como la confianza en el propio sistema.

Voy a trasladar de qué forma la DSA y, por lo tanto, el proyecto de ley que la incorpora pueden marcar en este contexto un antes y un después. Hasta ahora, el principio imperante en el mundo digital era el de exención de responsabilidad de los prestadores de servicios intermediarios por los contenidos alojados o transmitidos por ellos, fueran plataformas, servicios de *hosting* o cualquier otro tipo de intermediario de servicios digitales. Es decir, los prestadores no están obligados a monitorizar la información que transmiten o almacenan y, en principio, no son responsables de ese contenido. Esta ha sido siempre la postura regulatoria en relación con los servicios de la sociedad de la información.

El Reglamento de Servicios Digitales viene a condicionar este principio al cumplimiento de obligaciones esenciales por parte de los prestadores de estos servicios. En primer lugar, les impone obligaciones de diligencia debida, con el fin de prevenir o mitigar el ataque a nuestros derechos *online* o permitir una rápida reacción para reparar un eventual atentado a estos derechos. La primera de estas obligaciones, la más básica, es la de establecerse o designar un representante legal en un Estado miembro de la Unión Europea al que se puedan dirigir las autoridades competentes del país de establecimiento sobre cualquier cuestión relacionada con las obligaciones y responsabilidades de la DSA. Ese representante legal debe actuar en todo momento como punto de contacto. Esta obligación tan simple pero tan lógica es trascendental, porque ya no va a ser posible que un ciudadano europeo quede desamparado por el mero hecho de que el prestador de un determinado servicio digital no puede ser contactado en ningún país de la Unión Europea. Este simple hecho, el no designar un representante legal en el espacio europeo, es ya en sí una infracción sancionable.

Voy a hacer un somero repaso de las obligaciones que impone la DSA a los prestadores de servicios en el entorno digital para entender el valor añadido de la DSA en esa creación del entorno digital seguro que les comentaba. Un primer grupo de obligaciones trata de abordar el problema del contenido ilícito difundido en la red, ya se trate de productos ilegales, de productos falsificados, de contenido que constituya delito de odio, abuso sexual infantil o cualquier otro que sea considerado ilícito en la normativa nacional o comunitaria. Y aquí voy a recalcar mucho «en la normativa nacional o comunitaria», porque la DSA no especifica qué es contenido ilegal, no nos dice que es ilícito; es la propia normativa aplicable en cada uno de los Estados miembros la que nos lo va a decir. La DSA nos ofrece herramientas para impedir la circulación de todo lo que se considere ilícito según esa normativa, para ponerle freno cuanto antes y para, poco a poco, ir frenando incluso su circulación. Entre estas obligaciones están, por ejemplo, las obligaciones que tienen las plataformas de ofrecer, dentro del servicio que nos dan —la red social o el buscador—, un sistema ágil, fácil y directo para poder reportar la existencia de contenido ilegal. Nosotros estamos, por ejemplo, haciendo una compra *online* en Amazon y vemos que están vendiendo medicamentos que se deben vender con receta médica. Eso es una venta ilegal. Tenemos que poder reportar en Amazon, tenemos que poder reportar de forma ágil que eso que se está transmitiendo es ilegal. Pero la plataforma no solo tiene la obligación de crear y mantener ese sistema de notificación, sino que, además, tiene la obligación de gestionar las notificaciones que le hagamos de forma diligente, objetiva y no arbitraria. También tiene que informarnos sobre el curso que ha dado a ese reporte.

cve: DSCD-15-CO-477

Esta obligación de mantener el sistema de reporte es una herramienta novedosa, que va a permitir involucrar de forma efectiva, además, a la sociedad civil, a todos y cada uno de nosotros, pero no solo. Por ejemplo, si una persona identifica en un *marketplace* como Amazon la venta de productos falsificados —antes decía medicinas, pero imaginemos que son productos falsificados—, con la DSA, esta persona tiene que poder notificar de forma sencilla a la plataforma la presencia de esa falsificación para que esta retire los productos, y la plataforma debe informar a esa persona si el producto ha sido retirado o no. La DSA establece que los prestadores mantienen la exención de responsabilidad —esto es muy importante— por el contenido ilícito que se aloja en sus servicios mientras desconozcan que este contenido ilícito existe. Por lo tanto, en el momento en que se reporta el contenido ilícito y no hay respuesta por parte de la plataforma, la exención de responsabilidad decae. Esta es la primera de las aplicaciones prácticas de la DSA.

El reglamento establece también la figura de los alertadores fiables. Son entidades certificadas para notificar contenido ilícito en sus ámbitos de especialidad. La DSA impone a las plataformas la obligación de gestionar de forma prioritaria las notificaciones que hagan estos agentes. Siguiendo el ejemplo de las falsificaciones, imaginemos una asociación especializada en propiedad intelectual o incluso una asociación de consumidores que puede solicitar su certificación como alertador fiable a cualquiera de los DSC —a nosotros cuando estuviéramos habilitados— en el ámbito de las falsificaciones, mostrando cierto *expertise* o conocimientos. Si obtiene esa certificación, se convierte en un canal prioritario para detectar y notificar el contenido ilícito, y los *marketplaces* tienen que tratar estas denuncias de forma prioritaria cuando les vengan de un alertador fiable.

Para salvaguardar los derechos fundamentales, la DSA también obliga a poner a disposición de los usuarios sistemas para la gestión de discrepancias sobre las decisiones que adopte la plataforma, como retirar contenido o cerrarme una cuenta, por ejemplo, y yo tengo que poder activar mi derecho de rectificación o de discusión tanto ante la propia plataforma como, en su caso, ante organismos extrajudiciales de resolución de litigios, que también serían certificados por el coordinador de servicios digitales. Por ejemplo, alguien que se dedique al arbitraje podría ser certificado. Estos mecanismos sirven para reforzar la capacidad de los usuarios y otros agentes —los alertadores fiables certificados, por ejemplo— para trasladar rápidamente a la plataforma la existencia de contenido nocivo y pararla de forma inmediata. Además, la DSA refuerza las competencias de las autoridades que ya a fecha de hoy son responsables —jueces, fiscales, fuerzas y cuerpos de seguridad del Estado, agencia del medicamento, autoridad de consumo, autoridad audiovisual— y pueden exigir que las plataformas les informen debidamente y en tiempo razonable sobre qué curso han dado a las órdenes que se les hayan transmitido; una orden, por ejemplo, de retirada de un contenido o de remisión de evidencias o, incluso, solicitudes de información sobre usuarios que puedan estar accediendo a la plataforma. Todas estas autoridades ya no van a recibir el silencio por respuesta, porque con la DSA los prestadores de servicios digitales tienen que poner a disposición de las autoridades, primero, un punto de contacto al que poder dirigir esas órdenes y esos escritos y, además, informar sobre el curso que han dado a esas órdenes y escritos. El incumplimiento reiterado de esta obligación de informar, además de las consecuencias que pueda tener en el derecho nacional no dar seguimiento a una orden, por ejemplo, de un fiscal o de un juez, puede también acarrear sanciones, en cumplimiento de la DSA, de hasta el 6 % del volumen de negocios del prestador a nivel mundial.

Un segundo grupo de obligaciones que impone la DSA a los prestadores son las de transparencia. Estas obligaciones abarcan múltiples ámbitos y favorecen a numerosos agentes. Les doy algunos ejemplos. El reglamento obliga a los prestadores —piensen todo el rato en, por ejemplo, plataformas— a publicar sus condiciones de moderación de contenidos o a declarar los motivos de por qué adoptan una determinada decisión de moderación, por ejemplo, eliminar una cuenta, retirar un contenido o desmonetizar un contenido por el cual el que lo había subido estaba cobrando. Además, los usuarios tienen derecho a presentar una reclamación contra estas decisiones. La imposición de estas herramientas y el procedimiento asociado supone un aumento de la transparencia en esa toma de decisiones que, a partir de ese momento, permiten al usuario saber el porqué o también prevenir una retirada ilegal de su propio contenido cuando considere que es legal. Pongo un ejemplo. Un profesor que tenga subido material escolar en un servicio de *hosting* —por ejemplo, Dropbox, que lo utilizamos muchos— puede encontrarse con que le cierren la cuenta por vulneración de derechos de propiedad intelectual. Antes de hacerlo, el proveedor debe informarle de por qué le cierran la cuenta. A lo mejor, en ese caso, el profesor simplemente citando la fuente deja de infringir y no le retiran el contenido.

cve: DSCD-15-CO-477

Una segunda fuente de transparencia se deriva de la obligación para las plataformas de ofrecer información sobre determinados ámbitos que están sujetos a un especial escrutinio. Por ejemplo, la publicidad que presentan, qué parámetros se emplean en sus sistemas de recomendación de contenido o información sobre los comerciantes que operan en sus plataformas en el caso de los *marketplaces,* por ejemplo. Otro grupo de obligaciones fundamentales son las establecidas de forma muy específica para las plataformas y motores de búsqueda de muy gran tamaño. Aquí estamos pensando en Alphabet, Meta, TikTok, Google, los que nosotros conocemos. No solamente las plataformas, sino los servicios que prestan las plataformas, que también son objeto específico de la DSA. Estas plataformas, que se llaman por sus siglas en inglés VLOP y VLOSE —*Very Large Online Platforms* y *Very Large Online Search Engines*—, son las que, por número de usuarios en su servicio en la UE, tienen más de 45 millones de usuarios de promedio y se considera que pueden entrañar riesgos de mucho más alcance y repercusión para la sociedad en su conjunto. Aquí están incluidas Meta, con servicios como Facebook o Instagram; Google, con servicios como Google Play, Google Maps, Google Shopping y YouTube; otras como la App Store de Apple, AliExpress, Amazon, y luego prácticamente todas las designadas de pornografía, Pornhub… También están Booking, Shein, LinkedIn, Bing, TikTok, StripChat, Zalando, Wikipedia, en definitiva, todas esas plataformas de muy gran tamaño a las que se les exige que lleven una labor de detección, análisis y evaluación de riesgos sistémicos. Al entender que ese impacto que pueden tener es tan grande, los riesgos que puedan derivar de, por ejemplo, un algoritmo programado de forma sesgada son ya riesgos de naturaleza sistémica. Los riesgos pueden ser derivados del diseño o también del funcionamiento de su plataforma; por ejemplo, si un uso nos lleva a una multiplicación de *chatbots* que hace que, por ejemplo, un contenido sea viralizado de forma automática. Esto es, cómo se está utilizando, cómo se está usando esa plataforma.

Además de hacer ese análisis para detectar los posibles riesgos sistémicos, tienen que aplicar medidas de mitigación de esos riesgos. Esto es crucial para abordar problemas tan complejos como, por ejemplo, la difusión de material de abuso sexual de menores, de discurso de odio, de desinformación; es decir, los riesgos específicos para los menores por el uso de las plataformas, pero también los riesgos para la salud mental de las personas o para la privacidad de los datos de las personas. Aquí el reglamento incorpora un mecanismo muy novedoso para hacer todavía más efectivas estas obligaciones, que es la obligación que tienen los prestadores de gran tamaño de dar acceso a determinados investigadores certificados a los datos o a los sistemas necesarios para que estos investigadores puedan acometer sus análisis e investigaciones relacionados con los riesgos sistémicos. Es decir, se otorga al mundo académico una palanca para poder acceder a las entrañas de las plataformas y contribuir al análisis de cómo estos agentes impactan en nuestras sociedades en estos ámbitos tan delicados para verificar, por ejemplo, que sus algoritmos no están sesgados.

Con un marco normativo tan potente, la siguiente pregunta es: ¿cómo se van a supervisar y a hacer cumplir todas estas obligaciones? Aquí es donde entrará en juego la CNMC. La institución que presido fue designada en enero de 2024 coordinador de servicios digitales en España, como requiere el reglamento —el DSC del que hablaba al principio—, pero, como ustedes saben, no estamos habilitados legalmente para actuar y, por tanto, no podemos ejercer la mayor parte de nuestras funciones, especialmente aquellas que afectan a los prestadores de servicios establecidos en España. Ahí podemos hablar de Glovo, Idealista, Milanuncios; en fin, hay un montón de plataformas que están establecidas en España. Tampoco podemos certificar a nuestros posibles alertadores fiables y a los órganos de resolución extrajudicial o a nuestros académicos. Esta situación, obviamente, cambiaría si se aprobase el proyecto para el que me requieren hoy. La DSA establece una serie de funciones, obligaciones y facultades para los DSC para los coordinadores de servicios digitales. Voy a destacar algunas de ellas que no estamos pudiendo ejercer por falta de habilitación. Estamos llamados a cumplir un papel de coordinación, tanto entre las autoridades internacionales —todos los DSC de los demás Estados miembros y la Comisión— como sobre todo nacionales —los que sean competentes para prevenir o reparar esos atentados a nuestros derechos *online* de los que hablaba— para conseguir que esa prevención o reparación sea más ágil, más inmediata y efectiva. Así, dependiendo del tipo de ilícito identificado en la plataforma, reforzaríamos la labor de la autoridad correspondiente. Si se trata de un problema de consumo, las autoridades de consumo, o de supervisión del sector financiero en los casos de fraude financiero, o de supervisión de aduanas, de inspección de productos, venta de medicamentos, lucha contra las falsificaciones, protección de los derechos de propiedad industrial e intelectual y, por supuesto, Fiscalía y fuerzas y cuerpos de seguridad del Estado para todo tipo de delitos: abuso infantil, ventas de drogas, estafas… La DSA es una norma

cve: DSCD-15-CO-477

horizontal que afecta a múltiples ámbitos en la medida en que regula prestadores que actúan e interactúan en toda nuestra vida, pero en el entorno digital. La CNMC debe funcionar como un engranaje que ponga en contacto a todos esos supervisores de cada una de esas obligaciones y mecanismos para poder actuar de forma rápida. Podemos coordinar y, de hecho, lo estamos haciendo en estos momentos. Estamos en contacto con la Fiscalía, estamos en contacto con muchas de estas autoridades, pero no estamos respaldados por un procedimiento sancionador que eventualmente vamos a tener que necesitar, porque el cumplimiento de todas estas plataformas, como todos sabemos, no se hace de forma voluntaria. Además, esta falta de habilitación nos impide tener personal cien por cien dedicado a la DSA y para una coordinación ágil y eficaz es preciso tener un personal dedicado a ello. Con lo cual, imaginen ustedes lo que podríamos hacer si, además de lo que estamos haciendo, trasladando a DSC de otros lugares, pudiéramos investigar, pudiéramos formar parte de los equipos inspectores que en estos momentos puedan estar investigando cada una de estas plataformas.

Tengo muchos más ejemplos de cosas que se están haciendo en otras jurisdicciones con DSC que sí que están habilitados. Si les interesa, en el turno de palabra les puedo contar qué es lo que nuestros colegas en otras jurisdicciones están pudiendo hacer y nosotros no.

Termino. Simplemente quería indicarles una vez más que España está perdiendo una oportunidad de formar parte de esta malla de protección en el mundo *online;* además, con las lenguas que utilizamos en España, con una de ellas, como es el español, tan potente, con todos los contenidos que también nos vienen de Iberoamérica, y se está perdiendo esa supervisión precisamente por no estar habilitados.

Muchas gracias, señorías.

El señor **PRESIDENTE:** Muchas gracias, señora Fernández.

A continuación, tienen un turno de intervención los distintos grupos. Lo habíamos fijado en cinco minutos, pero han pedido que sean un poco más amplios, así que ponemos seis, hasta siete como mucho en esta primera intervención.

