G A _ P

Gómez-Acebo & Pombo

Boletín

DERECHO DIGITAL

N.º 18

G A _ P
Gómez-Acebo & Pombo

Contenido

Protección de datos personales en el ámbito digital

La indemnización de daños inmateriales en el Reglamento General de protección de datos

El Tribunal de Justicia de la Unión Europea (Sala Cuarta) resolvió una cuestión prejudicial planteada por el Bundesgerichtshof (Tribunal Federal de Justicia) alemán a raíz de la divulgación accidental, por parte de una empleada de un banco, de las expectativas salariales de un candidato a través de una red profesional. El afectado solicitó una orden de abstención frente a futuros tratamientos ilícitos y una indemnización por daño moral. El tribunal de primera instancia estimó ambas pretensiones; el Oberlandesgericht (Tribunal Superior Regional) de Fráncfort mantuvo la orden de abstención (con base en el artículo 17.1 del Reglamento General de protección de datos —RGPD—), pero denegó la indemnización por falta de prueba del perjuicio. Ambas partes interpusieron un recurso de casación.

El Tribunal de Justicia de la Unión Europea declara, en primer lugar, que el Reglamento General de protección de datos no reconoce una acción preventiva autónoma que permita obtener, por sí misma, una *orden de abstención* distinta de los derechos de supresión o limitación del tratamiento (arts. 17 y 18) ni el artículo 79 obliga a los Estados miembros a establecer tal remedio específico. No obstante, nada impide que el Derecho nacional prevea una acción de cesación, siempre que respete los principios de equivalencia y efectividad del Derecho de la Unión.

En segundo lugar, respecto del artículo 82.1 del Reglamento General de protección de datos, el concepto de *daño inmaterial* comprende sentimientos negativos como temor, enfado o humillación derivados de la pérdida de control sobre los datos, del riesgo de un uso indebido o de un menoscabo reputacional, siempre que dichos sentimientos y sus consecuencias estén probados y exista un nexo causal con la infracción. No se exige la superación de un umbral mínimo ni la acreditación de consecuencias tangibles adicionales.

En tercer lugar, la indemnización prevista en el artículo 82 tiene carácter estrictamente compensatorio: el grado de culpa del responsable no constituye un criterio autónomo de cuantificación. Corresponde al Derecho nacional fijar las reglas de cálculo, respetando los principios de equivalencia y efectividad. Incluso puede estipularse la fijación de una indemnización mínima o, según el ordenamiento, una reparación mediante disculpa, siempre que ello asegure una compensación íntegra del perjuicio.

Por último, la existencia o concesión de una orden de abstención no puede reducir ni sustituir

la indemnización reconocida en virtud del artículo 82.1 si ello compromete la reparación plena y efectiva del daño. La combinación de remedios sólo es conforme con el Reglamento General de protección de datos en la medida en que, en la práctica, garantice la restitución integral de la situación del interesado.

Iratze Arrigain García

El concepto de datos seudonimizados

El Tribunal de Justicia de la Unión Europea ha estimado el recurso de casación del Supervisor Europeo de Protección de Datos (SEPD), ha anulado la sentencia del Tribunal General de 26 de abril del 2023 (T-557/20) y ha devuelto el asunto para que se examine un motivo pendiente de resolución, reservándose las costas.

El litigio surgió en el marco del procedimiento del derecho a ser oído en la resolución del Banco Popular. La Junta Única de Resolución (JUR) recabó datos de accionistas y acreedores y remitió a Deloitte los comentarios de la fase de consulta vinculados a un código alfanumérico. El Supervisor Europeo de Protección de Datos apreció infracción del artículo 15.1*d* por no informar de Deloitte como destinataria, mientras que el Tribunal General había considerado que lo transmitido no constituía datos personales.

El Tribunal de Justicia corrige dos aspectos fundamentales. En primer lugar, aclara que la noción de *dato personal* (art. 3.1) coincide con la interpretación del Reglamento General de protección de datos: incluye toda información objetiva o subjetiva, como opiniones o valoraciones «sobre» su autor. Los comentarios remitidos por los interesados son, pues, datos personales de quienes los formularon, sin necesidad de un análisis adicional cuando su carácter opinativo resulta evidente. En segundo lugar, precisa que la seudonimización (art. 3.6) presupone la existencia de información adicional que permite la identificación, por lo que no equivale a anonimización ni excluye el carácter personal de los datos. Así, para la Junta Única de Resolución, que conservaba la clave, los comentarios seguían siendo datos personales; para Deloitte, sólo dejarían de serlo si existieran medidas que impidieran razonablemente la reidentificación.

En cuanto a la transparencia, el tribunal subraya que la obligación del artículo 15.1*d* de informar sobre destinatarios o categorías debe cumplirse desde el momento de la recogida y en función de la posición del responsable. Como la Junta Única de Resolución podía identificar a los autores, estaba obligada a informar de Deloitte como posible destinataria.

