Council of the European Union

Brussels, 23 November 2018
(OR. en)

14319/18

LIMITE

COPEN 394
CYBER 277
DAPIX 349
ENFOPOL 561

NOTE

From:	Presidency
To:	Committee of Permanent Representatives / Council
No. prev. doc.:	13826/18
Subject:	Data retention - State of play

I. Introduction

A common reflection process on data retention for the purposes of prevention and prosecution of crime in the light of ECJ judgements in the *Digital Rights Ireland*[1] and *Tele 2*[2] cases was launched under the MT Presidency and was continued by the EE and the BG Presidencies.

The December 2017 Justice and Home Affairs Council decided to focus on three main elements for the future work: ensuring availability of data (coherence with the draft e-Privacy Regulation); setting access safeguards; and restricting the scope of the data retention framework in view of the recent jurisprudence[3].

1 C-293/12
2 C-203/15
3 14480/1/17.

As far as coherence with the draft e-Privacy Regulation is concerned, the reform of the e-Privacy framework is relevant in the context of the data retention debate. To this end, DAPIX FoP Data retention held joint sessions with the Working Party TELECOM on 12 February and 17 May 2018. In this regard, the need to maintain flexibility within the new e-Privacy Regulation has been recognised as a crucial element in order to allow future developments either through the case-law of the ECJ, or through legislative reforms at national or European level.

To further substantiate the concept of restricted data retention (first level of interference) certain issues such as limiting the data categories, limiting the data retention periods, storage in the territory of the Union and storage in an encrypted fashion/pseudonymisation were specified in the report to the Council for further exploration. Concerning the concept of targeted access to retained data (second level of interference), various suggestions for substantive and procedural legal requirements were made. As a preliminary observation, it is the common understanding of the Member States that the findings of the ECJ in *Digital Rights Ireland* and *Tele 2* do not apply to subscriber data, but only to traffic and location data.

The BG Presidency started discussions in the DAPIX FoP Data retention working group on interference level 1 (**restricted data retention**). On 18 April Europol reported on the findings from the data matrix workshop and delegations discussed the possible follow-up. They also explored the concept of renewable retention warrants. On 17 May discussions on the data retentions periods were started, which were continued under the AT Presidency on 10 July. With this, the examination of the elements on interference level 1 were completed. On 11 September, the working group examined the substantive and procedural legal requirements which completed the discussions on interference level 2 (**targeted access to retained data**).

In this document, the AT Presidency provides a state of play of the discussions in DAPIX FoP Data retention, including the written contributions, on interference levels 1 and 2, alongside the most relevant passages from the jurisprudence of the ECJ in *Digital Rights Ireland* and *Tele 2*. On 21 November, CATS examined this state of play with a view to preparing discussions in the Committee of Permanent Representatives on 28 November and the JHA Council on 6/7 December.

II. Level 1 interference: restricted data retention

In *Tele 2* the ECJ states:

"(…) Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, 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****.*[4] *"*

The following paragraphs look at different options for restricted data retention (interference level 1):

1. Limiting data categories – works on a "data matrix" coordinated by Europol

The concept of **limiting data categories** seeks to explore whether data~~,~~ which is not strictly or objectively necessary for the purposes of the prevention and prosecution of crime and safeguarding public security~~,~~ can *a priori* be excluded from a data retention framework. As a means to limit data categories, work~~s~~ on a "data matrix" was undertaken. To this end, Europol was encouraged by the Council to facilitate preparatory work~~s~~ 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[5]. Two workshops with national cybercrime experts and investigators took place at Europol headquarters in The Hague**,** in March and May 2018.

4 *Tele 2*, para 108.
5 14480/1/17 REV 1.

An important finding of the workshops was that the relevant ETSI-standards, which serve as a basis for the discussions, have already "filtered" the data sets that are technically available. This means that data categories, which are not deemed necessary for the investigation and prosecution of crime, have already been excluded from the list beforehand. As a result, the experts considered that only very few additional data categories could be excluded from the list as not being necessary for the investigation and prosecution of crime. This is also due to the fact that different crime investigations and investigative techniques require different data categories to be used across Member States. These findings, among others, were summed up by Europol in two documents and presented to the DAPIX FoP Data retention group[6].

