PLEADING NOTES

EUROPEAN DATA PROTECTION SUPERVISOR

Joint hearing in cases C-793/19, C-794/19 Spacenet and C-140/20, Garda

15 minutes

Milord President, Milord the reporting judge, Miladies and Milords, and Milord Advocate-General,

The European Data Protection Supervisor thanks the Court for the invitation to attend the hearing today.

1. The first question asked by your Court concerns whether, traffic and location data should be given the same level of protection as the content of communications.

The Supervisor has always advocated for a high level of protection of traffic and location data.

In its Opinion 6/2017 on the proposal for a new 'e-privacy regulation', he has warned that the distinction between content data and metadata, of which traffic and location data are a subset, is not clear-cut, especially in the context of the Internet.

In its oral intervention before this Court in the *La Quadrature du Net* (Joined cases C-511/18 and C-520/18) and *Privacy International* cases (C-623/17), he has given practical examples of how traffic and location data, when accessed, can be equally intrusive as content of communications[1].

The Supervisor notes that the Court has clarified that legislation permitting access on a generalised basis to the content of electronic communications compromises the essence of the fundamental right to privacy, as guaranteed by Article 7 of the Charter (*Schrems I*, C-362/14, paragraph 94).

[1] Previously, the WP29 had advocated that Metadata and content be accorded the same high level of protection (Opinion 1/17, para. 18).

By way of contrast, the Court has stated in paragraph 39 of its *Digital Rights Ireland* judgment (C-293/12), that the retention of the data at stake in that case was not such as to adversely affect the essence of that right.

In very broad terms, if we were to consider general access to metadata with the potential to provide a full picture of the private life of individuals, the interference could then be considered comparable to access to content.

However, the Supervisor believes that if one looks more specifically at traffic and location data, these are different from content of communications insofar as access to traffic and location data may reveal the private life of individuals, whereas any access to content does reveal at least an aspect of the private life.

A circumstantial assessment of the categories of data at stake and on the concrete situation is always necessary.

This brings the Supervisor to answer the second question.

2. Does the requirement in Article 52(1) of the Charter that limitations may be imposed only if they are strictly necessary apply also, as is apparent from the case-law, to the retention of traffic and location data?

Of course the answer to this question can only be: yes.

Certainly the requirements of Article 52(1) of the Charter apply to the retention of traffic and location data independently and separately from any subsequent access or use of the data.

However, this does not mean that the retention of such data should be considered in a sort of 'watertight' isolation.

Retention of data at stake in the present proceedings is not an end in itself: a legislation providing for the storage of traffic and location data related to electronic communications without their access to achieve an objective of general interest would constitute an interference impossible to justify in relation to its necessity.

The crucial question is therefore the third one asked by this Court.

3. With its third question the Court asks as to scrutiny of the Court in reviewing the balance between fundamental rights and other objectives of general interest

(part a. of the question). It also asks (part b. of the question) to take a position on the approach adopted by the Court in *La Quadrature du Net*, ruling that effective action to combat criminal offences cannot justify a general and indiscriminate retention of traffic and location data, while specifying the possibilities available to Member States to provide for a retention of such data for the purpose of combating serious crime in accordance with Article 15(1) of Directive 2002/58 ('eprivacy directive'), interpreted in the light of Articles 7, 8 and 11 of the Charter.

a.

The scrutiny of the Court as such cannot be questioned if the Union has to remain a system based on the rule of law. I will move immediately to part b. of the question in which I will deal with the connected question of the intensity of the scrutiny.

b.

Can effective action to combat criminal offences justify a general and indiscriminate retention of traffic and location data? The Court, as we all know, clearly said: no (paragraph 142 of the ruling in *La Quadrature du Net*).

The question for the parties at the hearing today is to take a position on such a firm prohibition while indicating possible solutions which would remain in accordance with Article 15(1) of directive 2002/58.

To be in accordance with Article 15(1) of the e-privacy directive such a measure should:

(i) remain a genuine derogation to the principle of confidentiality - not be able by its vastness to swallow the rule; and,

(ii) the data retained should be linked, at least indirectly, to the objective pursued.

i. Let us begin with the principle that the exception cannot swallow the rule. The rule here is confidentiality.

But is confidentiality as provided for in Article 5 of the e-privacy directive critically compromised by general and indiscriminate retention of traffic and location data without that data being ever accessed?

The case-law of the Court clearly indicates that this is the case.

The Supervisor considers that at the stage where the retained data is limited to certain categories, and merely stored and not yet accessed, the retention of such data, while being an interference with the fundamental right to privacy, is not necessarily undermining the principle of confidentiality or substantially annihilating it.

The principle of confidentiality could be critically undermined if information is accessed without the required safeguards intended to ensure the necessity and proportionality of the access. The processing operation consisting of access to the data is the moment in which the interference with the fundamental right is at its highest[2].

ii. As to the existence of an objective link between the retained traffic and location data and the objective of general interest sought.

The Supervisor believes that in *La Quadrature du Net* the Court itself already gave a broad interpretation of the connection requirement. When the objective pursued by the retention of traffic and location data is safeguarding national security against a serious and genuine threat, the Court indeed stated that:

"*even if a measure is applied [...] without there being at first sight any connection [...] with a threat to the national security [...]it must nevertheless be considered that the existence of that threat is, in itself, capable of establishing that connection*". (*La Quadrature du Net*, paragraph 137).

