EUROLEX advokatų kontora law offices

K. Kalinausko str. 24-402, 03107 Vilnius, Lithuania
Tel +370 5 212 0 719 | Fax +370 5 212 0 709
info@eurolex.lt | www.eurolex.lt

Prof. Dr. iur. Vilenas Vadapalas
Attorney at law, Partner, EUROLEX Law Firm
Former Judge of the General Court of the European Union

24 February 2022

Legal opinion

The Greens/EFA Group in the European Parliament and the Member of the European Parliament Dr. Patrick Breyer asked me to present a legal opinion on two questions:

1. Is it in line with the CJEU case-law and fundamental rights to impose a permanent/revolving retention of traffic and location data for national security purposes, referring to the permanent risk of terrorist attacks etc., the way the Conseil d'Etat and the EU Commission are proposing (rather than only when there is a specific threat and for a short period of time limited by duration of the threat), and to access this data for other purposes than national security (e.g. tackling serious crime)?

2. Do the Commission's services proposals of parameters for geographical targeting and the targeting of specific categories of persons (pp. 5 and 6 of the Working paper WK 7294/2021 INIT of 10 June 2021) comply with the CJEU case-law and fundamental rights?

THE GREENS/EFA in the European Parliament

EUROPEAN PIRATES in the European Parliament

Definitions

CJEU, Court of Justice – Court of Justice of the European Union

The Charter or the EU Charter – Charter of Fundamental Rights of the European Union

La Quadrature du Net – CJEU judgements of 6 October 2020 in case C-623/17, *Privacy International* case C-623/17, and in Joined cases C-511/18, *La Quadrature du Net and Others*, C-512/18, *French Data Network and Others* and C-520/18, *Ordre des barreaux francophones et germanophone and Others*, ECLI:EU:C:2020:791

Commissioner of the Garda Síochána and Others– CJEU judgement of 5 April 2022 in Case C-140/20

The Decision – Decision N° 393099 of the Conseil d'État of 21 April 2021

The Directive – Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector

Working paper – Commission services non-paper annexed to the document of Council WK 7294/2021 INIT of 10 June 2021

Preliminary observations

According to Article 5 (1) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (thereafter – the Directive) the Member States shall ensure the confidentiality of communications and the related traffic data and prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication (Article 6 (1)). Under Article 23 of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (thereafter - GDPR), the Union or Member State law to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in the dispositions of the GDPR when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society.

The Court of Justice in framework judgements of 6 October 2020 on data retention concerning the British, French, and Belgian rules (Case C-623/17 (*Privacy International*), and Joined Cases C-511/18 (*La Quadrature du Net and Others*), C-512/18 (*French Data Network and Others*) and C-520/18 (*Ordre des barreaux francophones et germanophone and Others*) synthesized and summarized preceding case law of the CJEU on retention of traffic and location data (thereafter – *La Quadrature du Net*).

It is important to note that the preliminary reference in the leading case *La Quadrature du Net* was made by the Conseil d'Etat of France and concerned the interpretation of main legal source of the EU secondary law in the area of data retention - Article 15(1) of Directive. In secondary EU law, taking into consideration the general prohibition of data retention, the Article 15 (1) of the Directive is the main legal basis for the rules of data retention after the Court of Justice in Judgment of 8 April 2014, *Digital Rights Ireland and Others* (Joined Cases C-293/12 and C-594/12) declared invalid Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications.[1] In the main proceedings before the Conseil d'Etat, the applicants contested provisions of French legislation establishing *inter alia* the duty of providers of electronic communications operators, internet service providers and hosting providers to retain all traffic and location data for their users for one year, excluding the content of communications, their civil identification data and certain information relating to their accounts and, if applicable, the payments they make online, for the purposes of investigating, recording and prosecuting criminal offences and safeguarding national security.

The Court of Justice in *La Quadrature du Net* recalled that the Directive 2002/58/EC does not authorise the Member States to adopt, *inter alia* for the purposes of national security, legislative measures intended to restrict the scope of rights and obligations provided for in that directive, in particular the obligation to ensure the confidentiality of communications and traffic data, unless such measures comply with the general principles of EU law, including the principle of proportionality, and the fundamental rights guaranteed by the Charter of Fundamental Rights of the European Union. The Court held before that the Directive, read in the light of the Charter, precludes national legislation requiring providers of electronic communications services to carry out the general and indiscriminate transmission of traffic

[1] Article 15
Application of certain provisions of Directive 95/46/EC
1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union. <…>

data and location data to the security and intelligence agencies for the purpose of safeguarding national security. In *La Quadrature du Net*, the Court found that the Directive precludes legislative measures requiring providers to carry out the general and indiscriminate retention of traffic and location data as a preventive measure. Those obligations to forward and to retain such data in a general and indiscriminate way constitute particularly serious interferences with the fundamental rights guaranteed by the Charter, where there is no link between the conduct of the persons whose data is affected and the objective pursued by the legislation at issue. By contrast, the Court held that, in situations where the Member State concerned is facing a serious threat to national security that proves to be genuine and present or foreseeable, the Directive, read in the light of the Charter, does not preclude recourse to an order requiring providers of electronic communications services to retain, generally and indiscriminately, traffic data and location data. In that context, the Court specifies that the decision imposing such an order, for a period that is limited in time to what is strictly necessary, must be subject to effective review either by a court or by an independent administrative body whose decision is binding, in order to verify that one of those situations exists and that the conditions and safeguards laid down are observed. In those circumstances, the Directive also does not preclude the automated analysis of the data, inter alia traffic and location data, of all users of means of electronic communication. The Court adds that the Directive 2002/58/EC, read in the light of the Charter, does not preclude legislative measures that allow recourse to the targeted retention.

The Court of Justice in the Judgement of 5 April 2022 in Case C-140/20, *Commissioner of the Garda Síochána and Others* confirmed and further developed the basic principle that EU law precludes the general and indiscriminate retention of traffic and location data relating to electronic communications for the purposes of combating serious crime. The Court rejected *inter alia* the submission that particularly serious crime could be treated in the same way as a threat to national security which is genuine and current or foreseeable and could, for a limited period of time, justify a measure for the general and indiscriminate retention of traffic and location data. Such a threat is distinguishable, by its nature, its seriousness, and the specific nature of the circumstances of which it is constituted, from the general and permanent risk of the occurrence of tensions or disturbances, even of a serious nature, that affect public security, or from that of serious criminal offences being committed.

It is important to note that Article 4 (2) TEU excludes national security from the scope of EU law: national security remains the sole responsibility of each Member State. The CJEU in *La Quadrature du Net* rejected the argument that Directive 2002/58/EC is not applicable in cases of data retention for the purposes of national security. According to respondents in the main proceedings, since the Directive (Art. 1(3)) excludes "activities concerning public security, defence and State security" from its scope, the legislation at issue concerns national security that also falls outside the scope of EU law (Art. 4(2) TEU).[2] The CJEU underlined that the

[2] Under Article 4(2) "national security remains the sole responsibility of each Member State." Article 1 (3) excludes from the scope of the Directive „activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law."

legislative data retention measures regulate data processing by private service providers and not "activities characteristic to the State", for which the Directive is exempted. Therefore, the reference to Article 4(2) TEU cannot invalidate this conclusion, since the mere fact that such national measure has been taken for the purpose of national security cannot render EU law inapplicable and exempt Member States from their obligations to comply with that law. Moreover, it cannot make inapplicable or limit the scope of the rights guaranteed by the EU Charter of Fundamental Rights: right to liberty and security (Art.6), respect for private and family life (Art. 7), protection of personal data (Art. 8), non-discrimination (Art. 21). Under Article 52 § 1 of the Charter, limitation of rights and freedoms must be provided for only by law and with respect of their essence, the principles of proportionality and necessity, to protect the rights and freedoms of others. Corresponding protection is granted by the European Convention of Human Rights: right to respect for private and family life (Art. 8), freedom of thought, conscience and religion (Art. 9), prohibition of discrimination (Art. 14), limitation on use of restrictions on rights (Art. 18). Protection of fundamental rights would likely be undermined if data retention and the access to personal data for the purposes of protection of national security would be outside the principles and rules of the EU and the ECHR law. At the same time, it should be underlined that the right to security proclaimed in Article 6 of the Charter also implies the duty of State to take all due measures to protect the security of EU citizens, including protection from terrorist acts.

This legal opinion does not concern the legality of retention of location and traffic data by competent State authorities empowered by law to collect necessary data, prosecute and punish perpetrations of acts threatening national security. Such activities are governed by national law and fall outside the scope of EU law under Article 4 TEU. Under recital 11 of the Directive 2002/58, this Directive does not affect the ability of Member States to carry out lawful interception of electronic communications, or take other measures, if necessary for any of these purposes and in accordance with the European Convention of Human Rights as interpreted by the rulings of the European Court of Human Rights (thereafter – the Convention).[3] Such measures must be appropriate, strictly proportionate to the intended purpose and necessary within a democratic society and should be subject to adequate safeguards in accordance with the Convention.[4]

For the purposes of present legal opinion, the author follows the text of English translation of the Decision N° 393099 of the Conseil d'État of 21 April 2021.

