Council of the
European Union

Brussels, 2 March 2021
(OR. en)

6455/21

LIMITE

COPEN 89
CYBER 46
ENFOPOL 67
JAI 189
DATAPROTECT 46
EUROJUST 29

NOTE

From:	Presidency
To:	Delegations
Subject:	Retention of electronic communication data - exchange of views

Delegations will find enclosed a discussion paper for the informal videoconference of the Ministers of Justice on 11 March 2021.

I. Introduction

In 2014 the Court of Justice of the European Union (CJEU) declared the 2006 Data Retention Directive[1] to be invalid *ab initio*. Subsequently, in the Digital Rights Ireland (2014) and Tele2 cases (2016) the CJEU prohibited the EU and its Member States from laying down rules that entail a general and indiscriminate retention of data, setting limits on the data retention regime as practiced until that date, which led Member States to claim that the court's decision would make it more difficult to carry out effective criminal investigations.

Following this decision, a common reflection process to see how to move forward was launched in 2017 in the Council, also to explore possible options to ensure the availability of data for the purpose of preventing and fighting crime, with reference to the CJEU case law.

The findings of this reflection process and the state of play on data retention for the purposes of fighting crime were outlined by the Austrian Presidency in a report presented to the JHA Council in December 2018. Ministers discussed the way forward and supported the continuation of the work at experts' level to explore avenues to develop a concept of data retention within the EU.

The discussions organised by the Romanian Presidency on possible ways ahead led to the June 2019 Council Conclusions. The Commission was tasked to undertake targeted consultations with relevant stakeholders and to carry out, on that basis, a comparative study on data retention considering the various options, including the preparation of a new legislative proposal. A fact-finding study was completed last autumn.

---

1 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

In October 2020, the CJEU handed down its latest judgments in a series of data retention cases[2]. While confirming its prohibition of generalised and indiscriminate retention of data in principle, it set out a number of exceptions from that principle that Member States now wish to explore, in view of the important role of communications metadata in preserving national security, attributing crimes and identifying criminals.

More recently, the European Council Conclusions of December 2020 recognized how essential it is for law enforcement and judicial authorities to be able to exercise their lawful powers both online and offline to fight serious crime. In this regard, the Conclusions stressed the need to advance work on the retention of data necessary to fight serious crime, in the light of the latest case law of the CJEU and in full respect of fundamental rights and freedoms.

Consequently, in February 2021, the Council´s General Approach on the proposed ePrivacy Regulation included several aspects related to data retention, such as the exclusion from its scope of the processing of data for national security and an explicit reference to data retention for law enforcement and public security purposes.

In addition, at the CATS meeting held on 8 February 2021, a number of Member States supported the adoption of European legislation harmonising the legal regime for data retention and proposed that the issue be discussed at political level at the JHA Council on 11 March 2021.

---

2 Judgements of 6 October 2020 (Joined Cases C-511/18, C-512/18 and C-520/18; and Case C-623/17.

II. The October 2020 CJEU rulings

In the judgements of 6 October 2020, the CJEU confirmed its previous jurisprudence[3] that electronic communications data are confidential and, in principle, traffic and location data cannot be retained in a general and indiscriminate manner. The Court set out limited exceptions to this rule concerning national security, public defence and security or crime prevention, investigation, detection and prosecution.

Regarding the objectives or purposes that justify the exceptions to the rule of confidentiality and non-retention of traffic and location data, the Court clarifies that:

(a) In relation to national security

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 general and indiscriminate retention of traffic and location data for national security reasons is permissible only if there are concrete indications of a serious, real, current or foreseeable national security threat. In addition, a time limit for the retention has to be defined and, even though it can be extended upon the persistence of the threat, the retention cannot be systematic. In all cases, the decision imposing such an instruction must be subject to review by a court or by an independent administrative entity whose decision is binding.

(b) Regarding the objectives of combating crime and safeguarding public security

[3] Judgment of 8 April 2014, Joined Cases C-293/12 and C-594/12; and judgment of 21 December 2016, Joined Cases C-203/15 and C-698/15.

The general and indiscriminate, systematic and continuous data retention is not justified even for the fight against serious crime or prevention of serious threats to public security. However, the targeted retention of traffic and location data may be justified in such cases, as long as is limited with respect to the categories of data, the means of communication, the persons concerned and the time period. Targeted retention can be based on categories of persons or geographical criteria.

It also allows, under certain conditions, expedited retention of available data, for the purposes of combatting serious crime, and also allows for the general and indiscriminate retention of source IP addresses for the purposes of fighting serious crime or preventing serious threats to public security and provided that the retention period is limited in time.

For civil identity data general and indiscriminate retention for the purposes of fighting crime or preventing serious threats to public security in general and without specifying any retention period is also allowed.

Targeted retention, expedited retention, retention of IP addresses and civil identity data of users are also possible for national security purposes. Access to data must always be subject to appropriate procedural and substantive safeguards.

III. Debate

Seven years after the CJEU invalidated the Data Retention Directive, a solution is necessary.

Against this background, the Presidency considered the need to exchange views on how to seize the opportunities offered by these new judgments of the CJEU.

Therefore, the Presidency would like to invite Ministers to express their views on the following questions:

(a) Do you consider that legislation should be adopted to ensure a harmonized legal regime on data retention at EU level, taking due account of the case law of the Court?

(b) If so, should we adopt a comprehensive or a targeted approach?

(c) On the contrary, do you consider that police and judicial cooperation that may need the retention of data can take place solely based on national data retention laws, in line with the Charter of fundamental rights and the ECJ case law?