G A _ P

Gómez-Acebo & Pombo

Boletín

Derecho Digital

N.º 15

Contenido

Protección de datos personales en el ámbito digital

Infracción en materia de datos personales por parte de menores de edad

El 17 de mayo del 2023 se presenta una reclamación ante la Agencia Española de Protección de Datos (AEPD) por la toma y distribución de una fotografía de menores desnudos sin consentimiento. Los hechos ocurrieron en el vestuario de un club de fútbol, donde un menor de catorce años tomó una fotografía de otros cuatro compañeros de equipo menores de edad desnudos y la envió por Instagram a otros menores. La madre de uno de los menores afectados denunció la situación ante la agencia indicando que la imagen fue difundida sin el consentimiento de su hijo.

La agencia efectuó una investigación que confirmó que el menor había distribuido la fotografía sin el consentimiento de los menores involucrados ni de sus progenitores y determinó que la captación y distribución de dicha imagen constituía un tratamiento de datos personales sin base de legitimación que infringía el artículo 6 del Reglamento General de Protección de Datos. La agencia[1] incide en que la imagen de una persona es considerada un dato personal y en que su tratamiento requiere el consentimiento explícito del interesado o, en el caso de menores de catorce años, de sus representantes legales.

Una vez más, esta resolución subraya la importancia de proteger los datos personales de los menores y la necesidad de contar con el consentimiento adecuado para cualquier tratamiento de dichos datos.

Claudia Pérez Moneu

Directrices del Comité Europeo de Protección de Datos sobre seudonimización

El pasado 16 de enero, el Comité Europeo de Protección de Datos publicó las Directrices 01/2025 en materia de seudonimización (*Guidelines 01/2025 on pseudonymisation*, en adelante, las «directrices»), con la finalidad de ofrecer orientaciones en la aplicación de la seudonimización de datos personales de acuerdo con el Reglamento General de Protección de Datos, así como para resaltar las posibilidades de su uso y las ventajas para los responsables y los encargados del tratamiento. A fecha de la presente publicación, las directrices se encuentran en trámite de consulta pública, establecido entre el 17 de enero y el 14 de marzo.

Las directrices resaltan el papel de la seudonimización en la reducción del riesgo de divulgación de identificadores directos y, en el caso de una divulgación no autorizada, en la reducción de la gravedad del riesgo resultante de la falta de confidencialidad y del riesgo de las consecuencias negativas de dicha divulgación. Las directrices

[1] Véase la resolución de la Agencia Española de Protección de Datos en este ***enlace***.

también recalcan la importancia de la seudonimización en la consecución de los principios de protección de datos personales, en concreto, la minimización de datos, la confidencialidad, la licitud, la equidad, la seguridad, la imparcialidad, la limitación de la finalidad y la exactitud.

Asimismo, las directrices detallan el procedimiento de seudonimización y las medidas técnicas y organizativas que impiden la atribución no autorizada de datos seudonimizados, como, por ejemplo, el uso de funciones *hash* criptográficas, cifrado simétrico y asimétrico, y códigos de autenticación de mensajes (MAC), entre otras.

Las directrices aportan, así, una detallada guía sobre el proceso de seudonimización que profundiza en las disposiciones establecidas en el Reglamento de Protección de Datos con el objetivo de facilitar su aplicación por parte de los responsables del tratamiento.

Camino Bustinduy de la Guerra

Protección de datos: solicitudes excesivas

La Sentencia del Tribunal de Justicia de la Unión Europea de 9 de enero del 2025, C416/23, dilucida la cuestión prejudicial planteada por la autoridad austriaca de protección de datos para interpretar varios artículos del Reglamento General de Protección de Datos en el marco de una reclamación planteada por una persona física ante la citada autoridad alegando que no se le había respondido a su solicitud de acceso a sus datos personales. Sin embargo, la autoridad austriaca rechazó la reclamación por considerarla excesiva, dado que dicha persona había presentado numerosas reclamaciones similares en un corto periodo de tiempo.

