RGPD et messagerie professionnelle : pourquoi la majorité est en infraction sans le savoir

Presque tous les cabinets, cliniques ou bureaux de conseil envoient des documents contenant des données clients via des applications dont le serveur est hors de l'Espace Économique Européen. Sans mauvaise foi, mais dans bien des cas en violation du règlement sans que personne ne les ait avertis.

Le document qui voyage plus que vous ne le croyez

Une situation quotidienne : une conseillère fiscale reçoit par messagerie un document contenant les données d'un client. Un commercial transmet par chat un devis à un collègue. Une médecin partage par la même voie un rapport clinique avec un confrère. Personne n'y réfléchit à deux fois. C'est normal. C'est pratique. C'est ce qui se fait chaque jour dans n'importe quel bureau de n'importe quelle ville d'Europe.

Mais ce document, dans bien des cas, vient de voyager vers un serveur aux États-Unis. Il a été stocké — même temporairement, même « chiffré au repos » — dans un cloud que ni le professionnel ni son client ne contrôlent. Il est passé par des systèmes qui peuvent techniquement indexer des métadonnées associées au contenu. Et le Règlement général sur la protection des données européen a des choses assez claires à dire à ce sujet.

Ce que la réglementation exige

Le RGPD — et par extension la jurisprudence de la Cour de justice de l'Union européenne (notamment l'arrêt Schrems II, C-311/18, de 2020) — établit que les données à caractère personnel des citoyens européens doivent être adéquatement protégées. Si ces données sortent de l'Espace Économique Européen, le responsable du traitement doit garantir que le destinataire offre un niveau de protection « essentiellement équivalent » à celui de l'Europe. En pratique, cela signifie que l'envoi de données clients par des services dont les serveurs sont sous juridiction américaine, sans avoir effectué d'analyse d'impact et mis en œuvre des garanties supplémentaires — clauses contractuelles types, mesures techniques additionnelles comme un chiffrement vérifiable, etc. — peut constituer une violation du règlement. Même si personne n'a encore rien dit.

Et il ne s'agit pas seulement du contenu des messages. Les métadonnées — qui envoie quoi à qui, quand, à quelle fréquence, d'où — sont également des données à caractère personnel selon la réglementation, d'après l'interprétation répétée du Comité européen de la protection des données. Un service qui collecte les métadonnées des communications professionnelles d'un utilisateur traite des données à caractère personnel des clients de cet utilisateur, sans que ceux-ci en aient connaissance ni n'aient donné de consentement pour un tel traitement.

Le schéma mental commun — « j'utilise seulement l'application pour écrire ; l'application n'est pas un fournisseur de données de mon client » — est juridiquement incorrect. Si les données du client passent par l'infrastructure d'un tiers, ce tiers traite ces données. Et s'il les traite, il doit y avoir une base légale, un contrat de sous-traitance du traitement et des garanties adéquates.

Qui est responsable

La question de savoir qui porte la responsabilité juridique n'est pas académique. Le RGPD distingue le *responsable du traitement* (celui qui décide quelles données sont traitées et pourquoi) du *sous-traitant* (celui qui le fait matériellement, au nom du responsable). Le professionnel qui envoie des documents clients est le responsable. Le fournisseur de l'application de messagerie est, dans bien des cas, un sous-traitant de fait. Sans contrat de sous-traitance — et sans la plupart des clauses qu'un tel contrat devrait contenir — le responsable n'a pas rempli son obligation.

L'interprétation bienveillante est : « la majorité des professionnels ne le savent pas ». L'interprétation rigoureuse est : « l'ignorance ne dispense pas du respect de la loi ». Et l'interprétation de tout avocat spécialisé en protection des données consulté à ce sujet est, généralement, la rigoureuse.

Pour qui cela importe-t-il concrètement

Pour tout professionnel ou entreprise qui manipule, même occasionnellement, des informations personnelles de tiers :

- Les avocats qui reçoivent de la documentation de clients (contrats, plaintes, déclarations, rapports patrimoniaux).
- Les médecins et autres professionnels de santé qui partagent des données de santé — considérées comme une *catégorie particulière* par l'art. 9 du RGPD, avec un régime renforcé.
- Les conseillers fiscaux et gestionnaires administratifs qui déplacent des données d'identification, fiscales et bancaires.
- Les départements des ressources humaines qui gèrent la documentation professionnelle et personnelle des employés.
- Les commerciaux qui reçoivent des données de contact et, souvent, des informations commerciales sensibles de prospects et de clients.

Dans tous les cas, l'information est protégée par le RGPD. Dans tous les cas, dans la pratique courante, cette information transite par des canaux dont la juridiction ne permet pas d'être déclarée « essentiellement équivalente » au cadre européen sans garanties supplémentaires. Pas par mauvaise foi. Par habitude. Et à cause d'une infrastructure technologique qui a privilégié la commodité sur la conformité pendant quinze ans.

L'argument « tout le monde le fait »

Il convient d'anticiper l'objection la plus fréquente : « si tout le monde le fait, cela ne peut pas être un réel problème ». C'est un argument parfaitement compréhensible qui, juridiquement, n'a aucune force. Le fait qu'une pratique soit répandue ne la rend pas conforme au règlement. Les autorités de protection des données (comme la CNIL ou l'AEPD) ont sanctionné plusieurs entreprises ces dernières années précisément pour des utilisations de messagerie qui semblaient anodines jusqu'au moment de l'inspection.

