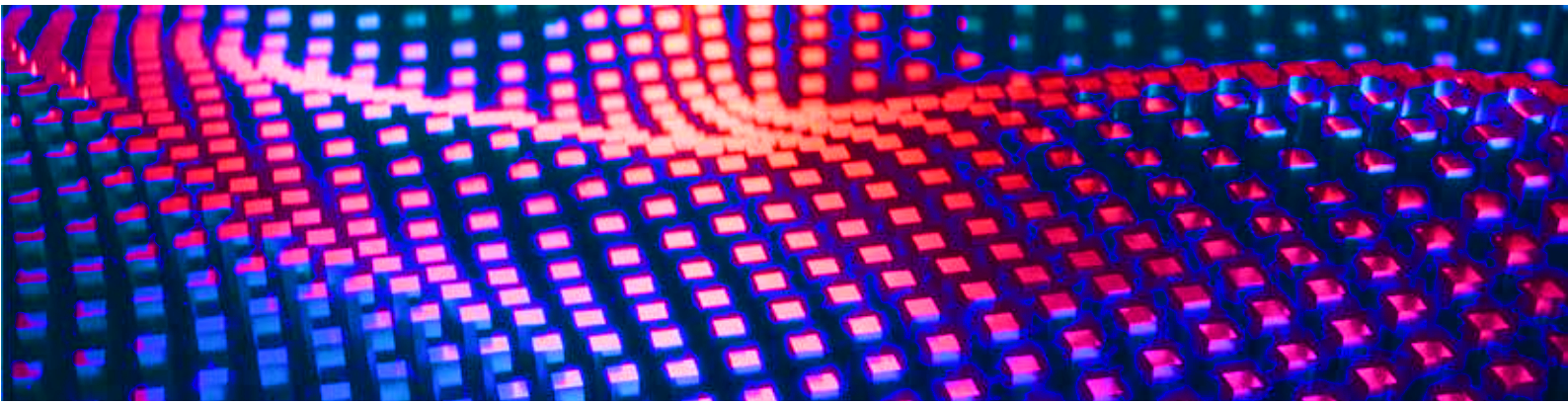
G A _ P

Gómez-Acebo & Pombo



Derecho Digital

2023 Nº 9

Contenido

Protección de datos personales en el ámbito digital 3

— Grabaciones en garajes 3

— Inclusión en archivo de morosos: es necesario el requerimiento de pago previo 3

— Derecho al olvido digital frente a libertad de expresión (SAN núm. 4609/2023, de 28 de septiembre) 4

— Protección de datos personales y consentimiento a la instalación de *cookies* 5

Propiedad industrial e intelectual 6

— Tecnología antipiratería y protección de datos personales 6

Digitalización y mercados digitales 7

— La Comisión publica una recomendación para evitar la divulgación de contenido ilícito y nocivo a raíz de los conflictos en Ucrania e Israel 7

Inteligencia artificial 9

— Acuerdo entre el Consejo y el Parlamento Europeo sobre la Ley de Inteligencia Artificial 9

— Pruebas para ensayar el cumplimiento de ciertos requisitos por parte de algunos sistemas de inteligencia artificial que puedan suponer riesgos para la seguridad, la salud y los derechos fundamentales de las personas 9

Metaverso 11

— Marcas en el metaverso 11

Seguridad 12

— Recomendación (UE) 2023/2113 de la Comisión, de 3 de octubre, sobre ámbitos tecnológicos críticos para la seguridad económica de la Unión Europea con vistas a realizar evaluaciones de riesgos adicionales conjuntamente con los Estados miembros 12

Infraestructuras y tecnología 14

— La Unión Europea impulsa un marco de medidas para reforzar el ecosistema europeo de semiconductores 14

Protección de datos personales en el ámbito digital

Grabaciones en garajes

El Tribunal Constitucional, mediante la Sentencia núm. 92/2023, de 11 de septiembre, ha concluido que las imágenes captadas en el garaje de una comunidad de propietarios en relación con la investigación de un individuo condenado por tráfico de drogas, sin autorización judicial previa, fueron obtenidas de manera ilícita al considerar que el lugar en cuestión mantenía una «legítima expectativa de privacidad». En concreto, el tribunal sostiene que se ha vulnerado el derecho fundamental a la intimidad personal del individuo.

