Reflexió · 16 de maig de 2026

← Anterior·Següent →

El secret professional en l'era digital

Quan la comunicació entre el professional i el seu client passa per un canal tècnicament inadequat, el secret no es trenca el dia de la filtració. Es va trencar molt abans, en el moment de triar l'eina.

Un problema que gairebé ningú veu

Un advocat rep al seu telèfon un document sensible d'un client. Un metge comenta amb un col·lega un diagnòstic delicat. Un psicòleg coordina amb un psiquiatre el tractament d'un pacient. Un assessor fiscal envia les dades d'una declaració pendent de revisió. Tots ho fan per missatgeria instantània. I gairebé ningú s'atura a pensar on acaben realment aquests missatges.

La resposta, en la majoria dels casos, és la mateixa: en un servidor que el professional no controla, en un país la legislació del qual no necessàriament coneix, gestionat per una empresa el model de negoci de la qual és —en termes econòmics directes— acumular dades. El missatge pot estar xifrat en trànsit. Però un cop arriba al servidor, és una còpia emmagatzemada en infraestructura d'un tercer, subjecta a les decisions operatives, jurídiques i comercials d'aquest tercer. No del professional.

El que la legislació diu

El Reglament General de Protecció de Dades europeu és inequívoc en el seu article 32: qui tracti dades personals ha d'aplicar mesures tècniques i organitzatives "apropiades" per garantir un nivell de seguretat adequat al risc. L'adequació de les mesures no s'avalua contra "el que l'app diu que fa", sinó contra el risc real. Si les dades d'un client acaben en un servidor la jurisdicció del qual no garanteix un nivell de protecció equivalent al de l'Espai Econòmic Europeu, el responsable del tractament —és a dir, el professional— està assumint un risc del qual probablement no és del tot conscient.

I no és només l'RGPD. El secret professional, regulat de forma específica per a advocats, metges, psicòlegs, auditors, periodistes i altres, exigeix que la comunicació amb el client sigui confidencial. No "confidencial en la mesura del possible". Confidencial sense matisos. Si el canal tècnic utilitzat no pot garantir-ho, el professional està assumint un risc que la deontologia de la seva professió no permet assumir.

La paradoxa és que el risc és invisible. Ningú audita la missatgeria del despatx. Ningú demana el contracte de processament de dades del proveïdor del xat. El risc emergeix només quan ja és tard: una filtració, una bretxa publicada, una ordre judicial complerta en un altre continent sense notificació a l'usuari.

El que un professional necessita tècnicament

El que un professional amb secret professional necessita és, en realitat, sorprenentment simple des del punt de vista dels requisits:

- Un canal on els missatges vagin directes del dispositiu de l'emissor al del receptor, sense passar per un servidor intermedi que emmagatzemi còpies.

- Una infraestructura la jurisdicció i polítiques de la qual estiguin alineades amb l'RGPD per construcció, no per declaració.
- Una forma d'identificar-se amb l'interlocutor sense haver de lliurar a un tercer els contactes professionals (noms de clients, números de telèfon, agenda).
- Algun sistema verificable —no basat en la paraula del proveïdor— per confirmar que el missatge ha arribat a la persona correcta.

No és una llista exigent. És, en realitat, el que es donava per fet en la comunicació professional pre-digital. Una carta certificada complia tots aquests criteris. Una trucada telefònica des de la centraleta del despatx a la del client, també. El que és estrany no és que es demanin aquestes garanties avui: el que és estrany és que s'hagin perdut en passar al canal digital, sense que ningú se n'adonés.

La diferència entre xifrar i no emmagatzemar

Hi ha una metàfora útil. Xifrar un missatge i guardar-lo en un servidor és equivalent a ficar un document en una caixa forta i deixar la caixa a casa d'un desconegut. La caixa forta és bona. El document, en principi, no es pot llegir. Però el document *segueix estant a casa d'un altre*. I aquest altre pot rebre una ordre judicial, pot patir un atac informàtic, pot canviar les seves condicions de servei, pot ser comprat per una altra empresa amb una altra ètica, pot desaparèixer demà.

L'alternativa estructural —no procedimental, no per confiança— és que el document no surti mai del despatx. Que viatgi directament de la taula del professional a la taula del client, sense passar per cap intermediari. Això és el que fa tècnicament la comunicació punt a punt entre dispositius: elimina l'intermediari. No és que l'intermediari sigui dolent. És que, per al cas del secret professional, l'intermediari és *innecessari*. I allò innecessari, en qualsevol sistema que aspiri a ser segur, s'ha d'eliminar per principi.

La pregunta de responsabilitat

Al final, la pregunta que tot professional amb deure de secret hauria de poder respondre amb un sí rotund és la següent:

> Si demà es filtra una conversa amb un dels meus clients i un tribunal o un col·legi professional em pregunta com gestiono la confidencialitat, ¿puc demostrar tècnicament que el canal que vaig usar no emmagatzema còpies en infraestructura de tercers? ¿Puc demostrar que les dades no van sortir mai dels dispositius de les dues persones que van participar en la conversa? ¿Puc demostrar, sense dependre de la paraula d'una empresa d'un altre continent, que la confidencialitat estava garantida per l'arquitectura i no per una promesa?

Si la resposta és no, el problema no és l'eina en concret. El problema és que s'ha delegat en una eina una responsabilitat que l'eina no estava dissenyada per suportar. És com ficar expedients confidencials en un sobre transparent i confiar que el carter no miri.

L'eina que un professional tria per comunicar-se amb els seus clients diu molt de com valora la seva confiança. Hi ha eines dissenyades perquè aquesta confiança no depengui de promeses, sinó de l'arquitectura. I hi ha eines que no ho estan. Conèixer la diferència és part de la feina.

Marc normatiu citat

- Reglament UE 2016/679 (RGPD), especialment arts. 5, 25 (protecció de dades des del disseny) i 32 (seguretat del tractament).
- Llei Orgànica 6/1985 del Poder Judicial i estatuts professionals respecte al deure de secret professional.
- Llei 41/2002 reguladora de l'autonomia del pacient, art. 7 (confidencialitat de la informació sanitària).
- Codis deontològics dels col·legis professionals respecte a la confidencialitat i el secret professional.

← AnteriorXifrar no és ser privat: el que les metadades expliquen sobre tuSegüent →RGPD i missatgeria professional: per què la majoria incompleix sense saber-ho

Lectures recents

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Emporta't aquest article on el necessitis.

↓ Markdown ↓ Text pla ↓ PDF

L'arxiu es descarrega al teu dispositiu. Des d'allà pots guardar-lo, importar-lo a Solo2, o compartir-lo on vulguis. Cuadernos no decideix el destí per tu.

Segell de lacre · SHA-256 4e4f8ed43a1fad5cb4154b1c2bbb79b6a0e433989e150ac42543af9588cbef3f

Cuadernos Lacre · Una publicació de Menzuri Gestión S.L. ·
escrita per R.Eugenio · editada per l'equip de Solo2.