En consecuencia, el fallo refuerza la amplitud del concepto de *dato personal*, delimita claramente la diferencia entre seudonimización y anonimización y recuerda que la transparencia *ex ante* sobre los destinatarios es esencial para la validez del consentimiento y la decisión del interesado de facilitar sus datos. Las instituciones deberán revisar sus cláusulas informativas para identificar de manera expresa a terceros (o a categorías de destinatarios) que intervengan en procedimientos consultivos o periciales.

Claudia Pérez Moneu

Respuesta de la AEPD a la cuestión previa sobre adecuación y proporcionalidad de sistemas biométricos para la autenticación

El 27 de marzo del 2025, la Agencia Española de Protección de Datos (AEPD) recibió una consulta previa de las fuerzas y cuerpos de seguridad del Estado sobre un sistema de autenticación basado en información biométrica para acceder a unas instalaciones de la Guardia Civil, dirigido tanto a visitantes como a trabajadores y a los residentes de las viviendas que se localizan en el recinto. De acuerdo con la consulta, el uso de la tecnología biométrica se justificaría porque se trata de una infraestructura crítica y el tratamiento va dirigido a la prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

En este sentido, la Agencia Española de Protección de Datos ha determinado que el sistema objeto de la consulta cumple el requisito de proporcionalidad establecido en la doctrina del Tribunal Constitucional y del Tribunal de Justicia de la Unión Europea, por cuanto responde al objetivo legítimo de proteger edificios e instalaciones de la Guardia Civil y resulta adecuado para alcanzarlo, ya que el tratamiento biométrico confiere mayor grado de fiabilidad que otros mecanismos de acceso a espacios protegidos, como el uso de tarjetas físicas, claves o control presencial, que no alcanzan un nivel equivalente de eficacia.

La agencia ha valorado que las fuerzas y cuerpos de seguridad del Estado han adoptado medidas técnicas para mitigar los riesgos respecto de los derechos de los interesados, como la generación local de identificadores no interoperables ni reversibles, el control exclusivo por el interesado, la ausencia de almacenamiento centralizado y la limitación estricta a los fines de autenticación. La agencia también ha tenido en cuenta que el sistema ofrece la posibilidad de ajuste en espacios residenciales o de menos criticidad.

En definitiva, la Agencia Española de Protección de Datos ha concluido que no se dispone de una alternativa que, con la misma eficacia, permita alcanzar los objetivos perseguidos con un grado menor de injerencia. Asimismo, entiende que las medidas adoptadas aseguran que, en el caso de que los derechos de los interesados se puedan ver afectados, ello será dentro de un límite proporcionado respecto de los fines legítimos que se pretenden alcanzar.

Camino Bustinduy de la Guerra

Inteligencia artificial

El «Código de buenas prácticas de inteligencia artificial de uso general» y las directrices complementarias de la Comisión

El 10 de julio del 2025, la Comisión Europea publicó el «Código de buenas prácticas de inteligencia artificial de uso general» con la finalidad de orientar a los proveedores de modelos de inteligencia artificial general en el cumplimiento de las obligaciones del Reglamento de Inteligencia Artificial, especialmente en materia de transparencia, derechos de autor y seguridad. Con carácter complementario, la Comisión Europea ha publicado directrices sobre conceptos clave (por ejemplo, el modelo de inteligencia artificial general, la obligación de documentación y los criterios de riesgo) con el objetivo de armonizar su interpretación. En septiembre del 2025 ya se han adherido al código numerosos proveedores de inteligencia artificial general, entre otros, Amazon, Google, Microsoft, y OpenAI.

El código se compone de tres capítulos: «Transparencia», «Derechos de autor» y «Seguridad y protección». Los dos primeros están dirigidos a todos los proveedores de inteligencia artificial general y establecen tanto compromisos de documentación, suministro de información y soluciones prácticas en relación con las características, limitaciones y posibles riesgos de sus modelos como la garantía del uso legítimo de contenido protegido por los derechos de autor. Por su parte, el capítulo «Seguridad y protección» describe medidas reforzadas de gestión de riesgos, notificación de incidentes y pruebas de robustez para los modelos más avanzados que puedan generar riesgos sistémicos.

Aun siendo una herramienta voluntaria, el código se configura como un estándar de referencia práctico que no sólo brinda a los proveedores de inteligencia artificial general la posibilidad de aligerar la carga administrativa derivada de las obligaciones del nuevo marco normativo establecido por el Reglamento de Inteligencia Artificial, sino que también refuerza la seguridad jurídica en el cumplimiento de sus disposiciones.

Camino Bustinduy de la Guerra

Proyecto de informe de la Comisión de Empleo y Asuntos Sociales del Parlamento Europeo recomendando a la Comisión Europea iniciar el proceso legislativo para una directiva de la Unión sobre gestión algorítmica en el lugar de trabajo

El Parlamento Europeo ha sometido a consulta un informe con recomendaciones dirigidas a la Comisión Europea sobre la digitalización, la inteligencia artificial y la gestión algorítmica en el entorno laboral.

