RGPD y mensajería profesional: por que la mayoría incumple sin saberlo

Casi cualquier despacho, consulta o asesoría envía documentos con datos de clientes por aplicaciones cuyo servidor está fuera del Espacio Económico Europeo. Sin mala fe, pero en muchos casos vulnerando el reglamento sin que nadie se lo haya advertido.

El documento que viaja más de lo que crees

Una situación cotidiana: una asesora fiscal recibe por mensajería un documento con datos de un cliente. Un comercial reenvía por chat un presupuesto a un compañero. Una médica comparte por la misma vía un informe clínico con un colega. Nadie piensa en ello dos veces. Es lo normal. Es lo cómodo. Es lo que se hace en cualquier despacho en cualquier ciudad de Europa todos los días.

Pero ese documento, en muchos casos, acaba de viajar a un servidor en Estados Unidos. Se ha almacenado — aunque sea temporalmente, aunque sea "cifrado en reposo" — en una nube que ni el profesional ni su cliente controlan. Ha pasado por sistemas que técnicamente pueden indexar metadatos asociados al contenido. Y el Reglamento General de Protección de Datos europeo tiene algo bastante claro que decir sobre eso.

Lo que la normativa exige

El RGPD — y por extensión la jurisprudencia del Tribunal de Justicia de la Unión Europea (en particular la sentencia Schrems II, C-311/18, de 2020) — establece que los datos personales de ciudadanos europeos deben estar adecuadamente protegidos. Si esos datos salen del Espacio Económico Europeo, el responsable del tratamiento debe garantizar que el destinatario ofrece un nivel de protección "esencialmente equivalente" al europeo. En la práctica, eso significa que enviar datos de clientes por servicios cuyos servidores están bajo jurisdicción estadounidense, sin haber realizado una evaluación de impacto y haber implementado salvaguardas suplementarias — cláusulas contractuales tipo, medidas técnicas adicionales como cifrado verificable, etc. — puede constituir una vulneración del reglamento. Aunque nadie haya dicho nada todavía.

Y no se trata solo del contenido de los mensajes. Los metadatos — quién envía qué a quién, cuándo, con qué frecuencia, desde dónde — también son datos personales según la normativa, según interpretación reiterada del Comité Europeo de Protección de Datos. Un servicio que recoge metadatos de las comunicaciones profesionales de un usuario está procesando datos personales de los clientes de ese usuario, sin que estos tengan conocimiento de ello, ni hayan prestado consentimiento alguno para tal tratamiento.

El esquema mental común — "yo solo uso la app para escribir; la app no es un proveedor de datos de mi cliente" — es jurídicamente incorrecto. Si los datos del cliente pasan por la infraestructura de un tercero, ese tercero está procesando esos datos. Y si está procesándolos, debe haber una base legal, un contrato de encargo del tratamiento, y garantías adecuadas.

Quién es responsable

La pregunta sobre quién carga con la responsabilidad jurídica no es académica. El RGPD distingue entre el *responsable del tratamiento* (quien decide qué datos se tratan y para qué) y el *encargado del tratamiento* (quien lo hace materialmente, en nombre del responsable). El profesional que envía documentos de clientes es el responsable. El proveedor de la app de mensajería es, en muchos casos, encargado de hecho. Sin contrato de encargo — y sin la mayoría de las cláusulas que tal contrato debería contener — el responsable no ha cumplido con su obligación.

La interpretación benigna es: "la mayoría de los profesionales no sabe esto". La interpretación rigurosa es: "el desconocimiento no exime del cumplimiento". Y la interpretación de cualquier abogado especialista en protección de datos consultado al respecto es, por lo general, la rigurosa.

Para quién importa esto en concreto

Para cualquier profesional o empresa que maneje, aunque sea ocasionalmente, información personal de terceros:

- Abogados que reciben documentación de clientes (contratos, demandas, declaraciones, informes patrimoniales).
- Médicos y otros profesionales sanitarios que comparten datos de salud — considerados *categoría especial* por el art. 9 RGPD, con régimen reforzado —.
- Asesores fiscales y gestores administrativos que mueven datos identificativos, fiscales y bancarios.
- Departamentos de recursos humanos que gestionan documentación laboral y personal de empleados.
- Comerciales que reciben datos de contacto y, a menudo, información comercial sensible de prospectos y clientes.

En todos los casos, la información está protegida por el RGPD. En todos los casos, en la práctica habitual, esa información transita por canales cuya jurisdicción no permite ser declarada "esencialmente equivalente" al marco europeo sin salvaguardas adicionales. No por mala fe. Por costumbre. Y por una infraestructura tecnológica que ha priorizado la comodidad sobre el cumplimiento durante quince años.

El argumento "todo el mundo lo hace"

Conviene anticipar la objeción más frecuente: "si todo el mundo lo hace, no puede ser un problema real". Es un argumento perfectamente comprensible y, jurídicamente, no tiene ninguna fuerza. El hecho de que una práctica esté extendida no la convierte en conforme con el reglamento. La AEPD (Agencia Española de Protección de Datos) ha sancionado en los últimos años a varias empresas precisamente por usos de mensajería que parecían inofensivos hasta el momento de la inspección.

La realidad operativa actual es que el riesgo es bajo en términos de probabilidad — es muy poco frecuente que una inspección de la AEPD audite las herramientas de mensajería específicas de un despacho mediano — , pero alto en términos de impacto si se materializa. Es un riesgo que la mayoría asume sin saber que lo está asumiendo. Es decir, sin haber evaluado si la herramienta utilizada está alineada con la responsabilidad jurídica del responsable del tratamiento.