[3] See, inter alia, the judgements of the ECtHR of 25 May 2021, *Big Brother Watch and Others v. the United Kingdom* and *Centrum för Rättvisa v. Sweden*, and in the judgment of 4 December 2015, *Roman Zakharov v. Russia.*

[4] Therefore, the Conseil d'Etat in point 93 of the Decision, made well-founded conclusion "*that the provisions of Article L. 822-2 of the French Internal Security Code do not fall within the scope of that Directive insofar as they lay down the period for which the intelligence services may retain data collected under the provisions of Article L. 851-1 of that Code, without governing the activities of providers of electronic communications services by imposing specific obligations on them. These provisions therefore cannot be regarded as implementing EU law and consequently, the pleas alleging a breach of the Directive of 12 July 2002, interpreted in light of the Charter of Fundamental Rights of the European Union, cannot be usefully cited in this respect*."

All underlining in this legal opinion is made by the author.

Question no.1

Is it in line with the CJEU case-law and fundamental rights to impose a permanent/revolving retention of traffic and location data for national security purposes, referring to the permanent risk of terrorist attacks etc., the way the Conseil d'Etat and the EU Commission are proposing (rather than only when there is a specific threat and for a short period of time limited by duration of threat), and to access this data for other purposes than national security (e.g. tackling serious crime)?

2.1. Analysis of the Decision of the Conseil d'Etat of 21 April 2021.[5]

Scope of analysis of the Decision. Decision of the Conseil d'Etat of 21 April 2021 (thereafter – the Decision) is a decision of the Conseil ruling as the Supreme Administrative Court of French Republic on appeal submitted by the associations of the providers of an electronic communications service. *Inter alia*, the applicants asked the Conseil d'Etat to "quash as *ultra vires* the implied rejection resulting from the silence maintained by the French Prime Minister of its application seeking to repeal Article R. 10-13 of the French Postal and Electronic Communications Code; <…>."

After the CJEU ruled in *La Quadrature du Net* on 3 questions submitted to the Court, the Conseil d'Etat held in the operative part of the Decision:

"*Article 1: The decisions of the French Prime Minister refusing to repeal Article R. 10-13 of the French Postal and Electronic Communications Code and the Decree of 25 February 2011 on the retention and communication of data enabling the identification of any person who has contributed to the creation of content published online are quashed, insofar as said regulatory provisions first, do not limit the purposes of the obligation to retain, in a general and indiscriminate manner, traffic and location data other than civil identity data, contact and payment details, contract and account data and IP addresses, to the safeguarding of national security and secondly, do not provide for a periodic review of the existence of a serious, real and current or foreseeable threat to national security. <…>*."

As far as the main points of Question no. 1 are concerned, the Court, in the operative part of the Decision, also held that the applicable dispositions of the EU law do not preclude legislative measures that:

"– allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and

[5] See original official French text of the Décision du Conseil d'Etat N° 393099 du 21 avril 2021 in - https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2021-04-21/393099

indiscriminately, traffic and location data in situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, where the decision imposing such an instruction is subject to effective review, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and that the conditions and safeguards which must be laid down are observed, and where that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists;

– provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended; <…>."

In my opinion, the operative part of the Decision is in general line with the well established case-law of the Court of Justice. Nevertheless, a legal analysis of the Decision necessitates the appraisal of the relevant dispositions of its *ratio decidendi* (rationale for the Decision). In legal theory and practice, *ratio decidendi* may constitute essential element of a judgment which create binding precedent, and must therefore be followed by inferior courts. I shall also take into account the fact that the operative part of the Decision keeps silence with regard to the well-established criteria of "*period that is limited in time to what is strictly necessary*", confirmed by Court of Justice in *La Quadrature du Net.*

It is also important to note that in the Decision, the Conseil d'Etat follows and quotes the main rules of applicable EU law and jurisprudence of the Court of Justice. In particular, the Decision stipulates:

"31. Conversely and secondly, EU law allows general and indiscriminate retention of traffic and location data other than IP addresses to be imposed on operators, for the sole purposes of safeguarding national security where a State is confronted with a serious threat to national security that is proven to be real and current or foreseeable, based on an injunction by an official authority, subject to effective control by a court or independent administrative authority, tasked, among other things, with verifying the reality of the threat, for a strictly limited period, but which can be renewed if the threat persists."

First point of Question no. 1 concerning the "permanent risk of terrorist attacks or specific threat limited by a period of time. " In common sense, a "threat" is a declaration of the intention or intent to inflict harm, to hurt, destroy, etc., whereas a „risk" is a situation involving exposure to danger, a possibility that a dangerous event may happen. In the context of this analysis, *"specific threat"* may also indicate several various and multiple identified threats of attack. In any case, a specific threat cannot be assimilated with the existence of a generally existing threat or risk of attack on national security or of serious attempts to

undermine it, however serious and grave the situation may be, without identifying and verifying that specific declaration(-s) or intent(-s), current or foreseeable, to commit such acts, exist(s). As far as the situation of a serious threat of general character menacing security of nation and State is concerned, such situation is described in Article 15 (1) of the European Convention of Human Rights providing for legitimate derogations in time of emergency:

„1. In time of war or other public emergency threatening the life of the nation any High Contracting Party may take measures derogating from its obligations under this Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law. <...>“[6]

As it was noted before, the operative part of the Decision clearly established the requirement of the “existence of a serious, real and current or foreseeable threat to national security”. The Decision does not make the existence of a specific threat *a condition sine qua non* for the purposes of legality of data retention. The Decision also does not require *expressis verbis* that the period of retention must be “limited to what is strictly necessary” according the terms used by the CJEU judgement in *La Quadrature du Net* („as long as serious, real and current or foreseeable threat to national security exist”).

As far as the existence of a high threat (or persistence of a high risk of terrorism) to national security in the circumstances of the case is concerned, the Conseil d’Etat has stated (our underlining added):

“44. Secondly, the evidence adduced, including but not limited to the preparatory stages conducted by the 10th chamber of the Litigation Section, shows that France is facing a threat to its national security, assessed in light all of the fundamental interests of the French nation listed in Article L. 811-3 of the French Internal Security Code cited in point 19, the intensity of which indicates that it is both serious and real. As at the date of this decision, this threat is not only foreseeable but also current. It arises first, from the persistence of a high risk of terrorism, as evidenced in particular, by the fact that six attacks occurred on French soil during the course of 2020, causing seven deaths and injuring 11 people. Two further attacks have already been foiled in 2021. The Vigipirate plan was implemented at the “Emergency attack” level between 29 October 2020 and 4 March 2021 and then the “Enhanced security – risk of attack” level since 5 March 2021, attesting to a sustained high level of threat on French territory. Furthermore, France is particularly exposed to the risk of spying and foreign interference, inter alia because of its military capacity and commitments and its

[6] The European Court of Human Rights in leading case concerning public emergency situations under Art. 15, *Lawless v. Ireland* (no. 3), 5310/71, observed that, meaning of the words "other public emergency threatening the life of the nation" was sufficiently clear: “an exceptional situation of crisis or emergency which affects the whole population and constitutes a threat to the organised life of the community of which the State is composed” (paragraph 28). The Court concluded that the existence at the time of a "public emergency threatening the life of the nation", had been reasonably deduced by the Irish Government from a combination of factors, namely: the existence in the territory of the Republic of Ireland of a secret army engaged in unconstitutional activities and using violence to attain its purposes; the fact that this army was also operating outside the territory of the State, thus seriously jeopardising the relations of the Republic of Ireland with its neighbour; the steady and alarming increase in terrorist activities from the autumn of 1956 and throughout the first half of 1957.

technological and economic potential. Numerous French businesses, both large groups and small and medium-sized enterprises, are thus the subject of malevolent activities targeting their know-how and potential for innovation, through industrial or scientific spying operations, sabotage, attacks on their reputation or poaching of experts. France also faces serious threats to public peace, associated with an increase in the activities of radical and extremist groups. These threats are sufficient to justify a general and indiscriminate retention obligation in respect of the connection data listed in Article R. 10-13 of the French Postal and Electronic Communications Code other than data relating to civil identity and IP addresses, Furthermore, the evidence adduced does not show that the retention period for these data of one year is not strictly necessary for the purpose of safeguarding national security. <...>

46. In light of the foregoing, with regard to the objective of safeguarding national security, the refusal to repeal Article R. 10-13 of the French Postal and Electronic Communications Code and Article 1 of the Decree of 25 February 2011 must be quashed solely insofar as their provisions do not require a periodic review of the existence of a serious, real and current or foreseeable threat to national security, with regard to the data they mention other than those pertaining to users' civil identity, accounts and payments and to IP addresses. The French government should therefore be ordered to supplement these provisions within six months of the date of this decision. Insofar as it is apparent from this decision, as stated in point 44, that the reality and severity of the threat to national security justify the obligation to retain all connection data to this end, in a general and indiscriminate manner, operators cannot, prior to the expiry of this period, deem themselves exempt from said obligation and the sanctions associated with the disregard thereof, on the grounds that the duration of the order imposed on them was not limited in time by the regulatory authority.<...>

66. The evidence adduced clearly shows that in 2015 and 2016, when the challenged decrees were adopted, France faced a serious, real and current threat to its national security, as evidenced by, among other things, the attack on "Charlie Hebdo" that occurred on 7 January 2015 and the series of attacks on 13 November 2015. Consequently, Book VIII of the French Internal Security Code was able, as stated previously, to impose an obligation on electronic communications operators, internet service providers and hosting providers to retain traffic and location data on a general and indiscriminate basis for the purpose of safeguarding national security. <...>

96. As recalled in point 66, on the date on which the challenged decrees were published, France was facing a serious, real and current threat to national security. Furthermore, the evidence adduced shows that this threat, as outlined in points 44 and 66, has remained at a high level between then and the date of this decision. Consequently, throughout this period, the French government was lawfully entitled to impose an obligation on electronic communications operators, internet service providers and content hosting providers to retain

traffic and location data on a general and indiscriminate basis for the purpose of safeguarding national security."