Por una parte, el informe recalca la necesidad de transparencia y consulta. En particular, los trabajadores y los autónomos deberán ser informados con claridad por sus empleadores y contratistas sobre el uso de sistemas para la gestión algorítmica en su entorno laboral, incluyendo qué categoría de datos se recogen, con qué finalidad y si hay toma de decisiones automatizada. Además, se establece que la implementación de nuevos sistemas de gestión algorítmica deberá ser objeto de consulta cuando implique alteraciones significativas de las condiciones laborales.

El informe también propone prohibir el tratamiento de datos personales cuando afecte, entre otros, al estado emocional o psicológico de los trabajadores o autónomos, a conversaciones privadas o al comportamiento en el tiempo libre o en estancias privadas. Asimismo, propone garantizar que ciertas decisiones (como la contratación, el despido o modificaciones en la retribución) no se adopten exclusivamente mediante gestión algorítmica, sino que deban estar sujetas a supervisión humana.

Por otra parte, el informe también aboga por reforzar la obligación de evaluar los riesgos que afecten a la salud y a la seguridad derivados del uso de una gestión algorítmica y la de adoptar medidas preventivas. Asimismo, se propone atribuir competencias a las autoridades nacionales de inspección laboral para supervisar la implantación de la gestión algorítmica en el lugar de trabajo.

En conclusión, la finalidad del informe es impulsar una directiva específica que permita complementar la regulación actual del Reglamento de Inteligencia Artificial y del Reglamento General de protección de datos para dar respuesta a las cuestiones específicas que plantea la adopción de sistemas de gestión algorítmica que están transformando el entorno laboral.

Camino Bustinduy de la Guerra

Comercio electrónico

La Directiva de comercio electrónico y la telemedicina

Como es sabido, la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico), dispone, en su artículo 3.1, que «todo Estado miembro velará por que los servicios de la sociedad de la información facilitados por un prestador de servicios establecido en su territorio respeten las disposiciones nacionales aplicables en dicho Estado miembro que formen parte del ámbito coordinado», entendiéndose por *ámbito coordinado* (art. 2) «los requisitos establecidos en los regímenes jurídicos de los Estados miembros y aplicables a los prestadores de servicios de la sociedad de la información o a los servicios de la sociedad de la información, independientemente de si son de tipo general o destinados específicamente a los mismos».

Pues bien, sobre esa base, el Tribunal de Justicia —en su Sentencia de 11 de septiembre del 2025 (C-115/24)— ha declarado que el citado artículo 3.1 de la Directiva sobre el comercio electrónico debe interpretarse en el sentido de que las prestaciones de telemedicina deben proporcionarse con arreglo a la legislación del Estado miembro en el que está establecido el prestador. Y en el mismo sentido opera, según el Tribunal de Justicia, la Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza, cuando dispone (art. 3*d*) que «en el caso de la telemedicina, la asistencia sanitaria se considerará prestada en el Estado miembro donde esté establecido el prestador».

Por lo demás, y en relación con la Directiva 2011/24/UE, el Tribunal de Justicia declara que debe interpretarse en el sentido de que «el concepto de *asistencia sanitaria transfronteriza* prestada en el caso de la telemedicina, a efectos de dicha disposición, corresponde únicamente a la asistencia sanitaria proporcionada a un paciente por un prestador de asistencia sanitaria establecido en un Estado miembro distinto del Estado miembro de afiliación de ese paciente, a distancia y, por tanto, sin la presencia física simultánea en el mismo lugar del citado paciente y del referido prestador, exclusivamente por medio de las tecnologías de la información y la comunicación».

Ángel García Vidal

Infracción de marca y almacenamiento de productos en el territorio de un Estado que no es el de registro de la marca

Según la Directiva (UE) 2015/2436 del Parlamento Europeo y del Consejo, de 16 de diciembre,

relativa a la aproximación de las legislaciones de los Estados miembros en materia de marcas (art. 10.2), el titular de una marca registrada está facultado para prohibir a cualquier tercero el uso, sin su consentimiento, en el tráfico económico, de cualquier signo relacionado con los productos o servicios *a*) cuando el signo sea idéntico a la marca y se utilice en relación con productos o servicios idénticos a aquellos para los que la marca esté registrada; *b*) cuando el signo sea idéntico o similar a la marca y se utilice en relación con productos o servicios idénticos o similares a los productos o servicios para los que esté registrada la marca, si existe un riesgo de confusión por parte del público (el riesgo de confusión comprende el riesgo de asociación entre el signo y la marca), o *c*) cuando el signo sea idéntico o similar a la marca, independientemente de si se utiliza para productos o servicios que sean idénticos o sean o no similares a aquellos para los que esté registrada la marca, cuando ésta goce de renombre en el Estado miembro y, con el signo usado sin justa causa, se pretenda obtener una ventaja desleal del carácter distintivo o del renombre de la marca o ese uso sea perjudicial para tal carácter distintivo o dicho renombre. En estos casos, el titular de la marca podrá prohibir, entre otras conductas, la de «ofrecer los productos, comercializarlos o almacenarlos con dichos fines u ofrecer o prestar servicios con el signo» (art. 10.3*b*).