Creo que no están en la sala representantes del Grupo Mixto, ni del Grupo Vasco, ni de Euskal Herria Bildu, ni de Junts per Cataluña, ni del Grupo Republicano. Con lo cual, tiene la palabra, en representación del Grupo Parlamentario Plurinacional SUMAR, la señora Andala.

La señora **ANDALA UBBI:** Gracias, presidente. Buenas tardes, señorías.

Buenas tardes, presidenta de la CNMC. En primer lugar, quería agradecerle que haya asistido hoy aquí, porque era importante la presencia de la CNMC como organismo coordinador de esa futura norma que ojalá consigamos aprobar pronto. Como usted ha dicho, es urgente porque, es verdad, nos viene algo importante, como es la regulación de todo el espacio digital, que ahora mismo es nuestra vida y nuestro día a día.

Creo que usted ha sido bastante clara. La verdad es que nosotras, nuestro Grupo Parlamentario, en su momento, cuando se designó la CNMC, teníamos ciertas dudas acerca de que asumiera más gestión de la que ya tiene, pero hoy me queda claro, como organismo coordinador, cómo puede delegar y cómo puede también coordinarse con otras instituciones.

Yo quería preguntarle algunas cosas que no me han quedado de alguna manera claras. ¿Cómo vais a poder vosotras, en un hipotético caso, detectar ese contenido ilegal? Me preocupa esa externalización de la supervisión, que no tengáis vosotras esa capacidad. Sé que, si se os dota de presupuesto y de capacidad, se podrá, pero me gustaría saber cómo planteáis ese modelo. ¿Van a ser detectores o servicios fuera de la CNMC u organismos delegados? ¿Cómo va a ser esa detección de contenido ilegal para reportárselo a las herramientas de notificación? Porque, como bien sabes, el *reporting* requiere mucho trabajo y, sobre todo, operatividad. ¿Pensáis crear vuestras propias herramientas para esa detección? Porque creo que es importante que resida en lo público la detección del contenido ilegal y no dejarlo a voluntades, porque, como bien sabes, las plataformas están dejando la verificación de Twitter en cualquier cuñado digital. Entonces, es importante que nosotros no cometamos ese patrón de delegarlo incluso en empresas privadas que puedan tener sus propios intereses en esa supervisión. Creo que ahí tenemos que poner el foco, en no delegarlo en manos privadas y estar atentas. Desde luego, nuestro grupo estará atento en esa parte.

Por otro lado, también has puesto énfasis en la parte de supervisión de algoritmos de estas plataformas. A nosotras nos preocupa siempre cómo va a ser de efectiva la norma para supervisar plataformas en casas extranjeras. Como bien sabe usted, se han puesto multas a estas plataformas. ¿Cómo está siendo? ¿Están, de verdad, respondiendo? ¿Está pudiendo hacerlo la Unión Europea? Te lo

cve: DSCD-15-CO-477

pregunto desde el desconocimiento. ¿Están cumpliendo? ¿El régimen sancionador de la Unión Europea está funcionando? Cuando escuchamos en los medios que se ha impuesto una multa de 1000 millones a Twitter porque no se sabe cómo está priorizando el contenido, ¿eso está siendo factible? ¿Cómo va a ser esa conversación? Como estamos hablando de una norma que aún no está, estoy hablando de futuribles, pero me gustaría saber cómo va a ser esa supervisión en el seno de la Unión Europea. De hecho, me gustaría saber por usted cuáles son esos pilotos que ya están funcionando y que pueden ser modelo para nosotras. Espero que nos inspiren para que esta norma salga por consenso algún día y conocer el punto de vista de cada uno.

Por último, me gustaría saber cómo va a ser vuestra coordinación con la Agencia de Supervisión de Algoritmos de Inteligencia Artificial. Entiendo que la agencia va a supervisar algoritmos de la AI Act, la normativa de inteligencia artificial de la Unión Europea, pero me gustaría saber cómo va a ser esa coordinación porque van a ir muy de la mano. De hecho, la inteligencia artificial podría servir como supervisor del propio contenido ilegal en el punto uno que le planteaba a usted. Comprendiendo que es un futurible y que usted probablemente necesite que esto se ponga en marcha para que pueda ser, es importante saber cómo va a ser esa coordinación y cómo va a ser la entrada de la academia a supervisar esos algoritmos, porque esas empresas no tienen un *open source;* si hacen un *open source* —o sea, una apertura de su código al público— es para que las comunidades de desarrolladores amplíen su propio proyecto personal o, bueno, de propiedad de empresa. ¿Cómo vamos a encajar la academia en supervisar sus algoritmos? Porque tenemos una gran preocupación con las plataformas inmobiliarias. De hecho, en todas las plataformas que utilizan algoritmos, ahora mismo el mayor escollo no es la regulación, sino cómo están alimentando sus propios algoritmos. No sé cómo lo están afrontando otros países y le pregunto si usted lo sabe.

Ya he consumido tres minutos y creo que usted ha sido bastante clara, así que nada más.

Gracias.

El señor **PRESIDENTE:** Gracias, señora Andala.

Por el Grupo Parlamentario VOX, tiene la palabra el señor Sáez.

El señor **SÁEZ ALONSO-MUÑUMER:** Gracias, señor presidente, y gracias también a la señora Fernández por su comparecencia en esta comisión.

Señora presidenta, la CNMC se convierte en pieza clave para la gobernanza democrática en servicios digitales y medios de comunicación en España. Señora Fernández, usted sabe de la importancia de que existan reguladores independientes para que los mercados sean competitivos. Señora Fernández, se lo dijimos en anteriores comparecencias y ahora lo repetimos: nos preocupa la colonización de las instituciones y de los organismos públicos por parte del Partido Socialista. Señora Fernández, nos preocupa porque el Partido Socialista ha demostrado que su único interés es reforzar el control sobre las empresas del sector. Señora Fernández, nos preocupa porque no existe ningún interés por parte del Partido Socialista en preservar el buen funcionamiento del mercado en interés de consumidores y usuarios. Señora Fernández, nos preocupa porque el Partido Socialista no entiende lo que significa el principio de certidumbre jurídica, que es el que garantiza que atraigamos inversiones. Señora Fernández, nos preocupa porque sin certidumbre jurídica la inversión buscará otros lugares y la economía y el empleo del país se verán afectados. Señora Fernández, nos preocupa el ataque a la independencia del Poder Judicial que se está llevando a cabo por parte de este Gobierno, un ataque claro a la certidumbre jurídica. Señora Fernández, nos preocupa porque lo que quiere realizar el Gobierno es un plan de control de los medios al más puro estilo totalitario. Señora Fernández, nos preocupa que el Gobierno pretenda utilizar a la CNMC para dar una apariencia de independencia a un control que pretende ejercer sobre todos los medios. Señora Fernández, nos preocupa la independencia de un organismo en el que se han nombrado consejeros que no consideramos que sean independientes —y así lo hicimos notar en la comparecencia— de los partidos políticos que apoyaron sus candidaturas. Señora Fernández, nos preocupa que la CNMC reciba presiones que impidan garantizar, preservar y promover el correcto funcionamiento de todos los mercados y sectores productivos, la transparencia y la competencia efectiva. Señora Fernández, nos preocupa porque lo que vemos y lo que se ve a nivel internacional es que España ha retrocedido diez posiciones en el año 2024 en el índice de percepción de la corrupción elaborado por Transparencia Internacional. Señora Fernández, nos preocupa que este Gobierno utilice el paraguas de la CNMC para imponer su ideología. Señora Fernández, nos preocupa porque para el Partido Socialista y sus socios la independencia de las instituciones es una amenaza a su forma de Gobierno y a su concepto de

cve: DSCD-15-CO-477

democracia. En estos momentos, señora Fernández, es cuando se debe demostrar independencia y esperamos sinceramente que la CNMC lo demuestre.

Y termino con unas palabras suyas: Es la certidumbre jurídica lo que va a garantizar que tengamos las inversiones necesarias; los mercados fuertes y trabajando en plena competencia son el mejor instrumento en el medio y largo plazo, y el papel de los reguladores es clave.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señor Sáez.

Por el Grupo Parlamentario Socialista, tiene la palabra el señor Rojo.

El señor **ROJO BLAS:** Muchas gracias, señor presidente. Señorías, muy buenas tardes.

Desde luego, tengo que agradecer a la señora Fernández su intervención, una intervención detallada y rigurosa, aportando muchísimos datos. Y, además, algo que consideramos importante: que en este mundo digital, en el que a veces se utilizan tecnicismos, hay que explicar muy bien lo que nos estamos jugando con el desarrollo de este proyecto de ley. Es decir, la ciudadanía debe entender lo que tenemos entre manos. Esto es lo que nos tiene que preocupar realmente más allá de otras consideraciones que ahora hacía el señor Sáez, desde luego creo que poco pertinentes, con respecto a la seguridad jurídica de los ciudadanos en un aspecto global como es el mundo digital. En mi intervención voy a poner en valor y voy a reflejar algunos de los aspectos que considero importantes para eso, para que la gente entienda la importancia de este proyecto de ley, es decir, la importancia de un desarrollo seguro del espacio digital, también en nuestro país, en algo que es global.

El mundo digital avanza a pasos agigantados, es cambiante y nos obliga, desde luego, a adaptarnos al mismo ritmo, un ritmo que, desde el punto de vista digital, es vertiginoso. Es indudable que este mundo digital ha transformado nuestra forma de vida en muchos campos, como pueden ser la medicina, la ciencia o incluso el entretenimiento. Hemos dado saltos de gigante en este aspecto y se han dado avances que han mejorado nuestra vida sin lugar a dudas. Pero la aparición de las redes sociales merece un tratamiento específico. Lo que empezó como un medio de expresión, de difusión de ideas y de conocimiento, de conexión con otras personas ha abierto la puerta a un mundo que, por desgracia, no es todo lo ético que nos gustaría. Las redes sociales también han generado una potencial audiencia, pero una audiencia que, sin saberlo, a veces acaba siendo cautiva porque ve limitada su capacidad para elegir el contenido de lo que quiere escuchar y ver. La definición de los algoritmos y su retroalimentación propicia la difusión de las noticias falsas y la desinformación, lo que a gran escala puede provocar hasta la injerencia en procesos electorales, y esto no es ciencia ficción, esto ya lo hemos vivido. Al mismo tiempo, la reducción en el control y verificación de los contenidos por parte de las grandes plataformas favorece, desde luego, los comportamientos más dañinos, y esto nos tiene que preocupar especialmente por los menores. Esas son las preocupaciones reales que debemos tener. Por ello, se hace necesaria una regulación que proteja los derechos de la ciudadanía, porque los derechos no pueden quedar supeditados a los intereses económicos de las grandes empresas multinacionales. Esto es algo que la Unión Europea ha tenido claro y se ha puesto manos a la obra, y es una prioridad de este Gobierno y así lo viene demostrando durante los últimos años.

Como saben, en esta comisión tenemos como tarea tramitar el proyecto de ley para la mejora de la gobernanza democrática en servicios digitales y medios de comunicación, que, desde luego, va a facilitar la denuncia de contenidos ilícitos, como usted bien indicaba, en estas grandes plataformas digitales. Por eso, además hemos creído oportuna esta comparecencia de hoy y, desde luego, estamos satisfechos con esta exposición inicial porque marca lo que tenemos que hacer con respecto a la ciudadanía: ponerla en alerta de lo importante que es aprobar este proyecto de ley. Este proyecto adaptará el ordenamiento jurídico español, como bien ha dicho, a la normativa europea sobre servicios digitales, fundamentalmente acorde a lo establecido en el Reglamento Europeo de Servicios Digitales, que es lo que se conoce como la DSA. Este reglamento va a imponer, principalmente a las plataformas digitales, la obligación de poner en práctica nuevas medidas para proteger mejor a los usuarios y aumentar la transparencia y la privacidad. Esto es lo que tienen que saber los ciudadanos y las ciudadanas. Con esta ley abordaremos retos de nuestro espacio digital muy importantes para nuestras vidas, como es la desinformación, la protección a los menores, los discursos de odio y la vulneración sistemática de la privacidad. Todo ello lo ha indicado usted en su intervención, pero hay que reiterarlo porque ahora son aspectos esenciales de la vida diaria en este mundo que vivimos. Se trata de que la democracia defienda el pluralismo, en el que creemos y

cve: DSCD-15-CO-477

firmemente, y los derechos digitales, pero que también se defienda a la democracia del acoso, de la manipulación o del odio a los ciudadanos y las ciudadanas.

Desde nuestro punto de vista, lo ha explicado todo y muy bien la señora Fernández, porque, miren, la Comisión Nacional de los Mercados y la Competencia, la CNMC, a la cual este proyecto de ley le otorga las competencias de control, supervisión, inspección y sanción, velará por que los proveedores de servicios digitales cumplan con el Reglamento Europeo de los Servicios Digitales, y esto lo tienen que saber los ciudadanos. Y en este punto quiero resaltar que vamos tarde. La CNMC podría contar con la habilitación legal necesaria hace meses, y si se ha tenido que incluir en este proyecto de ley es porque algunos grupos políticos decidieron, de forma irresponsable, no convalidar el Real Decreto 9/2024, norma que incluía ya dicha habilitación, de forma que podríamos estar ya trabajando en esta línea. Desde luego, ahora ya no tenemos excusas. Como representantes públicos tenemos una responsabilidad y la sociedad civil lo está esperando. Imagino que conocerá, señora presidenta —y todos los grupos políticos lo saben—, que hemos recibido una carta firmada por numerosas organizaciones y expertos a título individual que nos recuerdan la necesidad de llevar a cabo las reformas necesarias para que la CNMC pueda cumplir con las obligaciones que establece la DSA y, en última instancia, proteger a la ciudadanía frente a amenazas. Como saben, la Comisión Europea ha abierto diferentes investigaciones de mercado a los gigantes del sector y ha impuesto ya sanciones, entre otras a Meta, una multa de 797 millones de euros por infringir las normas de defensa de la competencia de la Unión Europea, y más recientemente a X, con un importe de 120 millones de euros por incumplir la Ley de Servicios Digitales.

Señorías, termino. Estamos ante algo muy importante y trascendental y tenemos que estar a la altura de las circunstancias, y aquí voy a señalar lo que ha dicho el presidente del Gobierno de España, Pedro Sánchez, que ha sido tajante en este sentido al asegurar que en España la ley está por encima de cualquier algoritmo o cualquier gran plataforma tecnológica y que quien vulnere nuestros derechos pagará las consecuencias. Esa es la línea a seguir y todos nos debemos comprometer.

Muchas gracias y seguimos avanzando, que es lo más importante. **(Aplausos).**

El señor **PRESIDENTE:** Muchas gracias, señor Rojo.

A continuación, para concluir el primer turno de intervención de los grupos, por el Grupo Parlamentario Popular tiene la palabra el señor Cortés.

El señor **CORTÉS CARBALLO:** Buenas tardes.