En primer lugar, el Tribunal de Justicia interpreta el artículo 57.4 del Reglamento General de Protección de Datos en relación con el concepto de *solicitudes*. El término *solicitud* debe entenderse de manera amplia, incluyendo las reclamaciones, ya que esta forma de solicitud también está prevista en el mencionado reglamento. Además, el artículo 57 describe las funciones de las autoridades de control y establece que deben tratar las reclamaciones presentadas por los interesados. Aunque el reglamento establece que el tratamiento de las funciones de las autoridades de control es gratuito, el artículo 57.4 introduce una excepción para las solicitudes que sean manifiestamente infundadas o excesivas, permitiendo a las autoridades establecer tasas razonables o negarse a actuar en tales casos.

En segundo lugar, se plantea si las solicitudes podrían obtener la calificación de *excesivas* simplemente por su número o si se requiere demostrar una intención abusiva por parte del solicitante. Si bien el reglamento no define expresamente el concepto *solicitudes excesivas*, el Tribunal de Justicia concluye que este calificativo no puede otorgarse únicamente por su número, sino que será necesario que la autoridad de control (en este caso, la autoridad austriaca) deberá demostrar la existencia de una intención abusiva en el sujeto que ha presentado dichas solicitudes.

Finalmente, en relación con la tercera cuestión prejudicial, se cuestiona si el artículo 57.4 del Reglamento General de Protección de Datos permite que la autoridad de control elija entre imponer una tasa razonable basada en los costes administrativos o negarse a actuar respecto de solicitudes excesivas. El artículo establece que ambas opciones son alternativas y no se especifica un orden de prioridad entre ellas, lo que implica que la autoridad de control tiene libertad para optar por una u otra. No obstante, en el contexto de ese reglamento, que busca garantizar la protección de los derechos de los interesados, la autoridad debe asegurarse de que su elección sea adecuada, necesaria y proporcional, teniendo en cuenta las circunstancias de cada caso. De

este modo, el reglamento permite a la autoridad de control decidir, en función de las circunstancias, si primero establece una tasa razonable o, en su defecto, se niega a actuar respecto a las solicitudes excesivas, debiendo asegurar en todo caso que la opción elegida sea proporcional y adecuada.

Iratze Arrigain García

Espacio Europeo de Datos de Salud

1. El 5 de marzo del 2025 se ha publicado en el *Diario Oficial de la Unión Europea*, el Reglamento (UE) 2025/327 del Parlamento Europeo y del Consejo, de 11 de febrero, relativo al Espacio Europeo de Datos de Salud, y por el que se modifican la Directiva 2011/24/UE y el Reglamento (UE) 2024/2847. No obstante, el reglamento no será aplicable inmediatamente, pues se prevé (art. 105) una *vacatio legis* de dos años desde el momento en que entre en vigor, plazo de dos años que, en relación con algunas cuestiones concretas, se amplía a cuatro o seis años.

2. Con la nueva regulación —y con el Espacio Europeo de Datos de Salud— se pretende, en primer lugar, facilitar el acceso por parte de los pacientes a sus datos de salud, así como permitir y favorecer su transmisión, incluso en un ámbito transfronterizo. Como se indica en la exposición de motivos del reglamento (apartado 6), «cada vez más personas que viven en la Unión cruzan las fronteras nacionales para trabajar, estudiar, visitar a familiares o por otros motivos». Y «para facilitar el intercambio transfronterizo de datos de salud, y en consonancia con la necesidad de facultar a los ciudadanos, éstos deben poder acceder a sus datos de salud en un formato electrónico que pueda ser reconocido y aceptado en toda la Unión».

   En segundo lugar, el reglamento también tiene por objetivo facilitar el uso de los datos de salud con un fin distinto al del tratamiento médico de la persona a la que pertenecen, como fines de investigación, de salud pública, etc. Este tipo de usos de los datos son denominados en el reglamento *usos secundarios*, por contraposición a los anteriores, que son llamados *usos primarios*[2].

