

**Question for written answer E-002044/2025
to the Commission**

Rule 144

Catherine Griset (PfE), Christophe Bay (PfE), Mélanie Disdier (PfE), Julie Rechagneux (PfE), Séverine Werbrouck (PfE), Fabrice Leggeri (PfE), Gilles Pennelle (PfE), Pascale Piera (PfE)

Subject: Message encryption

The Commission has begun to consider whether police forces could gain access to encrypted messages.

Although useful in the fight against organised crime, any backdoor could nevertheless be exploited by malicious actors, such as hackers, unscrupulous private companies or third country intelligence services.

As my colleague Aurélien Lopez-Liguori, Member of the French National Assembly, has noted, such backdoors would inevitably weaken encryption and therefore be a chink in the cybersecurity armour¹.

The risk is such that a provision to that effect was rejected in a National Assembly debate a few weeks ago.

1. Will the Commission take that security risk into account before introducing any legislative proposals that require the various messaging services to contain a backdoor?
2. If necessary, will it ensure that any authorisation to override message encryption can only be issued by a judge, as part of a criminal investigation and for a limited period of time?
3. Finally, how does it intend to require messaging services owned (as almost all are) by non-EU companies to contain backdoors?

Supporter²

Submitted: 21.5.2025

¹ <https://lcp.fr/actualites/narcotrafic-l-assemblee-refuse-l-acces-aux-messageries-chiffrees-contre-l-avis-de-bruno>

² This question is supported by a Member other than the authors: Marie-Luce Brasier-Clain (PfE)