Muchas gracias, señora Fernández, por acudir a esto que no sé cómo denominar, porque lo primero que hay que preguntar es qué hacemos aquí. Yo les voy a contar qué hacemos aquí, puesto que ninguno de mis compañeros ha tenido el valor de contarlo. Mire usted, el presidente del Gobierno anuncia una comisión de investigación contra Meta por poner en riesgo los datos de 6 millones de españoles. Después de eso, el Grupo Socialista se encuentra que aquí no hay ni comisión de investigación, ni Meta, ni nada que valga. Entonces se les ocurren —voy a contar cómo ha sido— unas comparecencias con motivo de la ley de gobernanza de los medios y los servicios digitales, razón por la cual después vamos a acordar los ponentes; curiosamente, ahora mismo estamos celebrando una sesión totalmente irregular, puesto que no hemos aprobado ningún ponente, pero usted está aquí y el siguiente también. **(Aplausos).** ¿Qué quiere decir esto? Que estamos dando coartada a un titular mediático del presidente del Gobierno, que dijo: sujétame el cubata que voy a traerme aquí a Mark Zuckerberg a comparecer en el Congreso. **(Aplausos).** Es eso lo que estamos haciendo aquí, no nos engañemos. Así de simple. Razón por la cual, fíjese, el portavoz del PSOE no le ha hecho ni una sola pregunta. ¿Se ha dado cuenta? No le ha preguntado absolutamente nada; absolutamente nada. Esta es la realidad de lo que hacemos aquí.

Luego, la segunda parte: la ley de gobernanza de medios y servicios digitales. Creo que así le han puesto ustedes a la ley. Esa es, digamos, la excusa, el marco en el que hacemos las comparecencias. Pues fíjese, usted lo ha dicho, usted ha hablado de la DSA: un reglamento de obligado cumplimiento. No hace falta ninguna ley para eso. De hecho, lo ha comentado abiertamente: en un real decreto se metieron las competencias de la CNMC para poder ejercer esa ley. No hace falta ninguna ley. Y si nos vamos a la ley de libertad de medios, de nuevo, otro reglamento. Tampoco hace falta ningún desarrollo reglamentario. Y precisamente para lo poco que hace falta el desarrollo reglamentario, que es para definir, por ejemplo, cuál es el proceso por el que se puede excepcionar o no el derecho del periodista a no revelar su fuente, mira por dónde eso no lo aborda. Luego, cuénteme usted qué sentido tiene esa ley, en la que precisamente lo más importante de todo es lo que usted ha comentado, doce meses después de haber traído un real decreto ómnibus trampa, que por eso se votó en contra. ¿Qué trabajo le costaba al Gobierno hacerlo a la

cve: DSCD-15-CO-477

semana siguiente, cuando nos hemos pronunciado públicamente, incluso con distintas proposiciones no de ley, sobre que estábamos a favor de apoyar estos cambios en los estatutos de la CNMC? Pero ustedes, como Gobierno, no han traído en doce meses ni un solo real decreto, que hubiese sido aprobado *ipso facto.* Luego, no vengan aquí a hablarme de la importancia de la ley.

Por tanto, ¿para qué sirve esa ley? Lo ha apuntado VOX. Sirve como coartada para intentar controlar a los medios de comunicación privados. ¿Por qué? Aplicamos un reglamento de obligado cumplimiento y aplicamos otro reglamento de obligado cumplimiento, y precisamente las cuatro cosas que habría que definir por parte del país no las incluye el texto. De hecho, usted, señora Fernández, no ha hecho ni una sola referencia al proyecto de ley. Por eso entiendo su posición. No sé si, desgraciadamente, el Grupo Socialista no la pedía a usted. Como usted bien sabe, no se la ha convocado a usted, se ha convocado a un subdirector de la CNMC. Quizá le habrán dicho: mire usted, no toque nada de la ley de medios, que eso no nos interesa. Pues yo, desgraciadamente, le voy a tener que preguntar por el objeto de la comparecencia ya que, como digo, todo lo que le he contado es la coartada de lo que hacemos aquí sentados. No nos engañemos. Un titular de un presidente que no sabía dónde se metía y una orden al grupo parlamentario —oye, búscale una excusa, un refuerzo legal— cuando todos sabemos que en unas ponencias como estas no hay obligación por parte del ponente de comparecer. Y ustedes han pedido a Mark Zuckerberg, VOX ha pedido a Elon Musk… ¡Venga, sujétame el cubata otra vez! Entonces, como ustedes comprenderán, eso es una tomadura de pelo en todos los aspectos. Pongamos las cosas en su sitio.

Ahora, señora Fernández, por intentar ser productivos, ya que estamos aquí —aunque la intervención que ha tenido hoy ya nos la ha hecho en varias ocasiones; ya ha puesto de manifiesto antes la urgente necesidad de estas competencias, pero entiendo que ha dicho: bueno, voy a repetir lo que ya he dicho en las comparecencias—, vamos al proyecto de ley. Sabemos todos cuál es la urgencia, pero no me ha hecho referencia, como le digo, a absolutamente nada del proyecto de ley, que se suponía que es el marco por el que estamos aquí. Entre otras cosas, sí ha hablado de la delegación de competencias, pero no ha hablado de todo lo demás, donde la CNMC también tiene la designación de la aplicación de la Ley de Libertad de Medios de la Unión Europea. Entonces, me gustaría que, en su siguiente intervención, se centrara precisamente en esas nuevas competencias que se le dan por ahí.

Como decía, al ser reglamentos, el 8 de agosto de este año ya se empezaba a aplicar la ley de medios. Por lo tanto, ¿qué ha cambiado? ¿Qué están haciendo ustedes como CNMC? Puesto que la ley ya se está aplicando, ¿qué aportarían?, ¿qué pueden hacer?, ¿qué no pueden hacer? Igual que ha hecho un resumen de lo que pueden hacer con la DSA, me gustaría que volviera a hacer un resumen de qué pueden o qué no pueden hacer sin esta ley con las competencias de la CNMC, en cuanto a la libertad de los medios de comunicación.

También, quiero recordar que llevamos desde febrero de 2024 con la DSA en vigor, desde 2024, y este Gobierno no ha tenido tiempo, desde febrero de 2024, a traer un real decreto con los cuatro artículos que modifican las competencias de la CNMC. Esto es un hecho; desde el 17 de febrero de 2024. Muy ocupados habrán estado ustedes para no poder traerlo en todo este tiempo.

Yo lo doy por hecho, pero le pregunto, ¿no cree que este proyecto de ley no deja de ser otra cosa que un intento de meter artículos para controlar a los medios de comunicación privados? El Consejo de Estado ha hecho un informe —no sé si usted ha tenido conocimiento de este informe—, en el cual, de alguna forma, habla de posible legalidad de la evaluación de concentraciones, de que el registro obligatorio de medios podría restringir el ejercicio del periodismo y de que el régimen sancionador es ambiguo. Le pregunto por esas tres cosas que son, precisamente, las que la CNMC tendrá que ejercer, entiendo yo, cuando tenga esas competencias. ¿Qué opina? Porque se va a encontrar que tiene que aplicar una legislación que el propio Consejo de Estado valora de esta manera: posible legalidad, restricción de derechos, régimen sancionador ambiguo… O sea, va a ser un problema para usted, según cuenta el Consejo de Estado. Entiendo que tendrá una opinión sobre esto.

Otra pregunta también directa. ¿Cree que la CNMC es la idónea para aplicar la ley de libertad de medios, cuando estamos hablando no solo de medios audiovisuales, sino de todos los medios? Pregunto. *A priori* suena raro. Pero, bueno, supongo que también tendrá una opinión. Cuando se enteró de que iba a ser el organismo designado, alguna opinión tendría a ese respecto.

Y, luego, me surge una duda —y con esto termino— la Ley Europea de Libertad de Medios, en su artículo 4, precisamente, habla de una excepción, que es el derecho de no revelar fuentes periodísticas, un tema tan de moda ahora por el juicio del fiscal general. Establece cuatro posibles excepciones que los

cve: DSCD-15-CO-477

países tendrán que decidir. Como vamos con retraso y, de hecho, en esta ley tampoco se ha decidido y sabe Dios cuando se aprobará alguna ley que lo decida, la pregunta es: ¿en qué situación queda ese artículo? Porque, si no se decide cuál es la excepción, ¿qué pasa?, ¿qué se aplica?, ¿no hay excepciones?, ¿seguimos como estamos?, ¿se puede acoger cualquiera? Tengo mis dudas jurídicas y no sé si usted, en este aspecto, me puede dar luz.

Y, por último, un consejo…

El señor **PRESIDENTE:** Muchas gracias. Hay ahora un segundo turno.

El señor **CORTÉS CARBALLO:** Vale, gracias. **(Aplausos).**

El señor **PRESIDENTE:** A efectos de que conste en acta y para evitar confusiones, en primer lugar, quiero aclarar que esta comisión ha sido convocada de forma absolutamente regular, de acuerdo con lo que nos han indicado los letrados de la Cámara. Y, en segundo lugar, lo que decidió la Mesa fue convocar a la Comisión Nacional de los Mercados y la Competencia y, por lo tanto, se dirigió a su presidenta, que ha decidido comparecer en persona, cosa que le agradecemos.

Las demás comparecencias serán tratadas a continuación en la Mesa y portavoces que ha sido convocada al finalizar esta sesión.

Tiene la palabra, por un tiempo aproximado de diez minutos, para contestar a estas consideraciones y preguntas de los grupos, la señora Fernández.

La señora **PRESIDENTA DE LA COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA, CNMC** (Fernández Vicién): Muchas gracias.

En primer lugar, contesto a las preguntas de la señora Andala. En cuanto a detección del contenido ilegal y cómo hacerlo, es cierto que, en la medida en que todos vivimos en el mundo *online,* si no hay colaboración de todos va a ser imposible. O sea, no podemos estar todos con mil ojos al mismo tiempo en todas partes. Y, por eso, el propio diseño de la DSA incorpora a la propia sociedad civil con alertadores fiables, que debe ser verificada su independencia y verificada su *expertise;* a los académicos, que también deben ser certificados para garantizar, fundamentalmente, estas dos cuestiones, su *expertise* y su independencia.

Luego, contamos, por supuesto, con todas las demás autoridades que son competentes por razón de la materia. Si los contenidos ilegales son de naturaleza audiovisual, la propia CNMC, como reguladora audiovisual, será la que detecte esos contenidos y pueda retirarlos; si estamos hablando de medicamentos, pues la Agencia del Medicamento; o si estamos hablando de productos de consumo, pues el que corresponda. En definitiva, lo que hace la DSA es vertebrar esa posible estructura, que nos permita llegar, entre todos, a la detección inmediata de esos contenidos ilegales para poderlos retirar cuanto antes; establecer los mecanismos para que esa retirada se haga de forma efectiva y para ver que, efectivamente, las plataformas están cumpliendo con esas obligaciones. Pero es cierto que hace falta la colaboración de la sociedad civil.

Por la parte que a nosotros nos toca, efectivamente, estamos desarrollando herramientas para poder investigar directamente. De hecho, en la parte audiovisual, precisamente porque tenemos que estar permanentemente analizando los contenidos, ya estamos lanzando los códigos de corregulación y estamos empeñados en el etiquetado de esos contenidos. Pero, al mismo tiempo, estamos desarrollando nuestras propias herramientas, porque sin eso es imposible.

En esta parte voy a hacer un apunte que es muy importante, porque estamos viendo en otros Estados miembros, donde nuestros colegas están empezando ya a reportarnos experiencias, que, por ejemplo, en todo el tema de moderación de contenidos lo que es bastante habitual es que se haga de forma robótica, es decir, que no sean las personas, sino que sean las máquinas. Y esto lo que están constatando muchos de nuestros colegas es que no funciona. Si, al final, es exclusivamente una máquina la que está permanentemente verificando los contenidos y no hay intervención personalizada, esas son lecciones que ya vamos aprendiendo y que, desgraciada o afortunadamente, para cuando estemos habilitados habrá ya un cierto *track,* con lo cual estamos siguiéndolo para podernos aprovechar de esas experiencias.

En cuanto a procedimientos sancionadores y si están funcionando, la comisión ha abierto ya más de quince procedimientos sancionadores a diferentes VLOP y VLOSE y ha lanzado requerimientos para ver si están cumpliendo para, en su caso, abrir sanciones a todas, excepto a Wikipedia, que es la única que no lo ha recibido. Ya ha sancionado a algunas.

cve: DSCD-15-CO-477

En el caso concretamente de X es un caso muy claro de patrones oscuros, porque daba a entender que estaba verificando la información que aparecía como verificada, cuando en realidad no lo estaba verificando; era falso. Con lo cual, ya no solamente son los 120 millones de euros, que podemos pensar todos que es muy poco; habrá multas más elevadas, pero esa no es la cuestión. La cuestión es, primero, el mensaje que se manda a los usuarios de X constatando que esa información no está verificada. Segundo, el descrédito que supone para la plataforma, en un mundo en el cual todo el mundo puede decirle a todo el mundo: no, no te creas nada porque esto ya se ha dicho que no.

Y al mismo tiempo, una cuestión que para mí es esencial, es que el propio Tribunal de Justicia de la Unión Europea ya ha declarado, sobre todas las cuestiones que en su momento le sometieron tanto Meta como otras plataformas en relación con el posible atentado a sus derechos —por ejemplo, el hecho de dar acceso a sus datos o a subsistemas para que los investigadores pudieran analizarlo era una de las reclamaciones que tenían las plataformas diciendo que eso atentaba contra sus derechos—, que las obligaciones que ha impuesto la DSA no violan derechos y, por lo tanto, tienen que cumplirlas. O sea, que, de alguna manera, tenemos ya ciertas declaraciones por parte del Tribunal que nos van a permitir seguir en la aplicación de la norma, y a la Comisión Europea darle esa fuerza.

En cuanto a la coordinación con la agencia de supervisión de algoritmos, en cuanto esté creada, funcione y nosotros estemos habilitados, si tiene funciones a la hora de verificar los algoritmos, obviamente, será una de aquellas autoridades con las que nos coordinaremos, sin duda.

Sobre la entrada de la academia. ¿Cómo va a entrar? De hecho, ya hay determinada normativa de actos delegados, que se van adoptando en los distintos grupos de trabajo de la DSA, y ya hay uno en el que se está discutiendo cuáles tienen que ser las características para que estos académicos se puedan certificar. Una vez que sean certificados, la DSA les obliga a dar acceso, y ya el Tribunal de Justicia ha dicho que no se violan derechos de la plataforma por dar acceso. Con lo cual, lo iremos viendo, pero, obviamente, ante un incumplimiento, lo que quedará es una posible infracción por parte de la propia Comisión Europea.

Creo que con esto he respondido a sus preguntas.

En cuanto a la intervención del señor Sáez, de VOX, no puedo estar más de acuerdo con usted con que el papel de los reguladores es clave. La independencia de los reguladores es vital y el mensaje que se manda, precisamente, tanto para inversores como para la propia sociedad de que la regla de derechos se cumple, es lo que motiva que estemos todos hoy aquí. Y yo creo que la propia Comisión Nacional de los Mercados y de la Competencia ha dado pruebas del estricto cumplimiento de la ley, de su independencia. Y le puedo asegurar que si esta casa lo hace —porque son ustedes los que, en definitiva, nos tienen que encomendar a nosotros las funciones de la ley—, las seguirá ejerciendo con la misma independencia, con la misma profesionalidad y con el mismo cumplimiento normativo que le caracteriza. No puedo estar más de acuerdo con usted en que las instituciones deben ser fuertes e independientes para vertebrar la arquitectura de un país. No le puedo decir más que esto.

