Council of the European Union

Brussels, 11 June 2021
(OR. en)

9283/21

LIMITE

COPEN 249
JAI 645
DATAPROTECT 143
TELECOM 232
ENFOPOL 204
CYBER 163
EUROJUST 61

**NOTE**

| | |
|---|---|
| From: | Presidency |
| To: | Delegations |
| Subject: | First reading of the judgment of the Court of Justice (Grand Chamber) of 2 March 2021 in Case C-746/18 |

Delegations will find enclosed a working paper from the Presidency on the above mentionned subject.

**ANNEX**

**Working Paper**

**First reading of the judgment of the Court of Justice (Grand Chamber) of 2 March 2021 in Case C-746/18**

The judgment of the Court of Justice (Great Chamber) of 2 March 2021 in Case C-746/18, while maintaining the previous case-law as regards the access of national authorities to data related to electronic communications, brings some novelties that will be necessary to examine in depth in the future.

The Court reaffirms that Union law precludes legislative measures that provide, as a preventive measure, for the general and indiscriminate retention of traffic and location data for the prevention, investigation, detection and prosecution of criminal offences in general i.e. not limited to specific categories of serious crime (see C-746/18, point 30 and the case-law cited).

In fact, only the fight against serious crime and the prevention of serious threats against public security can justify serious interference in fundamental rights related to the right to privacy and data protection, such as those involving the retention of traffic and location data.

Thus, only objectives to combat serious crime or to prevent serious threats to public security can justify the access, by public authorities, to a set of data enabling precise conclusions to be drawn on the people's private life, such as the habits of everyday life, permanent or temporary places of residence, daily or other travel, activities carried out, social relations of these persons and social media frequented by them (see C-746/18, point 33 and the case-law cited).

However, legislative measures aimed at processing the civil identification data of users of means of electronic communication, such as their retention and access, solely for the purpose of identifying them, without such data being associated with information relating to the communications made, may be justified by the objective of prevention, investigation, detection and prosecution of criminal offenses in general.

In fact, to the extent that such data do not in themselves make it possible to know the date, time, duration and recipients of the communications made, nor the places where such communications occurred or the frequency of such communications with certain persons during a given period, and therefore do not provide any information about the communications made or their private life, the interference caused by the retention of these civil identification data cannot be classified as serious (see C-746/18, point 34 and the case-law cited).

Moreover, the Court reaffirms that it is essential that access by the national authorities be subject to prior supervision by an independent court/administrative body and that such decision should be taken following a reasoned request (see C-746/18, point 51 and the case-law cited).

The Court reaffirms that prior supervision requires that the court/entity responsible for carrying it out has the necessary powers and guarantees to ensure that the various interests in question are reconciled. In the criminal investigation, such supervision requires that the court/entity is able to ensure a fair balance between the interests linked to the needs of the investigation in the fight against crime and the fundamental rights related to the respect for private life and the protection of personal data, acting objectively and impartially (see C-746/18, point 52).

The Court holds that the requirement of independence, which the prior review imposes, implies that where that review is carried out not by a court but by an independent administrative body, that body must have a status enabling it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence. It follows that such independent authority should be a third party in relation to the authority requesting access to the data should not be involved in conducting the criminal investigation in question but rather has to enjoy a neutral position vis-a-vis the parties to criminal proceedings (see C-746/18, points 53 and 54).

The Court of Justice has therefore concluded that this is not the case of a public prosecutor's office, which conducts the investigation and exercises public action and whose task is not to decide a dispute with complete independence, but to submit it, where appropriate, to the competent court, as a party to the criminal proceedings. The fact that a public prosecutor's office is obliged, by the rules governing its powers and statute, to verify the incriminating and exculpatory elements, to ensure the legality of the investigation and to act solely in accordance with the law, is not sufficient to give it the status of third party in relation to the interests concerned.

**Issues for debate**

1. In the scope of crime investigation in general, is access to the only users' civil identification data sufficient and technically relevant for the purposes of evidence, at a time when the digital transition is driven by the pandemic? What other minimum data should fall into this category for an effective fight against crimes?

2. Given that under Union law prior supervision by a public prosecutor's office of the kind described above is not sufficient, what are the impact on the national legal systems in force? Could that lead to preventing the Public Prosecutor from authorising access to data result in a less effective investigation and slower the process?