3. Además del derecho de acceso, el nuevo reglamento reconoce otra serie de derechos a las personas titulares de los datos de salud, derechos que podrán ejercer mediante los servicios de acceso a los datos de salud electrónicos o las aplicaciones relacionadas con dichos servicios. Se trata, en concreto, de los siguientes derechos:

   a) El derecho a introducir información en su historia clínica electrónica (art. 5), con el límite de que no podrán modificar directamente los datos de salud electrónicos introducidos por profesionales sanitarios.

   b) El derecho de rectificación (art. 6), que se ejercerá de conformidad con el artículo 16 del Reglamento (UE) 2016/679.

   c) El derecho de portabilidad de los datos o «derecho a permitir el acceso a la totalidad o [a] parte de sus datos de salud electrónicos personales a un prestador

[2] Para una exposición del contenido del Reglamento, se remite a García Vidal, Á., «Diez cuestiones clave sobre el nuevo "Espacio Europeo de Datos de Salud"», GA_P, *Análisis Farma y Salud*, febrero 2025 (véase este **enlace**), y García Vidal, Á., «La nueva obligación de poner datos de salud a disposición de terceros: problemática cuando los datos están protegidos», GA_P, *Análisis Farma y Salud*, enero 2025 (en este **enlace**).

de asistencia sanitaria o a solicitarle que los transmita a otro prestador de asistencia sanitaria de su elección, de forma inmediata, gratuita y sin obstáculos por parte del prestador de asistencia sanitaria o de los fabricantes de los sistemas utilizados por ese prestador de asistencia sanitaria» (art. 7). A efectos de facilitar la transmisión de los datos, se encomienda a la Comisión Europea la creación de un formato europeo de intercambio de historias clínicas (art. 15). Además, la portabilidad de los datos no sólo se aplica a la transmisión entre prestadores de asistencia sanitaria, pues los titulares de los datos de salud también pueden solicitar a un prestador de asistencia sanitaria que transmita — de forma inmediata, gratuita y sin obstáculos— una parte de sus datos de salud electrónicos personales a un destinatario claramente identificado en el sector de la Seguridad Social o de los servicios de reembolso.

d) El derecho a limitar el acceso de los profesionales sanitarios y de los prestadores de asistencia sanitaria a la totalidad o parte de sus datos de salud electrónicos personales (art. 8), sin que los prestadores de asistencia sanitaria puedan ver que se ha ejercido este derecho.

e) El derecho a obtener información sobre cualquier acceso a sus datos de salud electrónicos personales a través del servicio de acceso de los profesionales sanitarios obtenido en el contexto de la asistencia sanitaria (art. 9). Como mínimo, este derecho permitirá obtener información al respecto (durante tres años a partir de la fecha del acceso), que incluirá la relativa al prestador de asistencia sanitaria o a cualquier otra persona que haya accedido a los datos de salud electrónicos personales, la fecha y hora de acceso y los datos de salud electrónicos personales a los que se haya accedido. Se prevé, con todo, que los Estados miembros podrán introducir limitaciones a este derecho en circunstancias excepcionales cuando existan indicios concretos de que la divulgación pondría en peligro los derechos o intereses vitales del profesional sanitario o la asistencia prestada a la persona física.

Ángel García Vidal

Términos de cortesía en los procesos de compra en línea de billetes

En su Sentencia de 9 de enero del 2025 (*Mousse*, C-394/23, ECLI:EU:C:2025:2), el Tribunal de Justicia ha declarado que el Reglamento General de protección de datos [Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos] debe interpretarse en el sentido de que «el tratamiento de datos personales relativos al término de cortesía con que dirigirse a los clientes de una empresa de transporte, cuya finalidad es la personalización de la comunicación comercial basada en su identidad de género no parece ni objetivamente indispensable ni esencial para permitir la correcta ejecución de un contrato y, por tanto, no puede considerarse necesario para la ejecución de ese contrato».