En cuanto a los comentarios del señor Rojo, la situación en la que estamos ya reclama actuación, y eso yo creo que todos lo estamos pensando. Si leo la cantidad de expedientes abiertos por mis compañeros de los DSC de otros Estados miembros, no ya solamente con las grandes plataformas, hay montones de redes sociales de ámbito muchísimo más reducido que también tienen *challenges* para nuestros *teenagers,* para nuestros adolescentes con gran peligro. Si están establecidas en nuestro territorio, las tendríamos que estar parando nosotros. Por ejemplo, en Alemania hay un montón de actuaciones que ha llevado a cabo el propio DSC alemán para parar ciertos contenidos en redes sociales de menores y de *teenagers.* Es un ejemplo de las múltiples cosas que vemos en el equipo provisional que hemos montado en la Comisión para poder ir colaborando, que se nos llevan los demonios, pero es lo que es. En definitiva, es una realidad imparable y yo creo que tenemos que estar todos atentos para evitar que en el mundo *online* se cometan las atrocidades que se están cometiendo.

Me voy a referir ahora a la intervención del Grupo Popular. Es verdad que los dos son reglamentos de ejecución y aplicación inmediata, salvo en la parte que tiene que ver con las competencias que tienen que desempeñar las autoridades nacionales designadas, tanto el DSC como la autoridad designada por la EMFA. Toda la parte procesal de estos procedimientos de investigación requiere, obviamente, un control de legalidad y un nivel de rango normativo de ley, sea real decreto ley o ley, me da igual. O sea, ande o no ande, me da igual. La cuestión es que tengamos las competencias. Yo no puedo abrir un procedimiento sancionador sin una ley que me habilite. Actualmente, no tengo esa ley, no tengo ese rango legal que me lo permita. Lo mismo para las investigaciones, los requerimientos. Bueno, hoy discutían en uno de los

cve: DSCD-15-CO-477

grupos de trabajo de los DSC si nosotros podíamos o no podíamos recibir, por ejemplo, solicitudes de posibles académicos para su certificación, aunque no les podamos certificar; si podíamos encaminarlas a otros DSC para intentar que nuestros académicos no se quedasen fuera. Y está en duda, ni siquiera eso. Y eso no es un procedimiento sancionador. Es decir, necesitamos una adaptación y la necesitamos de forma urgente. La aplicación directa, en cuanto a los procedimientos de investigación, sí la tiene la propia Comisión Europea, pero para la parte que compete a las autoridades nacionales, desgraciadamente, no. Y me valdría un real decreto perfectamente.

También es verdad que ha habido una notificación de la sociedad civil pidiendo el desgaje de lo que es la parte de EMFA, de la parte de la DSA, porque al parecer la parte de la DSA, al ser una norma de naturaleza transversal y no tanto del contenido sino del mecanismo para poder actuar, puede suscitar menos problemas que quizá la EMFA. Son ustedes los que deciden cómo adoptan sus leyes. Lo único que les puedo decir es que para nosotros es vital poder actuar y que, además, a diferencia de EMFA, donde solamente hay dos Estados miembros ya plenamente habilitados, en la DSA solo somos tres los no habilitados: Portugal, nosotros y creo que es República Checa el tercero. Claro, cuando nos sentamos en las reuniones del *board* y todo el mundo empieza a contar lo que están haciendo y nosotros nos miramos así... Y corremos, además, el riesgo de que se alojen en nuestros territorios plataformas indeseadas, porque no podemos actuar. O sea, todos esos riesgos hay que medirlos. Si para esto hace falta separar una cosa de la otra, bienvenido sea, yo no tengo ningún problema.

Le digo cuáles son las competencias en materia de EMFA que nos adjudica el proyecto de ley para la mejora de la gobernanza democrática. Quizá la más importante es que se tiene que crear un registro de medios de comunicación, y ese registro de medios de comunicación se le encomienda a la CNMC. Ese registro estatal pretende que todos los medios de ámbito estatal se inscriban y mantengan actualizada la información sobre estructura de propiedad y los ingresos derivados de la publicidad institucional. Eso es lo que busca fundamentalmente. Ese es un registro de libre acceso y, además, se van a crear registros autonómicos que deben estar coordinados con este registro central, en los que se inscribirán los prestadores de servicios de medios de comunicación de ámbito autonómico.

Además, nos otorga la supervisión del cumplimiento de obligaciones de los prestadores de servicios de medios de comunicación en el ámbito estatal. En concreto, nos otorga también la supervisión para la garantía de la libertad editorial y la divulgación de los conflictos de intereses para que no haya injerencia en esa línea editorial. Nos otorga también competencias para evaluar el impacto sobre el pluralismo mediático de las operaciones de concentración en los mercados, no tanto desde la perspectiva de competencia —que ya la tenemos—, sino desde la perspectiva del pluralismo de los medios de comunicación, cuando se cumplan determinados umbrales. También tenemos que supervisar el cumplimiento —y esta creo que es muy importante— de las obligaciones que se imponen a los proveedores de sistemas de medición de audiencia, porque es precisamente la medición de audiencia la que permite generar recursos a los medios de comunicación.

Hasta la fecha ha habido una queja sistemática de falta de transparencia sobre las metodologías aplicadas precisamente por estos proveedores de sistemas de medición. Entonces, lo que nos otorga la ley es una supervisión sobre cómo los responsables de dichos sistemas deben facilitar a los prestadores de servicios el acceso a la información exacta, detallada, exhaustiva, inteligible y actualizada, sobre qué metodología están utilizando precisamente para medir esas audiencias. Porque no es lo mismo medir una audiencia de un medio generalista que, por ejemplo, de una revista especializada, y las consecuencias que eso tiene para la generación de ingresos en un caso o en el otro también son distintas. Además, nos permite exigir que haya una auditoría independiente sobre estas metodologías, y luego nos otorga competencias para promover códigos de autorregulación y corregulación, cosa que ya estamos haciendo en nuestra vertiente de autoridad audiovisual, donde estamos intentando, además, que el etiquetado de contenidos allá donde somos competentes —televisiones, pero también plataformas de intercambio de vídeos— nos permita, por ejemplo, enlazar con sistemas de verificación de edad de menores, etcétera.

Lo que no incluye el proyecto de ley son muchas de las cosas que tiene el propio Reglamento EMFA y que debería incluir, que, además, se le deben atribuir a una autoridad independiente —creemos que nosotros estaríamos bien posicionados para ello—, como, por ejemplo, la salvaguarda del funcionamiento independiente de los prestadores del servicio público de medios de comunicación, la supervisión de la asignación de fondos públicos para la publicidad estatal o la garantía del derecho de los usuarios a personalizar la oferta de medios de comunicación. Esto no está en la ley, está en el reglamento y se va a tener que incluir de alguna manera.

cve: DSCD-15-CO-477

En definitiva, como le decía al diputado de VOX, nosotros estamos para cumplir la ley, la ley que se decida en esta casa y lo que ustedes nos manden. Por lo tanto, si tienen que modificar esa ley, pues modifíquenla. Si consideran que un cumplimiento adecuado tanto del propio Reglamento EMFA como del DSA requiere añadir más funciones, pues nosotros estamos a su disposición.

El señor **PRESIDENTE:** Muchas gracias, señora Fernández.

Tal y como también hemos comentado, los grupos tienen ahora un turno breve de dos minutos por si quieren hacer alguna pregunta o pedir alguna aclaración.

Grupo Plurinacional SUMAR. **(Denegación).** No.

Grupo VOX, señor Sáez. **(Denegación).** Tampoco.

Por el Grupo Socialista, señor Rojo.

El señor **ROJO BLAS:** Gracias, señor presidente.

Fíjense, nos tiene que preocupar que no ha habido ni una sola alusión por parte de VOX —previsible— ni del Grupo Popular —me preocupa más— a la importancia de proteger a la ciudadanía, especialmente a los menores. Es que eso es lo que nos tiene que preocupar. Además, es triste, y hago esta intervención con lamento, que el portavoz del Grupo Popular haya acusado de estar aquí en una comparecencia irregular cuando ha tenido que ser el presidente, y le agradezco además su...

El señor **PRESIDENTE:** Se trata de un turno de aclaraciones a la compareciente. Le agradecería que no entrase en un debate que está cerrado.

El señor **ROJO BLAS:** No, no, me dirijo a la compareciente que está aquí. Los dos grupos políticos, el Grupo Popular y el Grupo Socialista, pidieron la comparecencia de la Comisión Nacional de los Mercados y la Competencia, y también parece que ha dudado que sea pertinente que venga aquí a sede parlamentaria, y digo que ha acusado de irregular también esta comparecencia. Ya le digo que agradezco, además, la apreciación de su propio partido político.

También se han lanzado aquí acusaciones graves, y creo que es importante que la ciudadanía lo conozca. Es verdad que en esta comparecencia estamos hablando de los derechos digitales como un reto y un hándicap que tenemos como país. Desde luego, lo tenemos que abordar de una manera determinante. Así, el Gobierno y el Partido Socialista lo están promoviendo. Allí están, lógicamente, las acciones que han llevado a cabo, porque ustedes votaron en contra del Real Decreto 9/2024 hace un año aproximadamente. Podrían haber votado a favor, y ya tendríamos esa habilitación.

Pero digo que me preocupa porque, en un sistema democrático, tenemos claro que para garantizar —como no puede ser de otra manera— la libertad de expresión y el pluralismo tenemos que evitar la desinformación y las noticias falsas. ¿Se sienten ustedes cómodos en un sistema en el cual van proliferando las noticias falsas y la desinformación como un peligro, desde luego, relevante para los derechos de la ciudadanía? ¿Se encuentran ustedes cómodos en este sentido? Creo que lo que hace el proyecto de ley es adaptar normativa europea en ambos sentidos —en los servicios digitales y también en los medios de comunicación— para tener más seguridad jurídica y más libertad con derechos básicos y sagrados que, desde luego, siempre tenemos que componer.

Por tanto, vuelvo a insistir —acabo ya, señor presidente—: lo importante es garantizar los derechos y proteger a la ciudadanía en el espacio digital. Eso es lo que el Partido Socialista está promoviendo y siempre va a promover sin agitar y sin confundir, como hacen otros partidos políticos. **(Aplausos).**

El señor **PRESIDENTE:** Muchas gracias.

Para concluir el turno de intervención de los grupos, tiene la palabra el señor Cortés, por el Grupo Parlamentario Popular.

El señor **CORTÉS CARBALLO:** Muchas gracias por su respuesta, pero lamento decirle que no me ha contestado a ni una sola de las preguntas que le he hecho. He pedido su apreciación, su opinión, y se ha limitado a explicarme lo que dice la ley de las competencias nuevas de la CNMC y un tema muy interesante sobre lo que no dice la ley que debería decir. Aprovecho para hacer una pregunta más: ¿no le parece precisamente muy raro que todo lo que tiene que ver con el control al propio Gobierno no lo meten en la legislación?

Para terminar, quiero decirle desde aquí que, uno, la preocupación de la protección de menores en Internet la hemos demostrado en nuestras enmiendas, precisamente en la ley de protección al menor en

cve: DSCD-15-CO-477

Internet, que es el ámbito donde hay que tenerla. Dos, nos hemos pronunciado públicamente más de una vez sobre que, si este Gobierno en dos años hubiera traído un real decreto con estas competencias de la CNMC para aplicar la DSA, lo hubiéramos aprobado sin dudarlo. Tanto es así que lo hemos dicho en proposiciones no de ley en comisión. Por tanto, le lanzo de nuevo el guante: saque de aquí las competencias a la CNMC para la DSA, intente mejorar esta ley, a ver si puede y a ver si son capaces de aprobarla. Porque me temo, señora Fernández, que, como lo mezclen todo, va a pasar otro año más y no vamos a poder aplicar todo lo que le preocupa al portavoz del Grupo Socialista en cuanto a la desinformación, control de plataformas, etcétera, etcétera. No es que no sean capaces, es que no quieren traer esto por separado, y sigo sin entender por qué.

Ruego que, si puede, me conteste a alguna de las preguntas. **(Aplausos).**

El señor **PRESIDENTE:** Muchas gracias, señor Cortés.

Para cerrar, las intervenciones con sus contestaciones, tiene la palabra la señora Fernández.

La señora **PRESIDENTA DE LA COMISIÓN NACIONAL DE LOS MERCADOS Y LA COMPETENCIA, CNMC** (Fernández Vicién): La verdad es que lo que me pide su señoría es que haga una evaluación del proyecto de ley que está hecha en el informe de la propia CNMC sobre el anteproyecto de ley. Él es el que analiza artículo por artículo y da una visión. Casi le voy a remitir al propio informe de la CNMC en el que valoramos el proyecto.

En la parte de EMFA, le he extractado nuestra opinión del propio informe, porque, efectivamente, hay una serie de competencias que no se determinan para quién van, simplemente. Llamamos la atención porque ese anteproyecto de ley puede no ser el cumplimiento efectivo del reglamento de EMFA.

En cuanto a lo demás, lo único que les puedo decir es que estamos en una situación en la que España está ante el Tribunal de Justicia por incumplimiento del reglamento DSA. EMFA no me consta, pero en cuanto a la DSA sí estamos en una última fase ya de decisión. En cualquier momento, el Tribunal de Justicia adopta una sentencia condenando a España con multa coercitiva diaria. La verdad es que me gustaría que, antes de que eso pudiera llegar a pasar, se pusieran ustedes de acuerdo y procurasen que, de alguna manera, pudiésemos ejercer las funciones que nos encomienda la ley.

Muchísimas gracias.

El señor **PRESIDENTE:** Muchas gracias, señora Fernández. Agradecemos mucho su contribución a la comisión.

Si les parece, interrumpimos durante tres minutos para poder despedir a la señora Fernández y que se incorpore el siguiente compareciente. **(Pausa).**

— DEL SEÑOR VALLINA RODRÍGUEZ, PROFESOR ASOCIADO DE INVESTIGACIÓN, IMDEA NETWORKS. POR ACUERDO DE LA COMISIÓN DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL. (Número de expediente 219/000542).

El señor **PRESIDENTE:** Continuamos con las comparecencias previstas para el día de hoy en relación con el proyecto de ley por la que se modifican diversas disposiciones legales para la mejora de la gobernanza democrática en servicios digitales y ordenación de los medios de comunicación.

El siguiente compareciente citado es don Narseo Vallina Rodríguez, profesor asociado de investigación de IMDEA Networks.

Tiene la palabra por un tiempo aproximado de veinte minutos.

El señor **VALLINA RODRÍGUEZ** (profesor asociado de investigación, IMDEA Networks): Muchas gracias, presidente y señorías. **(Apoya su intervención en una presentación digital).**

Es todo un honor para mí poder presentar los resultados científicos de un trabajo que hemos hecho en colaboración con la Universidad de Louvain, en Bélgica, y con la Universidad de Radboud.

En concreto, trata sobre un abuso que hemos detectado que involucraba a dos proveedores de tecnología concretos: Meta y Yandex. En este caso, estas compañías lo que estaban haciendo era una unión entre los paradigmas de rastreo que existen tanto en la web como en aplicaciones móviles, con el fin de desanonimizar con nombres y apellidos la actividad de los usuarios en la web.

Mi ponencia aquí es en relación con mi capacidad como investigador, y voy a intentar ser completamente neutral y ceñirme únicamente a los aspectos científicos y técnicos. Cualquier aspecto relacionado con si esto es un incumplimiento de una legislación existente o no es algo que debería

cve: DSCD-15-CO-477

competer, por ejemplo, a la Agencia Española de Protección de Datos o a la CNMC. Obviamente, voy a intentar mantener el rigor técnico durante toda la ponencia.

