Council of the European Union
General Secretariat

Brussels, 10 June 2021

WK 7294/2021 INIT

LIMITE

COPEN
CYBER
ENFOPOL
JAI
DATAPROTECT

WORKING PAPER

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

NOTE

From:	Commission
To:	Delegations
Subject:	Non-paper on the way forward on data retention – Presentation by the Commission and exchange of views

Delegations will find in the Annex a Non-paper from the Commission on the above mentioned subject.

Data retention – Commission services non-paper

Contribution to the Council COPEN Working Party meeting of 16 June 2021

This non-paper has not been adopted or endorsed by the European Commission. Any views expressed are the preliminary views of the Commission services and may not in any circumstances be regarded as stating an official position of the Commission.

1. Introduction

The laws of a majority of Member States provide for the retention and use of electronic communications metadata for the protection of national and public security and the fight against crime. At the same time, where such measures include indiscriminate and generalised data retention, they have raised important questions on interference with fundamental rights, including the rights to privacy and protection of personal data.

In its recent judgements[1], the Court of Justice of the European Union (CJEU) confirmed its previous jurisprudence[2] that electronic communications data are confidential and that, in principle, traffic and location data cannot be retained in a general and indiscriminate manner. At the same time, the CJEU identified certain situations where retention is permissible, based on clear and proportionate obligations laid down in law and subject to strict substantive and procedural safeguards. There are three data retention cases from Germany[3], Ireland[4] and France[5] still pending before the CJEU.

On 11 March 2021, Justice Ministers exchanged views on the retention of electronic communications (meta) data. There was broad support among Member States to explore the possibilities of new EU legislation on data retention, while some considered it necessary to have more discussions on how to ensure compliance with the various CJEU rulings before moving to the next step.

On 17 December 2020, the European Parliament adopted a resolution on the EU Security Union Strategy noting that in its October 2020 rulings, the CJEU upheld previous case law, concluding that only a targeted retention of data limited to specific persons or a specific geographical area is allowed but also specified that IP addresses assigned to the source of a communication may be subject to generalised and indiscriminate retention for the purpose of combating serious crime and serious threats to public security, subject to strict safeguards. The European Parliament adopted a resolution of 26 November 2020 on the situation of fundamental rights in the EU in 2018-2019 in which it calls on the European Commission to launch infringement procedures against Member States whose laws implementing the invalidated Data Retention Directive have not been repealed to bring them into line with the CJEU case law. In its resolution of 12 December 2018 on findings and recommendations of the Special Committee on Terrorism, the European Parliament urges the Commission to evaluate a

[1] Judgments in Case C-623/17, *Privacy International* and Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net a.o.* of 6 October 2020 and Case C-746/18 *Prokuratuur* of 2 March 2021.
[2] Judgments in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland a.o.* of 8 April 2014, Joined Cases C-203/15 and C-698/15, *Tele2 Sverige* a.o. of 21 December 2016 and Case C-207/16 *Ministerio Fiscal* of 2 October 2018.
[3] Joined Cases C-793/19 and C-794/19 - *SpaceNet a.o.*
[4] Case C-140/20 *Dwyer.*
[5] Joined cases C-339/20 and C-397/20 *VD a.o*.

legislative proposal on data retention that respects the principles of purpose limitation, proportionality and necessity, taking into account the needs of the competent authorities and the specificities of the field of counter-terrorism.

On 25 March 2021, the European Council called for "better exploiting the potential of data and digital technologies for the benefit of society, the environment and the economy, while upholding relevant data protection, privacy and other fundamental rights and ensuring the retention of data necessary for law enforcement and judicial authorities to exercise their lawful powers to combat serious crime".[6] Subsequently, in the Organised Crime Strategy of 14 April 2021,[7] the Commission announced that it would analyse and outline possible approaches and solutions, in line with the Court's judgements, which respond to law enforcement and judiciary needs in a way that is operationally useful, technically possible and legally sound, including by fully respecting fundamental rights. It would consult Member States before the end of June 2021 with a view to devising the way forward.