In conclusion, the Decision fails to demonstrate a specific threat to national security because (first of all, in paragraph 44) it refers to a mere general *risk* of terrorism and past attacks in France. I did not find any evidence given for the specific or identified preparation of a specific future attack. The Decision does not exclude that a serious, real and current threat to national security may be assimilated with the persistence of a high risk of terrorism, i.e. with situations of very high risk of terrorism having general character without strict necessity to verify and identify that a specific threat was present. On the contrary, the wording used by the CJEU in operative part of *La Quadrature du Net* Judgement, namely "[the] situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable" and that the data retention decision "is subject to effective review <…> to verify that one of those situations exists" means that the existence of specific threat must be necessarily shown and verified.

Conclusion. The Decision does not exclude the situations where a general, serious and grave threat or persistence of a high risk of terrorism exists, such threat or risk may justify, without the necessity of identifying and showing specific threat(-s), the "*retention of traffic and location data on a general and indiscriminate basis for the purpose of safeguarding national security"* as it is stated in point 96 of the Decision. Insofar, the Decision is not in line with the CJEU case-law and fundamental rights.

Second point of Question no. 1 concerning limited period of data retention. The question is to answer, first, whether, according to the Decision, national legislation and CJEU jurisprudence may, nevertheless, derogate in some situations from the obligation to ensure that a general and indiscriminate data retention be allowed only for a period that is limited in time to what is strictly necessary, but which may be extended if the threat persists. I note that the Decision states that national legislation shall "*provide for a periodic review of the existence of a serious, real and current or foreseeable threat to national security."* Does it mean, that the requirement of "periodic review" is equivalent to the requirement of *"retention of that data only for a period that is limited in time to what is strictly necessary, but which may be extended if the threat persists"*, according to *La Quadrature du Net* jurisprudence? Or, on the contrary, can the Decision be interpreted in the sense that a permanent retention could be a legitimate measure as long as *threat persists* and as far as a *periodic review* was provided by national legislation? According to the Court of Jusstice in *La Quadrature du Net*, para.138, *"[a]lthough it is conceivable that an instruction requiring providers of electronic communications services to retain data may, owing to the ongoing nature of such a threat, be renewed, the duration of each instruction cannot exceed a foreseeable period of time. Moreover, such data retention must be subject to limitations and must be circumscribed by strict safeguards making it possible to protect effectively the personal data of the persons*

concerned against the risk of abuse. Thus, that retention cannot be systematic in nature." It means, in my opinion, that a clear difference shall be drawn between requiring only the periodic review of a retention order, on one hand, and, on the other, fixing time limits for the duration of instruction which cannot exceed a foreseeable period of time.

Secondly, I must also underline that the Decision is based on well-established case-law of the Court of Justice providing for the necessity of *„verifying the reality of the threat, for a strictly limited period, but which can be renewed if the threat persists"* (point 31 of the Decision), that *"insofar as such retention entails a serious interference in the fundamental rights of the persons concerned, it can only be justified for the purpose of combating serious crime, preventing serious threats to public security and safeguarding national security"* (point 33). Thirdly, this question shall be examined also in the context of national legislative dispositions establishing several time limits of data retention by providers of electronic communications and corresponding to implementing decrees: one year[7], 4 months[8], 2 months.[9]

The AG Campos Sánchez-Bordona in his Opinion of 18 November 2021 in Joined Cases C-793/19 and C-794/19 *SpaceNet and Telekom Deutschland,* paragraph 68, maintained that a very limited retention period may make it harder to establish profiles, and the time period must be considered alongside the quantity of data retained and the techniques available for analysis (para 70).[10] In my opinion, the quantity of data retained and the techniques available for analysis" cannot be decisive criteria for establishing or qualifying time limits for data retention. Under Article 15 (1) of the Directive, Member States may adopt legislative measures providing for the retention of data for a limited period when such restrictions constitutes a necessary, appropriate and proportionate measure within a democratic society._

The Conseil d'Etat in this case found that *"the evidence adduced does not show that the retention period for these data of one year is not strictly necessary for the purpose of*

[7] According to the dispositions of French Post and Electronic Communications Code (CPCE), Criminal Code and Defence Code) "operations designed to erase or render anonymous certain categories of technical data may be deferred for a maximum period of one year". In particular, Article R. 10-13 CPCE) provides that electronic communications operators shall retain localisation and traffic data for the purposes of investigating, detecting and prosecuting criminal offences "for one year from the date of registration." Article 3 of that *Decree No 2011-219,* contested by the applicants in the main proceedings, provided that the data shall be retained for one year.

[8] Article L. 821-4 of the *Code de la sécurité intérieure* (Internal Security Code or CSI) provides: 'Authorisation to implement the techniques referred to in Chapters I to IV of Title V of this Book shall be issued by the Prime Minister for a maximum period of four months. … The authorisation shall contain the grounds and statements set out in points 1 to 6 of Article L. 821-2. All authorisations shall be renewable under the same conditions as those laid down in this Chapter.'

[9] The first authorisation for the implementation of automated processing practices provided for in point I of this article shall be issued for a period of two months. The authorisation shall be renewable under the conditions on duration laid down in Chapter I of Title II of this Book. The application for renewal shall include a record of the number of identifiers flagged by the automated processing and an analysis of the relevance of that flagging.

[10] In this respect, see also Conclusions de l'AG Pitruzzella présentées le 27 janvier 2022 dans l'Affaire C-817/19, *Ligue des droits humains contre Conseil des ministres*, points 234-240 (for the moment, available only in French) where the AG interpreted detention and the use of passenger name records (PNR).

safeguarding national security." It also held that applicable dispositions of French Postal and Electronic Communications Code and of the Act on trust in the digital economy do not provide for a periodic review, in light of the risks to national security, of the necessity of maintaining the obligation imposed on the persons concerned by the obligation to retain connection data. The Conseil d'Etat held that these provisions, insofar as they do not make the continued imposition of this obligation subject to verification at regular intervals, which should not reasonably exceed one year, of the persistence of a serious, real and current or foreseeable threat to national security, are, to this extent, contrary to EU law.[11] The Conseil d'Etat thus repealed Article R. 10-13 of the French Postal and Electronic Communications Code and Article 1 of the Decree of 25 February 2011. Therefore, I observe that the requirement of *"retention of that data only for a period that is limited"* or *„strictly limited period, but which can be renewed if the threat persists"* is absent from the operative part of the Decision. Nevertheless, this absence does not mean that the Conseil d'Etat ignored that the Directive 2002/58 establishes a principle of „retention of data for a limited period" or that the case-law of the CJEU requires that the „*retention of that data (be allowed) only for a period that is limited in time to what is strictly necessary, but which may be extended if the threat persists."*

For the sake of a comprehensive analysis, I shall also refer to some other points of the Decision concerning other time limits for data retention. According to the point 92 of the Decision, the applicant associations maintained that Article L. 822-2 of the French Internal Security Code breaches the Directive 2002/58/EC insofar as it provides for an excessive retention period for data gathered by the intelligence services. This article, in the version applicable to the dispute, provided:

"I. The intelligence gathered using an intelligence-gathering technique authorised pursuant to Chapter I of this Title shall be destroyed at the end of a period of: (...) 3. Four years from the date on which the information or documents mentioned in Article L. 851-1 were gathered. / The period for encrypted information starts from the date on which it is decrypted. It cannot be retained for more than six years from the date on which it is gathered. / Intelligence gathered that contains cyberattack information or is encrypted, and decrypted information associated with the latter, may be retained for longer than the periods mentioned in this point I, to the extent that it is strictly necessary for the purposes of technical analysis and excluding any use for the surveillance of the persons concerned".

