Council of the European Union

Brussels, 30 October 2017
(OR. en)

13845/17

LIMITE

JAI 983
COPEN 325
DAPIX 355
ENFOPOL 500
CYBER 166
EUROJUST 165
TELECOM 257

NOTE

From:	Presidency
To:	Delegations
Subject:	Retention of communication data for the purpose of prevention and prosecution of crime - specific elements in light of the ECJ case-law = exchange of views

I. Introduction

At the meeting of the DAPIX - FoP on 18 September 2017 delegations exchanged views on the possible options and related elements identified in the course of the common reflection process for ensuring the availability of communication data that could be used for the purposes of prevention and prosecution of crime. At the meeting on 16 October 2017, during a joint meeting of the DAPIX- FoP on data retention and WP on Telecommunications and Information Society (TELECOM), an initial exchange of views was held regarding the draft e-Privacy Regulation.

Taking into account views expressed by the Member States during previous meetings, the Presidency considers further work should focus on three main elements regarding a data retention regime for the purpose of prevention and prosecution of crime in light of the jurisprudence of the EUCJ.

1) Ensuring availability of data: in this regard, it is necessary to ensure coherence between the draft e-Privacy Regulation and retention of data for the purpose of prevention and prosecution of crime. First and foremost, the rules and obligations applicable to service providers in the context of the draft e-Privacy Regulation should not contradict the possibility for derogations on the basis of domestic or EU legislation with the purpose of retaining data for prevention and prosecution of crime. In this regard, specific attention should be paid to a better delimitation of the scope of application of the draft Regulation in light of the arguments of the Court stemming from the interpretation of the scope and structure of the current e-Privacy Directive.

2) Restricting the amount of data retained for the purpose of prevention and prosecution of crime, taking into account requirements of the jurisprudence, including further analysis of the elements identified by Europol and the EU CTC.

3) Limiting access to retained data through placing additional safeguards to restrict access to data only when strictly necessary and proportionate, including further analysis of the elements identified by the EU CTC and Europol.

On the issues related to the availability of data in the context of the draft e-Privacy Regulation, the WP TELECOM has been invited to further reflect on the issues discussed at the joint meeting on October 16. The Presidency will thereafter summarise the discussion.

With a view to allowing for a structured exchange among delegations at the DAPIX - FoP meeting on 6 November 2017, the Presidency would like to invite delegations to:

- present their views on the elements outlined below with a view to streamlining or complementing the specific elements and

- indicate whether in their opinion these elements could be considered in the context of developing a data retention framework at both the Member States and EU level.

The outcome of the discussion will be the basis for discussions in CATS with a view to preparing the debate of the Council in December on the state of play and next steps on this file.

II. Specific elements

The concept of restricted data retention and targeted access, as presented by the EU CTC and Europol could serve as a basis for developing a data retention framework, whether at national or EU level, as a preventive measure for a mandatory storage of communication metadata for the purposes of fighting serious crime, while taking into account the ECJ requirements.

Some delegations have underlined that in principle an EU instrument on data retention would ensure a common reference framework across the EU, ensuring legal certainty and predictability of the legal framework and a level playing field for all the stakeholders concerned. However, as a minimum, Member States should be able to adopt national measures on data retention for the purpose of prevention and prosecution of crime.

As emerging from the discussions at DAPIX -FoP, a certain number of general principles and specific elements to substantiate the concepts of restricted data retention and targeted access could be considered in the context of developing a data retention framework, as identified by Europol and the EU CTC.

General principles

The concepts of restricted data retention and targeted access are premised on the following general understanding:

- The Charter does not exclude limitations to the exercise of rights and freedoms laid down therein, provided such limitations fulfil the specific conditions set out in Article 52 (1) of the Charter and in particular provided they meet a strict proportionality and necessity test. It is recalled that, according to the settled case-law, a strict necessity test implies that there must not be a less intrusive measure that is equally effective to achieve the pursued objective.

- The Charter "does not prevent"[1] data retention legislation, but while the Court rules out general retention of data, it does not solely permits targeted data retention; therefore there are other legally possible regimes for non-general data retention.

[1] Cf. Tele 2, para. 108.

- The measure has to be limited to the strictly necessary, be based on objective evidence and needs to set out clear and precise rules. The ECJ mentions that such limitation could be done by restricting data retention to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) *persons who could, for other reasons, contribute, through their data being retained, to fighting crime*[2].

- The systematic storage of metadata for the purposes of fighting crime is possible, insofar as a strict proportionality and necessity test are met (as regards categories of data, means of communication, persons concerned and retention period); a connection between the data that is retained and the objective pursued must be established on the basis of objective criteria[3].

- The potential scope of application of a restricted data retention system needs to be effective for the protection of public security interests, so that the restrictions applied would not render the measure irrelevant for the purpose pursued (i.e. public security interests).

- The proposed solution will not contain general and indiscriminate data retention measures; they have been excluded by the ECJ as they interfere "in a particularly serious manner" with the rights to respect of private life and to the protection of personal data.