Además, dicho tratamiento de datos personales tampoco puede considerarse necesario para satisfacer intereses legítimos perseguidos por el responsable de dicho tratamiento o por un tercero en estas condiciones:

a) cuando el interés legítimo perseguido no se haya indicado a estos clientes en el momento de la recogida de los datos;

b) cuando dicho tratamiento no se haya llevado a cabo sin sobrepasar los límites de lo estrictamente necesario para la consecución de ese interés legítimo;

c) o cuando, a la vista de todas las circunstancias pertinentes, las libertades y los derechos fundamentales de dichos clientes pueden prevalecer sobre dicho interés legítimo, en particular, debido a un riesgo de discriminación basada en la identidad de género.

Ángel García Vidal

Competencia para resolver sobre la identidad de quién accede al historial clínico

La Sala de lo Contencioso del Tribunal Supremo ha admitido a trámite un recurso de casación en el que el alto tribunal está llamado a interpretar una cuestión de especial interés en relación con la protección de datos de carácter personal. En concreto, se trata de determinar qué órgano es competente para resolver una solicitud de un interesado para conocer la identidad de las personas concretas que han accedido a su historial médico.

En efecto, en su Auto de 6 de noviembre del 2024 (núm. rec. 6263/2024), la Sala de lo Contencioso del Tribunal Supremo admite a trámite el recurso de casación presentado, y fija, como cuestiones con interés casacional objetivo para la formación de jurisprudencia, las siguientes:

1) la determinación de si una solicitud de identidad de tercero que pudiera haber accedido a los datos personales que conciernen al solicitante —en este caso, a su historia clínica— es una materia propia de protección de datos de carácter personal o de acceso a la información pública, y ello a efectos de determinar el órgano competente para resolver dicha solicitud;

2) para el caso de que se entendiera que estamos ante una materia propia de acceso a la información pública, si el interesado tiene derecho a obtener del responsable del tratamiento la identidad de tercero que pudiera haber accedido a los datos personales que le conciernen —en este caso, a su historia clínica—.

Dado el interés de la materia, habrá que estar atentos a la sentencia que dicte en su momento el alto tribunal.

Ángel García Vidal

Inteligencia artificial

Directrices de la Comisión Europea sobre prácticas prohibidas de inteligencia artificial

El pasado 4 de febrero del 2025, la Comisión Europea publicó directrices que detallan las prácticas de inteligencia artificial (IA) prohibidas según el Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio, por el que se establecen normas armonizadas en materia de inteligencia artificial [...] (Reglamento de Inteligencia Artificial; también llamado *ley de inteligencia artificial*). Estas directrices buscan garantizar una aplicación coherente y efectiva

de la normativa en toda la Unión Europea, protegiendo los valores y derechos fundamentales de los ciudadanos.

Las principales prácticas prohibidas son las siguientes:

- Se prohíbe usar sistemas de inteligencia artificial que empleen técnicas que influyan en el comportamiento de las personas sin su conocimiento afectando a su capacidad de decisión y causando posibles perjuicios.
- Está prohibido desarrollar y usar sistemas que aprovechen vulnerabilidades de las personas relacionadas con la edad, discapacidad o situación socioeconómica para alterar su comportamiento de forma perjudicial.
- No se permite clasificar a las personas según su comportamiento social o características personales de forma que resulte en un trato desfavorable o desproporcionado.
- Se prohíbe usar la inteligencia artificial para predecir delitos basándose únicamente en el perfilado de la persona o en la evaluación de sus rasgos de personalidad.
- Se prohíbe usar sistemas de inteligencia artificial para identificar personas en espacios públicos en tiempo real sin una base legal específica, salvo en casos excepcionales, como la prevención de delitos graves y bajo estrictas salvaguardas.
- No se permite usar la inteligencia artificial para detectar emociones en entornos laborales y educativos, excepto cuando su propósito sea médico o relacionado con la seguridad.
- Se prohíbe usar la inteligencia artificial para clasificar a las personas basándose en datos biométricos que infieran características sensibles como raza u orientación sexual.
- Se prohíbe usar la inteligencia artificial para crear o ampliar bases de datos de reconocimiento facial mediante el *scraping* o «raspado» no dirigido de imágenes faciales de internet o de circuitos cerrados de televisión.