El rastro digital es retroactivo

Hay un segundo argumento, casi simétrico al anterior, que conviene anticipar: *"si esto fuese un problema serio, la administración ya habría empezado a inspeccionarlo"*. La realidad operativa actual le da razón superficial. Las inspecciones por uso indebido de mensajería en empresas pequeñas y, sobre todo, en autónomos son hoy casi inexistentes — no porque la conducta esté permitida, sino porque la administración, en España y en buena parte de la UE, carece de los efectivos humanos necesarios para auditar a millones de obligados.

Eso es lo que la práctica observada sugiere hoy. No es lo que la próxima década sugiere. Dos vectores convergen para alterar el equilibrio en plazos relativamente cortos.

Primero: el rastro digital es retroactivo. Cada mensaje enviado por una aplicación con servidor central queda registrado — al menos en metadatos — en una infraestructura que persiste. Lo que se envió hace seis meses sigue siendo técnicamente auditable hoy. Lo que se envíe hoy seguirá siendo auditable dentro de cinco años. La ausencia de inspección presente no es una garantía de ausencia de inspección futura. Es una postergación de la evaluación, no una exención.

Segundo: la capacidad de auditoría administrativa va a crecer aceleradamente. La introducción de herramientas de inteligencia artificial en los procesos de inspección elimina el cuello de botella humano que hasta ahora ha protegido — de hecho, no de derecho — a las empresas pequeñas y a los autónomos. Un sistema capaz de cruzar metadatos masivos, declaraciones fiscales, registros mercantiles y obligaciones de notificación de brechas no requiere inspectores: requiere acceso. Y el acceso, mediante requerimientos a proveedores con presencia jurídica en la UE, es perfectamente factible bajo el marco normativo actual.

A esto se añade un factor menos técnico pero igualmente determinante: los Estados europeos están en proceso sostenido de endeudamiento creciente y necesitan, casi sin excepción, ampliar su base recaudatoria. La sanción administrativa derivada del incumplimiento del RGPD es, en términos puramente fiscales, una fuente de ingresos creciente y políticamente cómoda. No es conjetura: es tendencia observable en las memorias anuales de las agencias de protección de datos europeas, donde el volumen total de sanciones lleva varios ejercicios consecutivos al alza.

La conclusión operativa para el responsable del tratamiento no es alarmista, sino fría: **la decisión sobre cómo se gestiona la comunicación con clientes hoy se evalúa contra la capacidad inspectora del año en que llegue la inspección, no contra la actual.** Y esa capacidad será, en plazos razonables, sustancialmente distinta de la de hoy. Quien empiece a hacer las cosas bien hoy no estará en regla solo a partir de hoy: el rastro generado a partir de este momento será coherente con la normativa, y eso protege retroactivamente el tramo que viene. Quien siga como hasta ahora estará acumulando rastro auditable cuya conformidad se evaluará contra los estándares — y los recursos — de los próximos años.

Qué cambia con una arquitectura distinta

Existen alternativas técnicas en las que los datos no se almacenan en infraestructura de terceros, sino que viajan directamente del dispositivo del emisor al del receptor. En esa arquitectura, el cumplimiento del RGPD respecto a transferencias internacionales no depende de cláusulas contractuales tipo, ni de la buena voluntad del proveedor, ni de auditorías futuras. Depende de que *no hay transferencia*. Y lo que no existe no se puede incumplir.

Esta no es una solución exclusiva ni la única posible. Pero es estructuralmente diferente, y el cumplimiento normativo deja de ser un anexo procedimental para convertirse en una consecuencia directa del diseño. Para un profesional que se toma en serio su responsabilidad como responsable del tratamiento, esa diferencia importa.

La próxima entrega de Cuadernos analizará en detalle la sentencia Schrems II y sus implicaciones prácticas para empresas pequeñas y medianas que dependen de servicios cloud estadounidenses, cinco años después de su publicación.

Fuentes y marco normativo

- Reglamento UE 2016/679 (RGPD), especialmente capítulo V sobre transferencias internacionales.
- STJUE C-311/18 ("Schrems II"), 16 de julio de 2020.
- EDPB — Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia.

- AEPD — Memorias anuales con casuística de sanciones por uso indebido de mensajería instantánea en entornos profesionales.

← AnteriorEl secreto profesional en la era digitalSiguiente →Cuando no hay nadie en medio

Lecturas recientes

- Análisis · 18 de mayo de 2026 Privacidad real vs aparente: las preguntas que conviene hacerse
- Análisis · 18 de mayo de 2026 Self-hosting como práctica profesional
- Concepto · 18 de mayo de 2026 Las 24 palabras: qué es una identidad criptográfica

Llévate este artículo donde lo necesites.

↓ Markdown ↓ Texto plano ↓ PDF

El archivo se descarga a tu dispositivo. Desde ahí puedes guardarlo, importarlo a Solo2, o compartirlo donde quieras. Cuadernos no decide el destino por ti.

Sello de lacre · SHA-256 b047dac7da6000abb9f24c30d25edec25f83256010d7be1d18454e2304d22563

Cuadernos Lacre · Una publicación de Menzuri Gestión S.L. ·
escrita por R.Eugenio · editada por el equipo de Solo2.