In point 93 of the Decision, the Conseil d'Etat noted that Article 1(3) of the Directive 2002/58/EC states that it "*shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, (...), and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law".* Therefore, the Conseil, d'Etat concluded:

[11] See points 44 and 45 of the Decision.

"In light of the foregoing, it is clear that the provisions of Article L. 822-2 of the French Internal Security Code do not fall within the scope of that Directive insofar as they lay down the period for which the intelligence services may retain data collected under the provisions of Article L. 851-1 of that Code, without governing the activities of providers of electronic communications services by imposing specific obligations on them. These provisions therefore cannot be regarded as implementing EU law and consequently, the pleas alleging a breach of the Directive of 12 July 2002, interpreted in light of the Charter of Fundamental Rights of the European Union, cannot be usefully cited in this respect."

Conclusion. The Decision of Conseil d'Etat is in line with the case-law of the CJEU with regard to the requirement to retain traffic and location data "only for a short period of time limited by duration of threat."

Third point of Question no. 1 concerning access to retained data. Persons likely to access traffic and location data

National legislation shall establish a strictly limited list or categories of State institutions empowered by law to get access to location and traffic data. It is the duty of the State that the access to this personal data would not be given to any other institutions or persons, except for the purposes of judicial procedure and respecting the rules of confidentiality. Indiscriminate retention by private operators creates the risk that such data would be accessible to unauthorized persons. A long period of retention may multiply such a risk.

In this case before the Conseil d'Etat, the applicant associations maintained that by not limiting the number of people who can access and use connection data, these provisions breach the rights to privacy and family life and the protection of personal data protected by the EU Charter.

The Conseil d'Etat first of all referred to the judgement of the CJEU in *Digital Rights Ireland* lying down the strict requirement of "*objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued*". On this basis, the Conseil quoted and examined applicable dispositions of French legislation (Code de la sécurité intérieure, etc.[12]) providing that a *"decree in the Conseil d'Etat, adopted following an opinion from the Commission nationale de contrôle des techniques de renseignement, designates the services, other than specialist intelligence services, under the authority of the Minister of Defence, the Minister of the Interior, the Minister of Justice and the Ministers responsible for the economy, the budget and customs, which may be authorised to use the techniques mentioned in Title V (of Book VIII of the legislative part of the code de la sécurité intérieure*) *in the conditions provided for in that Book. It shall set out, for each service, the purposes mentioned*

[12] In particullar, le code des postes et des communications électroniques, le code de procédure pénale, le code de la sécurité intérieure, la loi n° 2004-575 du 21 juin 2004, as well as the decrees, contested by the applicants: le décret n° 2011-219 du 25 février 2011; le décret n° 2015-1185 du 28 septembre 2015; le décret n° 2015-1639 du 11 décembre 2015; le décret n° 2016-67 du 29 janvier 2016; le décret n° 2020-1404 du 18 novembre 2020.

in Article L. 811-3 and the techniques that may be authorised". The challenged Decree of 11 December 2015 sets out a limited list, organised by intelligence technique and the purpose pursued, of the services authorised to use authorized techniques. "*Only officials, who have been designated and authorised by the minister or, by delegation, by the director to whom they report, can implement the intelligence-gathering techniques mentioned in Title V of this Book."* Only individually designated and authorised officials may use them. The principle of proportionality noted in that Code dictates that the number of authorised officials should not exceed the number required to carry out these activities. The period of validity of the authorisation shall also be specified. Secondly, it is the responsibility of the administrative tribunals and courts, when asked to rule on a plea of this nature, to verify that the access to the connection data of the people listed in the decrees adopted to implement applicable dispositions of the Code is limited to what is strictly necessary in respect of the purposes pursued. Consequently, the Conseil d'Etat dismissed the plea alleging that this Decree breaches Articles 7 and 8 of the Charter of Fundamental Rights of the European Union on the grounds that it does not limit the number of people able to access and use connection data.

The EU Charter guarantees the protection of personal data (Art. 8 (1)) and stipulates that personal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

Article 5 (1) of the Regulation 2016/679 provides that personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency"). It shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods in so far as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ("storage limitation"). It shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ("integrity and confidentiality").

As far as the legality of the access to personal data by competent authorities is concerned Article 6 of the GDPR is applicable and provides that processing shall be lawful only if and to the extent that processing is necessary for compliance with a legal obligation to which the controller is subject. The basis for the processing referred shall be laid down by the EU law or Member State law to which the controller is subject. According to this Article the purpose of the processing shall be determined in that legal basis. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, *inter alia*: the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage

periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing, etc. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued. Article 23 provides that these principles may be restricted (also in the sense of allowing retention and giving access to location and traffic data) when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection or prosecution of criminal offences and other legitimate purposes enumerated in this Article. Any legislative measure shall contain specific provisions as to the purposes of the processing or categories of processing and the specification of the controller or categories of controllers.

As far as the applicable guarantees provided in the EU Charter, secondary EU law and the jurisprudence of the CJEU are concerned, the conditions of legality of access by competent authorities were the subject of analysis made by the Court of Justice in the Judgement of 21 December 2016 in *Tele2 Sverige AB* (C-203/15).[13] First of all, the Court stated that, as regards compatibility with the principle of proportionality, national legislation governing the conditions under which the providers of electronic communications services must grant the competent national authorities access to the retained data must ensure that such access does not exceed the limits of what is strictly necessary (paragraph 116 of this Judgement). Further, since the legislative measures referred to in Article 15(1) of Directive 2002/58 must, in accordance with recital 11 of that directive, 'be subject to adequate safeguards', a data retention measure must, as follows from the case-law of the Court, lay down clear and precise rules indicating in what circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data. Likewise, a measure of that kind must be legally binding under domestic law (paragraph 117). In order to ensure that access of the competent national authorities to retained data is limited to what is strictly necessary, it is, indeed, for national law to determine the conditions under which the providers of electronic communications services must grant such access. However, the national legislation concerned cannot be limited to requiring that access should be for one of the objectives referred to in Article 15(1) of Directive 2002/58, even if that objective is to fight serious crime. That national legislation must also lay down the substantive and procedural conditions governing the access of the competent national authorities to the retained data (paragraph 118). Accordingly, and since general access to all retained data, regardless of whether there is any link, at least indirect, with the intended purpose, cannot be regarded as limited to what is strictly necessary, the national legislation concerned must be based on objective criteria in

[13] The Court made by analogy made also references to the Judgements of the European Court of Human Rights: ECtHR, 4 December 2015, *Zakharov v. Russia*, CE:ECHR:2015:1204JUD004714306, § 260, and in relation to Article 8 of the ECHR to ECtHR, 12 January 2016, *Szabó and Vissy v. Hungary*, CE:ECHR:2016:0112JUD003713814, §§ 77 and 80. See also Opinion of the GA Pitruzzella of 27 January 2022 in Case C-817/19, *Ligue des droits humains,* paragraphs 85, 86, 113, 114 et seq.

order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data of subscribers or registered users. In that regard, access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. However, in particular situations, where for example vital national security, defence or public security interests are threatened by terrorist activities, access to the data of other persons might also be granted where there is objective evidence from which it can be deduced that that data might, in a specific case, make an effective contribution to combating such activities (paragraph 119). It is essential that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior independent review, and that the decision of that court or other independent body should be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime (paragraph 120). Afterwards, the competent national authorities must notify the persons affected, under the applicable national procedures, as soon as that notification is no longer liable to jeopardise investigations. It is necessary to enable the persons affected to exercise their right to a legal remedy, where their rights have been infringed (paragraph 121). The Member States shall ensure the effective protection of retained data against risks of misuse and against any unlawful access to that data (paragraph 121). In any event, the Member States must ensure review, by an independent authority, of compliance with the level of protection guaranteed by EU law with respect to the protection of individuals in relation to the processing of personal data, that control being expressly required by Article 8(3) of the Charter and constituting, in accordance with the Court's settled case-law, an essential element of respect for the protection of individuals in relation to the processing of personal data. If that were not so, persons whose personal data was retained would be deprived of the right, guaranteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data (paragraph 122). In *Quadrature du Net*, § 176, the Court of Justice concluded that in order to meet the requirement of proportionality, according to which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary, national legislation governing the access of the competent authorities to retained traffic and location data cannot be limited to requiring that the authorities' access to such data should correspond to the objective pursued by that legislation, but must also lay down the substantive and procedural conditions governing that use.

Conclusion. The Decision is in line with the CJEU case-law and fundamental rights as far as the categories of persons likely to access traffic and location data are concerned.