La réalité opérationnelle actuelle est que le risque est faible en termes de probabilité — il est très rare qu'une inspection porte sur les outils de messagerie spécifiques d'un cabinet moyen —, mais élevé en termes d'impact s'il se matérialise. C'est un risque que la majorité assume sans savoir qu'elle l'assume. C'est-à-dire sans avoir évalué si l'outil utilisé est aligné sur la responsabilité juridique du responsable du traitement.

La trace numérique est rétroactive

Il existe un second argument, presque symétrique au précédent, qu'il convient d'anticiper : *« si c'était un problème sérieux, l'administration aurait déjà commencé à inspecter »*. La réalité opérationnelle actuelle lui donne raison en surface. Les inspections pour usage indu de messagerie dans les petites entreprises et, surtout,

chez les indépendants sont aujourd'hui presque inexistantes — non pas parce que le comportement est autorisé, mais parce que l'administration manque des effectifs humains nécessaires pour auditer des millions d'assujettis.

C'est ce que suggère la pratique observée aujourd'hui. Ce n'est pas ce que suggère la prochaine décennie. Deux vecteurs convergent pour modifier l'équilibre à des échéances relativement courtes.

Premièrement : la trace numérique est rétroactive. Chaque message envoyé par une application dotée d'un serveur central est enregistré — au moins dans les métadonnées — dans une infrastructure qui persiste. Ce qui a été envoyé il y a six mois reste techniquement auditable aujourd'hui. Ce qui sera envoyé aujourd'hui restera auditable dans cinq ans. L'absence d'inspection présente n'est pas une garantie d'absence d'inspection future. C'est un report de l'évaluation, pas une exemption.

Deuxièmement : la capacité d'audit administratif va croître de manière accélérée. L'introduction d'outils d'intelligence artificielle dans les processus d'inspection élimine le goulot d'étranglement humain qui a jusqu'ici protégé les petites entreprises et les indépendants. Un système capable de croiser des métadonnées massives, des déclarations fiscales, des registres du commerce et des obligations de notification de failles ne nécessite pas d'inspecteurs : il nécessite un accès. Et l'accès, via des réquisitions auprès de fournisseurs ayant une présence juridique dans l'UE, est parfaitement réalisable sous le cadre normatif actuel.

À cela s'ajoute un facteur moins technique mais tout aussi déterminant : les États européens sont dans un processus soutenu d'endettement croissant et ont besoin, presque sans exception, d'élargir leur base de recettes. La sanction administrative découlant du non-respect du RGPD est, en termes purement fiscaux, une source de revenus croissante et politiquement commode. Ce n'est pas une conjecture : c'est une tendance observable dans les rapports annuels des autorités européennes de protection des données, où le volume total des sanctions est en hausse depuis plusieurs exercices consécutifs.

La conclusion opérationnelle pour le responsable du traitement n'est pas alarmiste, mais froide : **la décision sur la manière de gérer la communication avec les clients aujourd'hui est évaluée par rapport à la capacité d'inspection de l'année où l'inspection arrivera, et non par rapport à la capacité actuelle.** Et cette capacité sera, dans des délais raisonnables, substantiellement différente de celle d'aujourd'hui. Celui qui commence à bien faire les choses aujourd'hui ne sera pas seulement en règle à partir d'aujourd'hui : la trace générée à partir de ce moment sera cohérente avec la réglementation, ce qui protège rétroactivement la période à venir. Celui qui continue comme avant accumulera une trace auditable dont la conformité sera évaluée par rapport aux normes — et aux ressources — des années à venir.

Ce qui change avec une architecture différente

Il existe des alternatives techniques dans lesquelles les données ne sont pas stockées sur des infrastructures tierces, mais voyagent directement de l'appareil de l'émetteur à celui du récepteur. Dans cette architecture, la conformité au RGPD concernant les transferts internationaux ne dépend pas de clauses contractuelles types, ni de la bonne volonté du fournisseur, ni d'audits futurs. Elle dépend du fait qu'il *n'y a pas de transfert*. Et ce qui n'existe pas ne peut être en infraction.

Ce n'est pas une solution exclusive ni la seule possible. Mais elle est structurellement différente, et la conformité réglementaire cesse d'être une annexe procédurale pour devenir une conséquence directe de la conception. Pour un professionnel qui prend au sérieux sa responsabilité en tant que responsable du traitement, cette différence compte.

Le prochain numéro de Cuadernos analysera en détail l'arrêt Schrems II et ses implications pratiques pour les petites et moyennes entreprises qui dépendent de services cloud américains, cinq ans après sa publication.

Sources et cadre normatif

- Règlement UE 2016/679 (RGPD), notamment le chapitre V sur les transferts internationaux.
- CJUE C-311/18 (« Schrems II »), 16 juillet 2020.
- EDPB — Recommandations 01/2020 sur les mesures complétant les instruments de transfert.
- Autorités de protection des données — Rapports annuels avec casuistique de sanctions pour usage indu de la messagerie instantanée dans les environnements professionnels.

← PrécédentLe secret professionnel à l'ère numériqueSuivant →Quand il n'y a personne au milieu

Lectures recentes

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Emportez cet article où vous en avez besoin.

↓ Markdown ↓ Texte brut ↓ PDF

Le fichier est téléchargé sur votre appareil. À partir de là, vous pouvez l'enregistrer, l'importer dans Solo2 ou le partager comme vous le souhaitez. Cuadernos ne décide pas de la destination pour vous.

Cachet de cire · SHA-256 62f64dcf1965713da8aa9340660b47655bed5675f299205d1cc65cacadbfd25a

Cuadernos Lacre · Une publication de Menzuri Gestión S.L. ·
écrite par R.Eugenio · éditée par l'équipe de Solo2.