Pues bien, el Tribunal de Justicia —en su Sentencia de 1 de agosto del 2025, C-776/24, ECLI: EU:C:2025:593— ha declarado que el titular de una marca protegida en un Estado miembro está facultado para prohibir a un tercero el almacenamiento en el territorio de otro Estado miembro de productos con un signo en las condiciones previstas en el artículo 10, apartado 2, de esa directiva con el fin de ofrecerlos a la venta o comercializarlos en el Estado miembro en el que esa marca esté protegida.

Además, según el Tribunal de Justicia, para «almacenar» un producto con un signo en las condiciones establecidas en el artículo 10, apartado 2, de dicha directiva, basta con disponer de un poder de control o de dirección sobre la persona que tiene el dominio directo y efectivo del citado producto.

Ángel García Vidal

Consulta pública de la Comisión sobre la Propuesta de Ley de Equidad Digital (Digital Fairness Act)

La Comisión Europea ha lanzado una consulta pública (de 17 de julio a 24 de octubre del 2025) y una convocatoria de datos con vistas a una futura ley de equidad digital orientada a reforzar la protección de los consumidores en entornos en línea, con especial atención a menores y colectivos vulnerables. La consulta, disponible en las veinticuatro lenguas oficiales de la Unión Europea, se prolongará doce semanas y su síntesis se publicará en un plazo de ocho semanas tras su cierre.

La iniciativa, basada en el artículo 114 del Tratado de Funcionamiento de la Unión Europea, prevé una propuesta legislativa en el tercer trimestre del 2026 y se plantea como complemento de los reglamentos conocidos como *ley de servicios digitales* (DSA) y *ley de mercados digitales* (DMA) y de la normativa de consumo, con el fin de colmar lagunas regulatorias y reducir la fragmentación que eleva costes y merma la seguridad jurídica.

El cuestionario aborda cuestiones como interfaces engañosas y técnicas manipuladoras, diseño adictivo *(infinite scroll, autoplay)* con especial incidencia en menores, dinámicas de

videojuegos, personalización y fijación dinámica de precios, *marketing* de *influencers*, prácticas de precios engañosas (*drip pricing*, descuentos ficticios) y cláusulas de contratos digitales que dificultan bajas o fomentan renovaciones automáticas.

En cuanto al impacto, la Comisión espera reforzar la confianza del consumidor, simplificar reglas y abaratar costes para operadores transfronterizos, además de generar efectos sociales positivos y salvaguardar los derechos fundamentales. El análisis incluirá un estudio específico y un diálogo práctico de aplicación, con participación de consumidores, autoridades, pymes, plataformas, *influencers*, organizaciones no gubernamentales y el sector académico.

Claudia Pérez Moneu

Disposiciones de aplicación del Reglamento (UE) núm. 910/2014

a) *Reglamento de Ejecución (UE) núm. 2025/1570 de la Comisión, de 29 de julio, por el que se establecen disposiciones de aplicación del Reglamento (UE) núm. 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a la notificación de información sobre dispositivos cualificados de creación de firma electrónica certificados y dispositivos cualificados de creación de sello electrónico certificados.*

   La Comisión Europea ha fijado el contenido mínimo, el formato y el canal electrónico seguro para que los Estados miembros notifiquen la información sobre dispositivos cualificados de creación de firma y sello electrónico certificados, o cuya certificación haya cesado, conforme al Reglamento (UE) núm. 910/2014, de 23 de julio, del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (Reglamento eIDAS). El objetivo es disponer de una fuente pública, transparente y fiable sobre su estado de certificación, de acuerdo con los artículos 31.3 y 39.3. El Supervisor Europeo de Protección de Datos emitió su dictamen el 6 de junio del 2025, y en el reglamento de ejecución se recuerda la aplicabilidad del Reglamento General de protección de datos y, en su caso, de la Directiva 2002/58/CE.

   Las notificaciones deberán realizarse por el canal seguro habilitado por la Comisión y habrán de actualizarse ante cualquier cambio, en particular sobre el estado de certificación. El anexo precisa los datos obligatorios, que comprenden la identificación del producto y versiones, el solicitante, la categoría del dispositivo, el certificado de conformidad y el informe de certificación, la identidad y el contacto del organismo emisor, las fechas de vigencia, el método de certificación y, en su caso, referencias a informes o documentos técnicos adicionales.