El tribunal basa su decisión en que las imágenes fueron obtenidas sin conocimiento del individuo mediante una cámara instalada en un garaje de una comunidad privada, espacio en el que se mantenía una expectativa razonable de privacidad.

Como resultado, se ha declarado nula la prueba por considerar que se ha obtenido ilícitamente y el tribunal ha ordenado retrotraer las actuaciones al momento previo al fallo en la instancia.

Claudia Pérez Moneu

Inclusión en archivo de morosos: es necesario el requerimiento de pago previo

El Tribunal Supremo, en su Sentencia núm. 1477/2023, de 23 de octubre, estimó el recurso de casación de un particular interpuesto frente a la entidad bancaria Ibercaja por incluir y mantener sus datos registrados en el fichero de morosos sin que se hubiese efectuado debidamente el requerimiento de pago previo, lo cual determinaba la existencia de una intromisión ilegítima en su derecho al honor.

Los hechos se remontan al 18 de mayo del 2019, cuando el Banco Sabadell denegó un préstamo al particular por estar incluido en un fichero de morosos. Éste descubrió, a raíz de ejercer su derecho de acceso al fichero, que fue dado de alta

por una supuesta deuda impagada de 1150,37 euros de la que no había sido requerido de pago ni advertido de inclusión en el registro de morosos. Por su parte, Ibercaja argumenta que la deuda originó de una cuenta abierta con la entidad en el 2016 y que en el contrato formalizado se le informaba de la posibilidad de incluir sus datos personales en ficheros relativos al incumplimiento de obligaciones dinerarias en caso de producirse impagos en la cuenta corriente desde el mismo momento de la suscripción, habiéndole, asimismo, requerido el pago mediante una carta remitida al domicilio indicado en el contrato y un correo electrónico, actuaciones que el Tribunal Supremo no tiene como acreditadas.

La demanda fue estimada íntegramente en primera instancia y confirmada en casación, entendiendo que Ibercaja cometió una intromisión ilegítima en el honor del afectado por incluir y mantener sus datos registrados en el fichero de morosos; sustentó su fallo en la consideración de que el artículo 38.1, apartado c, del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, establece el requisito del «requerimiento previo de pago a quien corresponda el cumplimiento de la obligación» para la inclusión de los datos en el fichero, artículo que no había sido derogado por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

Cristina Bonfanti Gris

Derecho al olvido digital frente a libertad de expresión (SAN núm. 4609/2023, de 28 de septiembre)

La Audiencia Nacional se ha pronunciado, en su Sentencia núm. 4609/2023 (Sala de lo Contencioso-Administrativo, Sección Primera), de 28 de septiembre, sobre la solicitud de recurso de un particular relativa a la resolución de la Agencia Española de Protección de Datos (AEPD) que inadmitía su reclamación en la que se requería eliminar la indexación de ciertas URL de los motores de búsqueda aparejadas a su nombre en las cuales se podía encontrar un vídeo con fecha del 2016 en el que se apreciaba al recurrente —que por entonces ocupaba un cargo relevante en una formación política— quemando propaganda electoral.

El recurrente invoca la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo del 2014, asunto C-131/12, y la normativa española de protección de datos relativa a la eliminación en los motores de búsqueda de los enlaces en caso de que sus contenidos sean «inadecuados, inexactos, no pertinentes, no actualizados o excesivos, o hubieren devenido por el transcurso del tiempo conforme a los artículos 15 y 93 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, y el artículo 17 del Reglamento (UE) 2016/679».

Además, pone de manifiesto la falta de motivación de la resolución de la Agencia Española de Protección de Datos, pero se considera que, si bien la motivación incluida en dicha resolución es «mínima», no ha generado una situación de indefensión para la parte actora.

En cuanto al debate de fondo, se efectúa la correspondiente ponderación de derechos fundamentales. De este modo, se confronta el derecho a la protección de datos —que se extiende más allá del derecho a la intimidad y abarca todos los datos personales relativos al ejercicio de cualquier derecho que asista a las personas, independientemente de su carácter o no constitucional—

con el derecho a la libertad de expresión —que, de igual forma, se extiende más allá del derecho a la información, ya que garantiza la posibilidad de manifestar ideas sin atender al límite de veracidad—.