This non-paper follows up on that announcement. It sets out a preliminary mapping of possible legislative and non-legislative approaches on data retention in light of the CJEU case law so far. It intends to stimulate a debate on the possible contours of national or EU data retention frameworks. It does not purport to be exhaustive, definitive or final; it should simply serve as a basis to guide discussions on how to take data retention forward in a more concrete way in the coming months.

The present non-paper focuses on policy directly related to data retention only. It does not address proposed changes to other secondary law, for instance as put forward in the Council's General Approach on the proposed e-Privacy Regulation.

The five possible approaches outlined in Section 3, points 3(a) to 3(e) of this non-paper are presented in a way to reflect the structure and logic of the *La Quadrature du Net a.o*. ruling.

2. Context

In the 6 October 2020 and 2 March 2021 judgements[8], the Court, while recognising that some data retention measures are permissible under Union law, confirmed that general and indiscriminate retention and transmission of traffic and location data is in principle precluded under EU law, whether for national security, criminal law enforcement or public security purposes. However, the Court also held that specific forms of retention, subject to strict safeguards, could be compatible with EU law, notably depending on:

(i) the **purpose of the retention**: national security, including terrorism, serious crime and serious threats to public security, and crime and threats to public security in general, and

(ii) the **categories of data to be retained**: traffic data and location data, IP addresses of the source of the connection, and civil identity data.

On that basis, the following actions may be considered for discussion:

1. **No EU initiative:** Member States would address the Court rulings at national level.

[6] Statement of the Members of the European Council, SN 18/21 of 25.03.2021.
[7] EU Strategy to tackle Organised Crime 2021-2025, COM(2021) 170 of 14.04.2021.
[8] Judgments in Case C-623/17 *Privacy International* and Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others* of 6 October 2020 and Case C-746/18 *Prokuratuur of 2 March 2021*.

2. **Guidance at EU level**: The Commission could issue guidance to Member States to support alignment of national approaches with the requirements of the Court.
3. **Legislation at EU level**: The Court's guidance could form the basis for a new EU legislative proposal on data retention, which could either address specific issues only (from amongst those in section 3) or a comprehensive data retention framework (incorporating all elements in section 3 below).

3. The policy approaches in more detail

Policy approach 1: no EU initiative

The Commission would refrain from any regulatory or non-regulatory initiative on data retention. It would be for Member States to address the consequences of the judgments at national level, in line with the Charter of Fundamental Rights and the CJEU case law, in order to take into account national specificities. The Commission would nevertheless be ready to support Member States in this process, e.g., by facilitating exchanges and organising expert meetings, including with other relevant stakeholders.

Question:

Do Member States see merits or drawbacks in maintaining a national approach to data retention legislative measures?

Policy approach 2: Non-regulatory initiative on data retention

This would consist of a Commission recommendation or a guidance document (Communication). This approach would follow the same structure as in point 3 below i.e., covering the various scenarios relating to all purposes and data categories or a combination thereof. The objective would be to assist Member States in bringing their laws into conformity with the rulings.

An advantage of this approach over legislation is that it could be carried out in less time than it takes to draft, negotiate and implement legislation and provides a margin of flexibility for Member States to apply the guidance to bring their laws in line with the rulings without prejudging a possible legislative proposal in the near future. A recommendation is, however, not legally binding or enforceable.

Question: Do Member States consider this a viable way forward?

Policy approach 3: regulatory initiative on data retention

In the following section, five different avenues to translate the CJEU jurisprudence into EU rules on data retention are set out below. A possible EU legislative initiative could be either **comprehensive**, i.e. covering the retention of **all (meta)data categories** (traffic and location data, IP addresses) and of civil identity data[9] and for **all purposes** (national security, serious crime/serious public security threats, general crime/public security threats), or **limited** to **specific data categories and/or specific purposes**. A framework could thus include all five sub-points below or a combination thereof. The five possible approaches outlined below in points 3(a) to 3(e) reflect the structure and logic of the *La Quadrature*

[9] Content data would not fall within the scope of a possible legislative instrument.

du Net a.o. ruling. In considering these points, Member States may also wish to consider the following question:

Question:

Could Member States consider a 'mixed' approach of both national and EU measures? If so, what aspects should be regulated at which level (EU or national)?

