Le secret professionnel à l'ère numérique

Lorsque la communication entre le professionnel et son client passe par un canal techniquement inapproprié, le secret n'est pas rompu le jour de la divulgation. Il a été rompu bien plus tôt, au moment de choisir l'outil.

Un problème que presque personne ne voit

Un avocat reçoit sur son téléphone un document sensible d'un client. Un médecin discute d'un diagnostic délicat avec un confrère. Un psychologue coordonne le traitement d'un patient avec un psychiatre. Un conseiller fiscal envoie les données d'une déclaration en attente de révision. Tous le font par messagerie instantanée. Et presque aucun ne s'arrête pour réfléchir à l'endroit où finissent réellement ces messages.

La réponse, dans la plupart des cas, est la même : sur un serveur que le professionnel ne contrôle pas, dans un pays dont il ne connaît pas forcément la législation, géré par une entreprise dont le modèle économique est — en termes économiques directs — d'accumuler des données. Le message peut être chiffré en transit. Mais une fois arrivé sur le serveur, il s'agit d'une copie stockée sur l'infrastructure d'un tiers, soumise aux décisions opérationnelles, juridiques et commerciales de ce tiers. Pas du professionnel.

Ce que dit la législation

Le Règlement général sur la protection des données européen est sans équivoque en son article 32 : quiconque traite des données à caractère personnel doit mettre en œuvre des mesures techniques et organisationnelles « appropriées » pour garantir un niveau de sécurité adapté au risque. Le caractère approprié des mesures ne s'évalue pas par rapport à « ce que l'application dit faire », mais par rapport au risque réel. Si les données d'un client finissent sur un serveur dont la juridiction ne garantit pas un niveau de protection équivalent à celui de l'Espace Économique Européen, le responsable du traitement — c'est-à-dire le professionnel — assume un risque dont il n'est probablement pas tout à fait conscient.

Et il n'y a pas que le RGPD. Le secret professionnel, régi de manière spécifique pour les avocats, médecins, psychologues, auditeurs, journalistes et autres, exige que la communication avec le client soit confidentielle. Pas « confidentielle dans la mesure du possible ». Confidentielle sans nuance. Si le canal technique utilisé ne peut le garantir, le professionnel assume un risque que la déontologie de sa profession ne permet pas de prendre.

Le paradoxe est que le risque est invisible. Personne n'audit la messagerie du cabinet. Personne ne demande le contrat de traitement des données du fournisseur de chat. Le risque n'apparaît que lorsqu'il est trop tard : une divulgation, une faille publiée, une ordonnance judiciaire exécutée sur un autre continent sans notification à l'utilisateur.

Ce dont un professionnel a techniquement besoin

Ce dont un professionnel soumis au secret professionnel a besoin est, en réalité, étonnamment simple du point de vue des exigences :

- Un canal où les messages vont directement de l'appareil de l'émetteur à celui du récepteur, sans passer par un serveur intermédiaire qui stocke des copies.
- Une infrastructure dont la juridiction et les politiques sont alignées sur le RGPD par conception, et non par déclaration.
- Une manière de s'identifier auprès de l'interlocuteur sans avoir à remettre à un tiers ses contacts professionnels (noms des clients, numéros de téléphone, répertoire).
- Un système vérifiable — non basé sur la parole du fournisseur — pour confirmer que le message est parvenu à la bonne personne.

Ce n'est pas une liste exigeante. C'est, en réalité, ce qui allait de soi dans la communication professionnelle pré-numérique. Une lettre recommandée répondait à tous ces critères. Un appel téléphonique depuis le standard du cabinet vers celui du client également. Ce qui est étrange, ce n'est pas que ces garanties soient demandées aujourd'hui : ce qui est étrange, c'est qu'elles aient été perdues lors du passage au canal numérique, sans que personne ne s'en aperçoive.

La différence entre chiffrer et ne pas stocker

Il existe une métaphore utile. Chiffrer un message et le stocker sur un serveur équivaut à placer un document dans un coffre-fort et à laisser le coffre chez un inconnu. Le coffre-fort est de bonne qualité. Le document, en principe, ne peut être lu. Mais le document *se trouve toujours chez quelqu'un d'autre*. Et cet autre peut recevoir une ordonnance judiciaire, subir une cyberattaque, changer ses conditions de service, être racheté par une autre entreprise ayant une autre éthique, ou disparaître demain.

L'alternative structurelle — et non procédurale ou basée sur la confiance — est que le document ne sorte jamais du cabinet. Qu'il voyage directement du bureau du professionnel au bureau du client, sans passer par aucun intermédiaire. C'est ce que fait techniquement la communication de point à point entre appareils : elle élimine l'intermédiaire. Ce n'est pas que l'intermédiaire est mauvais. C'est que, dans le cas du secret professionnel, l'intermédiaire est *inutile*. Et ce qui est inutile, dans tout système aspirant à être sécurisé, doit être éliminé par principe.

La question de la responsabilité

En fin de compte, la question à laquelle tout professionnel ayant un devoir de secret devrait pouvoir répondre par un oui catégorique est la suivante :

> Si demain une conversation avec l'un de mes clients est divulguée et qu'un tribunal ou un ordre professionnel me demande comment je gère la confidentialité, puis-je démontrer techniquement que le canal que j'ai utilisé ne stocke pas de copies sur des infrastructures tierces ? Puis-je prouver que les données n'ont jamais quitté les appareils des deux personnes ayant participé à la conversation ? Puis-je démontrer, sans dépendre de la parole d'une entreprise d'un autre continent, que la confidentialité était garantie par l'architecture et non par une promesse ?

Si la réponse est non, le problème n'est pas l'outil en lui-même. Le problème est qu'une responsabilité a été déléguée à un outil qui n'a pas été conçu pour la supporter. C'est comme placer des dossiers confidentiels dans une enveloppe transparente et faire confiance au facteur pour qu'il ne regarde pas.

L'outil qu'un professionnel choisit pour communiquer avec ses clients en dit long sur la manière dont il valorise leur confiance. Il existe des outils conçus pour que cette confiance ne dépende pas de promesses, mais de l'architecture. Et il y a des outils qui ne le sont pas. Connaître la différence fait partie du travail.

Cadre normatif cité

- Règlement UE 2016/679 (RGPD), notamment art. 5, 25 (protection des données dès la conception) et 32 (sécurité du traitement).
- Législation nationale relative aux professions réglementées et au secret professionnel.
- Législation relative à l'autonomie des patients et à la confidentialité des informations de santé.
- Codes de déontologie des ordres professionnels concernant la confidentialité et le secret professionnel.

← PrécédentChiffrer n'est pas être privé : ce que les métadonnées disent de vousSuivant →RGPD et messagerie professionnelle : pourquoi la majorité est en infraction sans le savoir

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 8517d61b6384eafe2063c330bd84b354a6b9daca8656a5273e4913bf47ba29d7

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