El tribunal realizó esta ponderación, y lo hizo a la luz de lo expuesto por el Tribunal de Luxemburgo en la Sentencia de 8 de diciembre del 2022, asunto C-460/20, y de las circunstancias particulares del caso. En consecuencia, tras un exhaustivo análisis, el tribunal concluye que «es claro que debe prevalecer el derecho a la libertad de información, pues el demandante en ejercicio de una actividad política, ha desempeñado un cargo público y ni en este procedimiento, ni ante la Agencia, ha presentado prueba alguna sobre la inexactitud de la información contenida en los enlaces; además, no ha transcurrido un tiempo excesivo entre la fecha de los enlaces y la del ejercicio de su derecho al olvido, por lo que tampoco puede decirse que la información haya quedado obsoleta o que sea particularmente sensible para el demandante pues según su propia valoración, los enlaces tiene incidencia en su esfera profesional».

Iratze Arrigain García

Protección de datos personales y consentimiento a la instalación de *cookies*

La Agencia Española de Protección de Datos (AEPD) ha impuesto por primera vez una multa a una empresa por el uso de patrones oscuros *(dark patterns)* de sobrecarga y de ocultación en el diseño de la interfaz de usuario.

Los patrones oscuros son configuraciones de interfaz cuya finalidad es influir a los usuarios en su interacción en línea para que, entre otras posibilidades, tomen decisiones perjudiciales con respecto a la protección de sus datos personales.

En este caso, la empresa ha sido sancionada por la aplicación de patrones oscuros en la sección «Lista de proveedores» dentro de «Política de privacidad» en su página web. Cuando el usuario accedía a esa sección, más de la mitad de los ciento treinta proveedores tenían la casilla «Aceptar tratamiento de datos por interés legítimo» marcada por defecto. Esta preselección dificultaba la oposición del usuario al no facilitase mecanismos que permitieran que el usuario desmarcase la opción de una sola vez o en un número razonable de veces.

En esta misma resolución, la Agencia Española de Protección de Datos sanciona a la entidad tanto por ofrecer una redacción ambigua y confusa de su política de privacidad como por irregularidades en la información de la política de cookies y su aceptación. En total, la sanción económica ascendió a 1200 euros por las diversas infracciones del Reglamento general de protección de datos.

Claudia Pérez Moneu

Propiedad industrial e intelectual

Tecnología antipiratería y protección de datos personales

En la actualidad existen determinados programas informáticos que envían un aviso a los titulares de propiedad intelectual sobre dicho programa cuando se realizan conductas infractoras (por ejemplo, cuando se lleva a cabo una reproducción ilícita). Surge entonces en estos casos la cuestión de determinar si este tipo de funcionalidades puede suponer una vulneración de los datos personales de los usuarios del programa, de modo que haya que considerar ilícita la prueba de la infracción de la propiedad intelectual obtenida por estos medios.

Pues bien, la cuestión ha sido analizada por la Audiencia Provincial de Barcelona (Sección Decimoquinta) en su reciente Sentencia 431/2023, de 27 de septiembre (JUR 2023\407928). A este respecto, el tribunal —reiterando una interpretación que ya había defendido en alguna ocasión anterior— declara que «no podemos aceptar que la instalación de un programa que pueda reportar su posible infracción al titular de sus derechos de autor, recopilando datos como la IP o el nombre de dominio de los ordenadores de dicha empresa, como ocurre en este caso, pueda vulnerar los derechos al tratamiento de datos personales». Y ello porque en este caso las direcciones IP y los nombres de dominio pertenecían a una persona jurídica y, como es sabido, la legislación sobre datos personales sólo protege los datos de personas físicas.

Asimismo, el tribunal también considera que no hay vulneración de datos personales de los trabajadores de la empresa que emplean los ordenadores, ya que éstos son puestos a su disposición para un uso profesional y, por lo tanto, «los datos relativos a los ordenadores y los programas informáticos con los que trabajan, no guardan relación alguna con la vida privada de los trabajadores».

