

Chiffrement : Signal, nouvelle coqueluche de la Commission européenne

Signal gagne en influence à la Commission européenne.

L'institution [recommande](#) depuis peu [l'application de messagerie instantanée](#) à son personnel, pour la communication avec le public.

Le sujet a été abordé le 19 février à l'occasion d'une réunion sur la future stratégie communautaire de sécurité. Cette dernière doit être formalisée d'ici à la fin de l'année.

En toile de fond, une succession d'alertes parmi lesquelles :

- L'[exfiltration de milliers de câbles diplomatiques](#) depuis COREU, réseau de communication censé faciliter la coopération en matière de politique étrangère
- Le [piratage d'ordinateurs](#) de la Délégation de l'Union européenne à Moscou

Le personnel de la Commission est déjà censé utiliser des e-mails chiffrés pour l'échange de données sensibles (hors éléments classifiés, soumis à un régime particulier).

Le choix de Signal s'inscrit dans cette lignée. Il intervient à l'heure où l'application concurrente Telegram est pointée du doigt pour un manque de transparence sur son chiffrement*.

Le dilemme du chiffrement

L'approche est délicate pour Bruxelles, qui prône dans le même temps une ouverture des messageries chiffrées aux forces de l'ordre. Apple (iMessage) et Facebook (Messenger, WhatsApp) ont été sollicités dans ce sens.

Le dernier rapport « [Internet Organised Crime Threat Assessment](#) » d'Europol illustre cette position. Les autorités des États membres y décrivent le chiffrement comme un frein majeur à la détection des activités criminelles.

Ferd Grappenhuis, ministre néerlandais de la Justice, l'a [confirmé](#) fin 2019 : l'UE « doit envisager une législation qui permette aux gouvernements d'accéder aux données chiffrées ».

Reste que la stratégie communautaire de cybersécurité, dans sa dernière révision [votée en 2017](#), pose le chiffrement comme un outil indispensable à la protection des données personnelles et des droits fondamentaux.

La directive e-privacy, en cours d'élaboration, inclut elle aussi des garde-fous. Mais elle introduit en parallèle des exceptions autorisant l'interception de communications au nom de l'intérêt public.

** WhatsApp fait l'objet des mêmes critiques, quand bien même l'application se fonde sur le même protocole que Signal. En l'occurrence, Open Whisper Systems.*