Reports of Cases

OPINION OF ADVOCATE GENERAL
CAMPOS SÁNCHEZ-BORDONA
delivered on 18 November 2021 [1]

Joined Cases C-339/20 and C-397/20

VD (C-339/20)
SR (C-397/20)

(Request for a preliminary ruling from the Cour de cassation (Court of Cassation, France))

(Reference for a preliminary ruling – Insider dealing and market manipulation – Directive 2003/6/EC – Article 12(2)(a) and (d) – Regulation (EU) No 596/2014 – Article 23(2)(g) and (h) – Directive 2002/58/EC – Article 15(1) – Supervisory and investigatory powers of the competent authorities – Power of the competent authorities to require existing telephone and exchanged data records – National legislation imposing on electronic communications operators an obligation to retain connection data on a temporary but general basis)

1. The requests for a preliminary ruling which have been joined in these proceedings are closely related to Cases C-793/19, *SpaceNet*, C-794/19, *Telekom Deutschland*, and C-140/20, *Commissioner of the Garda Síochána and Others*, on which I am also delivering my Opinions today. [2]

2. In my Opinions in *SpaceNet and Telekom Deutschland* and in *Commissioner of the Garda Síochána*, I set out my reasons for suggesting that the Court give the Bundesverwaltungsgericht (Federal Administrative Court, Germany) and the Supreme Court (Ireland) answers in line with the case-law relating to Directive 2002/58/EC, [3] as 'summarised' in the judgment in *La Quadrature du Net*. [4]

3. It is true, however, that the two requests for a preliminary ruling submitted by the Cour de cassation (Court of Cassation, France) are directly concerned not with Directive 2002/58 but with Directive 2003/6/EC [5] and Regulation (EU) No 596/2014. [6]

1 Original language: Spanish.

2 'Opinion in *SpaceNet and Telekom Deutschland*' and 'Opinion in *Commissioner of the Garda Síochána*', respectively.

3 Directive 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 (Directive on privacy and electronic communications) (OJ 2002 L 201, p. 37).

4 Judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791; 'the judgment in *La Quadrature du Net*').

5 Directive of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse) (OJ 2003 L 96, p. 16).

6 Regulation of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6 and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC (OJ 2014 L 173, p. 1).

4. Nonetheless, the issue in these two sets of proceedings is, in essence, the same as that in the abovementioned references for a preliminary ruling, namely whether Member States may impose an obligation to retain electronic communications traffic data in a general and indiscriminate manner. [7]

5. For that reason, although this case has to do with Directive 2003/6 and Regulation No 596/2014 (which are intended to combat dealings classifiable as market abuse), [8] I consider the Court's case-law as condensed in the judgment in *La Quadrature du Net* to be applicable in this context.

I. Legislative framework

A. European Union law

1. Directive 2002/58

6. According to Article 1 ('Scope and aim'):

'1. This Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the [Union].

2. The provisions of this Directive particularise and complement Directive 95/46/EC [of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31)] for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the [TFEU], such as those covered by Titles V and VI of the Treaty on European Union, 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.'

7. Article 2 ('Definitions') provides:

'Save as otherwise provided, the definitions in Directive 95/46/EC and in Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [(OJ 2002 L 108, p. 33)] shall apply.

[7] In this instance, location data appear to be excluded, although the dividing line between the two is not at all clear.

[8] In its broad sense – the sense in which I shall be using it in this Opinion – the term 'market abuse' encompasses 'unlawful behaviour in the financial markets and, for the purposes of this Regulation, it should be understood to consist of insider dealing, unlawful disclosure of inside information and market manipulation' (recital 7 of Regulation No 596/2014).

The following definitions shall also apply:

…

(b) "traffic data" means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

(c) "location data" means any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

…'

8. Article 15(1) states:

'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.'

2. Directive 2003/6

9. In accordance with Article 11:

'Without prejudice to the competences of the judicial authorities, each Member State shall designate a single administrative authority competent to ensure that the provisions adopted pursuant to this Directive are applied.

