Regeringskansliet

2021-07-16

Justitiedepartementet
Police Division
[redacted]

HOME-
CYBERCRIME@ec.europa.eu
[redacted]

Written input and comments to the Commission non-paper (WK 7294/21) on data retention

General

As expressed at the Council meeting on 11 March, Sweden sees added value in a legal EU-framework on data retention. A level playing field is useful for EU law enforcement agencies for several reasons, one being that an EU-framework will make it clear what evidence may be available in other members states. A framework providing a uniform set of provisions on data retention will also be of significance for the Telcom companies operating on the internal market.

Consequently, Sweden welcomes the work under way by the Commission on data retention and its cooperation with member states. The work by the Commission should have the objective to enabling the presentation of a legislative proposal.

National security falls outside the scope of EU Law

Sweden supports the general approach on the draft Regulation on ePrivacy. The general approach clearly states that measures on national security and defence fall outside the scope of the Regulation. Therefore, Sweden does not favour the inclusion of data retention for the purposes of national security and defence within a future EU-framework on data retention.

Targeted retention may be discriminatory and appears to be blunt

Sweden sees several difficulties in targeting the retention of data to a group of persons or a geographical area. Such a retention can be circumvented by anonymisation or the use of non-targeted equipment.

For these reasons, and since it cannot beforehand be known who will commit a crime or where a crime will be committed, targeted retention appears to be a blunt instrument for fighting crime. Furthermore, targeted retention may also cast suspicions on certain categories of persons and certain geographical areas in ways that may be both discriminatory and stigmatising.

A restricted and differentiated approach complies with EU Law

The Swedish legislation on data retention that entered into force on 1 October 2019 is adapted to the requirements of the Tele2-judgment and hence the judgment in La Quadrature du Net. In comparison with the situation before the Tele2-judgment (based on Directive 2006/24), the new Swedish legislation means that only strictly necessary communications metadata must be retained. Each type of data to be retained have been carefully examined from the perspective of need, necessity, and proportionality. Sweden therefore considers that the new Swedish legislation does not prescribe a general retention, but a restricted retention.

In addition, the legislation has adapted the retention periods to what is strictly necessary and differentiates between localisation (2 months), traffic (6 months) and subscriber data (10 months).

Also on retention periods, a careful assessment from the perspective of need, necessity, and proportionality is the basis for the differentiation of the different retention periods. In other words, the Swedish legislation as of 1 October 2019 sets out a differentiated as opposed to an indiscriminate approach.

The German legal framework on data retention, now the subject-matter of cases C-793-19 and C-794/19 at the Court of Justice (ECJ), prescribes an approach that is restricted and differentiated, similar to the Swedish approach. Sweden has therefore argued in its written submission to the ECJ that the German legislation is in conformity with EU Law. Also the Commission expresses in its written submission to the ECJ that the German legal framework, as regards the retention periods and the categories of data to be retained, is within what is strictly necessary.

Furthermore, Advocate-General Campos Sanchez-Bordonas argues in case C-520/18, points 92-93, that a restricted and differentiated data retention achieves the objective to efficiently prevent and address crime without leading to unwarranted intrusions into the right to a private life and the rights to freedom of expression and information since such a retention does not make it possible to obtain a precise and detailed picture of the involved persons.

However, the ECJ does not in its judgment in C-520/18 and La Quadrature du Net explicitly or directly judge on the restricted and differentiated approach. Sweden is therefore of the view that the ECJ has left the issue open. The future judgment in the joined German cases C793/19 and C-794/19 will therefore have an important impact om how we should perceive data retention.

In conclusion, there are a series of reasons why a restricted and differentiated approach on data retention for law enforcement purposes comply with EU Law. Sweden is therefore also of the view that a restricted and differentiated approach could be the basis for an EU legal framework on data retention.

IP-addresses and civil identity

In most investigative situations regarding internet-related crime, the law enforcement agency has obtained or is in possession of an ip-address from which a suspected criminal act originates. A request for access to communications metadata is therefore usually concerned with information about the identity of the person (the subscriber) who was using an ip-address at a certain point in time, i.e. the request is not concerned with an ip-address as such, but with subscriber data, or as the ECJ calls it, information about the civil identity of a person. This investigative method is also known as ip-tracing.

It should be pointed out that a subscriber is usually using an ip-address for a limited time period. It is therefore not normally possible to map the online activities of a person solely on the basis of the assigned ip-address.

Furthermore, it seems that the ECJ in its recent judgment in case C-597/19 of 17 June 2021 explicitly has allowed ip-tracing in cases concerning infringements of intellectual property rights.
In paragraph 120, the ECJ states that identifying the holders of those IP addresses is regarded as data related to the civil identity of users of electronic communications systems access to data.

The ECJ continues in point 121: "Such data relating to the civil identity of users of electronic communications systems do not normally, in themselves, make it possible to ascertain the date, time, duration and recipients of the communications made, or the locations where those communications took place or their frequency with specific people during a given period, with the result that they do not provide, apart from the contact details of those users, such as their civil status, addresses, any information on the communications sent and, consequently, on the users' private lives. Thus, the interference entailed by a measure relating to those data cannot, in principle, be classified as serious."

Consequently, the judgment of the ECJ in La Quadrature du Net, points 152-159, should be interpreted as referring to retention and access to information about the civil identity of a person. It is paramount that the retention of and access to information about the civil identity of a person that has used an ip-address is possible in order to fight crime in general, not only serious crime. Otherwise, many crimes that are not deemed as "serious crime", such as possession of child asexual abuse material and fraud, could not be investigated and impunity would follow.

Sweden is of the view that ip-tracing as described above must remain possible in a future EU-framework on data retention. Sweden is considering to seeking clarification on this point at the oral hearing before the ECJ in cases C-793/19, 794/19 and C-740/20.

Other important issues

There are also other important issues that Sweden sees a need to address in working towards an EU-framework on data retention, namely to:

- ensuring that a suspect can be identified regardless if Carrier Grade NAT is applied or not;

- including OTT-services (number independent communication services) in an obligation to retain communications metadata.