Council of the European Union

Brussels, 28 April 2022
(OR. en)

8179/22

LIMITE

CATS 22
JAI 489
COPEN 128
ENFOPOL 195
CYBER 122
TELECOM 151
DROIPEN 49
DATAPROTECT 103
EJUSTICE 41
MI 287
JAIEX 35

NOTE

From:	Presidency
To:	Coordinating Committee in the area of police and judicial cooperation in criminal matters
Subject:	Access to data in criminal investigations - Discussion paper

Delegations will find in Annex the courtesy translation of document 8179/22.

ANNEX

Discussion paper

Access to data in criminal investigations

In their joint statement of 24 March 2016 following the terrorist attacks two days earlier in Brussels, the EU Ministers for Justice and Home Affairs and representatives of EU institutions called for the need to "*find ways, as a matter of priority, to secure and obtain more quickly and effectively digital evidence, by intensifying cooperation with third countries and with service providers that are active on European territory, in order to enhance compliance with EU and Member States' legislation and direct contacts with law enforcement authorities*[1]".

On 22 and 23 June 2017, the European Council echoed this call by confirming that "*effective access to electronic evidence [was] essential to combating serious crime and terrorism and that, subject to appropriate safeguards, the availability of data should be secured*[2]".

Indeed, access to electronic data, beyond the need to facilitate the search for incriminating and exonerating evidence, has been made necessary by technological evolutions that are facilitating the boom in new forms of online crime and are offering traditional criminals new ways and tools to grow, at an unprecedented rate and scale. Criminal investigations are no longer conceivable without the use electronic evidence and, consequently, without being able to access the corresponding data. Investigators are encountering numerous obstacles when it comes to obtaining this evidence, in particular data volatility which requires the data to be stored in one way or another, and the fact that electronic services are often provided by foreign companies, which requires very often to seek international cooperation.

1 Joint statement of EU Ministers for Justice and Home Affairs and representatives of EU institutions on the terrorist attacks in Brussels on 22 March 2016

2 European Council conclusions, 22-23/06/2017.

In these circumstances, on 17 April 2018 the European Commission presented its legislative package for access to electronic evidence. The Council and the Parliament adopted their respective positions, and since then trilogues have been ongoing for more than 16 months and the Presidency is particularly involved in these negotiations which seek to address a real operational need.

The design of effective cooperation measures within the field of electronic evidence goes hand in hand with conditions for allowing the storage of and access to this type of evidence.

Since 2014, the Court of Justice of the European Union has been setting precedents in this matter.

As regards data storage, the Court has established the principle of prohibiting general and indiscriminate retention of connection data for the purposes of combating crime[3]. The Court therefore feels that data retention must not be targeted (especially based on geographical or personal criteria) and that it should be done using expedited retention (quick freeze) methods. This case law now appears well established, having been confirmed by the ruling of 5 April 2022 (case C-140/20, G.D).

The Court also outlined the process for accessing stored data, ruling that such access should be subject to prior review by an independent administrative authority or jurisdiction[4]. It specified that the requirement of independence entails that the authority entrusted with the prior review must not be involved in the conduct of the criminal investigation in question and must have a neutral stance vis-à-vis the parties to the proceedings.

This framework as established by the Court of Justice must also be considered alongside the new challenges facing Member States in terms of evolving technologies, especially encryption which is a major issue when it comes to data access for the purposes of combating crime.

---

3 CJEU, Grand Chamber, 21 December 2016, *Tele2 Sverige AB*, C-203/15; CJEU, Grand Chamber, 6 October 2020, *La Quadrature du Net e.a.*, C-511/18.

4 Cf. in particular CJEU, Grand Chamber, 2 March 2021, *H.K., Prokuratuur*, C-746/18, confirmed by the judgment of 5 April 2022.

The CATS Delegates are invited to respond to the following questions:

1. What are your initial thoughts on the CJEU judgment of 5 April 2022? Can you already foresee any particular implications in terms of your existing or upcoming national legislation?

2. As regards to access to stored data, the Court of Justice has insisted specifically on the requirements at the time of the request. In light of these judgments, what guarantees do you believe are particularly important when accessing evidence collected from electronic communications?