   El reglamento de ejecución se publicó en el *Diario Oficial de la Unión Europea* el 30 de julio del 2025, entró en vigor a los veinte días y será aplicable a partir del 19 de diciembre del 2025. Los fabricantes y prestadores cualificados deberán adaptar sus expedientes a los nuevos campos y garantizar la publicación y actualización de los informes, mientras que las autoridades nacionales deberán organizar los flujos de notificación para contar con una base pública completa y actualizada en la fecha de aplicación.

b) *Reglamento de Ejecución (UE) núm. 2025/1569 de la Comisión, de 29 de julio, por el que se establecen disposiciones de aplicación del Reglamento (UE) núm. 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a las declaraciones electrónicas cualificadas de atributos y las declaraciones electrónicas de atributos proporcionadas por un organismo del sector público responsable de una fuente auténtica, o en nombre de éste.*

El Reglamento de Ejecución (UE) núm. 2025/1569, de 29 de julio, desarrolla el Reglamento eIDAS en materia de declaraciones electrónicas de atributos, tanto cualificadas como emitidas por organismos públicos responsables de fuentes auténticas. Su objetivo es armonizar su expedición, crear una lista pública de organismos emisores, establecer dos catálogos (atributos y sistemas de declaración) y fijar el marco de cotejo con fuentes auténticas o intermediarios designados.

Los prestadores deberán aplicar la norma ETSI EN 319 401 v3.1.1 y el formato previsto para las carteras EUDI, respetar la minimización de datos, verificar la legitimación del representante cuando proceda y, si la declaración se entrega a una cartera, autenticarse frente a ella y comprobar que no esté revocada o suspendida. La revocación corresponde al emisor y será obligatoria, entre otros supuestos, a petición del interesado, por riesgos de seguridad o por exigencia normativa. El estado de validez deberá publicarse preservando la privacidad y evitando trazabilidad.

Los Estados miembros notificarán a la Comisión los organismos públicos emisores por canal seguro, y ésta publicará una lista firmada electrónicamente, accesible y legible por humanos y máquinas. Se crean además el catálogo de atributos (obligatorio para los del anexo VI del Reglamento eIDAS) y el catálogo de sistemas, ambos públicos y consultables, con identificadores únicos y metadatos semánticos. Para el cotejo de atributos, los Estados miembros deberán habilitar mecanismos electrónicos, eventualmente un punto único nacional, que permitan la verificación bajo control de acceso y con respuestas limitadas a la confirmación y la identificación del organismo verificador.

El reglamento de ejecución entrará en vigor a los veinte días de su publicación y será aplicable, en lo relativo a los artículos 6 a 9, a partir del 19 de agosto del 2026.

c) *Reglamento de Ejecución (UE) núm. 2025/1566 de la Comisión, de 29 de julio, por el que se establecen disposiciones de aplicación del Reglamento (UE) núm. 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a las normas de referencia para la verificación de la identidad y el cotejo de los atributos de la persona a la que va a expedirse el certificado cualificado o la declaración electrónica cualificada de atributos.*

El Reglamento de Ejecución (UE) núm. 2025/1566, desarrolla el artículo 24.1 *quater* del Reglamento eIDAS para fijar normas de referencia en la verificación de identidad y el cotejo de atributos en la expedición de certificados cualificados o declaraciones electrónicas cualificadas de atributos. Su finalidad es homogeneizar prácticas entre prestadores cualificados y garantizar resultados fiables e interoperables en la Unión Europea. La Comisión adopta como norma central la especificación técnica ETSI TS 119 461 V2.1.1 (2025-02), con adaptaciones

específicas, y remite a la ETSI EN 319 401 V3.1.1 como requisito de política general. Se recuerda la aplicabilidad del Reglamento General de protección de datos y, en su caso, de la Directiva 2002/58/CE, así como el dictamen del Supervisor Europeo de Protección de Datos de 6 de junio del 2025.

El reglamento de ejecución entró en vigor a los veinte días de su publicación (*DOUE* L de 30 de julio del 2025) y será aplicable a partir del 19 de agosto del 2027, otorgando un amplio periodo transitorio para auditorías y adaptación.

El anexo introduce exigencias reforzadas frente a la norma ETSI, entre ellas: revisión *inter pares* o certificación de nivel alto para procesos vinculados a pruebas fidedignas; evaluaciones acreditadas con certificado de conformidad y análisis de seguridad frente a amenazas; parámetros objetivos de error en procesos automatizados basados en metodologías de la Agencia de la Unión Europea para la Ciberseguridad (ENISA, por sus siglas en inglés) o equivalentes; validación de documentos físicos por laboratorios acreditados o autoridades nacionales cada dos años desde el 2027, y planes de cese del servicio alineados con el artículo 24.5 del Reglamento eIDAS.

En conjunto, se consolida un marco técnico armonizado para el proceso de incorporación cualificado, presencial, remoto, híbrido o automatizado, con obligaciones verificables y plazos claros para su despliegue.

d) *Reglamento de Ejecución (UE) núm. 2025/1567 de la Comisión, de 29 de julio, por el que se establecen disposiciones de aplicación del Reglamento (UE) núm. 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a la gestión de dispositivos cualificados de creación de firma electrónica a distancia y de dispositivos cualificados de creación de sello electrónico a distancia como servicios de confianza cualificados.*

El Reglamento de Ejecución (UE) núm. 2025/1567 de la Comisión desarrolla el Reglamento eIDAS en lo relativo a la gestión de dispositivos cualificados de creación de firma y sello electrónico a distancia como servicios de confianza cualificados. La norma busca reforzar la seguridad jurídica y la fiabilidad de estos servicios, que resultan esenciales en la transición digital de los procedimientos jurídicos y administrativos (art. 29 *bis* y 39 *bis* del Reglamento eIDAS).

