Analyse · 16 mai 2026

← Précédent·Suivant →

Chiffrer n'est pas être privé : ce que les métadonnées disent de vous

Le contenu chiffré et les métadonnées visibles sont deux choses distinctes. Lorsqu'un service parle de « chiffrement de bout en bout », il ne raconte que la moitié de l'histoire.

Le cadenas qui ne protège pas tout

Une grande partie des services de messagerie actuels annoncent un chiffrement de bout en bout. Et c'est vrai : le contenu des messages voyage chiffré, de sorte que personne en chemin — pas même le fournisseur de services — ne peut lire le texte pendant son transit. Jusqu'ici, l'affirmation est exacte.

Le problème est que le contenu n'est qu'une partie de l'histoire. Même si personne ne peut lire ce que vous dites, le service connaît d'autres éléments avec une très haute précision : avec qui vous parlez, à quelle heure, à quelle fréquence, depuis quel emplacement approximatif, sur quel appareil, combien de messages vous envoyez et recevez, quel nombre de fichiers vous partagez. Tout cela s'appelle des métadonnées. Et les métadonnées en disent, dans bien des cas, presque autant que le message lui-même.

Ce que les métadonnées révèlent

Il n'est pas nécessaire de lire un message pour savoir beaucoup de choses. Si une personne appelle ou écrit à un oncologue tous les mardis à neuf heures du matin pendant six mois, il n'est pas nécessaire d'écouter la conversation pour deviner ce qui se passe. Si deux personnes échangent cent messages par jour et cessent soudainement de le faire, il n'est pas nécessaire d'en lire un seul pour comprendre ce qui s'est produit. Si un conseiller fiscal reçoit vingt messages d'affilée du même client la veille d'une clôture trimestrielle, le schéma parle de lui-même.

Les métadonnées révèlent des schémas de comportement : qui est en relation avec qui, quels sont les horaires de chaque personne, quand elle est éveillée, quand elle dort, quand elle voyage, quels clients sont les plus actifs, quelles relations professionnelles sont les plus intenses. Un serveur qui collecte des métadonnées peut construire un profil détaillé de la vie personnelle et professionnelle de n'importe quel utilisateur sans jamais avoir lu un seul mot de ce qu'il écrit.

Il existe un exemple historique qui illustre cela avec dureté. L'ancien directeur de la NSA, Michael Hayden, l'a formulé sans nuance en 2014 : *"We kill people based on metadata"*. Cette affirmation faisait référence à des opérations militaires américaines contre des cibles identifiées uniquement par leurs schémas de communication. Pas un seul message lu. Seul le graphe de contacts et les horaires.

Le fait qu'un service collecte des métadonnées n'implique pas qu'il va les utiliser contre ses utilisateurs. Cela implique qu'il en a la capacité, et qu'un tiers ayant accès à ces données — par ordonnance judiciaire, par faille de sécurité ou par vente à des tiers si les conditions de service le permettent — l'a également.

L'accès au répertoire

Un autre vecteur qui passe presque inaperçu : la liste de contacts. Une grande partie des services de messagerie demandent l'accès au répertoire du téléphone lors de l'inscription. Ils téléchargent tous les numéros sur leur serveur pour montrer qui d'autre utilise le service. À partir de ce moment, l'entreprise dispose d'une carte complète des relations de l'utilisateur, même si celui-ci n'a jamais écrit le moindre message à personne.

Pour un professionnel soumis au secret professionnel — avocat, médecin, psychologue, conseiller — cette carte contient des clients. Si le répertoire a été téléchargé sur un serveur tiers, les noms des clients se trouvent dans une infrastructure dont la juridiction et les politiques ne sont pas contrôlées par le professionnel. Le secret professionnel n'est pas rompu le jour où quelqu'un divulgue une conversation : il a été rompu bien plus tôt, au moment d'accepter le téléchargement.

La différence entre chiffrer et ne pas collecter

Chiffrer, c'est protéger le contenu. Être privé, c'est ne pas collecter ce qui n'est pas nécessaire. Ce sont deux choses distinctes, et la différence est opérationnellement critique. Un service peut chiffrer tous les messages à la perfection et, en même temps, savoir presque tout sur ses utilisateurs grâce aux métadonnées. Les deux choses sont parfaitement compatibles. En fait, c'est le modèle économique dominant dans le secteur.

La bonne question pour évaluer la confidentialité réelle d'un service n'est pas *« chiffre-t-il le contenu ? »*. Cette question est réglée depuis des années. La bonne question est : *« quelles métadonnées génère-t-il et où sont-elles stockées ? »*. Et surtout : *« quelles métadonnées n'a-t-il pas besoin de générer ? »*.

Une architecture qui minimise les métadonnées par conception — et non par promesse ou par politique interne — est structurellement plus privée qu'une architecture qui les collecte et les chiffre. Car les données qui n'existent pas ne peuvent être divulguées, vendues, remises sur ordonnance judiciaire ou perdues lors d'une faille.

Pour le lecteur professionnel

Si votre activité professionnelle implique le secret, la confidentialité ou simplement le respect des informations de tiers, il convient de se poser les questions dans cet ordre :

1. L'application que j'utilise pour communiquer chiffre-t-elle le contenu ? (Probablement oui.)
2. Chiffre-t-elle les métadonnées ? (Probablement non.)
3. Génère-t-elle des métadonnées dont elle *n'a pas besoin* pour fonctionner ? (Presque certainement oui.)
4. Où sont stockées ces métadonnées et sous quelle juridiction ? (Probablement hors de l'Espace Économique Européen.)
5. Mon client ou mon patient sait-il que ses données s'y trouvent ?

La dernière question est la plus dérangeante. Car la réponse honnête, dans la plupart des cas, est non.

Cet article est le premier d'une série sur le fonctionnement réel des outils de communication professionnelle. Les prochains numéros aborderont la conformité RGPD dans la messagerie et le concept de secret professionnel à l'ère numérique.

Sources et lectures complémentaires

- Hayden, M. — Déclaration à la Johns Hopkins University, 2014 ("We kill people based on metadata"). Transcriptions publiques disponibles.

- RGPD (Règlement UE 2016/679), art. 4 et 5 — définition des données à caractère personnel et principes du traitement (les métadonnées sont bien des données à caractère personnel).
- EDPS et EDPB — avis sur le traitement des données relatives au trafic et des métadonnées dans les communications électroniques (Directive ePrivacy).

← PrécédentUne brève histoire du cachet de cireSuivant →Le secret professionnel à l'ère numérique

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 a1ce40ce269b3432f9466a7ec971bae0709a19e13557d3f222e967f077658902

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