Reflexión · 16 de mayo de 2026

← Anterior·Siguiente →

El secreto profesional en la era digital

Cuando la comunicación entre el profesional y su cliente pasa por un canal técnicamente inadecuado, el secreto no se rompe el día de la filtración. Se rompió mucho antes, en el momento de elegir la herramienta.

Un problema que casi nadie ve

Un abogado recibe en su teléfono un documento sensible de un cliente. Un médico comenta con un colega un diagnóstico delicado. Un psicólogo coordina con un psiquiatra el tratamiento de un paciente. Un asesor fiscal envía los datos de una declaración pendiente de revisión. Todos lo hacen por mensajería instantánea. Y casi ninguno se detiene a pensar dónde acaban realmente esos mensajes.

La respuesta, en la mayoría de los casos, es la misma: en un servidor que el profesional no controla, en un país cuya legislación no necesariamente conoce, gestionado por una empresa cuyo modelo de negocio es — en términos económicos directos — acumular datos. El mensaje puede estar cifrado en tránsito. Pero una vez llega al servidor, es una copia almacenada en infraestructura de un tercero, sujeta a las decisiones operativas, jurídicas y comerciales de ese tercero. No del profesional.

Lo que la legislación dice

El Reglamento General de Protección de Datos europeo es inequívoco en su artículo 32: quien trate datos personales debe aplicar medidas técnicas y organizativas "apropiadas" para garantizar un nivel de seguridad adecuado al riesgo. La adecuación de las medidas no se avalía contra "lo que la app dice que hace", sino contra el riesgo real. Si los datos de un cliente acaban en un servidor cuya jurisdicción no garantiza un nivel de protección equivalente al del Espacio Económico Europeo, el responsable del tratamiento — es decir, el profesional — está asumiendo un riesgo del que probablemente no es del todo consciente.

E no es solo el RGPD. El secreto profesional, regulado de forma específica para abogados, médicos, psicólogos, auditores, periodistas y otros, exige que la comunicación con el cliente sea confidencial. No "confidencial en la medida de lo posible". Confidencial sin matices. Si el canal técnico utilizado no puede garantizarlo, el profesional está asumiendo un riesgo que la deontología de su profesión no permite asumir.

La paradoja es que el riesgo es invisible. Nadie audita la mensajería del despacho. Nadie pide el contrato de procesamiento de datos del proveedor del chat. El riesgo emerge solo cuando ya es tarde: una filtración, una brecha publicada, una orden judicial cumplida en otro continente sin notificación al usuario.

Lo que un profesional necesita técnicamente

Lo que un profesional con secreto profesional necesita es, en realidad, sorprendentemente simple desde el punto de vista de los requisitos:

- Un canal donde los mensajes vayan directos del dispositivo del emisor al del receptor, sin pasar por un servidor intermedio que almacene copias.

- Una infraestructura cuya jurisdicción y políticas estén alineadas con el RGPD por construcción, no por declaración.
- Una forma de identificarse con el interlocutor sin tener que entregar a un tercero los contactos profesionales (nombres de clientes, números de teléfono, agenda).
- Algún sistema verificable — no basado en la palabra del proveedor — para confirmar que el mensaje llegó a la persona correcta.

No es una lista exigente. Es, en realidad, lo que se daba por sentado en la comunicación profesional pre-digital. Una carta certificada cumplía todos esos criterios. Una llamada telefónica desde la centralita del despacho a la del cliente, también. Lo extraño no es que se pidan estas garantías hoy: lo extraño es que se hayan perdido al pasar al canal digital, sin que nadie se diera cuenta.

La diferencia entre cifrar y no almacenar

Hay una metáfora útil. Cifrar una mensaje y guardarlo en un servidor es equivalente a meter un documento en una caja fuerte y dejar la caja en casa de un desconocido. La caja fuerte es buena. El documento, en principio, no se puede leer. Pero el documento *sigue estando en casa de otro*. Y ese otro puede recibir una orden judicial, puede sufrir un ataque informático, puede cambiar sus condiciones de servicio, puede ser comprado por otra empresa con otra ética, puede desaparecer mañana.

La alternativa estructural — no procedimental, no por confianza — es que el documento nunca salga del despacho. Que viaje directamente de la mesa del profesional a la mesa del cliente, sin pasar por intermediario alguno. Eso es lo que hace técnicamente la comunicación punto a punto entre dispositivos: elimina al intermediario. No es que el intermediario sea malo. Es que, para el caso del secreto profesional, el intermediario es *innecesario*. Y lo innecesario, en cualquier sistema que aspire a ser seguro, debe eliminarse por principio.

La pregunta de responsabilidad

Al final, la pregunta que todo profesional con deber de secreto debería poder responder con un sí rotundo es la siguiente:

> Si mañana se filtra una conversación con uno de mis clientes y un tribunal o un colegio profesional me pregunta cómo gestiono la confidencialidad, ¿puedo demostrar técnicamente que el canal que usé no almacena copias en infraestructura de terceros? ¿Puedo demostrar que los datos nunca salieron de los dispositivos de las dos personas que participaron en la conversación? ¿Puedo demostrar, sin depender de la palabra de una empresa de otro continente, que la confidencialidad estaba garantida por la arquitectura y no por una promesa?

Si la respuesta es no, el problema no es la herramienta en concreto. El problema es que se ha delegado en una herramienta una responsabilidad que la herramienta no estaba diseñada para soportar. Es como meter expedientes confidenciales en un sobre transparente y confiar en que el cartero no mire.

La herramienta que un profesional elige para comunicarse con sus clientes dice mucho de cómo valora su confianza. Hay herramientas diseñadas para que esa confianza no dependa de promesas, sino de la arquitectura. Y hay herramientas que no lo están. Conocer la diferencia es parte del trabajo.

Marco normativo citado

- Reglamento UE 2016/679 (RGPD), especialmente arts. 5, 25 (protección de datos desde el diseño) y 32 (seguridad del tratamiento).
- Ley Orgánica 6/1985 del Poder Judicial y estatutos profesionales respecto al deber de secreto profesional.
- Ley 41/2002 reguladora de la autonomía del paciente, art. 7 (confidencialidad de la información sanitaria).

- Códigos deontológicos de los colegios profesionales respecto a la confidencialidad y el secreto profesional.

← AnteriorCifrar no es ser privado: lo que los metadatos cuentan sobre tiSiguiente →RGPD y mensajería profesional: por qué la mayoría incumple sin saberlo

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 d8ac23b54f22331efe92005943176d6334328616d63e1b3f1ce9f6dac323da2a

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