LES FICHES RÉGLEMENTAIRES CLOUD TEMPLE

La messagerie chiffrée, en clair

DEFINITION

Une messagerie chiffrée est un service permettant d'échanger des messages de façon confidentielle grâce à des algorithmes de chiffrement. Seuls l'expéditeur et le destinataire peuvent lire le message, qui est chiffré avant l'envoi et déchiffré avec une clé après réception.

En principe, même le fournisseur de service ne peut pas accéder au contenu des messages, car il ne possède pas les clés nécessaires.

LE CONTEXTE

La réglementation des messageries chiffrées vise à équilibrer vie privée, sécurité des données et besoins des autorités. Aucun texte unique ne la régit : elle repose sur un ensemble de lois comme le RGPD, la directive ePrivacy, le Code des postes, ou la loi sur la cybersécurité (NIS2).

L'usage de ces messageries par des criminels pose des questions sur l'accès aux contenus chiffrés, souvent débattues, notamment lors de discussions législatives récentes contre le narcotrafic.

LES ENJEUX	CLARIFICATION
Sécurité du chiffrement	Ce modèle dépend entièrement de la gestion des clés. S'il est rigoureusement respecté, le fournisseur du service n'a aucun moyen d'accéder au contenu des messages. Pourtant, dans de nombreux cas, les clés de chiffrement sont créées, gérées, voire stockées par les serveurs du fournisseur, ne serait-ce que temporairement. Dans ces situations, le fournisseur peut techniquement accéder aux messages. Un chiffrement de bout en bout n'est donc véritablement protecteur que si la gestion des clés est strictement locale, sur les appareils des utilisateurs, et si aucune copie de ces clés n'est accessible au fournisseur.
La question des «backdoors»	Il s'agit d'un mécanisme volontairement intégré dans un système informatique, qui permet à une autorité ou à un acteur spécifique d'y accéder, même si le système est chiffré ou protégé. Ce mécanisme suscite beaucoup de controverse du point de vue de la protection des droits fondamentaux notamment du droit au respect de la vie privé. La Cour européenne des droits de l'homme a d'ailleurs souligné l'illégalité des "portes dérobées" systématiques en 2024.
Sécurité nationale VS Droit à la vie privée	La messagerie chiffrée illustre la tension persistante entre les impératifs de sécurité nationale et le respect de la vie privée. Si elle garantit la confidentialité des communications pour les citoyens, elle complique considérablement l'accès aux preuves dans le cadre d'enquêtes liées à la cybercriminalité, notamment en matière de trafic de stupéfiants ou de pédopornographie.

L'ANALYSE

Nicolas Abrioux, Security Governance Leader de Cloud Temple

«L'utilisation de la messageries chiffrées soulève un autre sujet : celui de la confiance. Qu'il s'agisse de l'éditeur, de l'hébergeur ou des autorités, il y aura toujours un acteur susceptible d'interférer avec vos communications chiffrées. La question est donc de savoir à qui accordez-vous votre confiance, et pour quels types d'échanges.
Où sont stockées les données ? Qui conçoit le système de messagerie, à quel point est-il sécurisé ? Qui gère l'infrastructure, les clés de chiffrement, les terminaux de messagerie ? Tous les usages de messagerie ne présentent pas les mêmes enjeux de sécurité. Dès lors, les approches hybrides peuvent s'avérer adaptées : solutions pratiques pour l'ordinaire, outils souverains ou renforcés pour les échanges les plus sensibles. »

PROCHAINES ÉTAPES

L'article 8 ter du projet de loi contre le narcotrafic prévoyait d'imposer aux fournisseurs de messageries chiffrées une obligation de rendre accessibles les contenus échangés en cas d'enquête, y compris par des moyens techniques.

Il a suscité une forte opposition des acteurs du numérique qui y voyaient une menace directe contre le droit au respect de la vie privé. Finalement jugé disproportionné et techniquement irréaliste, l'article a été retiré avant la promulgation de la loi le 13 juin 2025.

CLOUD TEMPLE
Innovative by design