Joint hearing in Case C-623/17 (*Privacy International*) with Joined Cases C-511/18 and C-512/18 (*La Quadrature du Net and Others*) and Case C-520/18 (*Ordre des barreaux francophones et germanophone and Others*)

9-10 September 2019

Pleading notes of the European Data Protection Supervisor (EDPS)

Mr President, Mr Judge-Rapporteur, Ladies and Gentlemen Members of the Court, Mr Advocate-General,

Thank you for inviting the European Data Protection Supervisor today.

Allow me to start with Question 1 regarding the scope of the ePrivacy Directive 2002/58.

We agree with the Commission's view that in all four cases under consideration by the Court today, the national measures restricting the confidentiality of communications in fact impose certain obligations on service providers, be it to transmit communications data to State authorities, to retain and provide access to data, or to perform certain processing operations on the basis of pre-defined parameters.

In consequence, we submit that in all four cases the measures in question fall within the scope of the ePrivacy Directive and must therefore comply with the requirements set out in Article 15(1) of the Directive and in Articles 7 and 8 of the Charter.

We also submit that measures directly implemented by the State would fall within the scope of EU law when they give rise to a corresponding obligation for service providers to facilitate or to tolerate such measures.

This does not mean, however, that any further processing of data thus obtained by competent authorities in any of the areas referred to in Article 1(3) of the Directive, such as national security, would fall within the scope of EU law.

I would like to comment briefly on the meaning of Article 6 of the Charter. The EDPS understands that this provision is intended to protect individual liberty and security against the State, not to guarantee it through the State. I would refer to the written observations of the Commission on this point.

Mr President, I will now turn to the question that the Court has specifically addressed to the EDPS. This question is, in our view, sufficiently broad to allow us also to provide elements that are relevant to Questions 2 to 4.

The Court asks whether the IP addresses or other data relating to electronic communications are capable of providing information on the content of communications and, inter alia, on the websites consulted.

The answer to this question is “Yes”.

IP addresses and other electronic communications data are indeed capable of providing information on the content of communications and, in many cases, on the websites consulted.

Nowadays, attributing an IP address to a specific user or an internet service is made more difficult by the use of shared IP addresses, Virtual Private Networks, encryption via the HTTPS protocol, or when website publishers use Content Delivery Networks to distribute data.

However:

In some cases, an IP address is enough to identify a single, unique destination point on the internet: directly typing a static IP address into the address bar of a

web browser or querying an IP WHOIS lookup service would allow to know the visited website[1].

To give an example: the IP address 212.77.1.32 leads directly to the website of the Holy See in Vatican City[2].

Other data relating to electronic communications – so-called metadata – include: the subject line of emails; addresses of websites visited (URLs); date, time and length of online conversations; geographical location of the device; e-mail headers; telephone numbers called; location of terminal equipment[3]. They can be as revealing as the actual contents of the communication.

For example, it is easy to infer some of the content of an email message from a subject field that reads "*Test results from your annual medical check-up last Monday*".

[1] Where a web server hosts more than one website, in such case, the IP address will not enable to identify which of these websites was accessed.

[2] Another example: 18.214.9.51 corresponds to the domain grindr.com, 'the largest social networking app for gay, bi, trans and queer people'.

[3] Further examples of metadata (contained in 'Access data' and 'transactional data') are listed in Annex 1 of the Commission's Proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters (COM/2018/225 final).

We should also keep in mind that the distinction between "content" and "metadata" is not clear-cut in a multiple service environment as the Internet[4]. This is why in the context of the proposal for the ePrivacy Regulation, the EDPS advised to attribute a high level of protection to metadata, as well as to content data[5].

Furthermore, the Court asks what information concerning the private lives of the persons concerned can be obtained from IP addresses or other data relating to electronic communications.

It is important to note in this context that today, "electronic communications" are no longer limited to telephone conversations or video conferences, or website browsing. The ever-evolving technological landscape, coupled with the increasing use of devices communicating with each other, in particular over the internet, has led to a massive increase in the amount of information about individuals that flows through electronic networks.

[4] EDPS opinion 6/2017 on the ePrivacy Regulation, footnote 63: For the technological background, please refer to the OSI model https://en.wikipedia.org/wiki/OSI_model and the Internet protocol suite https://en.wikipedia.org/wiki/Internet_protocol_suite.

