El Digital Omnibus y la necesidad de revisar el concepto de dato personal

Paula Ortiz López

Directora General I Executive Legal Advisor I Regulación digital, protección de datos & IA

El pasado 29 de junio, el Consejo aprobó definitivamente el reglamento que modifica el Reglamento de Inteligencia Artificial, la primera pieza del paquete Digital Omnibus en completar su tramitación. El aplazamiento de las obligaciones para los sistemas de alto riesgo hasta diciembre de 2027 y agosto de 2028 obedece a una lógica difícil de rebatir: las normas técnicas armonizadas que deben permitir a las empresas demostrar la conformidad no están disponibles, y una obligación que llega antes que los instrumentos para cumplirla solo produce costes e inseguridad. La segunda pieza, la que afecta al Reglamento General de Protección de Datos, sigue negociándose entre el Parlamento y el Consejo, y es la que concentra el debate jurídico de fondo.

El informe Draghi sobre competitividad señaló la complejidad regulatoria como uno de los principales obstáculos para el crecimiento de las empresas europeas, y la Declaración de Budapest de noviembre de 2024 reclamó una «revolución de la simplificación». La Comisión asumió el compromiso de reducir las cargas de información un 25 por ciento antes de 2030, y un 35 por ciento en el caso de las pymes. Alemania, con una de las culturas de protección de datos más exigentes del continente, llevaba años proponiendo ajustes concretos al RGPD, y los informes de evaluación de la propia Comisión habían identificado las mismas fricciones. El Digital Omnibus recoge esa agenda en clave normativa.

El paquete se presentó el 19 de noviembre de 2025, acompañado de la Estrategia de la Unión de Datos y de la Cartera Digital Empresarial Europea. El Omnibus se articula en dos propuestas de reglamento. La primera, todavía en tramitación y cuya adopción se espera para finales de año, modifica el RGPD, traslada al RGPD parte de las reglas hoy contenidas en la Directiva 2002/58/CE sobre privacidad electrónica, retoca la Directiva NIS2 e integra en el Data Act el Reglamento de Gobernanza de Datos, el de libre circulación de datos no personales y la Directiva de datos abiertos. Crea, además, un punto único de entrada para las notificaciones de incidentes de seguridad que hoy se tramitan por separado, con plazos y formatos propios, bajo NIS2, RGPD, DORA, eIDAS y CER. La segunda es la que modifica el Reglamento de Inteligencia Artificial, aprobada definitivamente el pasado junio.

La reforma del RGPD es la que ha suscitado más posiciones encontradas, porque reabre un texto que parte de la comunidad de protección de datos mira con especial cautela. Una carta abierta de EDRi, ICCL y noyb, suscrita por Max Schrems, sostiene que el borrador del Digital Omnibus no se limita a simplificar, sino que equivale a una desregulación y a una rebaja de derechos. La postura tiene la virtud de la claridad y el defecto de la premisa: da por sentado que el texto de 2016 alcanzó una perfección que ni sus propios redactores le atribuyeron, y prescinde de la jurisprudencia reciente del Tribunal de Justicia, que apunta precisamente en la dirección que la Comisión propone codificar. El Comité Europeo de Protección de Datos y el Supervisor Europeo, en su dictamen conjunto, adoptaron una posición más matizada, al considerar legítima la reducción de cargas administrativas siempre que no disminuya la protección de los derechos fundamentales. Entre ambas posiciones se dirime la cuestión central de la reforma: la definición misma de dato personal.

La definición de dato personal determina el ámbito de apli-

cación del RGPD y, con él, la competencia de las autoridades de control. Durante años, esas autoridades la han interpretado en una sola dirección, la expansiva, hasta atraer hacia el reglamento prácticamente cualquier información. La identificabilidad se apreciaba en abstracto, atendiendo a los medios de cualquier tercero y con independencia de las capacidades reales de la entidad que trataba la información. La propuesta introduce un criterio distinto: una información constituye dato personal para una entidad cuando esta dispone de medios que razonablemente pueda utilizar para identificar a la persona.