…'

10. Article 12 states:

'1. The competent authority shall be given all supervisory and investigatory powers that are necessary for the exercise of its functions. …

2. Without prejudice to Article 6(7), the powers referred to in paragraph 1 of this Article shall be exercised in conformity with national law and shall include at least the right to:

(a) have access to any document in any form whatsoever, and to receive a copy of it;

…

(d) require existing telephone and existing data traffic records;

…’

3. Regulation No 596/2014

11. The regulation contains these recitals:

‘(1) A genuine internal market for financial services is crucial for economic growth and job creation in the Union.

(2) An integrated, efficient and transparent financial market requires market integrity. The smooth functioning of securities markets and public confidence in markets are prerequisites for economic growth and wealth. Market abuse harms the integrity of financial markets and public confidence in securities and derivatives.

…

(62) A set of effective tools and powers and resources for the competent authority of each Member State guarantees supervisory effectiveness. Accordingly, this Regulation, in particular, provides for a minimum set of supervisory and investigative powers competent authorities of Member States should be entrusted with under national law. Those powers should be exercised, where the national law so requires, by application to the competent judicial authorities. …

…

(65) Existing recordings of telephone conversations and data traffic records from investment firms, credit institutions and financial institutions executing and documenting the execution of transactions, as well as existing telephone and data traffic records from telecommunications operators, constitute crucial, and sometimes the only, evidence to detect and prove the existence of insider dealing and market manipulation. Telephone and data traffic records may establish the identity of a person responsible for the dissemination of false or misleading information or that persons have been in contact at a certain time, and that a relationship exists between two or more people. Therefore, competent authorities should be able to require existing recordings of telephone conversations, electronic communications and data traffic records held by an investment firm, a credit institution or a financial institution in accordance with Directive 2014/65/EU. Access to data and telephone records is necessary to provide evidence and investigate leads on possible insider dealing or market manipulation, and therefore for detecting and imposing sanctions for market abuse. … Access to telephone and data traffic records held by a telecommunications operator does not encompass access to the content of voice communications by telephone.

(66) While this Regulation specifies a minimum set of powers competent authorities should have, those powers are to be exercised within a complete system of national law which guarantees the respect for fundamental rights, including the right to privacy. For the exercise of those powers, which may amount to serious interferences with the right to respect for private and family life, home and communications, Member States should have in place adequate and effective safeguards against any abuse, for instance, where appropriate a requirement to obtain prior authorisation from the judicial authorities of a Member State concerned.

Member States should allow the possibility for competent authorities to exercise such intrusive powers to the extent necessary for the proper investigation of serious cases where there are no equivalent means for effectively achieving the same result.

…

(77) This Regulation respects the fundamental rights and observes the principles recognised in the Charter of Fundamental Rights of the European Union [('the Charter')]. Accordingly, this Regulation should be interpreted and applied in accordance with those rights and principles. …

…'

12. Article 1 ('Subject matter') provides:

'This Regulation establishes a common regulatory framework on insider dealing, the unlawful disclosure of inside information and market manipulation (market abuse) as well as measures to prevent market abuse to ensure the integrity of financial markets in the Union and to enhance investor protection and confidence in those markets.'

13. Article 3 ('Definitions') states, in point 27 of paragraph 1, that, for the purposes of the regulation, 'data traffic records' means 'records of traffic data as defined in point (b) of the second paragraph of Article 2 of Directive 2002/58/EC …'.

14. Article 22 ('Competent authorities') stipulates:

'Without prejudice to the competences of the judicial authorities, each Member State shall designate a single administrative competent authority for the purpose of this Regulation. …'

15. Article 23 ('Powers of competent authorities') states:

'…

2. In order to fulfil their duties under this Regulation, competent authorities shall have, in accordance with national law, at least the following supervisory and investigatory powers:

(a) to access any document and data in any form, and to receive or take a copy thereof;

…

(g) to require existing recordings of telephone conversations, electronic communications or data traffic records held by investment firms, credit institutions or financial institutions;

(h) to require, insofar as permitted by national law, existing data traffic records held by a telecommunications operator, where there is a reasonable suspicion of an infringement and where such records may be relevant to the investigation of an infringement of point (a) or (b) of Article 14 or Article 15;

…

3. Member States shall ensure that appropriate measures are in place so that competent authorities have all the supervisory and investigatory powers that are necessary to fulfil their duties.

