Council of the European Union

Brussels, 23 May 2017
(OR. en)

9558/17

LIMITE

JAI 527
COPEN 172
DAPIX 204
ENFOPOL 260
CYBER 85
EUROJUST 79

NOTE

From:	Presidency
To:	Delegations
Subject:	Targeted data retention - Exchange of views

In its Judgement of 21 December 2016 *Tele2*[1], the Court ruled that Article 15(1) of Directive 2002/58/EC (the e-Privacy Directive)[2], read in the light of the Charter of Fundamental Rights, must be interpreted *"as precluding national legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication"* (paragraph 112).

1 Judgement of the Court of Justice of the EU (Grand Chamber) *"Tele 2 and Watson"* of 21 December 2016 in joined Cases C-203/15 and C-698/15.

2 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ L 201, 31.7.2002, p.37). This Directive is being thoroughly reviewed following the proposal submitted by the Commission in January 2017 to replace it by a Regulation (see Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), doc. 5358/17).

However, Article 15(1) *"does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary"* (Paragraph 108). According to the Court "*the retention of data must […] meet objective criteria, that establish a connection between the data to be retained and the objective pursued.*" (paragraph 110).

The Presidency would like to invite an exchange of views on **the concept of targeted retention of traffic and location data**, as set out by the Court in the *Tele2* judgement focusing in particular on each of the four criteria listed by the Court, while taking into account that they are closely intertwined

I. Regarding **the categories of data to be retained** the Court stipulated that *"while the effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be,* ***cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data*** *should be considered to be necessary for the purposes of that fight (see, by analogy, in relation to Directive 2006/24, the* Digital Rights *judgment, paragraph 51)"* (paragraph 103)

1. Further to the discussion on that issue at the DAPIX - FoP meeting of 15 May 2017, how could the types of data to be retained for the purposes of fighting crime be differentiated or limited according to the objective pursued?
2. Considering that some Member States have differentiated between data categories in their national legislation, more in particular with regard to the retention period, could more information be give on what basis these distinctions have been made?
3. Could anonymization or data encryption, or other technical means provide sufficient safeguards to mitigate the impact of a general data retention obligation with a broader scope?
4. Which data categories and which communication means are considered to be the most sensitive, from a data protection perspective?

II. Regarding **the means of communication affected (paragraph 108)**:

1. How can data retention be targeted in relation to the means of communication, based on objective criteria?
2. How to address the risk that criminals divert from using the means of communication targeted and resort to alternative means of communication?
3. To what extent are the means of communication that provide for encrypted communication relevant in this context?

III. Regarding **the persons concerned**, Paragraph 111 provides that *"As regards the setting of limits of such a measure with respect to the public and the situations that may potentially be affected, the national legislation must be based on objective evidence which makes it possible to identify a public whose data is likely to reveal a link, at least an indirect one, with serious criminal offences, and to contribute in one way or another to fighting serious crime or to preventing a serious risk to public security. Such limits may be set by using a geographical criterion where the competent national authorities consider, on the basis of objective evidence, that there exists, in one or more geographical areas, a high risk of preparation for or commission of such offences".*

1. On the basis of which criteria could it be possible to identify a public whose data is likely to reveal a link with serious criminal offences? How indirect may such a link be while abiding by the *Tele2* requirements?
2. How to substantiate the requirement of objective evidence upon which the geographical criterion would be based?
3. In general, how to target data retention to persons in line with the criteria suggested by the court in a non-discriminatory manner?
4. Could a system limiting the data retention to specific geographical areas on the basis of rotation be a way forward? If so, would it be necessary to demonstrate the existence of a link with serious criminal offences?
5. How to address the risk that criminals divert from the area under surveillance?
6. With a view to limiting the number of individuals affected by data retention, what other criteria could be considered that would not be based on the determination of a geographical area (e.g. on the basis of professional secrecy as referred to in paragraph 105? Is so, which?

IV. Regarding **the retention period (paragraph 108)** .

1. How far can the retention period be limited on the basis of objective criteria, while taking into account the practical needs of competent authorities?
2. Would it be possible, including from a technical point of view to differentiate the retention period e.g. on a case-by-case basis according to the needs of a specific investigation or the types of data?
3. What are the views on a combination between a minimum general retention period and a differentiated regime for retention once the investigation is open?

V. Paragraph 110 provides that the **substantive conditions** for data retention may *"vary according to the nature of the measures taken for the purposes of prevention, investigation, detection and prosecution of serious crime"* but that *"the retention of data must continue nonetheless to meet* ***objective criteria, that establish a connection between the data to be retained and the objective pursued.*** *In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and, thus, the public affected."*

1. To what extent can the nature of the measures taken be relevant in delimiting a data retention system?
2. Could you provide examples of "objective criteria", as mentioned in this paragraph?