El cambio codifica una evolución jurisprudencial de casi una década. En *Breyer* (C-582/14), resuelto en 2016 todavía bajo la Directiva 95/46, el Tribunal de Justicia examinó si una dirección IP dinámica era dato personal para el gestor de una página web que, por sí solo, no podía asociarla a ninguna persona. Concluyó que sí lo era, porque el ordenamiento alemán ofrecía vías legales para obtener esa identificación del proveedor de acceso a internet, de modo que la identificabilidad se medía contando con los medios de terceros. El Tribunal ha ido acotando después ese criterio. En *Scania* (C-319/22) precisó que el número de bastidor de un vehículo es dato personal únicamente para quien puede razonablemente vincularlo a una persona física. Y en la sentencia de septiembre de 2025 que enfrentó al Supervisor Europeo de Protección de Datos con la Junta Única de Resolución (SRB, por sus siglas en inglés) (C-413/23 P), dictada a raíz de la resolución del Banco Popular, confirmó esa dirección. La SRB había recogido las observaciones de los accionistas y acreedores afectados y las remitió seudonimizadas a Deloitte, como valorador independiente, sin la información que permitía atribuirlas a sus autores. El Tribunal precisó que la condición de dato personal debía apreciarse desde la posición del destinatario: si Deloitte no disponía de medios que razonablemente pudiera utilizar para reidentificar a los autores, aquellos comentarios no eran, para ella, datos personales. La consecuencia para la protección de datos es considerable: la seudonimización, además de medida de seguridad, pasa a ser un criterio para determinar si los datos siguen siendo personales para un destinatario concreto, porque unos mismos datos pueden serlo para quien conserva la información adicional que permite reidentificar y no serlo para quien carece de ella.

Las conclusiones del Abogado General Bobek en el asunto C-245/20, presentadas el 6 de octubre de 2021, ya habían advertido del problema de fondo: una interpretación tan amplia del dato personal y de su tratamiento somete a los particulares a obligaciones que desconocen y que difícilmente pueden observar, y esa distancia entre la norma y la realidad termina erosionando su autoridad. El propio Bobek avisaba de que esta deriva convertiría al RGPD en uno de los marcos normativos más ignorados de facto del Derecho de la Unión, e ilustraba el exceso con un supuesto deliberadamente cotidiano: quien reenvía a unos amigos un correo con un comentario poco favorecedor sobre un vecino realiza, en rigor, un tratamiento de datos personales ajeno a la exención doméstica. Una definición que lo abarca todo acaba por no proteger nada, porque dispersa la supervisión y trivializa las categorías que pretende reforzar. Con el criterio propuesto, quien pueda reidentificar seguirá dentro del reglamento; quien efectivamente no pueda, quedará fuera respecto de esos datos. El incentivo resultante favorece a quien diseña sistemas que impiden la identificación desde el origen, que es lo que la norma debería premiar.

Para la práctica, las consecuencias son inmediatas. La calificación de un conjunto de datos seudonimizados condiciona la cesión a terceros para análisis, la investigación clínica, la medición publicitaria o el entrenamiento de modelos, y hoy el asesor prudente trata casi todo como dato personal, porque el coste de equivocarse es alto y el criterio, movedizo. Un perímetro definido desde la posición de cada entidad permite graduar el asesoramiento en función de quién recibe los datos y de qué medios de identificación dispone.