  A differentiated approach as regards the two levels of interference (*first level interference* - the data retention obligation for the purposes of fighting serious crime, and *second level interference* - access to and use of data stored) could be considered, while aiming at a comprehensive safeguards framework that would be compatible with the Court's requirements as a result of the cumulative effect of the specific safeguards introduced at each of the two levels of interference. Both interference levels must comply with the necessity and proportionality tests.

- Strong safeguards and limitations as regards access and use by competent authorities of the data retained assist in mitigating the overall impact of the interference of the measure, in particular by ensuring that access is granted solely to specific data needed for a particular investigation**.** The latter should reduce the impact on individual freedoms and rights to a minimum.

---

2 Cf. Tele 2, para 106.

3 Cf. Tele 2, para 110 and most recently PNR Canada, para 191.

Level 1 interference: restricted data retention

A certain number of specific proportionality/necessity filters could be considered in this context:

- limiting data categories - applying a strict necessity test for the data categories that are indispensable for retention. A "peeling off" approach by singling out data categories not even potentially relevant for the purposes of fighting crime could be envisaged. Only those data categories that are absolutely and objectively necessary to safeguard public security would be retained. It would be important to establish and demonstrate this link. The necessity test would **not** focus on groups of persons or specific geographical areas within the territory of a Member State, to avoid possible discriminatory treatment implications. This would allow to restrict retention while corresponding to the law enforcement needs. As a basis for this assessment a matrix should be developed with different categories of metadata for which retention from a technical point of view is possible. The matrix should contain the main categories of data (e.g. content data, traffic data, location data, subscribers' data) and multi-level sub-categories. The latter differentiation should not only take into account legal and operational requirements, but should ensure that one sub-category contains solely data which can, from a technical perspective, be retained in their entirety. The objective would be to arrive at a matrix of "retainable" categories of data relevant for criminal investigations, while excluding all categories that are dispensable. The date delimitation should be future proof to allow for taking into account future technological developments.

- renewable retention warrants to providers operating in the territory of the MS on the basis of a strict necessity test carried out with regard to the various types of providers offering services based on their size and the type of service they offer (it may not be necessary to include all providers, as some have very specialized services) and regular threat assessments in individual MSs ;this measure could ensure that the link between the data retained and the purpose pursued is established and adjusted to the specific circumstances in each individual MS. It would therefore be possible that the retention warrants to providers would mandate retention of different types of data in the given period subject to the threat assessment.

- personal scope - it could be considered to exclude from the scope of application of the retention warrants certain categories of persons, e.g. persons subject to professional secrecy, based on an opt-out notification from the persons concerned; however, it might not be feasible to make these exemptions at the level of retention. In this case, exemptions could be foreseen at the access level. Furthermore the feasibility of excluding certain (categories of) service providers from the scope of the retention warrant could also be considered, taking into account the specific situation in the MSs.

- limited storage period - the prescribed storage period should not exceed what is strictly necessary for the purposes of prevention and prosecution of crime; to respond further to the requirement of the proportionality principle, a differentiation of the retention period across the different categories of data taking into account the sensitivity of the data concerned could be considered; irreversible erasure of the data at the end of the retention period should be prescribed unless the data is kept for business purposes.

- storage on the territory of the Union and in encrypted fashion/pseudonymisation - the ECJ requires "imposing minimum safeguards, so that the persons whose data has been retained have sufficient guarantees of the effective protection of their personal data against the risk of misuse[4]". Therefore, mandating requirements for data security, e.g. storing the data in the EU[5] could be considered. The impact on the various business models would have to be considered, as well as the possibility to pursue broader application of certain privacy- by- design solutions, such as, for example, homomorphic encryption, which allows encrypted searches with decryption possible only on the basis of a warrant. Another option to explore would be pseudonymisation, a method where names are replaced by an alias so that data is no longer connected to a name. In contrast to anonymisation, it is possible to re-identify the data with the name of the person. Review by an independent authority of compliance with the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data must be also ensured[6].

[4] Cf. tele 2, para 109.
[5] Cf. Tele 2 - para 122.
[6] Cf. Tele 2 - para 123.

Level 2 interference: Targeted access to retained data

The Court's criteria for access and use of stored data are clearly outlined in Digital Rights and Tele 2 cases. In this respect the following elements could be considered:

- restricting access solely for the purpose of fighting terrorism, and other forms of organised and serious crime, including cyber attacks;

- it could be also considered whether access could be granted for other crimes, insofar as there is a life threatening or urgent situation in a particular case , or if it may seriously impact on the physical or psychological integrity of the victim (e.g. online stalking or harassment), or in cases of missing persons;

- prescribing clear and precise rules indicating in what circumstances and under which conditions competent national authorities may be granted access to the data, including substantive and procedural conditions to that effect;

- "[…] access can, as a general rule, be granted […] only to the data of individuals suspected of planning, committing or having committed a serious crime or being implicated in one way or another in such crime. […] However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities. [7]"

- access should be made subject to prior review by a court or an independent administrative authority (exception in cases of urgency);

- exemptions for access could be considered for groups protected by the principle of professional secrecy (see also above under level 1 interference);

- notification to the person concerned, provided the interests of the investigations can no longer be jeopardised.

---

[7] Cf. Tele 2 - para 119.