Therefore, as far as the issue of limiting data categories is concerned, it can be concluded that it would be very difficult, if not impossible, to further exclude a significant number of data categories from storage in advance. The reason for this is that the relevant ETSI standards have already "filtered" the broader data sets that are technically available, because they have been specifically developed for law enforcement purposes. A further reduction of categories of retained data would therefore be detrimental to the effectiveness of law enforcement investigations. Furthermore, different crime investigations and investigative techniques in the Member States require different data categories. As those data categories which are not necessary for law enforcement purposes are already excluded, there is no general and indiscriminate retention of data as referred to in the *Tele 2* judgment of the ECJ.

6 For further details see documents: WK 4507/2018 INIT (Outcome 1. Workshop), WK 5900/2018 INIT (Outcome 2. Workshop).

2. Renewable retention warrants (RRW)

In working paper WK 3974/2018 INIT the BG Presidency presented the concept of renewable retention warrants (RRW). Although the ECJ had not raised this issue in its rulings, it was considered worthwhile to explore this concept. For the purpose of the discussion a RRW was defined as a

"warrant issued by a competent national authority addressed to (an) electronic service provider(s) (ESPs) operating in the territory of a Member State requesting the provider to retain (certain categories of) data which is valid for a specific period of time during which it can be renewed if it fulfils the specific conditions prescribed by national law for its renewal, including that its proportionality and necessity are justified by a prior and confirmed by a subsequent threat assessment."[7]

Hence, a RRW would limit the amount of data retained because of its fixed period of validity, its limitation to certain ESPs (e.g. by not including minor ESPs) and/or the possibility to limit the scope of the RRW to certain data categories only. Moreover, the requirement for the RRW to be authorised by a member of the judiciary, the need for renewal of the RRW after the expiry of the validity period and/or other procedural safeguards would ensure a regular review of the measure.

However, in the discussion in the DAPIX FoP Data retention meeting on 18 April 2018, the vast majority of Member States expressed reluctance about accepting the idea of RRWs to limit the amount of data retained[8]. Only one Member State, which uses a similar system, expressed support for the idea. The main arguments of the Member States opposing the RRWs were that in their national contexts the approach would be too complex and inefficient and that it would not at all fit into their national criminal law systems, in particular their laws on criminal procedure.

Given the reluctant view of most Member States towards RRWs and the fact that the concept was not brought up by the ECJ anyway, further exploration does not seem appropriate.

7 WK 3974/2018 INIT, page 1.

8 Reluctance towards the concept had also already been expressed **at**~~in~~ the meeting on 6 November 2017, when the concept of RRW was, alongside many other suggestions for future work, brought up by the EE Presidency in doc. 13845/17.

3. Limited storage periods

3.1 Length of the retention period

At the meeting on 17 May 2018, the BG Presidency asked delegations to give information about the length of the retention periods in their Member States. While the periods ranged from a few weeks to three years, in the majority of Member States (where there is a data retention regime in place) the retention period is either six or 12 months.

At the meeting on 10 July 2018, the AT Presidency asked those Member States where the national data retention regime had been challenged before the Constitutional Court or another court of last instance to give information about the rulings with special regard to the retention periods. It was found that in all but one Member State that commented on this issue, and irrespective of whether the data retention regime was upheld or declared invalid by the relevant national court, the length of the retention periods was not a central issue in the courts' considerations or even an issue at all. Only in one Member State, following the proceedings before the national Constitutional Court, was the retention period reduced from 12 to six months, while in another Member State the retention period was reduced following a suggestion by its national constitutional committee.

The considerations of the ECJ in *Tele 2* concerning the length of the retention periods are limited to the statement that the retention period adopted has to be limited to what is strictly necessary[9]. Several Member States emphasised that in their view a retention period of at least 12 months would be absolutely necessary for the purpose of effective law enforcement.