El texto establece, mediante un anexo técnico, las normas de referencia y especificaciones aplicables, destacando la incorporación de la ETSI TS 119 431-1 V1.3.1 (2024-12), junto con referencias normativas como la ETSI EN 319 401 V3.1.1 (2024-06) y los mecanismos criptográficos acordados por la Agencia de la Unión Europea para la Ciberseguridad (ENISA). Entre las exigencias novedosas sobresalen las siguientes:

a) la obligación de que los prestadores de servicios de aplicación de firma en servidor empleen personal y subcontratistas con cualificación acreditada y actualizada periódicamente frente a nuevas amenazas;

b) la obligación de auditorías de seguridad más estrictas, con escaneos de vulnerabilidades trimestrales y cortafuegos configurados restrictivamente;

c) la previsión de planes de cese de servicio ajustados al artículo 24.5 del Reglamento (UE) núm. 910/2014 (eIDAS);

d) controles criptográficos reforzados, con selección de técnicas conformes a los estándares europeos de ciberseguridad.

Asimismo, se impone que la declaración de prácticas del prestador de servicios incluya la referencia a la certificación del dispositivo cualificado de creación de firma electrónica, conforme al anexo II del Reglamento eIDAS. El reglamento reconoce la aplicabilidad del Reglamento (UE) 2016/679 (RGPD) y de la Directiva 2002/58/CE, garantizando la coherencia con el marco de protección de datos, y fija su entrada en vigor a los veinte días de su publicación, si bien será aplicable a partir del 19 de agosto del 2027.

e) *Reglamento de Ejecución (UE) 2025/1568 de la Comisión, de 29 de julio, por el que se establecen disposiciones de aplicación del Reglamento (UE) núm. 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a las modalidades de procedimiento aplicables a las revisiones* inter pares *de los sistemas de identificación electrónica y a la cooperación para la organización de dichas revisiones en el Grupo de Cooperación y por el que se deroga la Decisión de Ejecución (UE) 2015/296 de la Comisión.*

El Reglamento de Ejecución (UE) 2025/1568 de la Comisión establece las disposiciones aplicables a las revisiones *inter pares* de los sistemas de identificación electrónica previstos en el Reglamento (UE) núm. 910/2014 (eIDAS) y deroga la Decisión de Ejecución (UE) 2015/296. Su finalidad es armonizar el procedimiento, trasladando su organización al Grupo de Cooperación sobre la Identidad Digital Europea, en línea con las reformas introducidas por el Reglamento eIDAS 2 (arts. 12.6 y 46 *sexies*.7).

El procedimiento se inicia con la notificación previa del Estado miembro interesado, que debe acompañarse 1) de un documento de correlación de niveles de seguridad (anexo I); 2) un libro blanco del sistema (anexo II), y 3) un análisis de interoperabilidad con arreglo al Reglamento de Ejecución (UE) 2015/1501 (anexo III). Se exige que los documentos estén disponibles al menos en inglés, con salvaguardas de confidencialidad y reglas sobre conflictos de intereses.

En la fase organizativa, la Comisión fija la fecha de presentación al Grupo de Cooperación en un máximo de dos meses. Los Estados miembros designan un coordinador, hasta tres ponentes y un mínimo de un miembro activo. La revisión se estructurará en tres grupos de trabajo (de inscripción, de autenticación y gestión de medios, y de gestión y organización) vinculados a los niveles de seguridad del Reglamento de Ejecución (UE) 2015/1502. Los grupos pueden requerir información adicional, que se verá limitada únicamente por razones de seguridad nacional, secreto empresarial o falta de canal seguro de transmisión.

El texto establece plazos cerrados: tres meses para el borrador inicial, tres meses y dos semanas para el borrador final y el dictamen preliminar, y cuatro meses para el dictamen definitivo, con una prórroga máxima de dos meses. El Grupo de Cooperación publica el dictamen final sobre el grado de cumplimiento del Reglamento de Ejecución (UE) 2015/1502 y el nivel de seguridad declarado, salvo oposición del Estado miembro.

