

**Priority question for written answer P-005062/2021  
to the Commission**

Rule 138

**Lucia Ďuriš Nicholsonová** (Renew)

Subject: Addressing online child sexual abuse and end-to-end encryption

Currently, the task of searching for and removing child sexual abuse material (CSAM) online is left to the discretion of platforms. However, the Commission is due to present a legislative proposal in December to provide a permanent and across-the-board solution in this regard. The key question is what to do about content that is encrypted using end-to-end encryption (E2EE).

In this context, Apple has recently announced that it will introduce a technology that will allow it to scan content before it is encrypted, directly on the customer's device itself, called client-side scanning (CSS). However, due to pressure from some experts and the public, the introduction of this technology has been postponed.

1. What is the Commission's position on such a solution?
2. Does the Commission plan to base its solution to the CSAM problem on CSS in order to scan communications on devices across the board?
3. If so, does the Commission believe that this is consistent with the Commission's recent recommendation to its staff to use the Signal application for communications, which is widely regarded as one of the most secure messaging applications available due to its strong E2EE, since in the case of CSS, although E2EE will not be technically compromised, it will de facto lose its rationale?