Therefore, it can be concluded that the length of the retention period seems to be a less critical issue in the context of the jurisprudence of the ECJ, although it is of key importance that data are available for law enforcement purposes for an appropriate period of time.

9 *Tele 2*, para 108.

3.2. Differentiation between data categories on retention level

At the meeting on 10 July 2018, the AT Presidency asked delegations whether in their national system different retention periods would apply to different data categories. In response, the majority of Member States indicated that they did not differentiate between different data categories at the retention level, while only a few Member States answered that their national legislation provided for ~~a~~ differentiation, or would provide for a differentiation in the future. The ECJ does not provide an explicit statement about different retention periods for different kinds of data categories, but only mentions the possibility to differentiate between different categories of data[10]. It does not necessarily follow, therefore, that the differentiation has to relate to ~~a~~ different lengths of time periods for different data categories.

Another option than differentiating between data categories at the retention level would be to have different periods at the access level (see below).

3.3. Erasure of data at the end of the retention period

In *Digital Rights Ireland* the ECJ criticizes that "*Directive 2006/24 [data retention directive, declared invalid with Digital Rights Ireland judgement] does not ensure the irreversible destruction of the data at the end of the data retention period*."[11] Therefore, a concrete rule on the erasure of data at the end of the retention period seems to be necessary in a data retention regime.

At the meeting on 10 July 2018 all Member States participating in the discussion outlined that they do have **specific rules for the erasure (or in some case pseudonymisation) of data at the end of the retention period**. In addition, a number of Member States reported that storage of the data after the expiry of the obligatory retention period in their national legislation is lawful if it is necessary for the providers' business purposes. Law enforcement authorities can access such data as long as the respective rules of criminal procedure are complied with.

10 See footnote 2 (*Tele 2*, para 108).
11 See also *Tele 2*, para 122.

4. Requirements for data security – storage in the territory of the Union and storage in encrypted fashion/pseudonymisation

4.1. Data storage in the territory of the European Union

In *Tele 2* the ECJ states that

"[g]iven the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures. ***In particular, the national legislation must make provision for the data to be retained within the European Union*** *and for the irreversible destruction of the data at the end of the data retention period.*[12] *"*

At the meeting on 10 July 2018 (Working paper WK 7875/2018 INIT) the AT Presidency asked the Member States whether their national data retention systems provided for mandatory data storage in the territory of the European Union. Of those Member States who contributed to the discussion, a slight majority of delegations reported that storage within the EU (or EEA in one case) was compulsory. In half of these cases, data even has to be stored within the Member State itself. Among the Member States without a legal obligation to store data within the EU, some expressed their concerns about such an obligation, as it might lead to a different treatment of domestic and foreign providers.

Hence, Member States' positions and national data retention systems concerning the mandatory storage of retained data within the EU vary.

4.2. Data storage in encrypted fashion/pseudonymisation

The suggestion to store retained data in encrypted fashion or to protect them through pseudonymisation does not stem from *Digital Rights Ireland* or *Tele 2* directly, but was one of the suggestions for discussion put forward by the EE Presidency, to fulfil the ECJ's requirement to provide minimum security safeguards[13].

12 *Tele 2,* para 122.
13 See WK 13845/17, page 6.

In the discussions on 10 July 2018 only a very small number of Member States stated that they had experience with data security measures such as storage in an encrypted fashion or pseudonymisation. The majority of Member States contributing to the discussion explained that their national legislation did not provide for detailed or descriptive security measures. Some of them added they had a critical view of such measures, while others mentioned that they had already evaluated measures such as encryption or pseudonymisation of stored data or were currently in the process of evaluation.

Furthermore, when answering a more general question about technical measures to protect data, most Member States stated that their national laws on data retention did not contain specific rules about the safe storage of data, but that general rules were applied; some Member States leave it to the discretion of providers to put adequate data security measures in place. Only a small number of Member States indicated that there are specific requirements in their laws and/or technical regulations concerning the safe storage of data in their national data retention system.