[5] EDPS Opinion 6/2017.

Just to mention a few examples: mobile apps, smart watches, Internet of Things devices such as Wi-Fi-enabled fridges, smart speakers or connected vehicles.

Research has shown that a person can be identified already from a very limited set of mobile phone location data[6]. It has also been demonstrated that intimate details about a person's lifestyle and beliefs, such as political leanings and associations, medical issues, sexual orientation or habits of religious worship can be discovered through mobile phone traffic data[7].

Some applications for mobile devices are so specialized that just knowing that they are used will allow to profile a person: a list of all connections to a *Netflix* server could show leisure timeframes. Another app called *Grindr* is marketed as "*the world's #1 mobile social networking app for gay, bi, trans, and queer people*".

[6] EDPS opinion 6/2017 on the ePrivacy Regulation, footnote 66: De Montjoye, Y. A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013), Unique in the Crowd: The privacy bounds of human mobility, Nature SRep, 3, available at: http://www.nature.com/articles/srep0137.

[7] EDPS opinion 6/2017 on the ePrivacy Regulation, footnote 67: New York Times Editorial Board, Surveillance: A Threat to Democracy, 11 June 2013, available at: http://www.nytimes.com/2013/06/12/opinion/surveillance-a-threat-to-democracy.html?hp

For most people, going to work from home is a repetitive location change. By accessing an individual's location during several days, permanent or temporary places of residence and working places can be identified.

To give another example, the German politician Malte Spitz decided to publish his own electronic communications data collected from August 2009 to February 2010[8]. Combined with other public information relating to his life, such as Twitter feeds, blog entries and website, these data revealed when Spitz walked down the street, when he took a train, when he was on an airplane. It showed where he was in the cities he visited. It also showed when he worked and when he slept and which beer gardens he liked to visit in his free time.

All in all, such metadata potentially reveal an entire life.

We also note that the new definition of an "electronic communication service" in Article 2(4) of the European Electronic Communication Code includes "interpersonal communications services", such as instant messaging (for example, Facebook messenger, WhatsApp) and on-line chat. Such services will fall within the scope of Directive 2002/58 from December 2020.

[8] https://www.zeit.de/datenschutz/malte-spitz-data-retention

The combined effect of those developments are exponentially growing volumes of electronic communications data which, we wish to stress, are also inherently easier to extract and process than what we traditionally consider as "content data".

Mr President,

I now turn to the question whether, and to what extent, it would be possible to limit the retention and the access to electronic communication data, without those measures being capable of providing very specific information concerning the private lives of the persons concerned, while enabling the objectives set out in Article 15(1) of Directive 2002/58 to be effectively achieved.

The EDPS considers that it might be possible to provide for a limited yet effective electronic communications data retention and access regime in a manner compatible with the Charter.

I would like to focus on two particularly important aspects:

- the need to circumscribe the categories of data to be retained; and

- the need to enhance the safeguards regarding access to the data by competent authorities.

The EDPS is of the view that the retention and access to the retained data should not be considered in isolation. As observed by the Advocate-General in his opinion in *Tele 2*, "*the* raison d'être *of a data retention obligation is to enable law enforcement authorities to access the data retained, and so the issue of the retention of data cannot be entirely separated from the issue of access to that data.*"

Indeed, mandatory retention of user and traffic data is not a stand-alone measure in its own right; instead, it aims to ensure that law enforcement can have at its disposal electronic communications data from which communicating parties or individuals' whereabouts at specific moments in time can be deduced. We therefore believe that conditions for data retention must always be considered together with conditions for subsequent access.

Regarding the categories of data

I briefly described earlier the ever-evolving technological landscape, as well as the changes in the legal framework applicable to electronic communications.

Against this backdrop, it is all the more important to clearly circumscribe which categories or types of data could be subject to a limited retention obligation, and thus may become available for access ("reduce the volume" of the data).

The EDPS considers that any data retention legislation should lay down an exhaustive list of clearly defined categories of electronic communications data. The categories of data to be retained should be clearly linked to one or several of the specific purposes listed in Article 15(1) of the ePrivacy Directive and should not go beyond what is strictly necessary to achieve each of those purposes. Limited retention periods should be specified for each of the different categories of data.