Ángel García Vidal

Digitalización y mercados digitales

La Comisión publica una recomendación para evitar la divulgación de contenido ilícito y nocivo a raíz de los conflictos en Ucrania e Israel

El 26 de octubre la Comisión Europea publicó la Recomendación 2023/2425 sobre la coordinación de las respuestas a incidentes, especialmente derivados de la difusión de contenido ilícito, en anticipación de la plena entrada en aplicación del Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, también conocida como Reglamento de servicios digitales.

Ante los nuevos conflictos que amenazan la estabilidad europea con la guerra entre Rusia y Ucrania y el ataque terrorista de Hamás en Israel, la Comisión ha anticipado la aplicación del Reglamento de servicios digitales, que establece mecanismos de coordinación frente a situaciones de emergencia como la que estamos atravesando. Estos conflictos están provocando multitud de incidentes derivados de la difusión de contenido ilícito, por lo que la Comisión ha considerado emitir esta recomendación para adoptar medidas rápidas y coordinadas en la Unión Europea que den respuesta a estas situaciones de crisis con el objetivo de evitar que se propague de forma viral contenido terrorista y de incitación al odio en las plataformas en línea.

Por ello, y con vistas a evitar la desestabilización política y social en toda la Unión, la Comisión ha establecido una serie de recomendaciones específicas, entre las que cabe destacar las siguientes:

- La creación de una red informal entre los Estados miembros donde cada uno designará a un funcionario de alto nivel que lo represente; tal red tendrá como objetivo coordinar, antes de la entrada en vigor del Reglamento de servicios digitales, acciones relacionadas con la difusión de contenido ilícito en plataformas digitales.

- La participación voluntaria de los Estados miembros en los marcos de cooperación

voluntaria existentes, entre los que se incluye el Protocolo de Crisis de la Unión Europea, desarrollado en el 2019, que prevé una respuesta transfronteriza coordinada y rápida por parte de los proveedores de servicios en línea y de las fuerzas y cuerpos de seguridad.

Cristina Bonfanti Gris

Inteligencia artificial

Acuerdo entre el Consejo y el Parlamento Europeo sobre la Ley de Inteligencia Artificial

A principios de diciembre del 2023, el Parlamento Europeo y el Consejo han alcanzado un acuerdo sobre la propuesta de «Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión», presentada en el 2021 por la Comisión.

En todo caso, esto no supone todavía la aprobación definitiva de la normativa, no sólo porque el acuerdo es todavía provisional y está sujeto a que se cierren algunos flecos menores, sino también porque el texto consensuado debe ser sometido a los representantes de los Estados miembros (Comité de Representantes Permanentes o Coreper) y, posteriormente, ha de ser confirmado tanto por el Parlamento Europeo como por el Consejo.

Ángel García Vidal

Pruebas para ensayar el cumplimiento de ciertos requisitos por parte de algunos sistemas de inteligencia artificial que puedan suponer riesgos para la seguridad, la salud y los derechos fundamentales de las personas

El 9 de noviembre se publicó en el *Boletín Oficial del Estado* el Real Decreto 817/2023, de 8 de noviembre, que establece un entorno controlado de pruebas para el ensayo del cumplimiento de la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial.

El objetivo perseguido con este real decreto no es regular la propia inteligencia artificial, sino las aplicaciones de ésta que puedan representar riesgos para la seguridad, la salud y los derechos fundamentales. Así, en consonancia con las últimas acciones legislativas de la Unión Europea, se establece un entorno experimental controlado para comprobar la idoneidad, la aplicabilidad y la implicación en la práctica de la regulación más reciente sobre inteligencia artificial.

En cuanto al ámbito aplicativo del real decreto, éste se extiende —con ciertas exclusiones como, por ejemplo, los sistemas de inteligencia artificial para actividades militares, los que sirvan de técnicas subliminales que trasciendan la consciencia de las personas para alterar su comportamiento, o aquellos que tengan el fin de clasificar personas físicas atendiendo a su conducta social o a características personales— a las Administraciones Públicas, entidades del sector público y entidades privadas y, además, establece el proceso para seleccionar los sistemas y entidades que formarán parte de este entorno de prueba.

