Council of the European Union

Brussels, 7 November 2017
(OR. en)

14068/17

LIMITE

JAI 1012
COPEN 334
DAPIX 358
ENFOPOL 512
CYBER 172
EUROJUST 171
TELECOM 270
COSI 265

NOTE

From:	Presidency
To:	CATS
No. prev. doc.:	13845/17
Subject:	Data retention = preparation of Council debate

I. State of play

The common reflection process on issues related to data retention was launched under the Maltese Presidency[1] to assist Member States in analysing the requirements of the ECJ case -law and explore possible options for ensuring the availability of data for the purposes of prevention and prosecution of crime, while taking a multidisciplinary approach to that end.

At the informal meeting of Justice and Home Affairs Ministers in Tallinn on 6-7 July 2017, Ministers tasked the DAPIX - Friends of Presidency on Data Retention to examine any legislative and non-legislative options, including in the context of the proposed e-Privacy Regulation and to assess the feasibility of these options with a view to addressing issues arising from the recent ECJ case law on data retention.

[1] As confirmed by CATS on 8 March 2017 (doc. 6713/17).

The Estonian Presidency actively pursued work in this context. The group held 4 meetings to exchange views on the main options and related elements identified in the course of the common reflection process. 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 the outcome of discussions thus far, the Presidency considers that 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 prevent 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 scope of the data retention framework 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) Setting out strong safeguards for access to retained data based on strict necessity and proportionality test, including further analysis of the elements identified by the EU CTC and Europol.

Regarding the issues related to the availability of data in the context of the draft e-Privacy Regulation, the WP TELE has been invited to further reflect on the issues discussed at the joint meeting on October 16. The Presidency will thereafter assess the next steps in that context.

A number of specific elements on which further work should be carried out were identified by delegations with a view to restricting the data retention framework and ensuring strict safeguards for accessing and use of the data stored. The input of delegations at the last meeting of DAPIX - FoP on 6 November 2017 is also taken into account.

With a view to preparing the debate of the Council in December, CATS is invited to present their views on the elements outlined below. The objective of the Presidency is to streamline further the specific elements on which work should continue at expert level subject to the outcome of the Council debate.

II. Specific elements

The concept of restricted data retention and targeted access, as presented by the EU CTC and Europol[2] 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 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.

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.

[2] WK 9374/17 (p. 28-34), WK 9699/2017.

– The Charter "does not prevent"[3] 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.

– The measure has to be limited to what is 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[4].

– 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[5].

– 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 data retention framework should 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.

---

3 Cf. Tele 2, para. 108.
4 Cf. Tele 2, para 106.
5 Cf. Tele 2, para 110 and most recently PNR Canada, para 191.

– 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.

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 "peeling off", so that data which is not strictly essential and objectively necessary for the purposes of the prevention and prosecution of crime and safeguarding public security is not included in the data retention framework. It would be important to establish and demonstrate this link. In principle, the necessity test would **not** focus on groups of persons or specific geographical areas within the territory of a Member State. The latter is without prejudice to operational practices in the Member States regarding the supervision of groups of persons or locations in the context of criminal proceedings in line with national law.

As a basis for this approach a matrix should be developed with different categories of data 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 objective would be to arrive at a matrix of "retainable" categories of data relevant for criminal investigations, while excluding all categories that are not absolutely essential.

It is recalled that as referred at the Council in June, there is a common understanding of delegations that basic subscriber information, in particular an IP address attributed to an user does not fall within the scope of the Tele 2 Judgment[6]. Furthermore, the data delimitation should be future proof to allow for taking into account technological developments.

Europol is encouraged to facilitate preparatory works for such a data matrix at technical level in close cooperation with experts from the Member States with a view to further examination in DAPIX -FoP.

– **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; however, it does not seem feasible to make these exemptions at the level of retention. In this case, exemptions could be foreseen at the access level.

– **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).

[6] 9802/17.

– **ensuring the security of the data stored** - 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[7]". Therefore, mandating requirements for data security, e.g. storing the data in the EU[8] could be considered. The impact on the various business models should 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 or searchable encryption. 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[9].

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 for the purpose of fighting only certain categories of crime, e.g. serious crime (in terms of the penalty threshold envisaged at national level), or ;

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, or cyber- enabled crimes;

– 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;

---

7 Cf. tele 2, para 109.
8 Cf. Tele 2 - para 122.
9 Cf. Tele 2 - para 123.

– "[…] 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. [10]"

– 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.

_____

[10] Cf. Tele 2 - para 119.