The issue of data security is, in general, a current and important topic for Member States. At the same time, taking into consideration the view of many Member States and the fact that the ECJ does not explicitly mention data storage in an encrypted fashion or pseudonymisation[14] (as specific requirement, data storage in encrypted fashion/pseudonymisation does not seem to be an issue of first priority when exploring specific requirements for a data retention regime.

4.3. Review of safeguards against misuse of the data by an independent authority

The need for review of compliance with data protection safeguards by an independent authority is explicitly mentioned by the ECJ in *Tele 2*[15].

14 The ECJ only refers to security measures in general terms as an indispensable requirement for a future data retention regime, *Tele 2*, para 122.

15 *Tele 2*, para 123.

In the discussion on 10 July 2018 all participating Member States stated that a national authority had the power to review the safeguards of the providers in relation to data retention. Some Member States explicitly supported the statement that such a review of safeguards by an independent authority could be used as an argument to defend national legislation on data retention. **A data retention regime in accordance with Union law should therefore contain a provision for review of compliance with safeguards by a national independent authority.**

III. Level II Interference: Access Level

In *Digital Rights Ireland*, the ECJ states as follows:

„.. not only is there a general absence of limits in Directive 2006/24 but Directive 2006/24 also fails to ***lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that****, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter,* ***may be considered to be sufficiently serious to justify such an interference****. On the contrary, Directive 2006/24 simply refers, in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law."*[16]

However, specific answers to the question whether any distinction has to be made between the different categories of data were not given by the ECJ.

1. Differentiation between data categories at access level

Opinions about the technical feasibility of differentiation at the access level and its value to fulfil the requirements of the ECJ for a data retention regime were manifold. Some Member States were in favour of different access periods and deemed them to be technically feasible, while other Member States opposed this idea for a variety of reasons. In particular, making a distinction between the different categories at the access level was considered to be too costly and technically complex.

16 *Digital Rights Ireland*, para 60.

2. Substantive legal requirements for access to retained data

The discussion looked at different aspects, elements and options concerning **the substantive legal requirements** for access to and use of retained data. One of the main issues raised by the ECJ in the *Digital Rights Ireland and Tele2* judgements was the lack of objective rules and criteria, determining the crimes in respect of which data can be accessed and subsequently used for the purpose of prevention, investigation, detection or prosecution of crimes.[17]

In the course of the general discussion, Member States clearly emphasised the distinction between crime types, as well as their seriousness, as major aspects.

2.1. Serious Crime-/-Organised Crime-/-Terrorism

In *Digital Rights Ireland*, the ECJ states that the fight against "serious crime" is an objective of general interest, which would, in theory, be able to justify data retention measures. However, the objective general interest of **fighting serious crime alone cannot justify a general and indiscriminate data retention regime**[18], especially if the Directive only refers to the indefinite term of "serious crime, as defined by each Member State in its national law".[19]

In *Tele 2,* the ECJ refers to this reasoning and goes one step further stating that only the fight against serious crime can justify a measure like the contested national data retention regimes.

Regarding **organised crime** and **terrorism**, **the contributing Member States stated that these crime types are considered unambiguously (but not exclusively) serious and that therefore access to retained data is considered necessary**.

17 See above, *Digital Rights Ireland*, para 60.
18 *Digital Rights Ireland*, para 60.
19 Art. 1 (1) Directive 2006/24.

In addition, the discussion amongst Member States showed that Member States have specific legislation in place in their national laws determining the substantive conditions under which access to retained data is possible. For instance, some Member States have laid down a catalogue of crimes allowing access to retained data, while others define the threshold by a certain minimum punishment or require that pre-trial detention may be imposed for the respective crime. So, while Member States agreed that access to retained data should not only be possible in cases of organised crime and terrorism, but also for the investigation and prosecution of all other forms of serious crime, Member States must be competent for defining what constitutes a serious crime.