…

4. A person making information available to the competent authority in accordance with this Regulation shall not be considered to be infringing any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the person notifying in liability of any kind related to such notification.'

16. In accordance with Article 28 ('Data protection'):

'With regard to the processing of personal data within the framework of this Regulation, competent authorities shall carry out their tasks for the purposes of this Regulation in accordance with the national laws, regulations or administrative provisions transposing Directive 95/46/EC. With regard to the processing of personal data by [the European Securities and Markets Authority (ESMA)] within the framework of this Regulation, ESMA shall comply with the provisions of Regulation (EC) No 45/2001 [of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001 L 8, p. 1)].

Personal data shall be retained for a maximum period of five years.'

B. National law

1. Code monétaire et financier (Monetary and financial code; 'the CMF')

17. The first paragraph of Article L. 621-10 of the CMF, in the version in force at the material time, provided:

'Where necessary for the purposes of investigation or inspection, investigators or inspectors may require the disclosure of any documents on any medium. Investigators may also require data retained and processed by telecommunications operators under Article L. 34-1 of the Code des postes et des communications électroniques (Post and electronic communications code; 'the CPCE') and the service providers referred to in Article 6(I)(1) and (2) of Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (Law No 2004-575 of 21 June 2004 on confidence-building in the digital economy; "Law No 2004-575") and receive a copy thereof. …'

18. According to Article L. 621-10-2 of the CMF applicable in the present case:

'For the purposes of investigating market abuse … investigators may require data retained and processed by telecommunications operators, under the conditions and within the limits laid down in Article L. 34-1 of the [CPCE], and by the providers referred to in Article 6(I)(1) and (2) of [Law No 2004-575].

Conveyance of the data mentioned in the first paragraph of this article shall be the subject of prior authorisation by a connection data requests controller.

…’

2. The CPCE

19. According to Article L. 34-1 of the CPCE in force at the material time:

‘…

II. Electronic communications operators … shall erase or anonymise all traffic data, without prejudice to the provisions of paragraph III …

…

III. For the purposes of the investigation, detection and prosecution of criminal offences … operations aimed at erasing or anonymising certain categories of technical data may be deferred for a maximum period of one year. …

…

VI. Data retained and processed under the conditions defined in paragraphs III, IV and V shall relate exclusively to the identification of the users of the services supplied by providers, the technical characteristics of the communications effected by the latter and the location of the terminal equipment.

Such data may not under any circumstances relate to the content of the correspondence exchanged or the information consulted, in whatever form, in the course of those communications.

…’

20. Article R. 10-13 of the CPCE provided:

‘I. In accordance with Article L. 34-1(III), electronic communications operators shall retain, for the purposes of the investigation, detection and prosecution of criminal offences:

(a) information by which the user may be identified;

(b) data relating to the communications terminal equipment used;

(c) the technical characteristics, date, time and duration of each communication;

(d) data relating to the additional services requested or used and the providers thereof;

(e) data by which the addressee(s) of the communication may be identified.

II. In the case of telephony activities, the operator shall retain the data referred to in paragraph II and, in addition, any data by which the origin and location of the communication may be identified.

III. The data referred to in this article shall be retained for one year from the date of the registration thereof.

…'

21. The referring court notes that such connection data consist of data which, having been generated or processed as a result of a communication, relate to the circumstances of that communication and to the users of the service, to the exclusion of any indication as to the content of the messages.

II. Facts, disputes and questions referred

22. The facts forming the basis of these two references for a preliminary ruling are, in essence, the same.

23. Further to an application made by the public prosecutor on 22 May 2014, a judicial investigation was launched in respect of acts constituting the offence of insider dealing and concealment.

