Anàlisi · 16 de maig de 2026

← Anterior·Següent →

RGPD i missatgeria professional: per què la majoria incompleix sense saber-ho

Gairebé qualsevol despatx, consulta o assessoria envia documents amb dades de clients per aplicacions el servidor de les quals està fora de l'Espai Econòmic Europeu. Sense mala fe, però en molts casos vulnerant el reglament sense que ningú els ho hagi advertit.

El document que viatja més del que creus

Una situació quotidiana: una assessora fiscal rep per missatgeria un document amb dades d'un client. Un comercial reenvia per xat un pressupost a un company. Una metgessa comparteix per la mateixa via un informe clínic amb un col·lega. Ningú hi pensa dues vegades. És el normal. És el còmode. És el que es fa en qualsevol despatx en qualsevol ciutat d'Europa cada dia.

Però aquest document, en molts casos, acaba de viatjar a un servidor als Estats Units. S'ha emmagatzemat —encara que sigui temporalment, encara que sigui "xifrat en repòs"— en un núvol que ni el professional ni el seu client controlen. Ha passat per sistemes que tècnicament poden indexar metadades associades al contingut. I el Reglament General de Protecció de Dades europeu té alguna cosa força clara a dir sobre això.

El que la normativa exigeix

L'RGPD —i per extensió la jurisprudència del Tribunal de Justícia de la Unió Europea (en particular la sentència Schrems II, C-311/18, de 2020)— estableix que les dades personals de ciutadans europeus han d'estar adequadament protegides. Si aquestes dades surten de l'Espai Econòmic Europeu, el responsable del tractament ha de garantir que el destinatari ofereix un nivell de protecció "essencialment equivalent" a l'europeu. En la pràctica, això significa que enviar dades de clients per serveis els servidors dels quals estan sota jurisdicció estatunidenca, sense haver realitzat una avaluació d'impacte i haver implementat salvaguardes suplementàries —clàusules contractuals tipus, mesures tècniques addicionals com xifratge verificable, etc.— pot constituir una vulneració del reglament. Encara que ningú hagi dit res encara.

I no es tracta només del contingut dels missatges. Les metadades —qui envia què a qui, quan, amb quina freqüència, des d'on— també són dades personals segons la normativa, segons interpretació reiterada del Comitè Europeu de Protecció de Dades. Un servei que recull metadades de les comunicacions professionals d'un usuari està processant dades personals dels clients d'aquest usuari, sense que aquests en tinguin coneixement, ni hagin prestat cap consentiment per a tal tractament.

L'esquema mental comú —"jo només uso l'app per escriure; l'app no és un proveïdor de dades del meu client"— és jurídicament incorrecte. Si les dades del client passen per la infraestructura d'un tercer, aquest tercer està processant aquestes dades. I si les està processant, hi ha d'haver una base legal, un contracte d'encàrrec del tractament, i garanties adequades.

Qui és responsable

La pregunta sobre qui carrega amb la responsabilitat jurídica no és acadèmica. L'RGPD distingeix entre el *responsable del tractament* (qui decideix quines dades es tracten i per a què) i l'*encarregat del tractament* (qui ho fa materialment, en nom del responsable). El professional que envia documents de clients és el responsable. El proveïdor de l'app de missatgeria és, en molts casos, encarregat de fet. Sense contracte d'encàrrec —i sense la majoria de les clàusules que tal contracte hauria de contenir— el responsable no ha complert amb la seva obligació.

La interpretació benigna és: "la majoria dels professionals no ho saben". La interpretació rigorosa és: "el desconeixement no exonera del compliment". I la interpretació de qualsevol advocat especialista en protecció de dades consultat al respecte és, en general, la rigorosa.

Per a qui importa això en concret

Per a qualsevol professional o empresa que gestioni, encara que sigui ocasionalment, informació personal de tercers:

- Advocats que reben documentació de clients (contractes, demandes, declaracions, informes patrimonials).
- Metges i altres professionals sanitaris que comparteixen dades de salut —considerades *categoria especial* per l'art. 9 RGPD, amb règim reforçat—.
- Assessors fiscals i gestors administratius que mouen dades identificatives, fiscals i bancàries.
- Departaments de recursos humans que gestionen documentació laboral i personal d'empleats.
- Comercials que reben dades de contacte i, sovint, informació comercial sensible de prospectes i clients.

En tots els casos, la informació està protegida per l'RGPD. En tots els casos, en la pràctica habitual, aquesta informació transita per canals la jurisdicció dels quals no permet ser declarada "essencialment equivalent" al marc europeu sense salvaguardes addicionals. No per mala fe. Per costum. I per una infraestructura tecnològica que ha prioritzat la comoditat sobre el compliment durant quinze anys.

L'argument "tothom ho fa"

Convé anticipar l'objecció més freqüent: "si tothom ho fa, no pot ser un problema real". És un argument perfectament comprensible i, jurídicament, no té cap força. El fet que una pràctica estigui estesa no la converteix en conforme amb el reglament. L'AEPD (Agència Espanyola de Protecció de Dades) ha sancionat en els últims anys diverses empreses precisament per usos de missatgeria que semblaven inofensius fins al moment de la inspecció.