The assessment performed by the Court in paragraph 137 demonstrates that the objective link may be established, even when the data of all users are concerned, if a sufficiently important objective is at stake.

Now, the conclusion reached by the Court to allow general and indiscriminate retention only in relation to serious and genuine threats to national security is obviously very protective for the fundamental right to private life.

[2] See para 196 and 197 *Big Brother Watch* ruling of the ECTHR quoting the 2015 report of the European Commission for democracy "In this regard, the Venice Commission considered that the main interference with privacy occurred when stored personal data were accessed and/or processed by the agencies. For this reason, the computer analysis (usually with the help of selectors) was one of the important stages for balancing personal integrity concerns against other interests."

The FRA survey page 5: people are less concerned by access by LEA than by advertisers: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-fundamental-rights-survey-data-protection-privacy_en.pdf

The Supervisor has the mandate to protect private life and the data where nowadays our privacy resides.

Nevertheless, the Supervisor believes that for the purpose of detecting and prosecuting serious crimes, the legislator would not exceed the limit of its discretion if it provided for clear and exhaustive rules allowing the secure retention of selected categories of traffic and location data for a limited period of time.

This is of course on the strict condition that all the robust safeguards for access now clearly spelled out in the Court's case law since the *Tele2Sverige* ruling remain applicable and enforceable.

In such a way the law would sufficiently defend any individual from the risks of abuse[3] of the potentially very revealing data traffic and location related to electronic communications.

I will now move to your questions concerning the interplay of your case-law with that of the European Court of Human Rights ('ECtHR').

5. and 5a. Has the case-law *Big Brother Watch* and *Centrum for Rättvisa* of the ECtHR (Grand Chamber rulings of 20 may 2021) exhaustive character in the context of the harmonisation brought about by directive 2002/58? Does the ECtHR case law coincide with this Court's case law in regard to the distinction between objectives that justify the interference?

In response to your question 5, the Supervisor considers that the relevant case-law of the European Court of Human Rights cannot be deemed as being, in principle, exhaustive for the interpretation of the rights and obligations harmonized by the e-privacy directive.

The exhaustive nature of the ECtHR case-law depends on whether, within the Union, the rights protected by the Charter corresponding to those protected by the Convention enjoy a higher level of protection.

The Supervisor considers that Article 15 of the e-Privacy Directive, as it has been interpreted by your Court, establishes a higher level of protection of the right to

[3] See paragraph 132 of *La Quadrature du Net* ruling and case-law quoted therein

respect for private life than that deriving from the rulings in *Big Brother Watch* and others and *Centrum for Rättvisa*.

Indeed, paragraphs 131, 136 and 140 of the *La Quadrature du Net* judgment establish a hierarchy between the objectives of general interest that may justify limitations to the principle of confidentiality.

However, such a hierarchy cannot be found in the case law of the ECtHR. Thus the Supervisor concludes that the ECtHR case law does not coincide with the Court's.

In reply to the last aspect of question 5a: the Supervisor believes that certain justifications that the ECtHR accepted in these judgments in relation to mass interception of traffic and location data can be transposed to the context of the fight against serious crime, and remain relevant in the more harmonised context of Union law.

We are thinking in particular about paragraph 323 of *Big Brother Watch* concerning the proliferation of threats and access to increasingly sophisticated technology through which criminals can communicate undetected.

I come to your last question 5.b concerning the application to the present cases of the requirements resulting in particular from the *Zakharov* judgment of the ECtHR.

As a preliminary point, the Supervisor calls for caution in applying requirements - such as the ones laid down in the *Zakharov* judgment - conceived for measures of a different nature if compared with the measures with which your Court has to deal with in the present case.

Indeed, the minimum guarantees resulting from the *Zakharov* judgment require that the law state the nature of the offences liable to give rise to an interception warrant and define the categories of persons liable to be wiretapped: such requirements relate to transmission of data to public authorities and their subsequent access.

However, according to your case law resulting from the *Privacy International* and *La Quadrature du Net* judgments, such measures are to be kept distinguished from measures of retention by private entities.

Furthermore, it should be noted that the European Court of Human Rights, in its *Big Brother Watch* and *Centrum for Rättvisa* judgments, adapted these criteria to take account of the general nature of an interception measure[4].

In relation to the bulk interception regimes at stake in those cases, therefore, the European Court of Human rights requires only a statement of the grounds on which a mass interception might be authorised and of the circumstances under which an individual's communications might be intercepted.

Moreover, your Court has already accepted, in paragraphs 165 and 168 of the *La Quadrature du Net* judgment that measures interfering with the rights to data protection and to privacy for the purposes of combating crime may not apply to only suspected persons, with regard to certain categories of data.

****

As a conclusion, the Supervisor wishes to reiterate that it might be possible to envisage clear and precise legislation providing for a limited but effective regime for the retention and access to traffic and location data of electronic communications, including data of users that at first sight have no objective connection with the objective pursued, in a manner compatible with the Charter.

This could be done by limiting the categories of data to be retained, the retention period, and by strengthening and enforcing strictly the guarantees concerning the access of the competent authorities to data.

The Supervisor indeed reiterates that retention and access to stored data should not be considered in watertight isolation from each other.

Thank you for your attention.

[4] Essentially those cases concerned bulk interceptions by public authorities for purposes of foreign intelligence and national security, but in case of *Big Brother Watch*, also for the prevention and detection of serious crimes (although prosecution was excluded - See paragraph 369 of *Big Brother Watch* ruling.