El criterio tiene, con todo, el acierto del diagnóstico y la fragilidad de la ejecución. El nuevo artículo 41 bis remitiría a actos de ejecución la concreción de cuándo unos datos seudonimizados dejan de ser personales para un destinatario, con lo que el perímetro de todo el reglamento dependerá de normativa derivada


maite
CERTIFICADO DE APROBACIÓN
CONVOCATORIA
2026
MAITE.AI
CONSEJO GENERAL DE PODER JUDICIAL
No te reemplazamos.
Te hacemos un
Súper Abogado.
Maite.ai: El copiloto legal
impulsado por IA. Tan fácil
como WhatsApp.
Escanea el QR e introduce el código "REVISTAICAM"
para obtener un 25% de descuento en tu suscripción anual.
*Válido hasta el 30 de noviembre de 2026

aún inexistente. Hasta que llegue, y mientras la propuesta no aclare cómo se acredita la imposibilidad de identificar, el riesgo es sustituir una incertidumbre doctrinal por veintisiete lecturas nacionales de qué son «medios razonablemente probables». La industria, que respalda la nueva definición, reclama sobre todo previsibilidad: que la evaluación del riesgo de identificación atienda a medios plausibles en condiciones reales, y no a escenarios puramente teóricos ni a medios ilícitos como la piratería informática. Conviene recordar, además, que cambiar el texto puede resultar insuficiente si después lo interpretan quienes se oponen con vehemencia a los cambios.

No toda la propuesta merece el mismo juicio. El traslado de las reglas sobre cookies y tecnologías equivalentes al RGPD, a través del nuevo artículo 88 bis, solo alcanza a los datos personales, mientras que para los demás seguirá rigiendo la Directiva de privacidad electrónica y sus transposiciones nacionales. Una misma tecnología quedará sometida a dos marcos normativos según la naturaleza de la información a la que acceda, y la que no permite identificar a nadie puede acabar sujeta a condiciones más estrictas que la que sí lo permite. Difícilmente puede llamarse a eso simplificación.

Los otros dos frentes de la reforma responden a la misma lógica de perímetro. El primero afecta a las categorías especiales del artículo 9, que dispensan una protección reforzada a la información sobre la salud, las convicciones, el

origen étnico o la vida y orientación sexual. La propuesta busca circunscribirlas a los datos que revelen directamente esa información, en uno de los puntos más discutidos de la negociación, frente a la doctrina de la sentencia *OT* (C-184/20), que extendió el precepto a la información de la que puedan inferirse. La interpretación por inferencia, llevada al límite, produce resultados difíciles de sostener: el registro de ausencias de una plantilla sería un tratamiento de datos de salud, el historial de navegación también lo sería por la mera consulta de unos síntomas en un buscador, y las imágenes de cualquier cámara de videovigilancia, un tratamiento de datos sobre el origen racial. El considerando 51 del RGPD ya advertía que el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales. Las inferencias conservan tutela bajo los principios generales del reglamento, el artículo 22 en materia de decisiones automatizadas y la normativa laboral y antidiscriminatoria. El segundo frente habilita expresamente el interés legítimo del artículo 6.1.f) como base para el desarrollo y la operación de sistemas de inteligencia artificial, con salvaguardas reforzadas (minimización en la selección de fuentes, transparencia incrementada, derecho de oposición incondicional) y una excepción para el tratamiento residual de categorías especiales durante el entrenamiento. Parte de la crítica ha descrito esta habilitación como una autorización incondicionada para explotar datos personales. La lectura del texto conduce a una conclusión más modesta: el responsable deberá ponderar en cada caso sus intereses frente a los derechos de los afectados, seguirá sujeto al control de autoridades y tribunales, y soportará la carga de demostrar que el tratamiento es necesario y proporcionado.

La tesis de la carta abierta deja, sin embargo, una pregunta sin responder: por qué codificar la jurisprudencia del Tribunal de Justicia habría de constituir una rebaja de estándares. Confundir la codificación con la derogación es un error. La claridad es la que hace posible la protección, y la complejidad produce por sí sola un efecto desregulador cuando el obligado no alcanza a cumplirla. El RGPD es derecho vigente, y el derecho vigente se interpreta y, cuando procede, se revisa. Los trílogos decidirán en los próximos meses si el Digital Omnibus perfecciona los estándares. Simplificar bien es un ejercicio de sofisticación, y la sofisticación se demuestra en el detalle de los textos, no en las declaraciones de principios. Al debate sobre la protección de datos y el Omnibus le sobran, parece, convicciones y le falta lectura.

§