Before moving on to the safeguards required, the EDPS observes that the connection between the persons impacted by a retention measure and the objective pursued might not necessarily mean a direct implication in a criminal activity as a suspect or a person convicted of a criminal act. Indeed, data protection rules applicable in the law enforcement area explicitly acknowledge the necessity to process not only data related to suspects or persons convicted of

criminal offences, their contacts or associates, but also to victims or other parties to a criminal procedure, like witnesses or experts. This is why a number of EU instruments in this area, including the Law Enforcement Directive 2016/680, specifically require that a distinction be made between such different categories of data subjects[9].

In the specific context of retention of electronic communications data, it might not be possible to identify in advance those data subjects (or categories of data subjects) whose information may at some point in the future become part of a criminal investigation, for example as victims of serious crime.

Regarding the procedural safeguards

This Court has already ruled that, in order to ensure that access to the retained data is limited to what is strictly necessary, the national legislation has to lay down substantive and procedural conditions governing the access by the competent national authorities to the retained data.

The EDPS would like to emphasize in particular the importance of a prior authorisation by a court or by an independent administrative body as a general

[9] This principle is inspired by the Council of Europe Recommendation R (87) 15 and is also present in the Europol, Eurojust and EPPO Regulations

rule,[10] given the often very revealing nature of the data at issue. We also consider that only a limited number of competent authorities can be granted access to the retained data.

Furthermore, we would like to insist on the need to ensure meaningful oversight and *ex post* evaluation. In this respect, in addition to remedies and independent control as required under Articles 47 and 8(3) of the Charter, the following should be provided:

- effective mechanisms for *ex post* control combined with sanctions for non-compliance with the substantive and procedural requirements; and

- a periodic review of the suitability and effectiveness of the data retention and access system, based on objective and reliable information. A high degree of transparency, including about the practical implementation and outcomes, is essential for the legitimacy of any data retention scheme in a democratic society.

We believe that it is, ultimately, the responsibility of the legislator to regulate data retention and access in a comprehensive manner.

[10] Except in cases of validly established urgency (see *Tele 2*)

Mr President, Members of the Court,

I come to my conclusion.

In all four cases before the Court today, the measures in question fall within the scope of Directive 2002/58 and as a consequence must comply with the requirements set out in Article 15(1) of the Directive.

As shown, electronic communications data can provide revealing insights on a wide variety of aspects of a person's life.

Nevertheless, it might be possible to provide for a limited yet effective communications data retention and access regime in a manner compatible with the Charter. In this context, we submit that the retention and access to the retained data, including the substantive and procedural conditions, should not be considered in isolation.

It is the responsibility of the legislator to regulate data retention and access in a comprehensive manner and in particular to strengthen the safeguards for access of competent authorities to the retained data.

Such safeguards should in particular include prior authorisation by a court or an independent authority, and meaningful *ex post* controls, including sanctions for non-compliance.

I thank you for your attention.

***

EDPS' closing reply

Confidentiality of communications is essential for the functioning of a modern, democratic society.

And while the economic and social importance of trustworthy communications cannot be overstated, we would submit that the central legal function of the fundamental right to privacy (protected under Article 7 of the Charter) is the protection against any interference, especially from State authorities.

In our oral submissions we indicated several elements which should be considered when assessing the proportionality of an interference with the confidentiality of communications. I will not repeat those again.

Let me just emphasize again that the retention and access to data should not be considered in isolation.

It must be avoided that the retained data permit to reconstruct virtually all activities of the citizens.

I will end by paraphrasing what European Data Protection Authorities said over 15 years ago, when data retention was first debated at European level: not everything that is technically feasible or "might prove to be useful" for the purpose of fighting serious crime is "desirable or can be considered as a necessary measure in a democratic society"[11]. Mere convenience or cost-effectiveness is not sufficient[12].

Thank you.

Anna Buchta for the European Data Protection Supervisor

[11] Article 29 Working Party Opinion 9/2004 on a draft Framework Decision on the storage or data processed and retained for the purpose of provding electronic public communications services, WP99

[12] See also : EDPS Toolkit for assessing the necessity of measures that limit the fundamental right to the protection of personal data, 11 April 2017