In addition, several Member States put emphasis on the fact, that the **decision on whether access to retained data is granted has to be examined by a judicial or administrative independent authority on a case-by--case basis, taking into account considerations of proportionality and necessity in every individual case. Therefore, Member States need to have discretion when defining in their respective national (criminal) laws which crimes are to be considered "serious crimes" that justify access to retained data.**

2.2 Cybercrime and (other) crimes committed online

The positions expressed by the Member States were manifold. Some Member States explicitly cover cybercrime as a crime type which allows access to retained data, while others differentiate between serious and non-serious offences. Three further issues were brought up by some Member States: the general public considers some crimes committed online (e.g. online stalking, online harassment, online fraud) as presenting a severe danger due to the harm they cause regardless of the fact that these crimes do not necessarily fit into the pattern of "serious crime" due to their low maximum sentence. In addition, some forms of cybercrime (e.g. cyberattacks on critical infrastructure) pose severe threats to society as a whole. Member States also pointed to the fact that without access to retained data, criminal investigations in cybercrime cases would – more often than in other criminal cases – turn out to be futile because digital evidence would be unavailable.

2.3 "Search & Rescue"

Access to retained data for the purpose of searching for missing or abducted persons has not been specifically addressed in the ECJ rulings. Discussion amongst the Member States lead to the conclusion that often such cases do not **fall within the scope of criminal proceedings** but within other (public security) duties of the police or are conducted by other competent authorities (e.g. intelligence services). Hence, access to retained data in such cases was deemed to be **outside the scope of the ECJ rulings**.

3. Procedural legal requirements for access to retained data

The ECJ criticised in both rulings, *Digital Rights Ireland* and *Tele 2*, the lack of rules regulating the procedural criteria under which retained traffic and location data can be accessed.

The legal requirement set out by the ECJ was a call for the Member States to "*lay down clear and precise rules governing the scope and application of such a data retention measure and imposing minimum safeguards*" in order to give "*sufficient guarantees of the effective protection […] against the risk of misuse*."[20]

3.1 Review by a judicial or by an independent administrative authority including emergency cases

According to the ECJ, *"[…] it is essential that access of the competent national authorities to retained data should […] be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision […] should be made following a reasoned request […]*."[21]

Hence, one safeguard emphasised by the ECJ is the **prior review carried out by a judicial or an independent administrative authority**.

20 *Tele 2*, para. 109.

21 *Tele2,* para 120 (by analogy, in relation to Directive 2006/24, the Digital Rights Ireland judgement, para 62).

The vast majority of the Member States described their judicial review regimes as in line with the prerequisites set out by the ECJ, through a prior review by a court/judge, an independent administrative authority or the prosecution office. Special conditions apply for emergency cases, where the legal framework can provide for exceptions to the general rule of prior review, e.g. by providing for a notification system or an *ex post* approval in emergency cases. Only one Member State applies a general *ex post* review by a court.

During the discussions, many Member States highlighted a distinction between the different data categories when it comes to prior review regimes. **Subscriber data is considered not to be subject to prior review mechanisms, whereas access to retained traffic and location data in the context of criminal investigations are commonly considered to require a prior review by a court/judge or independent administrative authority, except in validly established cases of urgency.** This correlates with the fact that the scope of the ECJ's judgements in *Digital Rights Ireland* as well as *Tele 2,* only extends to traffic and location data and does not cover subscriber data (see also the Introduction above*)*.

3.2 Installation of a legal protection commissioner

It was further explored whether an independent legal protection commissioner could be appointed as an additional safeguard for the protection of individuals' fundamental rights.

However, during the discussion, Member States clearly stated their reluctance to introduce such an additional body. **In all, the usual review mechanisms in criminal proceedings on an administrative level or on a judicial level by the public prosecutor, the investigative judge or during the trial by the trial judge were deemed to ~~be~~ sufficiently guarantee~~ing~~ the protection of individuals' (fundamental) rights.**

3.3 Special rules for access to retained data of certain groups of persons

3.3.1 Exemptions for persons subject to professional secrecy

In *Digital Rights Ireland*, the ECJ stated that *"[..Directive 2006/24..] does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy."*[22]

Lawyers, doctors, journalists, members of the judiciary and members of parliament were mentioned exemplarily as possible individuals subject to professional secrecy or privilege. In the discussion on 11 September 2018, the questions of whether there should be exemptions to these individuals and, if so, how to define these exemptions were explored.