Approach 3(a): generalised retention of traffic and location data for national security purposes[10]

This approach could entail legislation harmonising obligations on electronic communication service providers, which include Over-The-Top (OTT) communications services, to retain traffic and location data in a generalised and indiscriminate manner based on a decision from independent national authorities, following a risk assessment taking into account specific national circumstances. It would not regulate the way in which state authorities themselves process these data for national security purposes, which the Court recognises as being outside the scope of the e-Privacy Directive, or how Member States approach their risk-assessments. Rather, the focus would be on the involvement of the providers in processing electronic communications metadata for national security purposes and on setting out appropriate access safeguards. For instance by articulating that:

- The threat to national security must be serious, genuine and present or foreseeable as assessed by national authorities according to Member States' individual threat/risk assessment taking into account national specificities.
- Decisions must be subject to effective (prior) review, either by a court or by an independent administrative body whose decision is binding and free from external influence.
- Decisions must be limited in time to what is strictly necessary (but without harmonising the duration as this depends on the level of existing threats and periodic national threat assessments).
- Appropriate access safeguards other than prior review e.g. ex-post review and supervision by an appropriate national authority.
- Required technical safeguards applicable to both providers and authorities to prevent unauthorised access, abuse or misuse of data.

Questions:

In light of the delineation of national and EU competences, what are Member States' views on a legislative initiative that would harmonise certain criteria relating to the retention of traffic and location data and related access conditions for national security purposes, for situations that involve private actors (for storage, transmission and providing access to data to relevant competent authorities)?

[10] In para. 135 *La Quadrature du Net*, the Court described national security as: "[I]t should be noted, at the outset, that Article 4(2) TEU provides that national security remains the sole responsibility of each Member State. That responsibility corresponds to the primary interest in protecting the essential functions of the State and the fundamental interests of society and encompasses the prevention and punishment of activities capable of seriously destabilising the fundamental constitutional, political, economic or social structures of a country and, in particular, of directly threatening society, the population or the State itself, such as terrorist activities."

Disclaimer: EU legislative competence as well as the appropriate legal base on which to harmonise certain data retention measures related to the processing of metadata for national security purposes requires further legal assessment and analysis. Therefore, the suggestions made above are to be seen in that context and should not pre-empt any particular outcome.

Approach 3(b): targeted data retention of traffic and location data for serious crime and serious threats to public security (and, a fortiori, safeguarding national security)

The CJEU held that targeted retention as a preventive measure for the purposes of combating serious crime and serious threats to public security, and equally of safeguarding national security, is possible, provided that such retention 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. Targeted retention may, in particular, be achieved by limiting retention to specific categories of persons or to specific geographical areas based on objective and non-discriminatory factors.

In relation to categories of persons, the Court indicates[11] that targeted retention legislation based on objective evidence can be directed at persons whose traffic and location data are likely to reveal a link, at least an indirect one, with serious criminal offences, to contribute in one way or another to combating serious crime or to preventing a serious risk to public security or a risk to national security. The persons thus targeted may, in particular, be persons who have been identified beforehand, in the course of the applicable national procedures and on the basis of objective evidence, as posing a threat to public or national security in the Member State concerned.

Geographical targeting measures may include areas where[12] the competent national authorities consider, based on objective and non-discriminatory factors, that there exists, in one or more geographical areas, a situation characterised by a high risk of preparation for or commission of serious criminal offences. Those areas may include places with a high incidence of serious crime, places that are particularly vulnerable to the commission of serious criminal offences, such as places or infrastructure which regularly receive a very high volume of visitors, or strategic locations, such as airports, stations or tollbooth areas.