Estas directrices, aunque no vinculantes, ofrecen claridad jurídica y ejemplos prácticos para ayudar a las partes interesadas a cumplir los requisitos establecidos en la ley de la inteligencia artificial.

Claudia Pérez Moneu

Avances en la redacción del código de buenas prácticas de la inteligencia artificial y en la plantilla para el resumen de los datos de entrenamiento

Al hilo de la reciente ley de inteligencia artificial, la Oficina Europea de la Inteligencia Artificial está impulsando la redacción de un código de buenas prácticas con el objetivo de detallar y aclarar las disposiciones relativas a los proveedores de modelos de inteligencia artificial de uso general sobre transparencia y derechos de autor, por medio de un proceso colaborativo que involucra a expertos independientes y a alrededor de mil partes interesadas. En particular, se encuentran participando en el proyecto proveedores de modelos de inteligencia artificial de uso general, proveedores intermedios, organizaciones del sector, participantes procedentes de la sociedad civil, titulares de derechos y académicos, entre otros.

El proceso de redacción interactivo está estructurado en cuatro grupos de trabajo sobre temas específicos y tendrá lugar hasta abril del 2025. En mayo se publicarán tanto la versión final del texto como el análisis que de él hagan la Oficina y la Junta de la Inteligencia Artificial. Finalmente,

la Comisión aprobará el código mediante un acto de ejecución.

Paralelamente, de manera complementaria a la redacción del código, la Oficina de la Inteligencia Artificial está avanzando en el desarrollo de la plantilla para el resumen de los datos de entrenamiento que los proveedores de modelos de inteligencia artificial de uso general están obligados a publicar de conformidad con la ley de inteligencia artificial. La plantilla establecerá la estructura y contenido mínimo de los datos de entrenamiento que serán requeridos a todos los proveedores de dichos modelos.

El código de buenas prácticas de inteligencia artificial de uso general y la plantilla para el resumen de los datos de entrenamiento confirman la apuesta de la Unión Europea por avanzar en la innovación de una manera equilibrada asegurando el respeto a los derechos e intereses legítimos que puedan verse afectados por los crecientes avances en la inteligencia artificial.

Camino Bustinduy de la Guerra

Opinión 28/2024 del CEPD, sobre ciertos aspectos de protección de datos relacionados con el tratamiento de datos personales en el contexto de los modelos de inteligencia artificial

El Comité Europeo de Protección de Datos (CEPD) ha emitido la Opinión 28/2024, sobre las implicaciones del Reglamento General de Protección de Datos (RGPD) en el contexto del desarrollo y despliegue de modelos de inteligencia artificial. La autoridad supervisora de Irlanda solicitó una opinión a dicho comité en relación con la aplicación del artículo 64.2 del citado reglamento para abordar cuestiones clave relacionadas con la protección de datos personales en el ámbito de la inteligencia artificial, especialmente en cuanto a la anonimización de los modelos de inteligencia artificial, la justificación del interés legítimo como base legal y las consecuencias de tratar datos de manera ilícita.

En cuanto a la anonimización, se señala que los modelos de inteligencia artificial entrenados con datos personales no pueden considerarse automáticamente anónimos, ya que la probabilidad de extraer información personal de los datos utilizados, directa o indirectamente, no puede ser descartada. De esta forma, la evaluación de anonimización debe realizarse caso por caso, teniendo en cuenta las medidas adoptadas por el responsable del tratamiento durante el desarrollo para minimizar la identificación de los datos.