Fourth point of Question no. 1: retention and access to traffic and location data for other purposes than national security (e.g. tackling serious crime). Point 58 of the Decision of the Conseil d'Etat states:

„In light of all the foregoing, the French government could not impose an obligation on electronic communications operators, internet service providers and hosting providers to retain connection data on a general and indiscriminate basis, other than the data mentioned in points 33, 34 and 36 on civil identity, IP addresses and information on accounts and payments, for the purposes of combating crime and preventing threats to public order, without breaching EU law. <...>"

At the same time, the Decision in its point 44 as quoted before is making reference to the facts that "*[n]umerous French businesses, both large groups and small and medium-sized enterprises, are thus the subject of malevolent activities targeting their know-how and potential for innovation, through industrial or scientific spying operations, sabotage, attacks on their reputation or poaching of experts. France also faces serious threats to public peace, associated with an increase in the activities of radical and extremist groups. These threats are sufficient to justify a general and indiscriminate retention obligation in respect of the connection data <...>."*

In this context, it is important to note that in the analysis of objectives pursued by the intelligence services, the Conseil d'Etat concluded that prevention of organised crime and delinquency must be regarded as relating to safeguarding national security within the meaning of Article 15 Directive 2002/58:

"67. Article L. 851-1 of the French Internal Security Code, in the version applicable to the dispute, provides that: *"In accordance with the conditions provided for in Chapter I, Title II of this Book, permission may be given to gather information or documents processed or retained by their networks or electronic communications services from electronic communications operators and the persons mentioned in Article L. 34-1 of the French Postal and Electronic Communications Code, as well as the persons mentioned in paragraphs 1 and 2 of Article 6 I of French Act no. 2004-575 of 21 June 2004 on trust in the digital economy, including technical data relating to the identification of subscriber or connection numbers to electronic communications services, an inventory of all the subscriber or connection numbers of a designated person, the location of the terminal devices used and a subscriber's communications based on a list of incoming and outgoing call numbers, and the duration and date of communications* (...)". Pursuant to Article L. 811-3 of that Code: "*Solely for the exercise of their respective missions, specialist intelligence services may use the techniques mentioned in Title V of this Book to gather intelligence relating to the defence and promotion of the following fundamental interests of the French nation: 1. / National independence, territorial integrity and national defence; 2 / Major foreign policy interests, the fulfilment of France's European and international commitments and the prevention of any form of foreign interference; / 3. France's major economic, industrial and scientific interests; / 4. The prevention of terrorism; / 5. The prevention of: a) Attacks on the republican form of institutions; b) Actions aimed at maintaining or reconstituting groups dissolved pursuant to Article L. 212-1; / c) Collective violence likely to cause serious disruption to public peace; /*

6. The prevention of organised crime and delinquency; / 7. The prevention of the proliferation of weapons of mass destruction". Insofar as these purposes contribute to protecting the fundamental interests of the French nation, they must be regarded as relating to safeguarding national security within the meaning of Article 15 of the Directive of 12 July 2002."

In my opinion, this conclusion of the Conseil d'Etat means that the Conseil d'Etat includes prevention of organised crime and delinquency into the objective of safeguarding national security. Consequently, it allows that national legislation may establish obligation to retain, in a general and indiscriminate manner, traffic and location data other than civil identity data, contact and payment details, contract and account data and IP addresses, for the purposes of prevention of organised crime and delinquency, under the condition of periodic review of the existence of a serious, real and current or foreseeable threat of organised crime and delinquency to national security. Therefore, targeted retention of traffic and location data does not constitute *conditio sine qua non* of legality of such retention for the purposes of combating organised crime and delinquency.

The Court of Justice in *La Quadrature du Net* described the notion of national security by following way:

"135 In that regard, it 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."

Essential distinction shall be made between retention obligations imposed on operators for the purposes of protecting national security including in the fields of counter-terrorism, counter-espionage and counter-nuclear proliferation, etc. aimed at safeguarding the fundamentals of democratic society and State, on one hand, and obligations imposed to them, as it is asked in Question no. 1, for „other purposes than national security (e.g. tackling serious crime)", and first of all, for the purposes of public security threatened by serious criminal acts, on the other hand.[14] Scope and content of such obligations are quite different, even if clear or precise separation of the areas of combating crime and pursuing national security goals is a difficult task due to the fact that these two areas of state activity largely overlap.

[14] Article 15(1) of the Directive allows only restrictions as necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. The later in addition enumerates breaches of ethics for regulated professions, important economic or financial interests of a Member State or of the European Union, including monetary, budgetary and taxation matters, the exercise of official authority in such cases and the protection of the data subject or of the rights and freedoms of others. In any case, data retention is an exceptional measure allowed only in the situations of serious threat to national security, defence, public and financial security of the MS and the Union.

As far as definition of serious crimes is concerned, the boundary between crime and serious crime falls, as a general rule, to be determined by the Member States. Article 83(1) TFEU introduces the term "particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis" and defines the areas in which the Union has competence to approximate substantive criminal law: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime. This provision, however, does not contain a definition or a closed or exhaustive list of acts that can be classified as "serious crime". Article 15(1) of the Directive 2002/58/EC forming permissive legal basis for national data retention laws does not limit the establishment of data retention measures exclusively to cases of combatting serious crime, but to all criminal offences.[15] Nevertheless, in the light of protection of fundamental right of personal data protection and the principle of proportionality, national derogations (retention and access to location and traffic of personal data) must be limited to what is strictly necessary, based on serious character of criminal offence and criminal sanctions imposed by national penal law.

AG Campos Sánchez-Bordona in his Opinion of 18 November 2021 in Joined Cases C-793/19 and C-794/19 *SpaceNet and Telekom Deutschland*, § 84, concluded that Article 15(1) of Directive 2002/58/EC, in conjunction with Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights and Article 4(2) TEU, must be interpreted as precluding national legislation which obliges providers of publicly available electronic communications services to retain traffic and location data of end users of those services on a precautionary, general and indiscriminate basis for purposes other than that of safeguarding national security in the face of a serious threat that is shown to be genuine and present or foreseeable. According to the AG Sánchez-Bordona, national legislation on the matter shall comply with the exhaustive regulation in Directive 2002/58, as interpreted by the Court.

Fourth point of Question No. 1 also raises additional question about expedited data retention and access to data retained collected by way of expedited retention. Under the point 55 of the Decision <… *in order to ensure that the interference entailed by a measure of that kind is limited to what is strictly necessary, first, the retention obligation must relate only to traffic and location data that may shed light on the serious criminal offences or the acts adversely affecting national security concerned. Second, the duration for which such data is retained must be limited to what is strictly necessary, although that duration can be extended where the circumstances and the objective pursued by that measure justify doing so".* Accordingly, as it is stated in this point, where the offence concerned is sufficiently serious to justify the

[15] See: Marcin Rojszczak. The uncertain future of data retention laws in the EU: Is a legislative reset possible? In: Computer Law & Security Review, Volume 41, July 2021, 105572, p. 4. https://reader.elsevier.com/reader/sd/pii/S0267364921000455?token=0CD37B48F97ABEC02BD48D9B017D49124E45B7DE76B2F7C6E5F1FFF6F40D5182CA2A9A8097452C211E67AD59FD726E29&originRegion=eu-west-1&originCreation=20220210114257

interference with privacy caused by the retention of connection data, in accordance with the principle of proportionality recalled in points 38 and 39, the judicial authorities may, without breaching either the Directive of 12 July 2002 or the GDPR, order operators of electronic communications services, internet service providers and website hosting providers to carry out an expedited retention of the traffic and location data they hold, either for their own purposes, or to fulfil a retention obligation imposed for the purposes of safeguarding national security.

Therefore, in this context, the Decision does not make clear difference between the purposes of expedited retention of data in situations of serious crimes, on one hand, and of such retention for the purposes of safeguarding national security, on the other. Equally, it seems that the Decision doesn't make difference with regard to the access to retained data by judicial authorities that "*they hold, either for their own purposes, or to fulfil a retention obligation imposed for the purposes of safeguarding national security*."

It is, however, necessary to note the conclusion made by the Court of Justice in *La Quadrature du Net*:

"164 To the extent that the purpose of such expedited retention no longer corresponds to the purpose for which that data was initially collected and retained and since any processing of data must, under Article 8(2) of the Charter, be consistent with specified purposes, Member States must make clear, in their legislation, for what purpose the expedited retention of data may occur. In the light of the serious nature of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter which such retention may entail, only action to combat serious crime and, a fortiori, the safeguarding of national security are such as to justify such interference. Moreover, in order to ensure that the interference entailed by a measure of that kind is limited to what is strictly necessary, first, the retention obligation must relate only to traffic and location data that may shed light on the serious criminal offences or the acts adversely affecting national security concerned. Second, the duration for which such data is retained must be limited to what is strictly necessary, although that duration can be extended where the circumstances and the objective pursued by that measure justify doing so."[16]

This is pertinent, according to the CJEU, only in situations, where these offences or acts have been already established or where such offences and acts may reasonably be suspected.[17] In *La Quadrature du Net* the Court stated:

[16] In operative part of the judgement the Court ruled that Article 15(1) of Directive 2002/58 does not preclude legislative measures that: "<…> allow, for the purposes of combating serious crime and, a fortiori, safeguarding national security, recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers.