Finalmente, se introduce un procedimiento simplificado de actualización en caso de *cambios significativos* que afecten a la

interoperabilidad, seguridad o fiabilidad del sistema, permitiendo limitar la revisión a los elementos alterados. El reglamento de ejecución recuerda la aplicación del Reglamento General de protección de datos (UE) 2016/679, del Reglamento (UE) 2018/1725 y de la Directiva 2002/58/CE. Con ello se dota de mayor seguridad jurídica, transparencia y uniformidad a la cooperación entre Estados miembros en materia de identificación electrónica.

f) *Reglamento de Ejecución (UE) 2025/1571 de la Comisión, de 29 de julio, por el que se establecen disposiciones de aplicación del Reglamento (UE) núm. 910/2014 del Parlamento Europeo y del Consejo en lo que respecta a los formatos y procedimientos de los informes anuales de los organismos de supervisión.*

El Reglamento de Ejecución (UE) 2025/1571 de la Comisión establece los formatos y procedimientos de los informes anuales de los organismos de supervisión, en aplicación del Reglamento (UE) núm. 910/2014 (eIDAS). Con fundamento en los artículos 46 *bis*, apartado 7, y 46 *ter*, apartado 7, del Reglamento 2024/1183 (eIDAS 2), la norma impone que dichos informes se presenten a la Comisión a través de un canal electrónico seguro y en un formato legible por máquina que facilite su tratamiento automatizado (cdo. 2). Asimismo, se prevé la reutilización de la información previamente transmitida (art. 1.2), reduciendo cargas administrativas.

El contenido mínimo de los informes varía según se trate de organismos de supervisión de carteras europeas de identidad digital (anexo I) o de servicios de confianza (anexo II). En ambos casos deberán incluir, entre otros, la identificación y estructura de la autoridad, la descripción de actividades de supervisión ordinarias y extraordinarias, el resumen de inspecciones *in situ*, las medidas adoptadas, las notificaciones de violaciones de la seguridad conforme a la Directiva (UE) 2022/2555, la cooperación con autoridades homólogas y con autoridades de control de protección de datos (art. 51 RGPD), así como una previsión de prioridades para el año siguiente. De manera específica, los informes de supervisión de los servicios de confianza deberán recoger, además, los resultados de la verificación de los planes de cese de prestadores cualificados (art.24. 2*h* eIDAS 2), las investigaciones derivadas de denuncias de proveedores de navegadores (art. 45 *bis* eIDAS 2), y las actividades relacionadas con las listas de confianza (art. 22 eIDAS y Decisión de Ejecución [UE] 2015/1505).

Entre las novedades más destacadas figura la homogeneización paneuropea del contenido y formato de los informes, con el objetivo de garantizar transparencia frente al Parlamento Europeo y al Consejo (arts. 46 *bis*.6 y 46 *ter*.6 eIDAS 2). Se introducen además obligaciones inéditas, como la inclusión de información sobre cancelaciones de registros por uso fraudulento de la cartera digital europea o sobre la cooperación en incidentes de ciberseguridad. El reglamento será obligatorio y directamente aplicable en todos los Estados miembros a los veinte días de su publicación en el *Diario Oficial de la Unión Europea* (art. 2).

g) *Reglamento de Ejecución (UE) 2025/1572 de la Comisión, de 29 de julio, por el que se establecen disposiciones de aplicación del Reglamento (UE) núm. 910/2014 del Parlamento Europeo y del Consejo en lo que respecta al formato y los procedimientos*

de notificación de intenciones y de verificación en relación con el inicio de servicios de confianza cualificados.

El Reglamento de Ejecución (UE) 2025/1572 de la Comisión desarrolla el Reglamento (UE) 910/2014 (eIDAS) en lo relativo a los procedimientos de notificación de intenciones y verificación para la obtención de la condición de prestador cualificado de servicios de confianza. La norma fija por primera vez un marco común, vinculante y homogéneo en toda la Unión con el objetivo de garantizar la igualdad de condiciones y la transparencia entre operadores.

Entre sus principales previsiones, el reglamento establece la obligación de que los organismos de supervisión adopten una metodología de verificación que integre tanto el examen documental como, en su caso, verificaciones *in situ* y entrevistas en coordinación con las autoridades competentes en materia de ciberseguridad (art. 1, en conexión con la Directiva (UE) 2022/2555 - SRI 2). Asimismo, impone a dichos organismos publicar de forma accesible la información esencial relativa a los canales de comunicación, a la documentación exigida, al procedimiento de reclamaciones y a la descripción del método de verificación (art. 2).

Por su parte, los prestadores de servicios de confianza deberán aportar en su notificación los datos de identificación, los contactos, los identificadores uniformes de recursos (URI) de referencia, los análisis de riesgos conforme al Reglamento eIDAS y a la Directiva (UE) 2022/2555, el detalle de los servicios que se han de cualificar, los informes de evaluación de la conformidad emitidos por organismos acreditados y un plan de cese del servicio (art. 3; *vide* art. 24.2 eIDAS).

Para determinar si el prestador de servicios de confianza y el servicio de confianza cualificado que se propone prestar cumplen los requisitos fijados por la normativa, los organismos de supervisión analizarán la información facilitada por el prestador de servicios de confianza y podrán llevar a cabo verificaciones *in situ*. La verificación deberá corroborar la suficiencia y validez de dichos informes, la ausencia de incumplimientos y la adecuación de la documentación técnica en línea con los actos de ejecución previstos en el artículo 20.4 del Reglamento eIDAS (art. 4).