Para comenzar, me gustaría presentar Meta Pixel. El Meta Pixel es un *software* o un producto desarrollado por Meta que permite a los proveedores de páginas web —por ejemplo, un periódico o un hotel— obtener analíticas e información sobre la actividad de los usuarios dentro de la página web. Para ello, se basa fundamentalmente en una *cookie* que vamos a llamar FBP y FBC, que lo que hace es obtener información única, en teoría con una validez que se ciñe únicamente a la página web en la que está presente —si has estado en una página de un hotel, esta *cookie* solo tendría relevancia dentro de esa página web—. Meta indica que tiene una validez de unos noventa días. Sin embargo, en función de cómo los desarrolladores integren esta tecnología pueden también obtener información adicional, por ejemplo, un *e-mail* que pueda estar introducido en un formulario de registro, que permitirá identificar a los usuarios a lo largo de todas las plataformas.

Hemos observado un nuevo paradigma de monitorización de las actividades de los usuarios en la web. Normalmente, cuando un usuario visita una página web se generan unas *cookies* y esas *cookies* no van con nombre y apellido necesariamente, sino que son, en teoría, anónimas; no obstante, sí permiten realizar una trazabilidad de las actividades de un usuario concreto en una página web. Incluso, muchos usuarios son conscientes de los riesgos de privacidad que esto puede involucrar y pueden implementar o usar capacidades habilitadas en los navegadores web, como el modo incógnito o incluso eliminar las *cookies.*

Hemos observado que Meta y Yandex estaban abusando al habilitar unas capacidades ofrecidas por el sistema operativo —y también los navegadores— para poder conectar el contexto del navegador web con el contexto de la aplicación nativa, en este caso Facebook e Instagram. En las aplicaciones nativas estas pueden tener acceso a la identidad de los usuarios, porque los usuarios están registrados en ellas. Entonces, al vincular todas las *cookies* —que en teoría son anónimas—, con esta identidad es posible desanonimizar el usuario que ha visitado una página web concreta. Además, esto permite vincular de forma inequívoca y persistente a lo largo del tiempo toda la actividad del usuario, incluso si el usuario borra las *cookies,* porque están asociadas a su identidad potencialmente. Esto afecta a poblaciones vulnerables y, de hecho, tenemos evidencia que sugiere que incluso páginas web públicas orientadas a poblaciones que necesitan un tratamiento para una enfermedad crónica pueden obtener esta información. Por lo tanto, hay un montón de usuarios —incluso de poblaciones vulnerables o que necesitan proteger de algún modo su privacidad— que están siendo expuestos a este tipo de tecnología y, como sabemos por el caso de Cambridge Analytica, también pueden ser víctimas de discriminación o de otro tipo de abusos en la red. Y no lo digo yo, esto también lo dice Google.

Cuando hicimos el descubrimiento varios medios cubrieron esta investigación y los representantes de Google hicieron esta cita, que dice: los desarrolladores de este informe usan capacidades presentes en muchos navegadores a través de iOS y Android en formas que no son esperables y que, además, violan, evidentemente, nuestros principios de seguridad y privacidad.

Ahora, permítanme explicarles cómo funciona técnicamente. Les pido perdón si esto resulta demasiado denso, voy a intentar hacerlo de la forma más accesible posible, sin perder ningún tipo de rigor. Imaginemos que nosotros estamos en un navegador y vamos a una página web, como www.congreso.es. Hay una resolución de ese dominio a una IP y nosotros nos conectamos a esa IP, y ahí vamos a obtener el contenido. Pero, además, hay una IP especial que se llama la IP de *localhost,* que es 127.0.0.1, que hace referencia a nuestro propio dispositivo. Entonces, esto permite que dos aplicaciones que corran dentro del mismo dispositivo puedan comunicarse entre ellas usando las tecnologías que se utilizan para conectarse a Internet. Lo curioso es que estas tecnologías fueron desarrolladas en los noventa, cuando se estandarizaron todos los protocolos de Internet, y entonces se consideraba todas las comunicaciones en *localhost* como comunicaciones confiables, porque en los noventa nadie preveía que íbamos a tener una plataforma en la que íbamos a ejecutar cientos de aplicaciones con un montón de servicios de analítica y de publicidad. Por tanto, utilizando este canal, es posible intercambiar las *cookies* que se generan en el navegador web con la identidad del usuario en la aplicación nativa, y esto viola todos los principios de privacidad y seguridad que existen en los sistemas operativos: el *same-origin policy,* el modo incógnito, incluso el *sandbox,* que es un principio de seguridad esencial en todos los sistemas operativos y que hace que dos programas no puedan hablar entre ellos sin ningún tipo de control.

Después de hacer un análisis empírico, hemos descubierto que solo hay dos organizaciones que estaban realizando este tipo de operación a escala: Yandex, que es un servicio de tecnología de publicidad

cve: DSCD-15-CO-477

y analítica de origen ruso, y Meta. De acuerdo con BuiltWith, que es una página web que indica las tecnologías que están siendo utilizadas para crear ciertos servicios, Yandex está presente en unos 3 millones de páginas web y Meta Pixel en unos 5,8 millones de páginas web. Pero estas son estimaciones, porque no sabemos realmente en qué número de páginas web pueden estar presentes.

Además, hay un aspecto curioso: para que esto sea efectivo necesitamos que estas tecnologías —como el Meta Pixel— estén presentes en un montón de páginas web, porque de esta forma pueden acceder a mucha más información de muchos más usuarios. Además, necesitamos una aplicación que sea suficientemente popular para poder recibir esas conexiones que vienen del navegador. Por otro lado, como he mencionado previamente, los usuarios se introducen y se registran en las aplicaciones nativas, por lo que tienen acceso a sus identidades. Y no solo eso, también las plataformas móviles ofrecen ciertos identificadores, que se llaman Mobile Advertising IDs, que los usuarios pueden resetear en cierto momento —como si eliminásemos las *cookies—,* pero casi nadie lo hace; para ello hay que ir a un menú específico de privacidad, tanto en Android como en iOS, y eliminar ese valor.

Un aspecto curioso en el caso de Meta es que todo parece una estrategia organizada, porque involucra tres servicios. Es decir, no es un error, es algo que requirió cierta coordinación a nivel corporativo porque hubo que hacer cambios tanto en Meta Pixel como en las aplicaciones de Facebook e Instagram, y estas aplicaciones normalmente tienen líneas de producto o equipos de desarrollo diferentes.

Creo que el impacto de nuestro descubrimiento ha sido bastante significativo para lo que se suele hacer en el área de privacidad y seguridad. Hemos influido positivamente en mejoras de seguridad en Chrome y en todos los navegadores que se utilizan en Android. También hemos notificado a casi todas las DPA de Europa —a través también del EDPB— e incluso internacionales, fuera de la Unión Europea, y sabemos que hay varias demandas colectivas en marcha en Estados Unidos, en Alemania y en Canadá.

Ahora, permítanme explicarles el contexto de por qué hemos llegado a esto. El primer anuncio de publicidad lo tenéis aquí. Apareció en octubre de 1994, en una página web que se llama hotwired.com. Ya en los noventa se dieron cuenta de que era posible utilizar las *cookies* para fines secundarios, en el mismo modo que están utilizando los canales de *localhost* para un fin que no es el esperable. Entonces, en este caso, las *cookies* se convirtieron en un mecanismo bastante efectivo para también monitorizar la actividad de los usuarios dentro de una página web, pero esto era insuficiente. Entonces, en la primera década del año 2000 empezaron a surgir las primeras redes de publicidad y los primeros servicios de analíticas, que se beneficiaban de su presencia en muchas páginas web para obtener mucha más información de los usuarios. Esto se convirtió en un problema y motivó muchos cambios y muchas mejoras de privacidad en casi todos los navegadores. Este es el caso, por ejemplo, de Meta Pixel y de Yandex Metrica. En 2010, esto evolucionó también a lo que se conoce como *real-time bidding,* es decir, en función de las actividades que el usuario realiza en la web, nuestro *slot* en una página web tiene cierto valor. Y para eso, para darnos información o anuncios que sean relevantes para nosotros, necesitan hacer una combinación y un procesado de todas las *cookies,* así saben qué nos interesa y nos ofrecen el anuncio más relevante para nosotros.

El caso de las tecnologías móviles es un poco diferente, porque tenemos lo que se conoce como el sistema de permisos. Cuando nosotros instalamos una aplicación, esta requiere unos permisos y el usuario puede dárselos o no. Lo que ocurre es que, muchas veces, estos permisos dan acceso a sensores como la geolocalización o incluso el micrófono, pero no solo eso, es que, cuando damos un permiso a una aplicación, todas las librerías de terceros que el desarrollador mete en esa aplicación también heredan todos los permisos que le damos a la aplicación. No hay separación de privilegios. Entonces, cada vez que instalamos una aplicación estamos dando los datos a un montón de organizaciones y realmente no somos conscientes de este impacto.

Además, existe, como he mencionado antes, el concepto de *sandboxing,* que se traduce en que dos procesos no puedan hablar directamente entre ellos porque, obviamente, podrían interferir o acceder a datos de otra aplicación, lo que sería una brecha de privacidad y de seguridad bastante significativa.

La tecnología está evolucionando en lo que se conoce ahora como *cross-platform tracking.* Los navegadores cada vez están poniendo más barreras para que las *cookies* de terceros no sean útiles. Podemos verlo en Safari, podemos verlo también en el anuncio de Chrome del *privacy sandbox.* Esto fuerza un poco a la industria a moverse a otro paradigma completamente diferente, que es lo que se conoce como *ID bridging.* Entonces, lo que hacen —gracias a la potencia del *Machine Learning* y de otras tecnologías— es poder combinar todas estas señales que ellos están cogiendo sobre nosotros para crear unos perfiles que sean muy detallados sobre nuestras actividades. Concretamente, cada vez que damos

cve: DSCD-15-CO-477

un *e-mail,* incluso en un hotel o un restaurante, esta información puede estar siendo compartida con este tipo de organizaciones. El *e-mail,* una vez que se computa lo que se conoce como el *hash,* es un identificador único y es fácilmente reversible. Entonces, tiene una capacidad de poder obtener toda nuestra actividad en todas las plataformas, incluso con programas de fidelización u otros tipos de programas. Esto es lo que nos lleva a *Local Mesh,* que es el ataque que hemos descubierto.

Como he mencionado, las aplicaciones móviles pueden acceder al *localhost* y, además, necesitamos una aplicación que corra como un servidor. Para eso necesita correr constantemente en el fondo para poder recibir comunicaciones de otros entornos. Y esto, en el caso de Android, se puede realizar sin ningún tipo de permiso. Además, los navegadores ofrecían capacidades para poder conectarse en *localhost.* Entonces, cualquier navegador podía permitir al código JavaScript de cualquier *tracker* coger información y poder intercambiarla directamente con la aplicación nativa. Además, como hemos dicho, el sistema operativo, aunque tenga el *sandbox,* permitía este tipo de comunicaciones sin ningún tipo de verificación ni de control.

Este es el diagrama de flujo de lo que observamos en el caso de Meta. Las aplicaciones de Meta las instalamos y nos registramos en ellas, por lo tanto, tienen nuestra identidad. No conozco a ningún usuario que utilice un servicio de Meta en el navegador; normalmente utilizamos las aplicaciones nativas. Entonces, cada vez que esta aplicación se va al fondo, lanza el servidor para escuchar comunicaciones del navegador. Cuando un usuario visita una página web con el Meta Pixel embebido por parte del desarrollador, genera la *cookie* FBP y la envía a los servidores de Meta directamente. Pero además la envía por *localhost* a la aplicación nativa. Y para esto utilizan una tecnología que se utiliza para comunicaciones *peer to peer.* Por ejemplo, si usáis Google Meet o una plataforma de videoconferencia en el navegador, se requiere crear conexiones entre pares. Entonces, utilizan esta tecnología de una forma muy concreta para poder embeber el valor de la *cookie* en la petición que va a la aplicación nativa. Por lo tanto, sugiere que hay cierta intencionalidad en el comportamiento. Y este es además el estándar del WebRTC, que es este protocolo que dice que este parámetro no puede ser modificado, pero, en el caso de Meta, estaban de forma intencionada usando una capacidad que veremos luego para realmente intercambiar esta información. Y, una vez que llega a la aplicación nativa, la agrega con nuestra identidad y la envía al servidor. El valor de la *cookie,* como está en los dos lados, es trivial, prácticamente, hacer una unión de toda la actividad que estamos realizando en la página web.

La primera evidencia de que esto estaba ocurriendo fue en septiembre de 2024. Y para ello tuvimos que requerir la información que está disponible en el HTTP Archive, que es un archivo de páginas web históricas. Pero, curiosamente, en noviembre de 2024, cambiaron del protocolo HTTP, que es el que se utiliza por defecto para conectarnos a servicios web, por WebSocket. No sabemos la razón, pero creemos que esto está motivado por una cuestión de transparencia. Muchos desarrolladores que utilizan el píxel en su página web empezaron a preguntar en los foros de desarrollo de Meta por qué estaban observando comunicaciones en *localhost* desde su página web, y era fácil atribuir este comportamiento a Meta. Entonces, esto era muy fácil porque, si eres un desarrollador de página web, puedes ir al navegador al modo de *debuggeo* para ver cómo se comporta la página web y puedes ver este tipo de conexión. Sin embargo, al cambiar a WebSocket, esto se hace mucho más opaco porque no aparece por defecto. Y, de hecho, en la parte de arriba podemos ver un usuario que dice que parece que este comportamiento se apagó o se deshabilitó el 1 de octubre, pero en realidad no fue eso, sino que Meta cambió a otro protocolo.

Curiosamente, estos desarrolladores indican que en los foros nunca hubo una respuesta por ningún representante de Meta. En noviembre de 2024, también tenemos evidencia de que cambiaron a WebRTC, que fue el protocolo que os mencioné antes en el diagrama de flujos. Y, en mayo de 2025, ya estaban implementando una capacidad nueva, un protocolo nuevo que no llegaron a desplegar porque —gracias a nuestro informe— Meta paró este tipo de operación.

Aquí podemos ver estadísticas disponibles directamente desde Chrome, porque Google tiene esta plataforma para ver cómo ciertas tecnologías web están siendo utilizadas. En este diagrama de barras, en rojo, podemos ver las peticiones que se hacen desde navegadores Chrome en móvil y, en azul, las que se hacen desde un *desktop,* desde un portátil. Y aquí podemos ver cómo el uso de esta función concreta que permitía a Meta embeber el valor del píxel en la comunicación se corresponde durante los periodos en los que realmente observamos este comportamiento, y se apagó justo el 3 de junio, que fue cuando salió en los medios.

Además, parece que Meta estaba intentando acceder de forma concreta a navegadores Android. Y aquí podemos ver cómo tenía un código que identificaba si el usuario estaba conectándose desde un

cve: DSCD-15-CO-477

navegador en Android. Esto también es técnicamente posible en iOS, pero por algún motivo decidieron no desplegar esta tecnología en iOS, posiblemente por los controles que Apple implementa a la hora de permitir ciertos comportamientos, como por ejemplo la ejecución de un servidor en el fondo.

También hay un aspecto curioso que es si esto se realizaba por defecto o si había alguna noción de consentimiento. Entiendo que el consentimiento es un concepto legal —no voy a entrar en eso—, pero lo que hicimos fue un experimento para ver si la comunicación ocurría por defecto tan pronto como la página web se cargaba en un navegador, sin ni siquiera pinchar en el *banner* de las *cookies.* Y aquí podemos ver que, en la mayoría de las páginas web en las que el Meta Pixel estaba embebido —en un 75 %—, esta comunicación ocurría por defecto. Por lo tanto, no estaban permitiendo a los usuarios ejercer su derecho a la privacidad.