[17] In *La Quadrature du Net* the Court stated: „161 However, during that processing and storage, situations may arise in which it becomes necessary to retain that data after those time periods have ended in order to shed light on serious criminal offences or acts adversely affecting national security; this is the case both in situations where those offences or acts having adverse effects have already been established and where, after an objective examination of all of the relevant circumstances, such offences or acts having adverse effects may reasonably be

„161 However, during that processing and storage, situations may arise in which it becomes necessary to retain that data after those time periods have ended in order to shed light on serious criminal offences or acts adversely affecting national security; this is the case both in situations where those offences or acts having adverse effects have already been established and where, after an objective examination of all of the relevant circumstances, such offences or acts having adverse effects may reasonably be suspected."

In this context, it seems also necessary to quote the Opinion of AG Campos Sanchez-Bordona of 18 November 2021 in joined cases *VD and SR*, C-339/20 and C-397/20:

"78. However, the sense of the judgment in *La Quadrature du Net* would not be respected if its findings on national security could be extrapolated to criminal offences, even serious ones, which affect not national security but public security or other legally protected interests.

79. It is for this reason that the Court carefully distinguished between national legislative measures which provide for the general and indiscriminate retention of traffic and location data for the purposes of protecting national security (paragraphs 134 to 139 of the judgment in *La Quadrature du Net*) and those which concern the combating of crime and the safeguarding of public security (paragraphs 140 to 151 of the same judgment). Those two types of measure cannot have the same scope, as that distinction would otherwise be rendered meaningless.

80. Traffic and location data retention measures aimed at combating serious crime are set out, as I have said, in paragraphs 140 to 151 of the judgment in *La Quadrature du Net*. To those must be added measures, serving the same purpose, which authorise the preventive retention of IP addresses and data relating to the civil identity of an individual (paragraphs 152 to 159 of that judgment), and the 'expedited retention' of traffic and location data (paragraphs 160 to 166 of the aforementioned judgment)."

As the Court of Justice emphasized in *Commissioner of the Garda Síochána*, paragraph 63, criminal behaviour, even of a particularly serious nature, cannot be treated in the same way as a threat to national security. To treat those situations in the same way would be likely to create an intermediate category between national security and public security for the purpose of applying to the latter the requirements inherent in the former. In this judgement the Court of Justice emphasized that Member States must make clear, in their legislation, the purpose for which the expedited retention of data may occur (paragraph 87). In this most recent judgment, the Court specified main principles for national legislation, limiting the scope of expedited retention (paragraphs 88-91).

The scope and strict limits of expedited data retention and the access to data retained during this so called "quick freeze" of traffic and location data shall be necessarily established by

suspected." See also: Adam Juszczak and Elisa Sason, Recalibrating Data Retention in the EU. The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this only the Beginning? EUCRIM, issue 4, 2001, p. 14, https://eucrim.eu/articles/recalibrating-data-retention-in-the-eu/

national legislation of each Member State. It is evident that the Court of Justice of the European Union does not exercise legislative functions. In the EU law, indiscriminate traffic data retention is allowed to counter a threat to national security. Under the case-law of the CJEU the indiscriminate data retention is justified only in order to avert a threat to national security; it is not compliant to use this massive data pool for general purposes of prosecuting serious crime. National legislation shall exclude eventual "grey" situations, where accession to the massive traffic and location data collected for national security purposes would be granted for new purposes (i.e. for prosecuting serious crime, in the case *Commissioner of the Garda Síochána*). Expedited data retention and the access to data retained during this so-called "quick freeze" of traffic and location data is a narrow exception of the general principle of confidentiality of communications and the related traffic data provided in Article 15 of the Directive 2002/58/EC. It could be regarded only as kind of "an exception from exception."

Provided that all other conditions defined by the CJEU are satisfied, national security threats justify indiscriminate data retention, whereas serious crimes only suffice to legitimize targeted data retention. Any exception from this rule, like the expedited data retention, shall be interpreted and applied only in *sensu stricto*.

Conclusion: the Decision is not in line with the case-law of the CJEU and fundamental rights, insofar as it assimilates the threat of organised crime and delinquency with the threat to national security without providing that only targeted data retention shall be allowed for the purposes of tackling organised crime and delinquency.

Answers to Question no. 1 with regard to the Decision.

1. The Decision does not exclude that in situations where general, serious and grave threat or persistence of a high risk of terrorism exists, such threat or risk may justify, without necessity of identifying and showing specific threat(-s), the "*retention of traffic and location data on a general and indiscriminate basis for the purpose of safeguarding national security,*" as stated in point 96 of the Decision. Insofar, the Decision is not in line with the CJEU case-law and fundamental rights.
2. The Decision of the Conseil d'Etat is in line with the case-law of the CJEU with regard to the requirement to retain traffic and location data "only for a short period of time limited by duration of threat."
3. The Decision is in line with the CJEU case-law and fundamental rights as far as the categories of persons likely to access traffic and location data are concerned.
4. The Decision is not in line with the case-law of the CJEU and fundamental rights, insofar as it assimilates the threat of organised crime and delinquency with the threat to national security without providing that only targeted data retention shall be allowed for the purposes of tackling organised crime and delinquency.

Analysis of Commission services non-paper annexed to the document of Council WK 7294/2021 INIT of 10 June 2021 (thereafter – Working paper)[18]

The Working paper describes the annexed document as a Commission services non-paper which expresses preliminary views of the Commission services. According to its introduction, it sets out a preliminary mapping of possible legislative and non-legislative approaches on data retention in light of the CJEU case law and intends to stimulate a debate on the possible contours of national or EU data retention frameworks. Nevertheless, an analysis of this document leads to the identification of suggested legal solutions of data retention problems in situations where there is an absence of a legal framework, after invalidation of Directive 2006/24/EC (Data Retention Directive, or DRD) in 2014 by the Court of Justice. In this context, as it is noted in the Working paper, the Member States either maintained, repealed or amended their national laws.

The text of the Working paper shows that the authors were guided by the main principles of the case-law of the CJEU. The authors recall that the Court already 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. In this document, the Commission services also noted that 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. The Commission announced that it would analyse and outline possible approaches and solutions and would consult Member States with a view to devising the way forward.

For the purposes of identifying what actions may be considered for discussion, the Working paper refers to the Judgements of the CJEU in *La Quadrature du Net* and Case C-746/18 *Prokuratuur* of 2 March 2021 and suggests that "<…> *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)*

[18] For the purposes of present legal opinion, the text of Working paper was given to me by the Member of the European Parliament Dr. Patrick Breyer. Text of this document is available on https://cdn.netzpolitik.org/wp-upload/2021/07/wk07294.en211.pdf

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

The Working paper sets out a preliminary mapping of possible legislative and non-legislative approaches to data retention in light of the CJEU case. According to the authors of the Working paper, the intention is to stimulate a debate on the possible contours of national or EU data retention frameworks. As it follows from the Working paper, it does not purport to be exhaustive, definitive or final; it should simply serve as a basis to guide discussions. The Working paper focuses on policy directly related to data retention only.

The Working paper suggests three possible policy approaches to data retention. First, 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. The second policy approach would consist of a Commission recommendation or a guidance document (Communication). The third approach would consist of a regulatory initiative on data retention in order to translate the CJEU jurisprudence into EU rules on data retention.

The Chapter of the Working paper named „Policy approach 1: no EU initiative" suggests that 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 Chapter of Working paper named „Policy approach 2: Non-regulatory initiative on data retention" also raises some doubts. According to the Working paper, its aim is to assist Member States in bringing their laws into conformity with the rulings of the CJEU. A non-regulatory approach would consist of a Commission recommendation or a guidance document (most probably a Communication). Such kind of legal instrument, however, will not be legally binding nor enforceable. As the Advocate General Pitruzzella states in his Opinion of 27 January 2022 in Case C-817/19, *Ligue des droits humains,* where measures involving interferences with the fundamental rights established by the Charter of Fundamental Rights of the European Union originate in a legislative act of the European Union, the onus is on the EU legislature to set out the essential elements which define the scope of those interferences. According to Article 52 (1) of the EU Charter, any limitation on the exercise of the rights and freedoms recognized by this Charter must be provided for by law and respect the essence of those rights and freedoms.[19]

[19] See also paragraph 85 of the Opinion of the AG Pitruzzella (currently available only in French): "*85. Selon une jurisprudence bien établie de la Cour, s'inspirant de la jurisprudence de la Cour EDH, l'exigence selon laquelle toute limitation à l'exercice d'un droit fondamental doit être « prévue par la loi » ne vise pas uniquement l'origine « légale » de l'ingérence – qui n'est pas en cause dans la présente affaire –, mais implique aussi que la base légale qui permet cette ingérence doit définir elle-même, de manière claire et précise, la portée de celle-ci. Ayant trait à la « qualité de la loi » et, donc, à l'accessibilité et à la prévisibilité de la mesure en cause, ce second volet que recouvre l'expression « prévue par la loi » au sens tant de l'article 52, paragraphe 1, de la Charte que de l'article 8, paragraphe 2, de celle-ci et de l'article 8 de la CEDH vise non seulement à assurer le respect du principe de légalité et une protection adéquate contre*

The Chapter named „Policy approach 3: regulatory initiative on data retention" shows „different avenues to translate the CJEU jurisprudence into EU rules on data retention" as suggested by the Commission services.