En segundo lugar, respecto a la aplicación del interés legítimo como base legal para el tratamiento de los datos en este contexto, el Comité Europeo de Protección de Datos subraya que los responsables del tratamiento deben llevar a cabo una evaluación detallada en tres pasos: 1) identificar claramente el interés legítimo; 2) verificar que el tratamiento sea necesario para alcanzar ese interés, y 3) asegurarse de que los derechos y libertades de los individuos no prevalezcan sobre ese interés. Esta evaluación debe considerar las expectativas razonables de los interesados y los posibles efectos del procesamiento en sus derechos, considerando además el contexto en el que los datos fueron obtenidos. En situaciones en las que los derechos de los interesados pudieran ser vulnerados, el responsable puede poner en ejecución medidas mitigadoras para reducir el impacto negativo. Dichas medidas deben adaptarse a las características específicas de cada caso y del modelo de inteligencia artificial en cuestión.

Finalmente, el texto aborda las consecuencias de un tratamiento ilícito de datos personales en las distintas fases de desarrollo y despliegue de

un modelo de inteligencia artificial, analizando tres posibles escenarios. En el primer escenario, si los datos personales son conservados y tratados en la fase de despliegue, se debe evaluar si la falta de base legal en la fase de desarrollo afecta a la legalidad del tratamiento posterior. En el segundo escenario, si el tratamiento es realizado por otro responsable en la fase de despliegue, se debe revisar si se ha realizado una evaluación adecuada para garantizar el cumplimiento del Reglamento General de Protección de Datos. En el tercer escenario, cuando los datos se tratan ilegalmente para el desarrollo del modelo, pero luego se anonimiza, el procesamiento posterior no estará afectado por la ilegalidad inicial, siempre que no se procesen más datos personales.

Iratze Arrigain García

Comercio electrónico

Supresión de la plataforma europea de resolución de litigios en línea

El Reglamento (UE) 2024/3228, adoptado el 19 de diciembre, establece la derogación del Reglamento (UE) núm. 524/2013 y la supresión de la plataforma europea de resolución de litigios en línea. Asimismo, introduce modificaciones en los Reglamentos (UE) 2017/2394 y (UE) 2018/1724 con el fin de eliminar cualquier referencia a esta plataforma en la normativa vigente.

La decisión de suprimir la mencionada plataforma se fundamenta en su limitada eficacia para la resolución extrajudicial de litigios entre consumidores y comerciantes en línea. A pesar de registrar entre dos y tres millones de visitas anuales, sólo una minoría de los usuarios hacía uso del sistema para presentar reclamaciones. De éstas, únicamente el 2 % recibía una respuesta positiva por parte de los comerciantes, lo que se traducía en menos de doscientos asuntos gestionados por entidades de resolución alternativa cada año en toda la Unión Europea. Esta escasa utilización de la plataforma ha llevado a la Comisión Europea a concluir que su mantenimiento no responde a los principios de eficiencia y eficacia exigidos por la normativa de la Unión.

El reglamento establece que el 20 de julio del 2025 será la fecha efectiva de la derogación del Reglamento (UE) núm. 524/2013 y de la eliminación definitiva de la plataforma europea de resolución de litigios en línea. A partir del 20 de marzo del 2025 ya no se podrán presentar nuevas reclamaciones a través de esta plataforma. A más tardar el 20 de julio del 2025, toda la información almacenada en la plataforma, incluidos los datos personales, será eliminada de forma definitiva.

Claudia Pérez Moneu

Identidad digital europea

Actos de ejecución de la Cartera de Identidad Digital Europea

El 28 de noviembre del 2024, la Comisión aprobó los primeros cinco actos de ejecución de la Cartera Europea de Identidad Digital, en particular:

— El Reglamento de Ejecución (UE) 2024/2977 establece normas en relación con la expedición de datos de identificación de la persona y las declaraciones electrónicas de atributos expedidos a unidades de cartera.

