Reflexión · 16 de maio de 2026

← Anterior·Seguinte →

O segredo profesional na era dixital

Cando a comunicación entre o profesional e o seu cliente pasa por un canal tecnicamente inadecuado, o segredo non se rompe o día da filtración. Rompeuse moito antes, no momento de elixir a ferramenta.

Un problema que case ninguén ve

Un avogado recibe no seu teléfono un documento sensible dun cliente. Un médico comenta cun colega un diagnóstico delicado. Un psicólogo coordina cun psiquiatra o tratamento dun paciente. Un asesor fiscal envía os datos dunha declaración pendente de revisión. Todos o fan por mensaxería instantánea. E case ninguén se detén a pensar onde acaban realmente esas mensaxes.

A resposta, na maioría dos casos, é a mesma: nun servidor que o profesional non controla, nun país cuxa lexislación non necesariamente coñece, xestionado por unha empresa cuxo modelo de negocio é —en termos económicos directos— acumular datos. A mensaxe pode estar cifrada en tránsito. Pero unha vez chega ao servidor, é unha copia almacenada en infraestrutura dun terceiro, suxeita ás decisións operativas, xurídicas e comerciais dese terceiro. Non do profesional.

O que a lexislación di

O Regulamento Xeral de Protección de Datos europeo é inequívoco no seu artigo 32: quen trate datos persoais debe aplicar medidas técnicas e organizativas "apropiadas" para garantir un nivel de seguridade adecuado ao risco. A adecuación das medidas non se avalía contra "o que a app di que fai", senón contra o risco real. Se os datos dun cliente acaban nun servidor cuxa xurisdición non garante un nivel de protección equivalente ao do Espazo Económico Europeo, o responsable do tratamento —é dicir, o profesional— está asumindo un risco do que probablemente non é do todo consciente.

E non é só o RGPD. O segredo profesional, regulado de forma específica para avogados, médicos, psicólogos, auditores, xornalistas e outros, esixe que a comunicación co cliente sexa confidencial. Non "confidencial na medida do posible". Confidencial sen matices. Se o canal técnico utilizado non pode garantilo, o profesional está asumindo un risco que a deontoloxía da súa profesión non permite asumir.

A paradoxo é que o risco é invisible. Ninguén audita a mensaxería do despacho. Ninguén pide o contrato de procesamiento de datos do provedor do chat. O risco emerxe só cando xa é tarde: unha filtración, unha brecha publicada, unha orde xudicial cumprida noutro continente sen notificación ao usuario.

O que un profesional necesita tecnicamente

O que un profesional con segredo profesional necesita é, na realidade, sorprendentemente simple desde o punto de vista dos requisitos:

- Un canal onde as mensaxes vaian directos do dispositivo do emisor ao do receptor, sen pasar por un servidor intermedio que almacene copias.

- Unha infraestrutura cuxa xurisdición e políticas estean aliñadas co RGPD por construción, non por declaración.
- Unha forma de identificarse co interlocutor sen ter que entregar a un terceiro os contactos profesionais (nomes de clientes, números de teléfono, axenda).
- Algún sistema verificable —non baseado na palabra do provedor— para confirmar que a mensaxe chegou á persoa correcta.

Non é unha lista exixente. É, na realidade, o que se daba por sentado na comunicación profesional pre-dixital. Unha carta certificada cumpría todos eses criterios. Unha chamada telefónica desde a centralita do despacho á do cliente, tamén. O estraño non é que se pidan estas garantías hoxe: o estraño é que se perderan ao pasar ao canal dixital, sen que ninguén se dese conta.

A diferenza entre cifrar e non almacenar

Hai unha metáfora útil. Cifrar unha mensaxe e gardala nun servidor é equivalente a meter un documento nunha caixa forte e deixar a caixa en casa dun descoñecido. A caixa forte é boa. O documento, en principio, non se pode ler. Pero o documento *segue estando en casa doutro*. E ese outro pode recibir unha orde xudicial, pode sufrir un ataque informático, pode cambiar as súas condicións de servizo, pode ser comprado por outra empresa cunha outra ética, pode desaparecer mañá.

A alternativa estructural —non procedimental, non por confianza— é que o documento nunca saia do despacho. Que viaxe directamente da mesa do profesional á mesa do cliente, sen pasar por intermediario algún. Iso é o que fai tecnicamente a comunicación punto a punto entre dispositivos: elimina ao intermediario. Non é que o intermediario sexa malo. É que, para o caso do segredo profesional, o intermediario é *innecesario*. E o innecesario, en calquera sistema que aspire a ser seguro, debe eliminarse por principio.

A pregunta de responsabilidade

Ao final, a pregunta que todo profesional con deber de segredo debería poder responder cun si rotundo é a seguinte:

> Se mañá se filtra unha conversa cun dos meus clientes e un tribunal ou un colexio profesional me pregunta como xestiono a confidencialidade, ¿podo demostrar tecnicamente que o canal que usei non almacena copias en infraestrutura de terceiros? ¿Podo demostrar que os datos nunca saíron dos dispositivos das dúas persoas que participaron na conversa? ¿Podo demostrar, sen depender da palabra dunha empresa doutro continente, que a confidencialidade estaba garantida pola arquitectura e non por unha promesa?

Se a resposta é non, o problema non é a ferramenta en concreto. O problema é que se delegou nunha ferramenta unha responsabilidade que a ferramenta non estaba deseñada para soportar. É como meter expedientes confidenciales nun sobre transparente e confiar en que o carteiro non mire.

A ferramenta que un profesional elixe para comunicarse cos seus clientes di moito de como valora a súa confianza. Hai ferramentas deseñadas para que esa confianza non dependa de promesas, senón da arquitectura. E hai ferramentas que non o están. Coñecer a diferenza é parte do traballo.

Marco normativo citado

- Regulamento UE 2016/679 (RGPD), especialmente arts. 5, 25 (protección de datos desde o deseño) e 32 (seguridade do tratamento).
- Lexislación nacional sobre estatutos profesionais e o deber de segredo profesional.
- Lei 41/2002 reguladora da autonomía do paciente, art. 7 (confidencialidade da información sanitaria).
- Códigos deontolóxicos dos colexios profesionais respecto á confidencialidade e o segredo profesional.

← AnteriorCifrar non é ser privado: o que os metadatos contan sobre tiSeguinte →RGPD e mensaxería profesional: por que a maioría incumpre sen sabelo

Lecturas recentes

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Leva este artigo onde o necesites.

↓ Markdown ↓ Texto plano ↓ PDF

O arquivo descárgase no teu dispositivo. Desde aí podes gardalo, importalo a Solo2, o compartilo onde queiras. Cuadernos no decide o destino por ti.

Selo de lacre · SHA-256 50babc0e6aca503527a886ba4e4dba659d447cb8618cfc655347a230a9c1976e

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