Nuestra responsabilidad fue divulgar esto a todas las plataformas afectadas y, hacia mayo del 2025, cuando ya teníamos evidencia de que esto era un abuso bastante concreto, hicimos una notificación a todos los navegadores que estaban potencialmente afectados y, gracias a ello, tanto Firefox como Chrome hicieron parches de seguridad para limitar este abuso.

DuckDuckGo y Brave son dos navegadores que están orientados a la privacidad y no eran vulnerables a este ataque, pero únicamente porque tienen listas negras de dominios que están asociados con *trackers* y no permitían ni siquiera que se ejecutase esto, pero la capacidad de poder comunicarse en *localhost* sí es posible porque son navegadores que están basados en Chrome. Aun así, la comunicación en *localhost* es posible en la plataforma Android y también en iOS. Como he dicho, hicimos una notificación también a todos los reguladores con los cuales tenemos un contacto directo. Tuvo un impacto mediático significativo, sobre todo por el artículo en *Ars Technica,* que es un medio norteamericano especializado en tecnología. También salió en *El País.* Y aquí podemos ver también cómo Privacy International, que es una ONG de privacidad, definía que Meta y Yandex rompen la seguridad para salvar su *business model.* Esto lo dicen ellos, no lo digo yo. Además, también hicimos el esfuerzo de comunicar este tipo de abuso a los diferentes organismos de estandarización de protocolos y de tecnologías en Internet, como el IETF y el W3C, a los que les presentamos nuestros descubrimientos.

Para finalizar, es un paradigma de rastreo del que prácticamente podemos ver cómo todos los índices sugieren que es intencionado y, además, está diseñado para ser opaco y romper las garantías de seguridad y privacidad de casi todas las plataformas. No solo era invisible a los usuarios, parece ser que también fue diseñado para ser invisible a los desarrolladores y a los reguladores. No hay ningún tipo de consentimiento ni de *awareness,* no fuimos capaces de encontrar ninguna información en la documentación de Meta sobre esta capacidad.

El impacto en España puede ser de varias decenas de millones, teniendo en cuenta las estadísticas de la CNMC sobre el número de usuarios que tienen dispositivos Android en España y también la penetración de Instagram y de Facebook en nuestro país. Esto muestra que es necesario cerrar un vacío regulatorio, pero también desarrollar tecnologías que permitan a los reguladores, de alguna forma, hacer el cumplimiento regulatorio, porque son tecnologías muy complejas y están hechas para ser un tanto engañosas, para que no sean fácilmente identificables. En el caso de Yandex, hay otras características que hicieron el descubrimiento mucho más complejo.

Finalizo señalando que la Carta de los Derechos Fundamentales de la Unión Europea, en los artículos 7 y 8, reconoce el respeto de la vida familiar y privada y también la protección de datos de carácter personal. También tenemos un marco legislativo integrado por el GDPR, el ePrivacy, DSA y DMA. Desde mi perspectiva de científico creo que tenemos la ley, pero nos faltan los policías. Necesitamos también desarrollar tecnología escalable, porque son mecanismos muy difíciles de monitorizar y también de detectar.

Para terminar, quiero dar las gracias a mis colaboradores y manifestar que estoy encantado de poder responder cualquier pregunta que tengan.

El señor **PRESIDENTE:** Muchas gracias, señor Vallina.

A continuación, por un tiempo aproximado de siete minutos, los grupos presentes en la sala tienen ocasión de formular las preguntas y observaciones que estimen convenientes.

En primer lugar, por el Grupo Plurinacional SUMAR, tiene la palabra la señora Andala.

La señora **ANDALA UBBI:** Buenas tardes, profesor. Lo primero, muchas gracias.

Comparto que hablar de tantas cosas, como de informática, obviamente, es complejo. Me parece muy inteligente por parte de ellos —obviamente, es premeditado—, tirar del *hosting* local, y no a través de un

cve: DSCD-15-CO-477

API, para enviar toda esa información a sus propios servidores y que se haya elegido unas tecnologías y no otras. Esto pone el acento en lo que siempre nos dicen: que son empresas sin ningún interés, que simplemente… Sin embargo, de hecho, ellas participan de muchos procesos regulatorios. Con esta exposición que acabas de hacer se pone el acento sobre la importancia de que no son actores ajenos y que buscan un modelo productivo y, sobre todo, voraz, porque a través de este intercambio entre *localhost* probablemente están haciendo un *broadcast* entre miles y miles de servidores. Y no quiero ni imaginarme toda la información que han estado recogiendo. Vosotros los habéis detectado hace un año, pero conseguir toda esa información nuestra que puedan tener matcheada a través del *localhost* resulta brillante por su parte, como también lo es por la vuestra que lo hayáis podido ver —no sé si has dicho en Stack Overflow o en su propia plataforma—, porque, si no han llegado a contestar, no sé cómo habéis podido detectar ese cambio a *WebSockets.* Si es por el mensaje de ese usuario, tengo fe en que, como las comunidades de desarrolladores son tan frikis, también están supervisando y ayudando a la academia. Y no sé cómo podemos atraer hacia las organizaciones públicas a esas comunidades de desarrolladores, que responden ante tantas dudas —sabes que siempre gastamos la broma de decir que me he sacado la carrera en Stack Overflow— para combatirlo. No sé cuál es realmente vuestra relación con la institución pública. Me gustaría saber cómo lo habéis hecho llegar, si fue a través de una colaboración, y también si tenéis una comunicación fluida con la Unión Europea. Habéis dicho que habéis comunicado esta publicación, y no sé si vuestro trabajo encuentra líneas de financiación o de trabajo para poder sacar esto a la luz, que me parece importante, porque resulta fundamental para el desarrollo de políticas públicas.

Y, si habéis salido vivos de esto, mi pregunta es cuál ha sido la respuesta de estas plataformas, si os han llegado a contestar, porque esto es algo reputacional. Es muy complejo de entender, y muchas veces decimos que nos escucha el móvil. Pero no, no nos escucha; vosotros acabáis de descubrir que es a través del *localhost.* Simplemente, están parasitando nuestra casa a través de los móviles y están accediendo absolutamente a toda esa información. ¿Ellos os han contestado cuando han recibido esta información o, simplemente, han parado de hacerlo? ¿O lo siguen haciendo porque no hay una regulación? Me preocupa si esto se sigue haciendo hoy en día.

Aquí lo dejo, aunque, la verdad, preocupadas, a la vez que esperanzadas ya que lo hayáis podido descubrir. Como bien dices, tenemos que desarrollar herramientas que puedan ir de la mano de comunidades que lo puedan detectar de manera más precoz.

Gracias.

El señor **PRESIDENTE:** Muchas gracias.

Por el Grupo Parlamentario VOX, tiene la palabra el señor Rodríguez.

El señor **RODRÍGUEZ ALMEIDA:** Muchas gracias, señor presidente.

Muchas gracias, señor Vallina Rodríguez.

Brevemente ha dado usted datos muy elocuentes sobre una situación que plantea muchas incógnitas y preocupaciones. El mundo digital está cambiando muchos comportamientos, muchos hábitos y fenómenos, como en lo relativo a las decisiones de compra. Entiendo que todo ello trae causa precisamente de la irrupción de las tecnologías sobre las decisiones de compra y la posibilidad de acceder a una información muy precisa respecto a preferencias de compra, hábitos de compra y capacidad económica. Creo que es sobre esto de lo que estamos hablando, de si esa información debe ser salvaguardada o si debe ser requerido el consentimiento, como ha explicado. Le agradezco el matiz, porque creo que está muy bien traído que es un concepto jurídico, un bien jurídico que hay que proteger.

Me ha gustado mucho su referencia a poblaciones vulnerables, al hecho de que se está accediendo a una información sobre población vulnerable, y, en este sentido, le agradecería que, si pudiese, desarrollase un poco la definición de esa población. Creo que todos entendemos más o menos a quiénes se puede referir, especialmente a menores, pero también estoy pensando en los muchos trastornos o dificultades que, efectivamente, pueden meter en un problema no pequeño a la persona si se le presentan las cosas sin los filtros que facilita la realidad física y que la inmediatez del uso de tecnologías digitales no permite.

Con respecto a la cifra del 75,8 % de páginas web que por defecto lo tienen incorporado, especialmente el Meta Pixel, me gustaría poder confirmarlo, porque es un dato muy preocupante, si es como lo ha dicho, es decir, si no hay consentimiento por parte del usuario para prestar esa información. Insisto en que estamos hablando acerca del consentimiento, que creo que es el eje más importante sobre el que hacer pivotar el tema que estamos tratando. Si puede confirmar que, efectivamente, no hay ningún consentimiento por parte del usuario, y no me refiero al momento de acceso, sino con carácter previo, que entiendo que puede ser un

cve: DSCD-15-CO-477

argumento para algún operador; si se ha producido un consentimiento generalizado al configurar el dispositivo, no al acceder a cada página web, es decir, si se ha sistematizado o se ha prestado previamente en la configuración del sistema operativo del dispositivo o navegador con el que se está accediendo a esas páginas web posteriormente. Si es posible que se haya prestado previamente, de modo que entonces ese dato del 75,8 % debería ser matizado o podría ser puesto en cuestión.

Hablaba usted del 1 de octubre como fecha en la que Meta anuncia que había cambiado e intervenido, pero lo que ha puesto de manifiesto es que simplemente ha cambiado esa cadena y ahora es distinta. Una pregunta que creo que también es de interés es si esto sigue pasando a día de hoy.

Ha hablado de las adaptaciones que se han hecho en los navegadores. Es un gráfico muy elocuente y, además, ha señalado en qué han consistido las mejoras de seguridad en cada uno de esos navegadores. Pero, después del descubrimiento de la amenaza o el riesgo que han descrito ustedes en su estudio, creo que interesa saber si esto sigue pasando a día de hoy. Y, si es así, en qué en qué volumen, o si prácticamente ha sido erradicado, porque, efectivamente, los dos navegadores que siguen manteniendo cierta vulnerabilidad convendrá conmigo en que son minoritarios respecto al uso.

También me ha sorprendido mucho la diferencia estadística respecto a navegadores en dispositivos móviles y en dispositivos de escritorio. Esa gráfica marca una gran diferencia. En rojo están los móviles y en azul los de escritorio. ¿Podría explicar un poco a qué se debe tanta diferencia? Entiendo que hay interés respecto al tipo de dispositivo que esté manejando el usuario y creo que vale la pena que se explique por qué hay tanta diferencia entre uno y otro.

Ha dicho que no somos conscientes de la magnitud del problema. Le pregunto si usted tiene alguna sugerencia para aumentar esa conciencia sobre la magnitud del problema y la información que se está facilitando, es decir, qué podemos hacer sobre esa concienciación. Aprovechando la coyuntura de que tiene delante de usted a responsables públicos, a legisladores, ¿qué sugiere que se podría hacer para aumentar esa conciencia entre los usuarios?

Se me está acabando el tiempo, pero quiero referirme, aunque sea muy rápidamente, al tema que posiblemente más me preocupa. En esta Cámara, en la Comisión de Calidad Democrática, por ejemplo, se ha hablado del tema de las *fake news,* sobre todo para influir en procesos electorales. ¿Cree que detrás de todo esto, de los anunciantes y las personas interesadas en acceder a esta información, pueden estar también Gobiernos? Lo digo porque esta es una cuestión sobre la que se habla poco, y recordará que Mark Zuckerberg en agosto de 2024 declaró que había cedido a las presiones de la Administración Biden para censurar contenido en Facebook y en Instagram con un claro sesgo ideológico. Lo digo porque ya se ve que en esto no están solo interesados en cuestiones económicas, sino que juzgamos asuntos más importantes. No solo el dinero es importante, sino también cuestiones de calidad democrática y de soberanía nacional. Me interesaría saber si tiene algún dato al respecto.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señor Rodríguez.

A continuación, por el Grupo Parlamentario Socialista, tiene la palabra la señora Sanz.

La señora **SANZ MARTÍNEZ:** Gracias, presidente.

Profesor Vallina, muchas gracias por su comparecencia y por la claridad con la que ha expuesto unos hechos que, a la luz de la evidencia científica presentada, constituyen uno de los mayores escándalos de vigilancia digital descubiertos en el ámbito europeo. Le estaríamos muy agradecidos si pudiera proporcionarnos la excelente presentación que ha utilizado en su ponencia.

Su intervención nos obliga, como representantes públicos, a asumir con rigor la responsabilidad de proteger a la ciudadanía frente a prácticas que vulneran el derecho fundamental a la privacidad y la intimidad. Este caso no es un problema técnico aislado; es la demostración de que, cuando un gigante tecnológico quiere saltarse las reglas, hoy en día tiene demasiadas facilidades para hacerlo y muy pocos frenos efectivos, y eso en un Estado de derecho es inaceptable. Señorías, lo que el profesor Vallina nos ha explicado hoy, con enorme rigor, puede sonar complejo en lo técnico, pero tiene una traducción muy sencilla en términos democráticos: millones de personas han sido vigiladas en su navegación por Internet, incluso cuando creían estar protegidas, sin saberlo y sin haberlo autorizado. Aplicaciones como Facebook e Instagram, instaladas en teléfonos Android, han utilizado puertos internos del propio dispositivo para escuchar qué páginas se visitaban y asociar esa información a la identidad real de cada usuario. No hablamos de lo que ocurre dentro de la red social, sino de lo que cada persona hacía en el resto de la *web,* al margen de las aplicaciones de Meta. Y esto se ha hecho, según la investigación internacional,

cve: DSCD-15-CO-477

saltándose las protecciones del navegador, del sistema operativo Android e, incluso, del modo incógnito, que muchos ciudadanos usan precisamente para tener un mínimo de privacidad. La imagen es clara: se abre una puerta trasera oculta en el móvil para que una empresa pueda asomarse a ver lo que hacemos en Internet sin que nos demos cuenta.

Señorías, seamos sinceros, ¿cómo se sentirían si descubrieran que un tercero ha estado espiando en silencio durante meses todo lo que han estado haciendo ustedes en su dispositivo móvil? Piénsenlo. Y no podemos minimizar la gravedad del caso pensando que solo se trataba de personalizar anuncios, porque, cuando alguien accede a nuestros hábitos digitales, al detalle de nuestras búsquedas o a momentos en los que estamos vulnerables o indecisos, esa información puede ser utilizada para fines muy diversos y peligrosos. Para entender la intencionalidad y la gravedad de la práctica, conviene subrayar tres aspectos muy importantes. En primer lugar, no estamos ante un fallo puntual, sino ante un sistema diseñado para funcionar así durante años y desplegado a escala masiva en millones de páginas web y en millones de dispositivos. En segundo lugar, el incentivo económico es obvio. Conocer en detalle todo lo que una persona hace dentro y fuera de la plataforma permite perfilar, segmentar y explotar comercialmente su comportamiento con un nivel de precisión que ninguna otra industria ha tenido jamás. Y, en tercer lugar, todo esto se ha hecho sin informar a los usuarios y, por tanto, sin un consentimiento válido.

Por eso, este caso no va solo de privacidad, va de poder, de una asimetría brutal entre los datos que acumulan unas pocas empresas y la capacidad de defensa que tiene el usuario individual. Además, esta práctica no solo vulneró derechos: también generó importantes beneficios económicos y estratégicos para Meta. Al conocer el comportamiento del usuario más allá de sus propios servicios, la empresa podía hipersegmentar a los usuarios y ofrecer a los anunciantes campañas más eficaces y mejor pagadas, aumentando sus ingresos publicitarios y su ventaja frente a otros competidores, propiciando así su dominio en el mercado de la publicidad digital. Y esto amplía aún más la gravedad del caso. Además de una vulneración de derechos, es un acto con consecuencias económicas que alteran la competencia y afectan al conjunto del ecosistema digital.