— El Reglamento de Ejecución (UE) 2024/2979 constituye un marco normativo sobre la integridad y las funcionalidades básicas de las carteras europeas de identidad digital.

— El Reglamento de Ejecución (UE) 2024/2980 establece obligaciones en relación con el sistema de notificaciones a la Comisión en el ecosistema de la Cartera Europea de Identidad Digital.

— El Reglamento de Ejecución (UE) 2024/2981 recoge normas de referencia, especificaciones y procedimientos en relación con la certificación de las carteras europeas de identidad digital.

— El Reglamento de Ejecución (UE) 2024/2982 establece los protocolos y las interfaces de las soluciones de cartera que admitirá el marco europeo de identidad digital, para la expedición de datos de identificación de la persona y declaraciones electrónicas de atributos a unidades de cartera, la presentación a las partes usuarias de la cartera y a otras unidades de cartera, la comunicación de las solicitudes de supresión de datos a las partes usuarias y la denuncia por éstas ante las autoridades de control establecidas.

Camino Bustinduy de la Guerra

Ciberseguridad

Reglamento (UE) 2024/2847 del Parlamento Europeo y del Consejo, de 23 de octubre, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales

El Reglamento (UE) 2024/2847 (Reglamento de Ciberresiliencia), adoptado el 23 de octubre del 2024 por el Parlamento Europeo y el Consejo, tiene como objetivo fundamental reforzar la ciberseguridad de los productos digitales (tanto *hardware* como *software*) en la Unión Europea, desde su desarrollo hasta su desactivación, fijando

estándares y obligaciones particulares que se detallan a continuación.

En primer lugar, con respecto a los productos con componentes digitales, según el riesgo que suponen, establece una diferenciación entre importantes —como los sistemas de gestión de redes, navegadores independientes e integrados, etc.— y críticos —como dispositivos de equipos informáticos con cajas de seguridad, o tarjetas inteligentes que incluyan elementos seguros—.

En segundo lugar, el reglamento impone obligaciones a los operadores económicos en varias fases de la vida del producto. En principio, los fabricantes deben diseñar y producir los productos de conformidad con lo establecido en el anexo I, parte I, del reglamento; llevar a cabo una evaluación de riesgos de ciberseguridad asociados, y proporcionar soporte continuo para la actualización y mantenimiento de estos componentes digitales, entre otros. Asimismo, se impone a los fabricantes la obligación de notificar a un equipo de respuesta a incidentes de seguridad informática (CSIRT) o a la Agencia de la Unión Europea para la Ciberseguridad (ENISA) cualquier vulnerabilidad aprovechada en su producto con elementos digitales de la que tengan conocimiento, y establece unos plazos y un contenido concreto para ello. También prevé, para los fabricantes y otras personas físicas o jurídicas, la notificación voluntaria de cualquier incidente que repercuta en la seguridad del producto. Del mismo modo, los importadores sólo podrán introducir en el mercado los productos que cumplan el anexo mencionado anteriormente, y a los distribuidores se les impone el deber de diligencia debida en relación con los requisitos establecidos en el reglamento.

En relación con las sanciones, las autoridades de vigilancia del mercado designadas en cada Estado miembro monitorizarán el cumplimiento del reglamento, si bien el régimen de sanciones incluye multas de hasta quince millones de euros o el 2,5 % del volumen de negocios anual global del infractor en caso de que sea una empresa. El reglamento será aplicable a partir del 11 de diciembre del 2027; aunque algunas de sus disposiciones entrarán en vigor antes y serán aplicables desde el 11 de septiembre del 2026.

Iratze Arrigain García

Para más información, contacte con las siguientes letradas del Grupo de Propiedad Intelectual:

Sofía Martínez-Almeida y Alejos-Pita
Socia
smartinez@ga-p.com

Rais Amils Arnal
Socia
ramils@ga-p.com