The authors of the Working paper suggest that the *„generalised retention of traffic and location data for national security purposes 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.

In „Approach 3(b)," the Working paper deals in general terms with targeted data retention of traffic and location data for serious crime and serious threats to public security (and, a fortiori, safeguarding national security); in „Approach 3 (c)," it deals with the expedited retention (quick-freeze) of traffic and location data for serious crime and the safeguarding of national security and in „Approach 3 (d)," it deals with the generalised retention of IP addresses assigned to the source of an Internet connection for serious crime and serious threats to public security. General considerations expressed by the authors of the paper remain in line with the case-law of the CJEU and fundamental rights.

First point of Question no. 1: "Permanent risk of terrorist attacks or specific threat limited by a period of time." The Working paper suggests that in legislation harmonising obligations on electronic communication service providers, „the focus would be on the

l'arbitraire, mais répond également à un impératif de sécurité juridique."

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 „[t]he 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." With regard to targeted data retention, the authors of the paper conclude that geographical targeting measures may include areas where 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. However, as it was already shown in this legal opinion, the CJEU jurisprudence, and in particular, the operative part of its Judgement in in *La Quadrature du Net,* do not allow to assimilate the "situations where the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable" with the situations of high risk to national security of the Member States. Moreover, in my opinion, the broad formula making reference to "Member States' individual threat/risk assessment taking into account national specificities" does not correspond to the requirements of legal clarity and certainty. An interference with the fundamental rights (such as the retention of traffic and location data) must be based on clear and precise essential elements defined in the EU legislation and shall correspond to principles enshrined in Article 52 (1) of the EU Charter and Article 18 of the European Convention of Human Rights concerning limitations on the use of restrictions on human rights. Any limitation on the exercise of the rights and freedoms recognized in the Charter and the Convention must be clearly provided for by law and respect the essence of those rights and freedoms.

Conclusion. Insofar as legislative suggestions of the Commission concerning situations where the Member State is confronted with a serious threat to national security do not correspond to the requirements of legal clarity and certainty, the Working paper is not in line with the CJEU case-law and fundamental rights.

Second point of Question no. 1: Limited time of data retention. The Working paper expressly states that „[d]ecisions 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)." According to the Working paper „[t]argeted retention must also be limited in time but with the possibility to extend or renew the measures if necessary."

Conclusion. As regards limited time of data retention the Working paper is in general line with the case-law of the CJEU and fundamental rights.

Third point of Question no. 1: Access to data. It is important to note that the purposes of the Working paper are limited to data retention issues. The Working paper does not address any specific legal issue of the access to traffic and location data, as it „focuses on policy directly related to data retention only". At the same time, this documents underlines the

necessity of the „appropriate access safeguards other than prior review e.g. ex-post review and supervision by an appropriate national authority“ and „[r]equired technical safeguards applicable to both providers and authorities to prevent unauthorised access, abuse or misuse of data.“ The Working paper also repeats the conclusion of the Court that data retained under targeted retention obligations may be accessed for national security purposes but not for crimes in general._This general approach of the authors of the Working paper is in line with the general line of the CJEU case-law and main principles of fundamental rights.

Conclusion. The Working paper does not address any specific legal issue with regard to the access to traffic and location data.

Fourth point of Question no. 1: Retention and access to traffic and location data for other purposes than national security (e.g. tackling serious crime). Insofar as this document presumably only addresses targeted data retention of traffic and location data for serious crime and serious threats to public security (and, a fortiori, recommends targeted retention for safeguarding national security without making such kind of retention binding), it is in general line with the case-law of the CJEU and fundamental rights. Requirements of targeted retention are subject to my answer to Question no. 2.

Conclusion. Insofar as the Working paper suggests that only targeted retention of traffic and location data is permitted in situations of threats of serious crime and threats to public security, it is in general line with the case-law of the CJEU and fundamental rights.

Answers to Question no. 1 with regarding the Working paper.

1. Regarding the Commission services' legislative suggestions contained in Chapter „Policy approach 3: regulatory initiative on data retention“, the Working paper is not in line with the CJEU case-law and fundamental rights when it addresses situations where the Member State is confronted with a serious threat to national security in a way which does not correspond to the requirements of legal clarity and certainty.

2. As regards the limited time of data retention, the Working paper is in general line with the case-law of the CJEU and fundamental rights.

3. The Working paper does not address any specific legal issue with regard to the access to traffic and location data.

4. Insofar as the Working paper suggests that only targeted retention of traffic and location data is permitted in situations of threats of serious crime and threats to public security, it is in general line with the case-law of the CJEU and fundamental rights.

Question no. 2

Do the Commission's services proposals of parameters for geographical targeting and the targeting of specific categories of persons (pp. 5 and 6 of the Working paper WK 7294/2021 INIT of 10 June 2021) comply with the CJEU case-law and fundamental rights?

The purpose of targeted retention is not to preventively collect and examine all available data but instead to obtain information concerning specific persons or groups of persons potentially involved in serious criminal acts. Authorities are collecting traffic and location data necessary to combat crime in a specific, defined area or place and with regard to specific persons or groups of persons.

The Chapter of the Working paper named "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)," contains general observations and several possible legislative suggestions about what could harmonise obligations on electronic communications service providers concerning targeted retention.

The Working paper sums up well-known conclusions of the Court of Justice in cases *Tele2* (paragraphs 108 and 111) and *La Quadrature du Net* (paragraphs 148-150) concerning data retention limited to specific categories of persons or to specific geographical areas and based on objective and non-discriminatory factors. In particular, the authors recall 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. The persons thus targeted may, in particular, be persons who have been identified beforehand on the basis of objective evidence, as posing a threat to public or national security. Geographical targeting measures may include areas where 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. It 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.

In the Working paper, the Commission's services suggest that:
„<...> 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 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."

With regard to geographical targeting, the Commission's services propose to consider such targeting parameters as *„an obligation on providers 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.)."* 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.).

With regard to the targeting of specific categories of persons Working paper contains suggestions based on principles of nondiscrimination and objective evidence to consider following parameters: (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 or together with an obligation to retain IP addresses and, possibly, related identifiers that facilitate identification of a user.

It is true that the CJEU in *Quadrature du Net* , paragraph 147, confirmed that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data for the purposes of combating serious crime, preventing serious threats to public security and equally of safeguarding national security, 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. Does it mean that targeted retention may be allowed simply on preventive basis as a kind of periodic risk-assessment by national authorities, or, on the contrary, targeted retention must be permitted only when threat to public 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, as the Working paper seems to suggest? In this respect, the position expressed by the Commission's services seems unclear.

The Court of Justice pointed out in *Commissioner of the Garda Síochána*, paragraph 84, that in any event, the fact that it may be difficult to provide a detailed definition of the circumstances and conditions under which targeted retention may be carried out is no reason for the Member States, by turning the exception into a rule, to provide for the general retention of traffic and location data."

The terms "threat" and "risk" may not be used as synonyms since "threat" is a declaration of the intention or intent to inflict harm, to hurt, destroy, etc., whereas „risk" is a situation involving exposure to danger, a possibility that a dangerous event may happen. Thus, targeted retention cannot be used as purely preventive measure without clear legal safeguards. The terms "threat" and "risk" cannot be synonyms and put in on the same footing in legal formula defining conditions of legality of targeted retention. The Court of Justice used both of them together in *La Quadrature du Net* (paragraph 148) when concluded that Article 15(1) of Directive 2002/58 does not preclude legislation based on objective evidence which makes it possible to target persons whose traffic and location data is 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 Working paper describes specific targeted persons as "individuals whom authorities have a reason to believe have a link to serious crime"and their „known associates". In my opinion, however, such parameter cannot justify the surveillance of broad categories of individuals.

According to the terms of the Working paper, geographical targeting measures „may include areas where 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."

It is true that the Court of Justice in *La Quadrature du Net*, paragraph 150 held that the „limits on a measure providing for the retention of traffic and location data may also be set using a geographical criterion where the competent national authorities consider, on the basis of 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."

Nevertheless, legislative suggestions, even of preliminary character as it is in the Working paper, cannot be limited to lying out or repeating main well-known conclusions of the CJEU. In particular, I doubt that the formula „one or more geographical areas" repeated in the Working paper may be sufficient in drafting legislative proposals without establishing necessary legislative limits and safeguards necessary to avoid general and indiscriminate data retention for the purpose of combating serious crime. This approach of the Commission's

services, as far as the expression „more geographical areas“ is concerned, and especially based only on the existence of a high risk of criminal offences, would extend data retention and surveillance measures to vast territories of the Member States. Shall the specific threat of committing serious crimes in defined areas be necessarily shown and verified, in order to conclude that in these areas the high risk of committing serious criminal acts exists? As for specific targeted persons, in particular “known associates”, what level of objective evidence shall be needed for the retention of their traffic and location data? In such a situation, the combination of both geographical and personal targeting together with objective information about the threat of committing serious crimes may be a reasonable formula allowing to better identify potential criminal offenders and eliminate serious, genuine and present or foreseeable threats of criminal acts.