Y aquí llegamos al núcleo político del problema: el marco actual de protección de datos no basta. El Reglamento General de Protección de Datos es sólido, pero no fue concebido para atajar estrategias que evolucionan a la velocidad del mercado y que aprovechan vulnerabilidades internas de dispositivos y de sistemas operativos. Necesitamos un enfoque regulatorio específico para los servicios digitales que vaya más allá de la supervisión *a posteriori* y que permita anticipar riesgos, auditar sistemas, exigir explicaciones técnicas y sancionar conductas de forma proporcionada y disuasoria. Y aquí es donde la reforma legislativa que este Parlamento tiene sobre la mesa con el proyecto de ley para la mejora de la gobernanza de los servicios digitales se vuelve esencial; un proyecto de ley con el que damos cumplimiento al Reglamento Europeo de Servicios Digitales, el DSA, y dotamos a la CNMC de competencias sancionadoras y de supervisión digital.

Y esto, señorías, no es una mera cuestión administrativa, es la condición para que España pueda defender de forma efectiva los derechos de sus ciudadanos frente a plataformas que operan a escala global. Sin esa capacidad, este Congreso puede debatir y denunciar, pero carece de un instrumento operativo para exigir cambios, investigar prácticas opacas o detener abusos como el que nos ocupa. Una CNMC con competencias claras permitirá requerir información técnica obligatoria, abrir auditorías independientes, evaluar riesgos sistémicos y aplicar multas que realmente alteren los incentivos de estas empresas, y, sobre todo, permitirá que España no dependa exclusivamente de lo que decidan autoridades de otros países. La defensa de los derechos de los ciudadanos españoles debe tener un anclaje institucional propio, con capacidad de reacción inmediata ante vulneraciones graves.

Lo que ha relatado el profesor Vallina no es una anécdota ni un caso aislado, es una prueba de estrés para nuestra arquitectura institucional. En Estados Unidos las consecuencias económicas de este caso ya se estiman en más de 32 000 millones de dólares en potenciales sanciones. En Europa abre interrogantes sobre las posibles infracciones del Reglamento General de Protección de Datos, la Directiva de ePrivacy, el Digital Markets Act y el Digital Services Act. Estamos ante un fenómeno transnacional que ya no puede afrontarse únicamente con herramientas legislativas pensadas para un mercado analógico. Señorías, este caso es una llamada de atención. La tecnología no es neutral y la falta de control no es inocua. Tenemos la responsabilidad de responder con seriedad y determinación. La ciudadanía, que ha mostrado un enorme interés por este caso, espera una respuesta clara y firme, y hoy contamos con la evidencia, con el contexto político y con la urgencia necesaria para actuar.

Muchas gracias. **(Aplausos).**

cve: DSCD-15-CO-477

El señor **PRESIDENTE:** Muchas gracias, señora Sanz.

Para concluir el turno de observaciones y preguntas de los grupos, por el Grupo Parlamentario Popular tiene la palabra el señor Pedreño.

El señor **PEDREÑO MOLINA:** Muchas gracias, señor presidente.

Buenas tardes, señor Vallina Rodríguez. Muchas gracias por estar aquí, por su tiempo y por la explicación.

A mí me ha gustado la clase. La verdad es que ha estado muy bien y se lo agradezco. Ha sido muy claro con un tema muy complicado. Además, creo que esto es muy importante, porque usted es un investigador y este no es su mundo. Lo que usted hace es dar rigor científico a determinadas investigaciones, que en este caso han tenido traslación a poner de manifiesto un tema grave, gravísimo, muy importante, sobre ataques y vulneración de la privacidad digital de las personas o de algunos usuarios. Como ha explicado, entendemos que es de forma premeditada, con mala intención y entiendo que esto estará no sé si en los tribunales de justicia o en algún organismo encargado de velar y vigilar para sancionar, para que esto no suceda, para que se resuelva, para que no vuelva a ocurrir, etcétera.

Señor Vallina Rodríguez, no sé si a usted cuando le llamaron para comparecer no le sonó raro que fuera una comparecencia para una ley de mejora de la gobernanza de servicios digitales y ordenación de los medios de comunicación. No sé si fuera por la hora, pero yo estaba totalmente desubicado. O sea, esto es una lección, una clase magistral de protocolos, de sistemas operativos, de intercambio de información, pero aquí venimos a debatir sobre una ley relacionada con los medios de comunicación. Entonces, quiero que sepa que el que esté usted hoy aquí no lo hemos decidido nosotros. Usted es una víctima del Gobierno. Se lo tengo que decir; sé que no es un mundillo, pero usted es una víctima de los señores que tiene usted a su izquierda, que son los que decidieron imponer que viniera un investigador como usted, que seguro que tiene cosas muchísimo más importantes que hacer, a las que dedicar su tiempo y mucho más productivas que venir a satisfacer la orden dada por el presidente del Gobierno a los señores que tiene usted a la izquierda para intentar airear la situación de Meta, que es un tema que, como usted ha comentado al principio, tiene que estar en los tribunales. No es una cuestión para una comparecencia sobre una ley de medios de comunicación. Por tanto, usted es una víctima de eso. Y nosotros, los que estamos aquí, también lo somos, porque realmente nos están haciendo perder el tiempo los partidos que tiene usted a la izquierda. Y, sinceramente, yo creo que igual no tendría que haberse prestado a venir aquí, porque, como digo, su trabajo es importante y tendría que estar haciendo lo que normalmente hace, y no estar sometiéndose la investigación a un objetivo absolutamente político, que es el que nos trae aquí.

Fíjese que nadie le ha preguntado nada, y yo creo que tampoco le voy a preguntar. Creo que es importante que sepa que, cuando en esta comisión o en esta Cámara, en general, vamos a debatir una ley, es habitual que se llame a comparecientes expertos para que nos den su punto de vista sobre la misma. A mí me gustaría preguntarle sobre la ley, me gustaría preguntarle sobre la EMFA, me gustaría preguntarle cómo tenemos que adaptarla a esta ley o cómo esta ley se adapta a la Ley Europea de Libertad de Medios de Comunicación. Me gustaría preguntarle por qué tenemos que modificar la Ley de Comunicación Audiovisual en la propuesta que hace el Gobierno, cuáles son las ventajas de hacerlo. Me gustaría preguntarle sobre los cambios en la Ley de Servicios de la Sociedad de la Información, que es una ley muy antigua y que esta norma propone cambiar, y por qué, cómo lo ve usted. Pero creo que este no es el objetivo por el que usted ha venido. Usted ha venido porque en un momento determinado el presidente del Gobierno, el señor Pedro Sánchez, anuncia que hay un delito que está cometiendo Meta y entonces decide traer aquí a Mark Zuckerberg y a todos los que tienen algo que ver con Meta. Y lo utilizan a usted como telonero de esta fiesta que va a empezar cuando se cierre esta comisión, que es cuando tenemos que decidir, porque así se consideró unánimemente, el calendario de los que vienen a participar, entre los cuales que hubiera estado usted habría sido muy ilustrativo, por supuesto, pero no con la intención con la que se ha realizado.

Por tanto, creo que esto tiene que estar en los tribunales de justicia. Entiendo que tiene que haber alguna denuncia basada en la información que figura en los informes de investigación que ustedes han desarrollado. Y le voy a preguntar solo por eso, porque hemos estado viendo la Agencia de Protección de Datos y creo que no nos consta que haya ninguna denuncia allí, por si usted conoce el recorrido judicial que está teniendo la base de su investigación. Y, como digo, y en nombre de mi grupo, agradezco que personas como usted, con su brillante currículum y su implicación, aporten en una sociedad absolutamente

cve: DSCD-15-CO-477

digital que podamos tener a expertos que puedan ayudarnos a solventar, prevenir o identificar este tipo de problemas, que seguro seguirán surgiendo. Como usted ha dicho al principio, están los tribunales superiores de justicia y los organismos regulatorios, como la Agencia de Protección de Datos y la CNMC.

En definitiva, sinceramente, quería pedirle disculpas, porque este no es un ámbito como un auditorio de científicos y expertos, y creo que le han traído aquí sin que hubiera un calendario consensuado para ello, dentro del marco de juego establecido. Pero, ya que ha venido, le pregunto si sabe usted si los informes realizados por IMDEA han servido o forman parte de algún expediente de denuncia y dónde, qué información nos puede dar al respecto si es que puede hacerlo.

Muchísimas gracias. **(Aplausos).**

El señor **PRESIDENTE:** Muchas gracias, señor Pedreño.

Tiene ahora la palabra, por un tiempo aproximado de diez minutos, el señor Vallina para contestar a los anteriores intervinientes.

El señor **VALLINA RODRÍGUEZ** (profesor asociado de investigación, IMDEA Networks): Muchas gracias por las preguntas. Voy a ir en orden y espero no perderme ninguna cuestión que hayan puesto sobre la mesa.

Sobre el ataque en sí, nos sorprendió para mal lo que mencionaba sobre la brillante técnica del ataque. Incluso interaccionando con diferentes proveedores de navegadores, hubo momentos en que nos pareció que esto era cruzar una línea muy roja y que nunca se había cruzado en el pasado. Creo que pilló un poco por sorpresa a todo el mundo, incluso a los organismos estandarizadores, como el IETF y el W3C.

En cuanto a las comunidades de desarrollo, esto conecta con un punto mencionado posteriormente sobre la conciencia social. Creo que uno de los grandes problemas es que los desarrolladores de páginas web y de aplicaciones móviles realmente no son conscientes de lo que están haciendo cuando meten este tipo de rastreadores en las páginas web que hacen. Tal vez ellos lo ven como una forma de monetizar y sacar rendimiento a las páginas web, pero todo esto está ocurriendo con tecnología que, volviendo al aspecto de la soberanía digital, no está en Europa. Estos servicios no van a invertir en Europa porque, si vemos todo lo que ocurre y todos los equipos de desarrollo que tienen, casi todo está en Estados Unidos. Como mucho hay alguno en Suiza o en Alemania, pero aquí únicamente tienen servicios comerciales. No creo que sea una limitación para que estas empresas inviertan o no en nuestro país. Y, al final, estamos dando muchos datos muy sensibles a empresas que pueden caer en manos de Gobiernos, incluso perder la soberanía, y, cómo no, pueden incluso tener implicaciones de seguridad nacional. O sea, no sabemos a quiénes estaban espiando.

En cuanto a la financiación, este estudio fue financiado con fondos públicos. Somos un centro de investigación público de la Comunidad de Madrid, y esto vino con financiación de la Agencia Estatal de Investigación, de la Comunidad de Madrid y también en este caso hubo una parte de financiación de Holanda y de Bélgica. Es un ejemplo de cómo la financiación pública puede revertir en la sociedad intentando descubrir ciertos abusos que son realmente de importancia general y social.

En cuanto a la respuesta de las plataformas, nadie de Meta contactó con nosotros. Sí hubo un *statement* en varios medios, incluyendo Ars Technica, y, si mal no recuerdo, en respuesta a la declaración de Google, Meta vino a decir que era una interpretación errónea que ellos habían hecho de las políticas de gobernanza de Play Store. En el caso de Yandex sí nos mandaron un correo —no respondimos a ese correo por mantener la neutralidad—, y venían a decir que ellos habían hecho esta tecnología sin intención de abusar de las capacidades, pero que realmente era para hacer un *bridging* de web y *mobile tracking,* y que, sobre la base de nuestros descubrimientos, cesaron en este tipo de actividad, que fue lo mismo que también hizo Meta.

En cuanto a las poblaciones vulnerables —creo que es el siguiente punto—, tenemos evidencia de páginas web de pacientes de cáncer, tenemos evidencia de páginas web de clínicas, tenemos evidencia de páginas web de farmacias con tiendas, tenemos evidencia de servicios financieros y de compañías de seguros. Creo que sí son un montón de datos que pueden revelar mucha información sobre nosotros y sobre nuestras sociedades. Obviamente, Meta obliga a que los usuarios de Facebook y de Instagram tengan una edad mínima para poder utilizar y crear cuenta en las plataformas, pero sí hay evidencia de sobra que demuestra que hay muchos menores que están utilizando la plataforma.

Sobre las acciones —creo que conecta con lo que usted me ha mencionado— desconozco el camino regulatorio que ha tomado en Europa. Nosotros hicimos nuestra obligación de reportar esto a las agencias

cve: DSCD-15-CO-477

de protección de datos. Dimos la evidencia que se nos solicitó e incluso dimos las técnicas de análisis que utilizamos en nuestro estudio. Todo es público, de hecho. Es también una forma de devolver a la sociedad la financiación pública que recibimos para hacer esta investigación. Entonces, seguimos los principios de lo que se conoce como Open Science, y está todo disponible. Sí sé, porque es público, que hay acciones de demandas colectivas en Estados Unidos, en Canadá y en Alemania, pero es porque son marcos legislativos en los que estas demandas colectivas sí son efectivas y prácticas. Hasta donde yo sé, porque no soy un legislador, creo que en España esto todavía no está habilitado, pero creo que realmente sería un esfuerzo de legislación que beneficiaría enormemente a los consumidores, si hubiese algo parecido en España.

Salté a lo del consentimiento; vuelvo al 75,8 % de las webs. Como he dicho, el consentimiento es un concepto legal, entonces, no es un consentimiento en sí, sino que simulamos el consentimiento. Lo que hicimos fue lo que se conocen como técnicas de *crawling,* que es un poco como lo que hacen los *bots* de ir a páginas web, pero íbamos a la página web para analizar el contenido y el comportamiento dinámico de esta página web. Lo que hicimos fue, antes de entrenar al *bot* para que cliquease en nada en la página web, incluyendo un consentimiento de aceptación de *cookies,* veíamos que ese comportamiento se ejecutaba por defecto en el 75 % de las páginas web. Obviamente, sería una agencia reguladora la que tendría que determinar si esto es una violación del consentimiento o no. Sí hay investigación de varias investigadoras, colegas mías, Nataliia Bielova y Cristiana Santos, que han demostrado que incluso los formularios de consentimiento son *trackers.* O sea que hay bastante problema ahí detrás.

Sobre si sigue pasando hoy, hay un principio empírico que dice que cualquier estudio que se haga en Internet sobre un análisis empírico de *software* o de Internet nunca va a ser completo. Es decir, podemos demostrar la evidencia de que algo ocurre, pero no podemos demostrar que algo no ocurre. Entonces, no tenemos evidencia de que esto siga sucediendo. Sí hicimos un análisis y vimos que había otros usos que parecen legítimos de *localhost,* por ejemplo, páginas web financieras que utilizan esto para saber si eres un *bot* o no. Entonces, hay usos legítimos, lo que pasa es que consideramos que esto se puede hacer con consentimiento; o sea, si yo soy el usuario de un banco y necesito que el banco acceda a mis puertos locales, me puede pedir consentimiento y lo puedo dar. No tiene por qué ocurrir de una forma completamente opaca. El permiso que se está introduciendo ahora en el estándar web de Local Network Access va a intentar estandarizar este tipo de mecanismo para que el usuario pueda dar consentimiento.