Targeted retention must also be limited in time but with the possibility to extend or renew the measures if necessary. The Court stipulates that data retained under such "targeted" retention obligations may be accessed for national security purposes but not for crimes in general.

Possible legislation could harmonise obligations on electronic communications service providers, which include OTT communications services, to retain traffic and location data with:

- a focus on geographical targeted retention.
- harmonising the access safeguards.
- providing a fixed retention period that may be modulated according to the sensitivity of the data or other criteria to be determined (based/justified on objective criteria).
- data irreversibly deleted after expiration of the period.
- data stored in the EU, and

[11] Cf. *La Quadrature du Net,* paras. 148-149.
[12] Cf. *La Quadrature du Net* para. 150.

- setting out the types of serious crimes covered e.g. based on penalty thresholds (a custodial sentence of a minimum or maximum of at least [X] number of years) and/or a list[13].

The following targeting parameters may be considered:

- *Geographical targeting*: Taking due account of Article 21 (non-discrimination) of the Charter of Fundamental Rights and based on objective and non-discriminatory factors, providing an obligation on providers[14] to retain traffic and location data for a specific and renewable period and subject to periodic risk-assessments by national authorities in a number of sensitive areas e.g., a certain radius around sensitive critical infrastructure sites, transport hubs, areas with above average crime rates or that may be a target for serious crime or are high security risk e.g. affluent neighbourhoods, places of worship, schools, cultural and sports venues, political gatherings and international summits, houses of parliament, law courts, shopping malls etc.).
- *Targeting of specific categories of persons*: Taking due account of Article 21 (non-discrimination) of the Charter of Fundamental Rights and based on objective evidence, the following parameters could be considered: (1) known organised crime groups; (2) individuals convicted of a serious crime; (3) individuals who have been subject to a lawful interception order; (4) individuals whom authorities have a reason to believe have a link to serious crime; (5) individuals on a watch list such as for terrorism or organised crime; (6) known associates of individuals in points (1) to (5).

Such an approach could be combined with an obligation on service providers to collect subscriber/identification data about all of their clients, both those with indefinite contracts as well as 'pay-as-you-go' SIM cards[15] (related to sub-point 3(e) below) or together with an obligation to retain IP addresses and, possibly, related identifiers that facilitate identification of a user (related to sub-point 3(d) below).

Questions:

What are the legal challenges for Member States and the technical challenges for providers to comply with a targeted retention obligation and how could they be overcome? Please be as specific and concrete as possible in your responses.

What is the 'objective evidence' (in the case of persons) and what are the 'objective and non-discriminatory factors' (in the case of geographical areas) or other objective criteria that Member States could consider in drawing up a targeted retention framework?

Do Member States consider there is merit in revisiting the 'data matrix' exercise initiated by Europol in 2018 to try to find ways to devise a targeted retention system that fulfils the Court's requirements?

[13] A legal technique used in other EU legislative instruments. The objective is not to harmonise the concept of serious crime.

[14] This could take the form of a direct or fixed obligation on providers for certain designated areas (airports, critical infrastructure etc.) but with the possibility to activate or trigger targeted retention on other areas based on national orders depending on current security needs (e.g. high-level summit of heads of states or large-scale conferences etc.).

[15] While providers would normally collect subscriber information for indefinite contracts, there is no equivalent obligation in all the Member States to do so for 'pay-as-you-go' SIM cards.

Do Member States consider there is merit in devising a targeted retention system by developing criteria to limit the means of communication or the number or type of electronic communications service providers subject to retention obligations (e.g. based on size, geographical coverage, number of subscribers, cross-border presence)?

Can Member States share their views of what serious threats to public security entails?