La realitat operativa actual és que el risc és baix en termes de probabilitat —és molt poc freqüent que una inspecció de l'AEPD auditi les eines de missatgeria específiques d'un despatx mitjà—, però alt en termes d'impacte si es materialitza. És un risc que la majoria assumeix sense saber que l'està assumint. És a dir, sense haver avaluat si l'eina utilitzada està alineada amb la responsabilitat jurídica del responsable del tractament.

El rastre digital és retroactiu

Hi ha un segon argument, gairebé simètric a l'anterior, que convé anticipar: *"si això fos un problema seriós, l'administració ja hauria començat a inspeccionar-ho"*. La realitat operativa actual li dóna raó superficial. Les inspeccions per ús indegut de missatgeria en empreses petites i, sobretot, en autònoms són avui gairebé inexistents —no perquè la conducta estigui permesa, sinó perquè l'administració manca dels efectius humans necessaris per auditar milions d'obligats.

Això és el que la pràctica observada suggereix avui. No és el que la propera dècada suggereix. Dos vectors convergeixen per alterar l'equilibri en terminis relativament curts.

Primer: el rastre digital és retroactiu. Cada missatge enviat per una aplicació amb servidor central queda registrat —almenys en metadades— en una infraestructura que persisteix. El que es va enviar fa sis mesos segueix sent tècnicament auditable avui. El que s'enviï avui seguirà sent auditable d'aquí a cinc anys. L'absència d'inspecció present no és una garantia d'absència d'inspecció futura. És una postergació de l'avaluació, no una exempció.

Segon: la capacitat d'auditoria administrativa creixerà acceleradament. La introducció d'eines d'intel·ligència artificial en els processos d'inspecció elimina el coll d'ampolla humà que fins ara ha protegit les empreses petites i els autònoms. Un sistema capaç de creuar metadades massives, declaracions fiscals, registres mercantils i obligacions de notificació de bretxes no requereix inspectors: requereix accés. I l'accés, mitjançant requeriments a proveïdors amb presència jurídica a la UE, és perfectament factible sota el marc normatiu actual.

A això s'hi afegeix un factor menys tècnic però igualment determinant: els estats europeus estan en procés sostingut d'endeutament creixent i necessiten, gairebé sense excepció, ampliar la seva base recaptatòria. La sanció administrativa derivada de l'incompliment de l'RGPD és, en termes purament fiscals, una font d'ingressos creixent i políticament còmoda. No és conjectura: és tendència observable en les memòries anuals de les agències de protecció de dades europees, on el volum total de sancions porta diversos exercicis consecutius a l'alça.

La conclusió operativa per al responsable del tractament no és alarmista, sinó freda: **la decisió sobre com es gestiona la comunicació amb clients avui s'avalua contra la capacitat inspectora de l'any en què arribi la inspecció, no contra l'actual.** I aquesta capacitat serà, en terminis raonables, substancialment diferent de la d'avui. Qui comenci a fer les coses bé avui no estarà en regla només a partir d'avui: el rastre generat a partir d'aquest moment serà coherent amb la normativa, i això protegeix retroactivament el tram que ve. Qui segueixi com fins ara estarà acumulant rastre auditable la conformitat del qual s'avaluarà contra els estàndards —i els recursos— dels propers anys.

Què canvia amb una arquitectura diferent

Existeixen alternatives tècniques en què les dades no s'emmagatzemen en infraestructura de tercers, sinó que viatgen directament del dispositiu de l'emissor al del receptor. En aquesta arquitectura, el compliment de l'RGPD respecte a transferències internacionals no depèn de clàusules contractuals tipus, ni de la bona voluntat del proveïdor, ni d'auditories futures. Depèn que *no hi ha transferència*. I allò que no existeix no es pot incomplir.

Aquesta no és una solució exclusiva ni l'única possible. Però és estructuralment diferent, i el compliment normatiu deixa de ser un annex procedimental per convertir-se en una conseqüència directa del disseny. Per a un professional que es pren seriosament la seva responsabilitat com a responsable del tractament, aquesta diferència importa.

La propera entrega de Cuadernos analitzarà en detall la sentència Schrems II i les seves implicacions pràctiques per a empreses petites i mitjanes que depenen de serveis cloud estatunidencs, cinc anys després de la seva publicació.

Fonts i marc normatiu

- Reglament UE 2016/679 (RGPD), especialment capítol V sobre transferències internacionals.
- STJUE C-311/18 ("Schrems II"), 16 de juliol de 2020.
- EDPB — Recomanacions 01/2020 sobre mesures que complementen els instruments de transferència.
- Agències de protecció de dades — Memòries anuals amb casuística de sancions per ús indegut de missatgeria instantània en entorns professionals.

← AnteriorEl secret professional en l'era digitalSegüent →Quan no hi ha ningú al mig

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 88e9f3c65d6293ffcc182df246c026d96a8a0bcd5df41d86b43de2e740ce0f07

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

Aquest web no usa cookies i no carrega recursos de tercers. Usa un comptador anònim de visites allotjat per nosaltres (Umami, al nostre servidor europeu) i el mínim JavaScript necessari per a la teva preferència de tema clar/fosc. Sense trackers, sense perfilat, sense compartir dades. Si vols seguir-nos: RSS.