RGPD e mensaxería profesional: por que a maioría incumpre sen sabelo

Case calquera despacho, consulta o asesoría envía documentos con datos de clientes por aplicacións cuxo servidor está fóra do Espazo Económico Europeo. Sen mala fe, pero en moitos casos vulnerando o regulamento sen que ninguén llo advertira.

Para entendernos: A túa asesora fiscal envíache un documento por WhatsApp. Chégache ao móbil en Madrid, pero antes pasou por un servidor en Texas. O RGPD ten algo bastante claro que dicir diso — e a maioría de despachos leva anos incumpríndoo sen sabelo.

O documento que viaxa máis do que cres

Unha situación cotiá: unha asesora fiscal recibe por mensaxería un documento con datos dun cliente. Un comercial reenvía por chat un orzamento a un compañeiro. Unha médica comparte pola mesma vía un informe clínico cun colega. Ninguén pensa niso dúas veces. É o normal. É o cómodo. É o que se fai en calquera despacho en calquera cidade de Europa todos os días.

Pero ese documento, en moitos casos, acaba de viaxar a un servidor nos Estados Unidos. Almacenouse —aínda que sexa temporalmente, aínda que sexa "cifrado en repouso"— nunha nube que nin o profesional nin o seu cliente controlan. Pasou por sistemas que tecnicamente poden indexar metadatos asociados ao contido. E o Regulamento Xeral de Protección de Datos europeo ten algo bastante claro que dicir sobre iso.

O que a normativa exixe

O RGPD —e por extensión a xurisprudencia do Tribunal de Xustiza da Unión Europea (en particular a sentenza Schrems II, C-311/18, de 2020)— establece que os datos persoais de cidadáns europeos deben estar adecuadamente protexidos. Se eses datos saen do Espazo Económico Europeo, o responsable do tratamento debe garantir que o destinatario ofrece un nivel de protección "esencialmente equivalente" ao europeo. Na práctica, iso significa que enviar datos de clientes por servizos cuxos servidores están baixo xurisdición estadounidense, sen ter realizado unha avaliación de impacto e ter implementado salvaguardas suplementarias —cláusulas contractuais tipo, medidas técnicas adicionais como cifrado verificable, etc.— pode constituír unha vulneración do regulamento. Aínda que ninguén dixera nada aínda.

E non se trata só do contido das mensaxes. Os metadatos —quen envía que a quen, cando, con que frecuencia, desde onde— tamén son datos persoais segundo a normativa, segundo interpretación reiterada do Comité Europeo de Protección de Datos. Un servizo que recolle metadatos das comunicacións profesionais dun usuario está procesando datos persoais dos clientes dese usuario, sen que estes teñan coñecemento diso, nin prestaran consentimento algún para tal tratamento.

O esquema mental común —"eu só uso a app para escribir; la app non é un provedor de datos do meu cliente"— é xuridicamente incorrecto. Se os datos do cliente pasan pola infraestrutura dun terceiro, ese terceiro está

procesando eses datos. E se está procesándoos, debe haber unha base legal, un contrato de encargo do tratamento, e garantías adecuadas.

Quen é responsable

A pregunta sobre quen carga coa responsabilidade xurídica non é académica. O RGPD distingue entre o *responsable do tratamento* (quen decide que datos se tratan e para que) e o *encargado do tratamento* (quen o fai materialmente, en nome do responsable). El profesional que envía documentos de clientes é o responsable. O provedor da app de mensaxería é, en moitos casos, encargado de feito. Sen contrato de encargo —e sen a maioría das cláusulas que tal contrato debería conter— o responsable non cumpriu coa súa obrigación.

A interpretación benigna é: "a maioría dos profesionais non sabe isto". A interpretación rigorosa é: "o descoñecemento non exime do cumprimento". E a interpretación de calquera avogado especialista en protección de datos consultado ao respecto é, polo xeral, a rigorosa.

Para quen importa isto en concreto

Para calquera profesional ou empresa que manexe, aínda que sexa ocasionalmente, información persoal de terceiros:

- Avogados que reciben documentación de clientes (contratos, demandas, declaracións, informes patrimoniais).
- Médicos e outros profesionais sanitarios que comparten datos de saúde —considerados *categoría especial* polo art. 9 RGPD, con réxime reforzado—.
- Asesores fiscais e xestores administrativos que moven datos identificativos, fiscais e bancarios.
- Departamentos de recursos humanos que xestionan documentación laboral e persoal de empregados.
- Comerciais que reciben datos de contacto e, a miúdo, información comercial sensible de prospectos e clientes.

En todos os casos, a información está protexida polo RGPD. En todos os casos, na práctica habitual, esa información transita por canais cuxa xurisdición non permite ser declarada "esencialmente equivalente" ao marco europeo sen salvaguardas adicionais. Non por mala fe. Por costume. E por unha infraestrutura tecnolóxica que priorizou a comodidade sobre o cumprimento durante quince anos.

O argumento "todo o mundo o fai"

Convén anticipar a obxección máis frecuente: "se todo o mundo o fai, non pode ser un problema real". É un argumento perfectamente comprensible e, xuridicamente, non ten ningunha forza. O feito de que unha práctica estea estendida non a converte en conforme co regulamento. A AEPD (Axencia Española de Protección de Datos) sancionou nos últimos anos a varias empresas precisamente por usos de mensaxería que parecían inofensivos ata o momento da inspección.