Approach 3(c): expedited retention (quick-freeze) of traffic and location data for serious crime and the safeguarding of national security

The CJEU held that competent authorities may issue an order, subject to effective judicial review, requiring electronic communications service providers to carry out, for a specified (renewable) period of time, the **expedited retention** of traffic and location data in their possession, subject to strict access safeguards. This resembles the so-called "**quick freeze**" or "**data preservation**" mechanism.

Legislation could include similar access, security and oversight conditions as for targeted retention above, including delineating serious crimes by custodial sentence or list.

Obviously, such a mechanism makes sense only if some metadata are retained in the first place by service providers, e.g. for business purposes.

Questions:

Given that a "quick freeze" provision can apply only if there is metadata available to "freeze", can Member States share any experience relating to the normal period of availability of metadata, absent a general retention obligation? Can Member States point to any ideas stemming from that experience that may be helpful in this context?

Can Member States share any experience relating to the use of expedited retention in their current legislation?

Which options do Member States see for operationalising this mechanism to meet its objective to support investigations into serious crime and protection of national security?

Approach 3(d): generalised retention of IP addresses assigned to the source of an Internet connection for serious crime and serious threats to public security

IP addresses assigned to the source of a communication can be retained as they are less sensitive than other traffic and location data, and are indispensable to investigate cybercrime, such as online child sexual abuse. Strict safeguards would apply: purpose limitation, limited retention period, strict access conditions.

Possible legislation could harmonise an obligation for electronic communication service providers, which include OTTs, to retain the IP addresses of the senders. The legislation could also set out a specific and reasonable retention period, delineate the types of serious crimes covered (e.g. based on

penalty thresholds and/or a list) and the applicable procedural and substantive access safeguards, including in cross-border cases.

This approach would provide a tool for investigators to fight cybercrime and cyber-enabled crime, including cross-border. It would provide clarity for joint cross-border investigations and prosecutions. It could also provide a path to overcome the challenges posed by CGN-NAT technology (where hundreds of users may be behind one IP address), for example by obliging communication providers to retain the so-called source port number or other technical identifiers that facilitate identification of a user.

Approach 3(d) and 3(e) could be combined as they are similar in sensitivity and approach.

Questions:

Do Member States see the benefits of this approach? Do they see any drawbacks in this approach e.g. that the IP address of the destination of a communication is not retained? Is there a lawful way to overcome this limitation?

Are there other technical identifiers that could, in line with the jurisprudence, be captured in such legislation for example time stamps and source-port numbers to allow for identification of individuals where IP addresses are shared across multiple users, as may be the case e.g. in mobile communications?

What cybercrimes are not currently covered by the notion of 'serious crime' in Member States' legislation?

Approach 3(e): generalised retention of civil identity data to fight crime and public security threats in general

Generalised and indiscriminate retention of "civil identity data" is possible.

Possible legislation could mandate the generalised retention of civil identity data. This would extend also to OTTs.

The term "data related to civil identity" is described by the Court as data that should not make it possible to get to know the date, time, duration and addressees of the communications, nor the places where they took place, or how often this happened with specific persons within a given period. Apart from "contact details of [those] users", it is not, however, specified what this term encompasses and to what extent, if any, it is different data compared with "subscriber data"[16]. In the digital environment, the notion of civil identity should cover data identifying the subscribers.

Approach 3(d) and 3(e) could be combined as they are similar in sensitivity and approach.

[16] Subscriber data normally refers to the information enabling identification of the sender of a communication (e.g. name, address, username, phone number) and can also include information such as ID number, nationality and date of birth, postal or geographic address, billing and payment data, telephone, or email, the type of service and its duration, as well as related technical data.

Questions:

Is retention of 'civil identity data' effective to fight crimes?

What specific elements should be included in this data category?

Member States are kindly requested to comment, including in writing, on the considerations and questions presented in all the above sections and to present potential alternatives and approaches. Responses need not be limited to the specific questions asked. Member States are also invited to set out other elements for discussion that may not be included here. Any submissions in writing are to be sent by 16 July 2021.