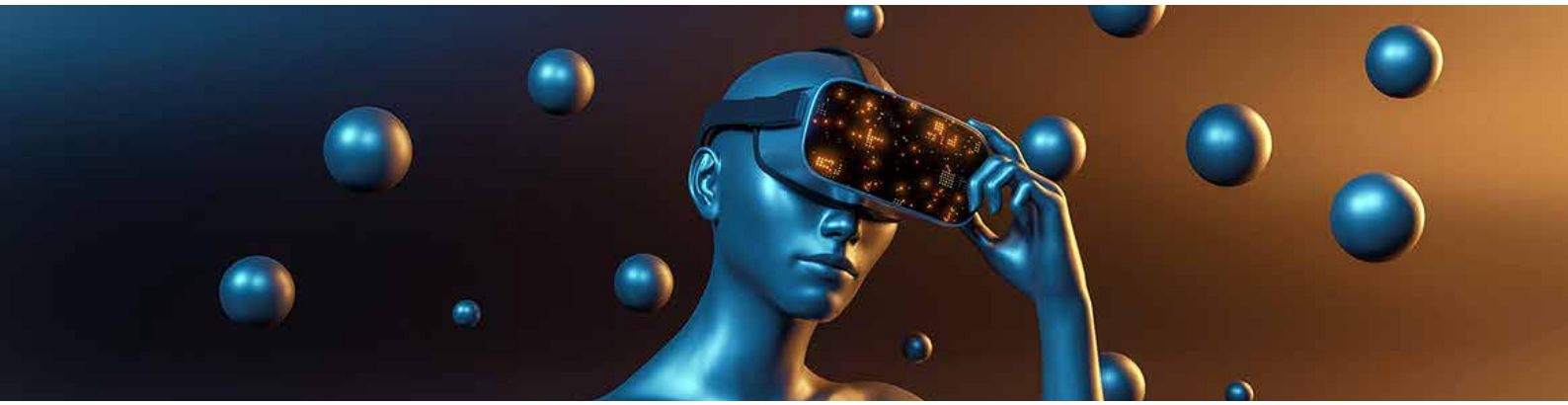
En el texto se detalla el proceso de participación en dicho entorno, incluyendo los requisitos de elegibilidad, el proceso de registro, y los criterios que aplicará la Subdirección General de Inteligencia Artificial y Tecnologías Habilitadoras Digitales para evaluar las solicitudes presentadas y seleccionar a los proveedores de inteligencia artificial que finalmente podrán participar en dicho entorno.

En consecuencia, el proveedor de sistemas de inteligencia artificial admitido deberá implementar los requisitos establecidos en el artículo 11 del real decreto, que incluyen, entre otros: *a*) establecer un sistema de gestión de riesgo; *b*) garantizar que los datos utilizados cumplen los criterios de calidad especificados; *c*) actualizar la documentación técnica del sistema, que deberá ser elaborada conforme a las especificaciones; *d*) permitir el registro automático de eventos y almacenar la información relativa a ellos; *e*) contar con un diseño que evite la generación de sesgos discriminatorios, y *f*) facilitar instrucciones de uso en forma electrónica, ofreciendo detalles claros, actualizados y precisos sobre sus características.

Una vez implantados dichos requisitos, los proveedores involucrados confeccionarán una declaración de cumplimiento y, posteriormente, articularán un sistema para monitorizar el funcionamiento después de su comercialización. Asimismo, los proveedores de sistemas de inteligencia artificial deberán elaborar un informe de acuerdo con las guías ofrecidas por la Subdirección General de Inteligencia Artificial y Tecnologías Habilitadoras Digitales.

Finalmente, una vez terminadas estas fases y habiendo evaluado el órgano competente los resultados, éste procederá a publicar un informe con las conclusiones y recomendaciones, que serán de utilidad para la regulación normativa eficaz y realista de los sistemas de inteligencia artificial.