A realidade operativa actual é que o risco é baixo en termos de probabilidade —é moi pouco frecuente que unha inspección da AEPD audite as ferramentas de mensaxería específicas dun despacho mediano—, pero alto en termos de impacto se se materializa. É un risco que a maioría asume sen saber que o está asumindo. É dicir, sen ter avaliado se a ferramenta utilizada está aliñada coa responsabilidade xurídica do responsable do tratamento.

O rastro dixital é retroactivo

Hai un segundo argumento, case simétrico ao anterior, que convé anticipar: *"se isto fose un problema serio, a administración xa tería comezado a inspeccionalo"*. A realidade operativa actual dálle razón superficial. As inspeccións por uso indebido de mensaxería en empresas pequenas e, sobre todo, en autónomos son hoxe case

inexistentes —non porque a conduta estea permitida, senón porque a administración, en España e en boa parte da UE, carece dos efectivos humanos necesarios para auditar a millóns de obrigados.

Iso é o que a práctica observada suxire hoxe. Non é o que a próxima década suxire. Dous vectores converxen para alterar o equilibrio en prazos relativamente curtos.

Primero: o rastro dixital é retroactivo. Cada mensaxe enviada por unha aplicación con servidor central queda rexistrado —polo menos en metadatos— nunha infraestrutura que persiste. O que se enviou hai seis meses segue sendo tecnicamente auditable hoxe. O que se envíe hoxe seguirá sendo auditable dentro de cinco anos. A ausencia de inspección presente non é unha garantía de ausencia de inspección futura. É unha postergación da avaliación, non unha exención.

Segundo: a capacidade de auditoría administrativa vai crecer aceleradamente. A introdución de ferramentas de intelixencia artificial nos procesos de inspección elimina o pescozo de botella humano que ata agora protexeu —de feito, non de dereito— ás empresas pequenas e aos autónomos. Un sistema capaz de cruzar metadatos masivos, declaracións fiscais, rexistros mercantís e obrigacións de notificación de brechas non require inspectores: require acceso. E o acceso, mediante requirimentos a provedores con presenza xurídica na UE, é perfectamente factible baixo o marco normativo actual.

A isto engádese un factor menos técnico pero igualmente determinante: os Estados europeos están en proceso sostido de endebedamento crecente e necesitan, case sen excepción, ampliar a súa base recadatoria. A sanción administrativa derivada do incumprimento do RGPD é, en termos puramente fiscais, unha fonte de ingresos crecente e politicamente cómoda. Non é conxectura: é tendencia observable nas memorias anuais das axencias de protección de datos europeas, onde o volume total de sancións leva varios exercicios consecutivos ao alza.

A conclusión operativa para o responsable do tratamento non é alarmista, senón fría: **a decisión sobre como se xestiona a comunicación con clientes hoxe avalíase contra a capacidade inspectora do ano en que chegue a inspección, non contra a actual.** E esa capacidade será, en prazos razoáveis, sustancialmente distinta da de hoxe. Quen comece a facer as cousas ben hoxe non estará en regra só a partir de hoxe: o rastro xerado a partir deste momento será coherente coa normativa, e iso protexe retroactivamente o tramo que vén. Quen siga como ata agora estará acumulando rastro auditable cuxa conformidade se avaliará contra os estándares —e os recursos — dos próximos anos.

Que cambia cunha arquitectura distinta

Existen alternativas técnicas nas que os datos non se almacenan en infraestrutura de terceiros, senón que viaxan directamente do dispositivo do emisor ao do receptor. Nesa arquitectura, o cumprimento do RGPD respecto a transferencias internacionais non depende de cláusulas contractuais tipo, nin da boa vontade do provedor, ni de auditorías futuras. Depende de que *non hai transferencia*. E o que non existe non se pode incumprir.

Esta non é unha solución exclusiva nin a única posible. Pero é estructuralmente diferente, e o cumprimento normativo deixa de ser un anexo procedimental para converterse nunha consecuencia directa do deseño. Para un profesional que se toma en serio a súa responsabilidade como responsable do tratamento, esa diferenza importa.

A próxima entrega de Cuadernos analizará en detalle a sentenza Schrems II e as súas implicacións prácticas para empresas pequenas e medianas que dependen de servizos cloud estadounidenses, cinco anos despois da súa publicación.

Nota editorial: cando estes Cuadernos nomean empresas ou produtos, non é para acusar. Quenes os constrúen fan traballos que millóns de persoas usan e aprecian. O que sinalamos é estrutural — o modelo, non a marca. As marcas aparecen como exemplo porque son as que o lector recoñece.

Fontes e marco normativo

- Regulamento UE 2016/679 (RGPD), especialmente capítulo V sobre transferencias internacionais.
- STXUE C-311/18 ("Schrems II"), 16 de xullo de 2020.
- EDPB — Recomendacións 01/2020 sobre medidas que complementan os instrumentos de transferencia.
- Axencias de protección de datos — Memorias anuais con casuística de sancións por uso indebido de mensaxería instantánea en contornas profesionais.

← AnteriorO segredo profesional na era dixitalSeguinte →Cando non hai ninguén no medio

Lecturas recentes

- Análise · 18 de maio de 2026 Privacidade real vs aparente: as preguntas que convén facerse
- Análise · 18 de maio de 2026 Self-hosting como práctica profesional
- Concepto · 18 de maio de 2026 As 24 palabras: que é unha identidade criptográfica

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 8f90c0a7f9f535626228c024c8d78e019a12c846ea9e9cd8554840d4a6ab1bec

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