Sobre la diferencia estadística del uso de *mobile web* contra el *desktop,* es lo que mencioné que se alinea con el uso de estas tecnologías por parte de Meta. Como veíamos, puse el ejemplo de un cacho de código en el que estaban intentando identificar si el usuario era un usuario de Android móvil. Entonces, esto demuestra que el pico de uso de esas tecnologías realmente está en gran medida asociado temporalmente, o hay una correlación temporal, con el uso de esta tecnología por parte de Meta. No tenemos información para saber realmente los usos, pero sugiere que realmente ese pico es atribuible a Meta, porque acabó el 3 de junio, que fue cuando todo salió a la luz.

Sobre la conciencia social, creo que hay un problema muy gordo, conectado un poco con lo que mencionabas de los desarrolladores, y es que en las carreras de ingeniería no se enseña privacidad. Los desarrolladores web no tienen idea de que realmente tienen que desarrollar tecnología que cumpla los requisitos regulatorios, y no tienen idea de lo que ocurre cuando introducen este tipo de *trackers,* de compañías principalmente norteamericanas, pero también chinas. Hay también un problema de educación de los usuarios. Me aterra, incluso dentro de mi círculo familiar, que muchas veces se diga: Me da igual que me espíen, no tengo nada que esconder. Bueno, si estás contratando un seguro, tienes un cáncer y vas a una página web pública, pues igual sí tienes algo que esconder. Entonces, es una cuestión de la fatiga de muchos usuarios, que tienen que aceptar muchos formularios. Hay también un problema de transparencia en las políticas de privacidad, que es un texto legal muy difícil de entender. Hay un área científica, que se llama *usable security and privacy,* que se centra en cómo hacer mecanismos más usables para mejorar la transparencia y la privacidad de las plataformas. Pero no es mi área, no puedo comentar mucho más de esto.

Hay otro aspecto, no solo de soberanía nacional, y es que estamos en manos de lo que decidan las agencias reguladoras de otros países. Muchas veces estos abusos tienen que ir, principalmente, por países, como Irlanda. Entonces, puede haber un desalineamiento entre los intereses de los países y los intereses generales de otros países de la Unión Europea. No sé muy bien cómo se podría arreglar esto legislativamente hablando, pero yo creo que es un problema bastante grave, desde la perspectiva del usuario.

cve: DSCD-15-CO-477

En cuanto a que tenga usos por parte de Gobiernos —me estoy quedando sin tiempo—, la evidencia de Cambridge Analytica. Hay un libro muy interesante de un periodista que se llama Byron Tau, que se centra en el uso de la interconexión entre los Gobiernos y las industrias tecnológicas norteamericanas. También tenemos la evidencia del caso Snowden, de que los operadores de telefonía estaban al servicio también del Gobierno de Estados Unidos.

A la diputada del PSOE, no sé si quiere que le conteste algo, porque creo que expuso principalmente una posición.

Voy a finalizar rápidamente con el posicionamiento de los representantes del Grupo Popular. Para mí, como investigador, es un deber moral, si se me llama, venir a presentar esto y lo hice realmente encantado; no me supuso ningún esfuerzo. Y creo que es una forma, también, de trasladar a la sociedad los descubrimientos que se hacen científicamente. Y si al menos ha servido para que los legisladores entiendan un poco mejor cómo funciona la tecnología, salgo de aquí completamente satisfecho. **(Aplausos de las señoras y los señores diputados del Grupo Parlamentario Socialista y del Grupo Parlamentario Plurinacional SUMAR).** No es una cuestión de alineamiento político; es una cuestión de que creo que realmente es un deber moral explicar cómo estas tecnologías funcionan y explicar a la sociedad que esto es un problema. Y, al final, creo que son todos ustedes los que deben reunirse y ponerse de acuerdo para que realmente la ley salga adelante. El DSA realmente cubre aspectos de privacidad. Hay un artículo muy interesante de Jorge García Herrero, que es un abogado experto en privacidad, y, de acuerdo con su análisis, puede ser la mayor multa en la historia a Meta, y puede ser la mayor multa por artículos específicos del DSA, no por el RGPD. Entonces, realmente, sí es de relevancia para el DSA. Luego, las motivaciones políticas que hay detrás a mí me son indiferentes y es un juego que a mí me viene de lado. O sea, no debería entrar ahí. **(El señor Conde López: Pues has entrado).**

De hecho, el artículo 40 del DSA, si mal no recuerdo, permite que los investigadores podamos acceder a la tecnología. Y creo que Meta es una de las operadoras que se están posicionando en contra de ese acceso. Nuestra labor fue poner encima de la mesa de una forma accesible para todos los reguladores y para todas las agencias que nos solicitaron esta información, no solo españoles, sino a nivel europeo, e intentar que este tipo de abusos no ocurra. Como mencioné al principio, creo que algo muy positivo para la legislación española, para que este tipo de casos puedan ser llevados a los tribunales, sería seguir el modelo de Alemania o de Austria y permitir que haya demandas colectivas o una *class action,* como ocurre en Estados Unidos. Realmente, así se separaría el Poder Legislativo de un ente judicial un poco más independiente, que creo que es un problema también que se mencionó en la ponencia anterior de la presidenta de la CNMC.

Yo siempre estaré disponible para cualquier petición de cualquier partido político que me solicite ayuda o información sobre este tipo de acciones. Llevo más de quince años haciendo esto, colaboro mucho con la Agencia Española de Protección de Datos, recibí tres veces el premio de investigación de la Agencia Española de Protección de Datos y dos veces el de la francesa. Investigaciones que hicimos en 2018 llegaron al Senado de Estados Unidos y un coautor presentó nuestros resultados al Senado de Estados Unidos sobre la privacidad en menores. Influimos también en la legislación norteamericana COPPA, sobre la protección de menores. Entonces, creo que es un deber moral como científico, si se me solicita, venir aquí y explicarlo, independientemente de cualquiera estrategia política que pueda haber detrás. **(Aplausos).**

El señor **PRESIDENTE:** Muchas gracias, señor Vallina.

Tal y como hicimos en la anterior comparecencia, si los grupos quieren intervenir brevemente es el momento.

Grupo SUMAR.

La señora **ANDALA UBBI:** Profesor, muchas gracias.

Tú mismo acabas de dar una conclusión brillante. Yo creo que como legisladores es un deber acercar la academia a la institución, si no, no vamos a poder legislar. Aquí hay más de cuarenta y cuatro comisiones y subcomisiones y no somos expertas en todas las materias y agradecemos que hagáis esa devolución a la sociedad civil instruyéndonos. De verdad, vamos a coger tu *paper* y tu presentación y cada vez que digan que las tecnológicas son neutrales, vamos a poner las diapositivas para que, efectivamente, no vengan las plataformas a hacer su propio *lobby* y podamos constatar con estos datos de manera fehaciente su manipulación del mercado y de ese bien público, que creo que aún no se está comprendiendo, que es el dato como bien común que hay que proteger y no dispersar en casas y plataformas ajenas.

cve: DSCD-15-CO-477

Reitero el agradecimiento. No te conocíamos como grupo parlamentario, pero agradecemos que, en este caso, el Grupo Socialista haya puesto tu nombre sobre la mesa. Me alegro de que la Comunidad de Madrid financie con fondos públicos su instituto y su investigación y que se esté invirtiendo en esto.

Gracias.

El señor **PRESIDENTE:** Muchas gracias, señora Andala.

Señor Rodríguez.

El señor **RODRÍGUEZ ALMEIDA:** Muchas gracias, presidente. Profesor, muchas gracias.

La verdad es que es de las pocas veces que un compareciente con tan poco tiempo responde prácticamente a todas las preguntas, al menos las que hemos formulado desde este Grupo Parlamentario VOX, y es de agradecer.

Dos cuestiones muy rápidas. Una, se ha referido a ese *bridging* —el puenteo, por así decirlo— en donde se hablan aplicaciones y navegadores entre sí, y que una de las empresas que lo hacía declaró que había dejado de hacerlo. Como el otro gran operador es Meta, la pregunta es obligatoria, ¿tiene constancia o sabe si Meta ha declarado si ha dejado de hacerlo o no? Ya digo que lo hice en la parte anterior, insisto, me preocupa saber si estos problemas siguen sucediendo. Sé que ya ha explicado usted la dificultad técnica para pronunciarse al respecto, pero me interesa saberlo. Tengo la obligación de preguntarlo porque es para saber la urgencia en la toma de decisiones o para tomar acciones al respecto en forma de iniciativas parlamentarias.

Se ha dicho una cosa sobre la que me gustaría saber su opinión; yo le voy a dar la mía. La portavoz del Grupo Socialista ha dicho que la tecnología no es neutral. Personalmente, no comparto esa afirmación, entiendo que la tecnología es ambivalente; es decir, se puede hacer un buen o un mal uso de la tecnología, igual que de cualquier capacidad humana, o como un arma de fuego, que se puede usar para una legítima defensa personal o para defender a una persona vulnerable o se puede usar para matar a un inocente, es decir, depende de quien tenga acceso a esa arma. Por lo tanto, yo sí creo que la tecnología en sí misma es neutral y lo importante es el uso que se haga de ella. Esto es quizás algo más filosófico que técnico, pero si tuviese alguna opinión al respecto, yo estoy muy interesado en oírla.

Muchas gracias.

El señor **PRESIDENTE:** Muchas gracias, señor Rodríguez.

Por el Grupo Socialista, señora Sanz.

La señora **SANZ MARTÍNEZ:** Muchas gracias, presidente.

En primer lugar, quiero decirle que sus primeras explicaciones ya me parecieron cristalinas y no me generaron ni la menor duda en cuanto a la descripción de este caso, cuya gravedad yo he pretendido resaltar en mi intervención.

Y, en segundo lugar, quería transmitirle que no compartimos en absoluto lo que ha expresado en su intervención el portavoz del Grupo Popular, minusvalorando la importancia de tener en estas Cortes una información técnica de rigor como la que usted nos ha proporcionado hoy, con el objetivo de que los legisladores seamos plenamente conscientes de la necesidad urgente de crear la regulación necesaria para atajar este tipo de prácticas que son inadmisibles y que vulneran derechos esenciales. Y esa es precisamente la pretensión de estas comparecencias en esta comisión, en el marco del proyecto de ley que estamos desarrollando para la gobernanza de los servicios digitales y el cumplimiento del Digital Services Act europeo. Por eso, queremos agradecerle, sinceramente, su valiosa contribución para que todo el mundo pueda entender la importancia de este proyecto legislativo.

Muchas gracias. **(Aplausos).**

El señor **PRESIDENTE:** Muchas gracias, señora Sanz.

Finalmente, por el Grupo Parlamentario Popular, señor Pedreño.

El señor **PEDREÑO MOLINA:** Gracias, presidente.

Señor Vallina Rodríguez, voy a finalizar igual que empecé, dándole las gracias por lo que nos ha contado y agradeciendo y significando su bagaje científico.

Yo me he dedicado mucho tiempo a la investigación y a mí me han llamado para comparecer en el Congreso y yo he comparecido para alguna ley. Yo he comparecido en el Congreso y mi investigación era sobre la ley. **(Rumores).** El tema está en que hoy tenemos una comparecencia que es sobre una ley, esta ley de medios de comunicación, que no lo han nombrado en ningún momento. **(Continúan los rumores.—La señora Sanz**

cve: DSCD-15-CO-477

Martínez: Qué pesado.—La señora Blanquer Alcaraz: No se ha leído la ley, que se lea la ley). Es una comparecencia sobre esta ley ¿no? ¿No es esta ley? Bueno, voy a leer la convocatoria: mejora de la gobernanza de los servicios digitales y la redacción de los medios de comunicación. **(Continúan los rumores).** Ese es el motivo de la comparecencia. Y, por tanto, lo que nos hubiera gustado es que se hubiera consensuado el nombre de los comparecientes. La suya es muy valiosa, pero le tengo que decir que en cuanto finalice esta comisión vamos a tener una reunión para decidir un calendario de comparecientes para esta ley y ahí está su nombre. **(El señor Martín Urriza: ¿Y eso le interesa al ponente?).** Lo digo para que sepa en qué situación está usted aquí.

Dicho lo cual, no tengo ninguna duda de que los que sois investigadores, los que nos hemos dedicado a la investigación, sobre todo con entidades públicas, estamos al servicio de toda la sociedad, claro que sí. Yo no le estoy afeando ni diciendo que usted no tenga ninguna validez para estar aquí. Repito que alabo su investigación, le doy las gracias por lo que ha hecho y creo que es trascendental que las investigaciones de las universidades y de los centros de investigación repercutan en la mejora de la sociedad y no simplemente en meros artículos de investigación. Pero lo que le digo es que estamos justificando unas comparecencias y aquí estamos dedicando nuestro tiempo para valorar los artículos de un proyecto de ley que ha presentado el Gobierno, ni más ni menos. No quiero ahondar en esto, pero yo creo que ha entendido suficientemente lo que le he dicho y creo que el resto de los grupos también.

De nuevo quiero agradecerle y que sigan por este camino. Me parece muy valioso, sobre todo en una sociedad digital tan expuesta como la que tenemos ahora mismo.

Nada más y muchas gracias. **(Aplausos).**

El señor **PRESIDENTE:** Muchas gracias, señor Pedreño.

Tras las consideraciones de los grupos, señor Vallina Rodríguez, tiene usted cinco minutos para cerrar la comparecencia.

El señor **VALLINA RODRÍGUEZ** (profesor asociado de investigación, IMDEA Networks): Creo que la principal pregunta es si Meta paró esto. El día que salió el artículo, paró. Esto está especificado, además, en el artículo de Ars Technica, que le invito a leer. Lo que no puedo saber es lo que motivó a Meta el parar esto, si fue una conversación que tuvieron a lo mejor con los equipos legales de Google —que pudo haber ocurrido— o si fue la exposición pública. No se lo puedo decir. Lo que sí puedo confirmar también es que, si hay demandas contra ellos, continuar haciendo esto sería un poco arriesgado. Entonces, después de toda esta exposición pública, no creo que tengan un incentivo de hacerlo. Pero estas son cuestiones que deberían lanzarles a Meta cuando vengan.

También estoy de acuerdo con usted en lo de que la tecnología es neutral y que todo depende de los usos. Por eso, creo que es realmente necesario tener una regulación que especifique qué usos son los válidos y los que no. Es como la energía nuclear, puede ser muy valiosa, pero también puede ser utilizada para matar a millones de personas. Este debate es bastante ilustrativo de cómo hacer esto y llevar esto adelante.

Tengo una nota aquí del Grupo Parlamentario SUMAR. El artículo está ahora mismo siendo revisado por pares y, en el momento en el que sea aceptado, también lo haremos público, y estaría a disposición de quien lo quiera mirar.

Para acabar con el representante del Grupo Popular, creo que, con su última frase, al final, estamos alineados. Estamos de acuerdo en que como científicos tenemos que aportar a la sociedad y, si a mí se me invita —independientemente de las estrategias políticas, como he dicho previamente—, tengo una obligación moral de participar. Igual que hablé con otros reguladores de otros países, si se me llama para este foro, debo hacerlo igualmente.

Muchas gracias. Yo creo que, por mi parte, nada más. **(Aplausos de las señoras y los señores del Grupo Parlamentario Socialista y del Grupo Parlamentario Plurinacional SUMAR).**

El señor **PRESIDENTE:** El agradecimiento es de la comisión por haberse presentado a darnos su informe. Le agradecemos mucho su presencia.

Se levanta la sesión.

Eran las ocho y treinta y un minutos de la noche.

cve: DSCD-15-CO-477