Several Member States do have exemptions for persons subject to professional secrecy, and some stated that they considered such exemptions to be in line with the settled ECJ case law, even though their respective legal regimes did not yet provide for such exemptions. One Member State mentioned that there are additional safeguards for certain groups of people, requiring particular care and additional considerations in light of those groups' obligation of professional secrecy.

However, some Member States raised concerns that such restriction would not be feasible from a practical perspective, as the fact that a certain person is a member of a certain group of professionals would often not be known at the point in time when access to retained data was obtained, especially at the beginning of an investigation. If the person's identity was revealed only at a later stage of the proceedings, the accessed data could be considered unlawfully obtained evidence and would be eliminated from the file. Furthermore, concerns were raised that such exemptions for certain groups of professionals would run counter to the objectives of efficient criminal prosecution as these persons could be the subject of an investigation too.

3.3.2 Access to data of persons who are not suspects or accused persons

In order to investigate and prosecute crime, there might not only be a need to access retained data of suspects or accused persons, but also to access retained data of victims, witnesses or persons remotely connected to a crime.

22 *Digital Rights Ireland*, para. 58.

The ECJ states in this context, that it sees the necessity of a threshold as follows: *"[I]n 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."*[23]

Member States were invited to discuss possibilities to access retained data of persons who are not suspects or accused persons.

The main concerns raised by several Member States related to the fact that often proceedings are commenced not against certain individuals, but against (at least in the beginning) unknown perpetrators. Therefore, an *ex ante* exclusion of individuals subject to data access would hinder or even harm effective investigation.

Hence, **most Member States are not in favour of limitations with regard to accessing data of persons other than suspects or accused persons as long as there is a connection to the investigations/criminal proceedings**.

3.4 Notifications of the persons affected and legal remedies

The AT Presidency also invited the Member States to discuss the necessity of notifying persons affected by access to their retained data as well as to the requirements of an *ex-post* review of the decision authorising the access.

In *Tele 2*, the ECJ states that it is necessary to install rules for a notification as well as to pave the way for a judicial review as follows: "*That notification is, in fact, necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy*."[24]

23 *Tele 2*, para. 119.
24 *Tele 2*, para. 121.

As a preliminary issue, the question of a definition of "affected persons" was raised and lead to various answers. Accused persons or suspects were unanimously considered to fit in this category. According to some Member States, persons connected to the suspect/accused or all persons who participated in the communication concerned by the relevant traffic data might fall within the category as well. Other Member States draw the line between victims, witnesses, suspects/accused persons, on the one hand, and, on the other hand, third parties who despite the fact that they might appear in some investigatory measure, nonetheless do not fall within the scope of the term "affected" (e.g. cell phone tower inquiries).

In a second step, the AT Presidency invited Member States to discuss the necessity of notifying affected persons that their data have been accessed. Discussions showed a wide range of options: several Member States (only) notify the suspect or the accused person, some apply a more general approach, others consider this an issue of the parties' right to access the criminal file and still others do not actively notify persons of access to retained data. Furthermore, several Member States stated the need for exceptions to notification obligations, e.g. when the identity of a person whose data is concerned cannot be determined without further investigations or for cases when the notification of the affected person is detrimental to ongoing investigations. Also, it was argued that in the latter case it should be possible to postpone notifications to a later date.

Regarding the right to a **legal remedy**, only a few Member States already grant a remedy during preliminary proceedings; most Member States give appeal rights to accused persons only during the trial phase. A few Member States additionally grant affected persons under certain conditions a right to request information on whether they have been affected by access to retained data during criminal proceedings or not and if so, additional legal remedies against such access. One Member State mentioned that individuals (not limited to affected persons) may bring a claim for legal remedy whether or not they have been notified, if they have reasonable cause.

IV. Conclusion

The Presidency invites the Committee of Permanent Representatives and Council to take note of the-State of play of the discussions in the DAPIX FoP Data retention working group set out above and to share ideas about the way forward.