Iratze Arrigain García



Metaverso

Marcas en el metaverso

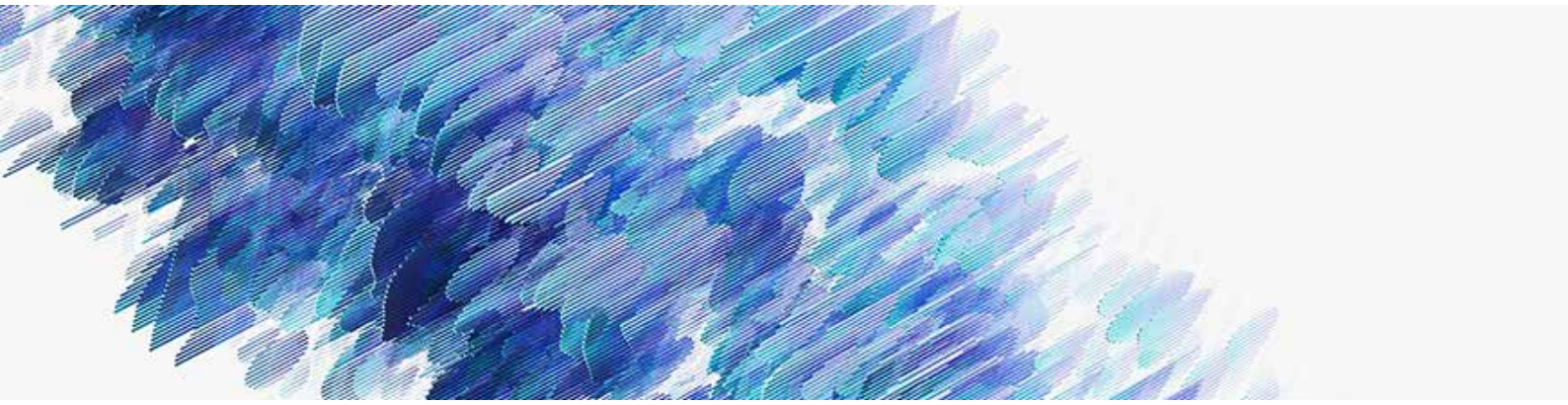
Los problemas que el desarrollo de los metaversos y de los *tokens* no fungibles suponen para los titulares de marcas está encontrando ya reflejo en la práctica judicial española. Es muy relevante a este respecto el Auto núm. 168/2023 dictado por el Juzgado de lo Mercantil núm. 1 de Alicante como Tribunal de Primera Instancia de Marca de la Unión Europea (JUR 2023\387863).

En esta resolución judicial, además de afirmarse que «es claro que el desarrollo de estos nuevos universos digitales supone un reto para los titulares marcarios y la defensa de la propiedad intelectual», se adoptan medidas cautelares de cesación de uso de marcas ajenas en un metaverso y como distintivo de *tokens* no fungibles.

El litigio enfrenta al titular del metaverso Uttopion, que es titular de la marca figurativa de la Unión «Uttopion» y de la marca, también de la Unión, denominativa «Uttopian», registradas para distintos productos y servicios propios del metaverso, con un tercero que cuenta con su propia plataforma de metaverso identificada con el término «Utopia» a la que puede accederse a través del dominio https://utopia.io y donde se puede adquirir una colección de NFT (*tokens* no fungibles) bajo el nombre «Utopia Avatars», que utiliza la marca «Utopia» junto con el término *avatars*. Así las cosas, la parte actora considera que el uso de los signos «Utopia», «Utopia Avatars» y «Utopian» implica infracción de las citadas marcas.

Por su parte, el juzgado, en el referido auto, entiende que hay *fumus boni iuris* y que los signos empleados por la parte demandada pueden menoscabar las funciones de las marcas de la actora, razón por la cual acuerda la adopción de medidas cautelares.

Ángel García Vidal



Seguridad

Recomendación (UE) 2023/2113 de la Comisión, de 3 de octubre, sobre ámbitos tecnológicos críticos para la seguridad económica de la Unión Europea con vistas a realizar evaluaciones de riesgos adicionales conjuntamente con los Estados miembros

La Comisión Europea, en virtud del Tratado de Funcionamiento de la Unión Europea, específicamente de su artículo 292, ha adoptado una recomendación que responde a la creciente importancia de abordar los riesgos emergentes para la seguridad económica en un contexto de tensiones geopolíticas, integración económica y avances tecnológicos acelerados.