As for the criterion indicated in the Working paper, 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“, it cannot *per se* justify data retention and access to data without the existence of a serious threat of committing serious criminal acts that is shown to be genuine and present or foreseeable in several specific areas. The criterion of „areas, [where] a situation characterised by a high risk of preparation for or commission of serious criminal offences“ is rather a recognition that such areas exist without the necessity to show that the threat of criminal acts was real. For instance, in such interpretation, „targeted“ geographic data retention may even become general and indiscriminate in broad areas covering a big part of the territory and the infrastructure of a Member State. Reference to „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.“ looks like an extensive enumeration of all possible areas and places and doesn‘t help much in targeting the data retention measure.[20]

Moreover, serious doubts are arising with regard to use in the Working paper of formula "a certain radius around sensitive critical infrastructure sites." By contrast, the CJEU case-law only refers to such sites themselves (without mentioning a "radius"). Under such indefinite and vague formula used in the Working paper, it would be sufficient than an area has an "above average crime rate" (including slightly above average), whereas the CJEU refers to a *high* incidence of *serious* crime ("high" implying more than a little above average). Are "affluent neighborhoods", schools, courts, shopping malls etc. that do not "regularly receive a very high volume of visitors", really "*particularly* vulnerable to the commission of *serious* criminal offences" as it is, on the contrary, required by the case-law of the Court of Justice? Certainly not. When assessing proportionality of data retention measures, it is necessary to take into account that such places as especially the sites of worship and political gatherings host particularly sensitive activities revealing religion and political opinion. Using the unclear notion „certain radius“ with regard to sensitive critical infrastructure sites, in particular with regard to places of worship and political gatherings, means not only lack of

[20] See also note no. 14, page 6 of the Working paper.

legal clarity and certainty: In practical terms, if it would be used in legislative measures on the EU and nationals levels, it could also lead to high risk of non-respect of fundamental rights.

Geographic targeting of general character executed at the same time in multiple areas shall be excluded. On the contrary, this kind of data retention shall be really „targeted“ and allow to obtain necessary information concerning persons posing a threat to public or national security in the Member State concerned and to draw, for the purposes of combating serious crime, conclusions as to their presence and activity in those places or geographical areas at a specific time during the period of retention. In this respect, the CJEU concluded in *Commissioner of the Garda Síochána*:

“81 In addition and above all, a targeted measure of retention covering places or infrastructures which regularly receive a very high volume of visitors, or strategic places, such as airports, stations, maritime ports or tollbooth areas, allows the competent authorities to collect traffic data and, in particular, location data of all persons using, at a specific time, a means of electronic communication **in one of those places**. Thus, such a targeted retention measure may allow those authorities to obtain, through access to the retained data, information as to the presence of those persons in the places or geographical areas covered by that measure as well as their movements between or within those areas and to draw, for the purposes of combating serious crime, conclusions **as to their presence and activity in those places or geographical areas at a specific time during the period of retention.”**

With regard to geographical targeting, I shall conclude that the targeting parameters put forward in the Commission’s services’ suggestions may lead to imposing unjustified legal obligations on providers to retain traffic and location data in very broad, multiple and indefinite geographic areas.

The Court of Justice, in its Judgement of 2 March 2011 in Case C-746/18, *H. K., v Prokuratuur*, paragraph 32, repeatedly held that the question whether the Member States may justify a limitation on the rights and obligations laid down, inter alia, in Articles 5, 6 and 9 of Directive 2002/58, must be assessed by measuring the seriousness of the interference entailed by such a limitation and by verifying that the importance of the public interest objective pursued by that limitation is proportionate to the seriousness of the interference. So far as it concerns the objective of preventing, investigating, detecting and prosecuting criminal offences, which is pursued by the legislation at issue in the main proceedings, in accordance with the principle of proportionality, the only actions to combat serious crime and measures to prevent serious threats to public security are capable of justifying serious interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, such as the interference entailed by the retention of traffic and location data, whether the retention be general and indiscriminate or targeted (paragraph 33). Accordingly, and since general access to all retained data, regardless of whether there is any, at least indirect, link with the intended purpose, cannot be regarded as being limited to what is strictly necessary, the national

legislation concerned must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data in question. In that regard, such access can, as a general rule, be granted, in relation to the objective of fighting crime, only to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime (paragraph 50).

As for specifically targeted persons defined in the Working paper as „known associates" of "individuals whom authorities have a reason to believe have a link to serious crime", it is clear to me that such a parameter is too broad and unclear to justify the surveillance of such undefined category of individuals and the retention of their traffic and location data. It does not correspond to the principles of protection of fundamental rights. Moreover, such a "targeted retention", as suggested by the CJEU in *Tele2*, shall not easily lead to or be perceived as discrimination. In any case, data retention, according to the CJEU, shall be allowed only if it is necessary, shall respect the principle of proportionality and shall not be systematic in nature.

In this respect, the CJEU in *Commissioner of the Garda Síochána* concluded:

"78 Member States thus have, inter alia, the option of imposing retention measures targeting persons who, on the basis of an identification, are the subject of an investigation or other measures of current surveillance or of a reference in the national criminal record relating to an earlier conviction for serious crimes with a high risk of reoffending. Where that identification is based on objective and non-discriminatory factors, defined in national law, targeted retention in respect of persons thus identified is justified."

Certainly, it would be premature to expect that the Working paper must already enumerate in detail all necessary and specific rules for harmonising national legislation in the area which until now remains rather a "grey area" of traffic and localisation data retention.[21] National legislation of many Member States, as cases currently pending or decided by Court of Justice show, contain various extensive models of data retention. Additionally, several Member States remain reticent as to the necessity of EU legislative measures in this area and consider that it is mainly subject to their exclusive competence of protecting national and public security.

[21] It is also interesting to note, that in oral proceedings in Case C-817/19, *Ligue des droits humains,* Case C-817/19, Judge von Danwitz proceeded by pointing out that the notion that locations and behaviors suitable for crime should be subjected to mass surveillance was stretchable to an almost unlimited extent. "Why not rock concerts?", he asked. "Why not museum visits?". Surprisingly, the EU Commission basically agreed with him, saying that yes indeed, rock concerts could be prone to drug-related offenses ("I don't have any police experience, but I could imagine that there could be much drug-related crime occurring at rock concerts."). - See, for instance, recent article of Adam Juszczak and Elisa Sason. Recalibrating Data Retention in the EU. The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning? In: EUCRIM, 2021-4, pp. 238-266. https://eucrim.eu/articles/recalibrating-data-retention-in-the-eu/

The EU and national legislation permitting in exceptional cases to derogate from the fundamental right of personal data protection shall be clear, precise and create legal certainty to all subjects of data processing. AG Petruzella in his Opinion of 27 January 2022 in Case C-817/19, *Ligue des droits humains (paragraphs* 114 and 142) reminded that the Court in *Digital Rights* case emphasized the importance of a clear delimitation of finalities of restrictive measures in the area of fundamental rights. He repeatedly explained that, when measures entailing interferences with the fundamental rights established by the Charter find their source in a legislative act of the Union, it is for the Union legislature to determine, in compliance with the criteria of clarity and precision mentioned above, as well as the principle of proportionality, the exact scope of such interferences. When the instrument chosen by that legislator is a directive, it cannot, in view of the Advocate General, be delegated to the Member States, when transposing it into their national laws, the determination of elements defining the scope of the interference, such as, in the case of limitations to the fundamental rights set out in Articles 7 and 8 of the Charter, the nature and extent of the personal data subject to processing. As the Court of Justice held in *La Quadrature du Net*:

"141. National legislation providing for the general and indiscriminate retention of traffic and location data for the purpose of combating serious crime exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter (see, to that effect, judgment of 21 December 2016, *Tele2*, C-203/15 and C-698/15, EU:C:2016:970, paragraph 107)."

Answer to Question no. 2.

The Commission services' proposal of parameters for geographical targeting and the targeting of specific categories of persons does not comply with the principles of legal clarity and certainty and with the CJEU case-law and fundamental rights insofar as:

- it would allow geographical targeting measures where the competent national authorities consider that there exists, in several geographical areas, a situation characterised by a high risk of preparation for or commission of serious criminal offences and thus making such data retention general and indiscriminatory without establishing necessary legal safeguards;

- with regard to geographical targeting, the parameters suggested by the Commission's services may lead to imposing unjustified legal obligations on providers to retain traffic and location data in very broad, multiple and indefinite geographic areas;

- it would allow the targeted retention of data of „known associates" of "individuals whom authorities have a reason to believe have a link to serious crime" without requiring to verify that such persons represent a specific threat of committing serious criminal acts.

Prof. Dr. iur. Vilenas Vadapalas
Attorney at law, Partner, EUROLEX Law Firm
Former Judge of the General Court of the European Union