Council of the European Union

Brussels, 19 February 2021
(OR. en)

6231/21

LIMITE

COPEN 77
CYBER 38
ENFOPOL 53
JAI 148
DATAPROTECT 38
EUROJUST 25

NOTE

From:	Presidency
To:	Delegations
Subject:	Examination of the ECJ rulings of 6 October 2020 (case C-623/17 and joint cases C 511/18, C-512/18 and C-520/18) - presentation by the Presidency and exchange of views

Delegations will find in Annex Presidency´s working paper for the above-mentioned subject.

ANNEX

Working Party on Cooperation in Criminal Matters | COPEN - Data Retention

Working Paper

One of the priorities of the Portuguese Presidency of the Council of the European Union for the area of justice is the fight against terrorism and organized crime. This priority gains particular relevance in the present context where we all rely more than ever on information systems, mobile devices and the Internet to work, communicate, shop, share and receive information, and which has also accelerated online criminal activity.

Traces of such online criminal activity are often difficult to obtain, and electronic communications service providers are often the only ones holding information that can help identify individuals behind criminal activity. However, this information - in particular internet protocol (IP) addresses and other metadata bearing evidence of communications - is considered sensitive in nature and must be deleted, unless there is a legal basis for its preservation. Accordingly, the retention of non-content communication data by operators is a decisive factor in guaranteeing the availability of data that law enforcement authorities require to effectively fight against crime.

As Presidency, Portugal will continue the important discussion on data retention, following the judgments of the Court of Justice of the European Union on the matter, and building on the excellent work already developed by previous presidencies.

I. Context

In the judgements of 6 October 2020, the Court of Justice of the European Union confirmed its previous jurisprudence that electronic communications data are confidential and, in principle, cannot be retained in a general and indiscriminate manner. Nevertheless, the Court takes that opportunity also to clarify certain limited exceptions to this rule in specific situations concerning national security, public defense and security or crime prevention, investigation, detection and prosecution. The Court further states that these exceptions are exhaustive and can never become the rule.

The Court also stresses that the retention of data should be guided by objective criteria, namely a link, at least an indirect one, between the data of the persons concerned and the objective pursued. Regarding the objectives/purposes that justify exceptions to the rule of confidentiality and non-retention of communications data, the Court clarifies that:

1. In relation to national security:

There is no doubt that the primary interest in protecting the essential functions of the State and the fundamental interests of society can justify the retention of data, being, therefore, a legitimate objective for this retention. However, the Court made clear that the general and indiscriminate retention of traffic and location data for national security is a legitimate objective only if there are concrete circumstances of a national security threat that must be serious, real, current or foreseeable. In addition, a time limit for the retention has to be defined and, while an order can be renewed, the retention cannot be systematic. The retention must be subject to review by a court or by an independent administrative entity whose decision is binding.

2. Regarding the objectives of combating crime and public security:

The Court considers that general and undifferentiated, systematic and continuous data retention is not justified even in the fight against serious crime or serious threats to public security. However, the targeted retention of traffic and location data may be justified.

The Court allows the targeted retention of traffic and location data for the purposes of fighting serious crime or serious threats to public security as long as such targeted retention is limited with respect to the categories of data, the means of communication and the persons concerned, and takes place for a limited period of time. The Court also refers to the possibility to set the limits of targeted retention based on categories of persons or geographical criteria. Access to data must be subject to the appropriate procedural and substantive safeguards.

However, this targeted retention does not apply to the retention of two types of data, namely the IP address of the source of a communication and civil identity data. In these cases, the Court shows some flexibility towards the general retention of these two types of data, depending on the purposes pursued.

In particular, the Court allows for the general and indiscriminate retention of source IP addresses for the purposes of fighting serious crime and provided that the retention period is limited in time. Access to data must be subject to appropriate procedural and substantive safeguards.

For civil identity data, on the other hand, the Court allows their general and indiscriminate retention for the purposes of fighting crime in general and without specifying any specific retention period.

It is also worth noting that data, including subscriber, traffic and location data, for consumer protection and commercial purposes is retained in a general and undifferentiated fashion, for different periods, according to national law or commercial practices.

II. Topics for discussion

Based on the jurisprudence of the Court of Justice, the Portuguese Presidency proposes to further discuss two topics:

- Selective/targeted retention;

- Retention of source IP addresses and civil identity data.

In order to structure our discussions, and based on the introductory explanation presented in the beginning of this document, the Presidency proposes some questions and welcomes the views and opinion of the Member States on the topics for discussion that follow.

a) Regarding selective/targeted retention, we invite Member States to comment on the following:

1. Considering the recent jurisprudence of the Court of Justice, what are the Member States' views on the categories of data that should be retained based on law enforcement operational needs? How can the categories be limited e.g. volume, sensitivity, retention period etc.?

2. What are Member States views on the means of communication that should be covered? What are their views on the types of providers, including OTTs? Can these be limited based on size, geographical coverage, number of subscribers, cross-border presence?

3. Do Member States consider the reference to categories of person in the recent Court of Justice case-law problematic? How could such concept be developed and applied having in mind non-discriminatory concerns? What kind of objective criteria can be applied to defining such a category of persons?

4. What would Member States consider an appropriate retention period? Which objective criteria can be applied to determine such a period, e.g. sensitivity of the data?

b) Regarding the retention of IP addresses and civil identity data, we would like to invite the Member States to comment on the following:

1. Do Member States interpret the possibility of retention of source IPs addresses, established in the recent case law of the Court, as including both static and dynamic IPs? Would or should this include source-port numbers? What are the views on only retaining source but not destination IP addresses?

2. Do Member States consider it to be in line with the jurisprudence of the ECJ that Internet Protocol addresses, strictly needed to identify a subscriber, should include first login IP, last login IP or the login IP used at a specific moment in time? Should this be considered as 'subscriber' or 'traffic' data if the IP address is used solely to identify a person?

3. Considering the ECJ jurisprudence, do Member States agree that IP addresses for the purpose of identifying a subscriber should be accessed by Criminal Justice Authorities below the threshold of “serious crime”, in line with the ECtHR jurisprudence (K.U. v. FINLAND, Application no. 2872/02) that considers that "Limiting access to or disclosure of subscriber information to investigations of serious crime would prevent governments from meeting their obligations to protect individuals and their rights against crime"? Which crimes would fall below the serious crime threshold under national laws?