La base de esta iniciativa es la Comunicación conjunta sobre la Estrategia Europea de Seguridad Económica, en la cual la Comisión y el alto representante reconocen la necesidad de un enfoque estratégico global para salvaguardar la seguridad económica en la Unión Europea). Esta estrategia se articula en torno a tres pilares fundamentales: la promoción de la base económica y la competitividad de la Unión, la protección contra riesgos y la asociación con otros países para abordar preocupaciones e intereses comunes.

En este marco, se identifican cuatro amplias categorías de riesgos en la Estrategia Europea de Seguridad Económica: la resiliencia de las cadenas de suministro (incluida la seguridad energética), la seguridad física y ciberseguridad de las infraestructuras críticas, la seguridad tecnológica y filtraciones de tecnología, y la utilización de dependencias económicas como arma y coerción económica.

Para abordar específicamente los riesgos en el ámbito de la seguridad tecnológica, se establecen tres criterios definidos y orientados al futuro: el carácter facilitador y transformador de la tecnología, el riesgo de fusión del uso civil y militar y el riesgo de uso indebido de la tecnología para violaciones de los derechos humanos.

La recomendación prioriza la evaluación colectiva de riesgos en cuatro ámbitos tecnológicos críticos: semiconductores avanzados, inteligencia artificial, tecnologías cuánticas y biotecno-

logías. Se enfatiza que esta evaluación debe llevarse a cabo con los Estados miembros antes de fines del 2023 y se destaca que la lista de tecnologías críticas es un documento dinámico que podría modificarse conforme a los avances tecnológicos.

Claudia Pérez Moneu

Infraestructuras y tecnología

La Unión Europea impulsa un marco de medidas para reforzar el ecosistema europeo de semiconductores

El Parlamento Europeo y el Consejo han aprobado el Reglamento (UE) 2023/1781, de 13 de septiembre, por el que se establece un marco de medidas para reforzar el ecosistema europeo de semiconductores y se modifica el Reglamento (UE) 2021/694 (Reglamento sobre chips), en lo sucesivo, el «Reglamento sobre semiconductores».

La base de la economía digital se sostiene sobre los semiconductores al estar presentes en una gran mayoría de los dispositivos digitales, como los teléfonos móviles. Por ello, y debido en gran parte a su fuerte dependencia de terceros países en la fabricación y diseño de chips, la Unión Europea ha establecido la puesta en marcha de una serie de medidas que pretenden dar a la Unión un papel más importante en el ecosistema de los semiconductores, entre las que cabe destacar las siguientes:

a) La creación y promoción de la iniciativa «Chips para Europa», que tiene por objetivo desarrollar capacidades tecnológicas a gran escala y apoyar las actividades de investigación e innovación conexas en toda la cadena de valor de los semiconductores de la Unión Europea.

b) La creación de normas para identificar y apoyar instalaciones pioneras de producción integrada que promuevan la seguridad del suministro y la resiliencia del sector de los semiconductores en la Unión Europea.

c) La implantación de un mecanismo de coordinación entre la Comisión y los Estados miembros para elaborar un inventario y supervisar el sector de los semiconductores en la Unión Europea.

De esta forma, el Reglamento sobre semiconductores pretende garantizar las condiciones necesarias para la capacidad de innovación y la competitividad en la Unión y mejorar el funcionamiento del mercado interior en el ámbito de los semiconductores.

Cristina Bonfanti Gris

Para más información, contacte con los siguientes letrados del Grupo de Propiedad Intelectual:

Jesús Muñoz-Delgado Mérida

Socio
jmunoz@ga-p.com

Sofía Martínez-Almeida y Alejos-Pita

Socia
smartinez@ga-p.com

Advertencia legal: Este boletín sólo contiene información general y no se refiere a un supuesto en particular. Su contenido no se puede considerar en ningún caso recomendación o asesoramiento legal sobre cuestión alguna.

© Gómez-Acebo & Pombo Abogados, 2023. Todos los derechos reservados.