El reglamento de ejecución prevé un periodo transitorio de doce meses, siendo aplicable a partir del 19 de agosto del 2026 (art. 5). Se subraya además la necesaria compatibilidad con el Reglamento (UE) 2016/679 (RGPD) y la Directiva 2002/58/CE en cuanto al tratamiento de los datos personales (cdo. 4).

Con este nuevo marco se dota al sistema de cualificación de servicios de confianza de una mayor seguridad jurídica, uniformidad y transparencia procedimental reforzando la confianza en el ecosistema europeo de identificación y transacciones electrónicas.

Iratze Arrigain García

Plataformas en línea

Aprobación de las Directrices de la Comisión sobre la protección de los menores en el marco de la Ley de Servicios Digitales

El 14 de julio del 2025, la Comisión Europea aprobó definitivamente las Directrices sobre privacidad, seguridad y bienestar digital de los menores en línea, previstas en el artículo 28.4 del Reglamento (UE) 2022/2065 (Digital Services Act, DSA).

Tal como se adelantó en el boletín de julio, donde se informó del borrador presentado el 13 de mayo, estas directrices ofrecen una guía práctica para que las plataformas digitales cumplan sus obligaciones de protección de los menores reforzando las exigencias de privacidad desde el diseño, la verificación de la edad, las configuraciones seguras por defecto y las salvaguardias frente a contenidos nocivos y prácticas manipuladoras.

Con su adopción formal, las directrices pasan a formar parte del marco regulador europeo de protección de la infancia digital, complementando iniciativas como la estrategia europea en favor de una internet más adecuada para los niños (BIK+, por sus siglas en inglés) y los códigos de conducta voluntarios, y en sintonía con las reformas legislativas en curso en España en esta materia.

Claudia Pérez Moneu

Ciberseguridad

Recomendación del Consejo de 6 de junio del 2025 del Plan Director de la Unión Europea para la Gestión de Crisis de Ciberseguridad

El Consejo de la Unión Europea aprobó el 6 de junio del 2025 la Recomendación (UE) relativa al Plan Director para la Gestión de Crisis de Ciberseguridad (C/2025/3445), que deroga la Recomendación (UE) 2017/1584 e instituye un marco actualizado de actuación frente a incidentes de ciberseguridad a gran escala y crisis cibernéticas. El texto, adoptado al amparo de los artículos 114 y 292 del Tratado de Funcionamiento de la Unión Europea, responde a la creciente sofisticación de las amenazas híbridas y a la necesidad de un enfoque coordinado que trascienda las capacidades nacionales.

Entre sus principales novedades se aclara el alcance de los conceptos de *incidente significativo*, *incidente de ciberseguridad a gran escala* y *crisis de ciberseguridad* y se delimitan los supuestos que justifican la activación de mecanismos de coordinación a nivel de la Unión. Asimismo, se impone a los Estados miembros la obligación de disponer de planes nacionales de respuesta coherentes con la Directiva (UE) 2022/2555 (SRI 2) garantizando su integración en los marcos nacionales de gestión de crisis y su interoperabilidad con la red de equipos de respuesta a incidentes de ciberseguridad (CSIRT) y la red europea de organizaciones de enlace para las crisis de ciberseguridad (EU-CyCLONe).

El plan refuerza la articulación entre los niveles técnico, operativo y político: la red de CSIRT conserva el protagonismo en la cooperación técnica y el análisis de incidentes; la red EU-CyCLONe, apoyada por la Agencia de la Unión Europea para la Ciberseguridad (ENISA), actúa como interfaz operativo-estratégica, y el Consejo, mediante el dispositivo de respuesta política integrada de la Unión Europea a las crisis (RPIC), asume la coordinación política cuando procede (arts. 4 y ss.). De este modo se institucionaliza la complementariedad entre el plan director y los instrumentos horizontales de gestión de crisis de la Unión, tales como el sistema de alerta rápida general de la Comisión (ARGUS), el Mecanismo de Protección Civil de la Unión Europea (Decisión núm. 1313/2013/UE) o el mecanismo de respuesta a las crisis del Servicio Europeo de Acción Exterior.

El texto destaca igualmente la incorporación de ejercicios anuales de ciberseguridad coordinados por la Comisión y la Agencia de la Unión Europea para la Ciberseguridad (ENISA) así como la posibilidad de recurrir a la Reserva de Ciberseguridad de la Unión Europea prevista en el Reglamento (UE) 2025/38 (art. 55*b.v*), y la promoción de la cooperación civil-militar y con socios estratégicos, en particular la OTAN. Por último, se prevé la creación de diagramas de flujo de procesos en el plazo de un año para visualizar los canales de intercambio de información y la adopción de directrices de aplicación por el Consejo a la luz de los ejercicios prácticos.

Iratze Arrigain García

G A _ P
Gómez-Acebo & Pombo

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