24. On 23 and 25 September 2015, the Autorité des marchés financiers (Financial Markets Authority; 'the AMF') sent the Public Prosecutor's Office a report enclosing documents from an investigation, carried out by that authority, that included, in particular, personal data relating to the use of telephone lines.

25. In order to collect the data relating to the use of those telephone lines, officers from the AMF had relied on Article L. 621-10 of the CMF.

26. Following that report, the scope of the judicial investigation was extended, further to three supplementary applications to that effect made on 29 September and 22 December 2015 and 23 November 2016, to include certain securities and related financial instruments, on the grounds of the same offences and the further offences of aiding and abetting, corruption and money laundering.

27. Having been charged with carrying out acts in connection with those securities that constitute the offences of insider dealing and money laundering, VD and SR made an application for annulment by which they sought to have certain procedural documents excluded for infringement of, inter alia, Articles 7, 8, 11 and 52 of the Charter and Article 15 of Directive 2002/58.

28. Their claims having been dismissed by judgments of 20 December 2018 and 7 March 2019, respectively, of the chambre de l'instruction de la cour d'appel de Paris, 2e section (Indictment Division of the Court of Appeal, Paris, Second Section, France), the defendants appealed those judgments to the Cour de cassation (Court of Cassation), which has referred the following questions to the Court of Justice for a preliminary ruling:

'(1) Do Article 12(2)(a) and (d) of Directive 2003/6 … and Article 23(2)(g) and (h) of Regulation … No 596/2014 …, read in the light of recital 65 of that regulation, not imply that, account being taken of the covert nature of the information exchanged and the fact that the potential subjects of investigation are members of the general public, the national legislature must be able to require electronic communications operators to retain connection data on a

temporary but general basis in order to enable the administrative authority referred to in Article 11 of the Directive and Article 22 of the Regulation, in the event of the emergence of grounds for suspecting certain persons of being involved in insider dealing or market manipulation, to require the operator to surrender existing records of traffic data in cases where there are reasons to suspect that the records so linked to the subject matter of the investigation may prove relevant to the production of evidence of the actual commission of the breach, to the extent, in particular, that they offer a means of tracing the contacts established by the persons concerned before the suspicions emerged?

(2) If the answer given by the Court of Justice is such as to prompt the Cour de cassation (Court of Cassation) to form the view that the French legislation on the retention of connection data is not consistent with EU law, could the effects of that legislation be temporarily maintained in order to avoid legal uncertainty and to enable data previously collected and retained to be used for one of the objectives of that legislation?

(3) May a national court temporarily maintain the effects of legislation enabling the officials of an independent administrative authority responsible for investigating market abuse to obtain access to obtain connection data without prior review by a court or another independent administrative authority?'

III. Procedure before the Court of Justice

29. The requests for a preliminary ruling were registered at the Court on 24 July 2020 and 20 August 2020 respectively.

30. Written observation were lodged by VD, SR, the Spanish, Estonian and French Governments, Ireland, the Polish and Portuguese Governments and the European Commission.

31. The hearing held on 14 September 2021 was attended by VD, SR, the French, Danish, Estonian and Spanish Governments, Ireland, the European Commission and the European Data Protection Supervisor.

IV. Analysis

A. Preliminary considerations

32. The national legislation relevant to these two sets of proceedings have been the subject of a number of domestic court rulings which warrant mention.

1. Judgment of the Conseil constitutionnel (Constitutional Council, France) of 21 July 2017

33. The referring court has noted that the first paragraph of Article L. 621-10 of the CMF was declared unconstitutional by judgment of the Conseil constitutionnel (Constitutional Council) of 21 July 2017. [9]

[9] The Conseil constitutionnel (Constitutional Council) held the procedure used by the AMF to access connection data to be incompatible with the right to privacy, protected by Article 2 of the Declaration of the Rights of Man and of the Citizen.

34. However, the Conseil constitutionnel (Constitutional Council) postponed the effects of the declaration of unconstitutionality until 31 December 2018.

35. In the meantime, the national legislature introduced into the CMF Article L. 621-10-2, which established a system of prior authorisation, to be given by an independent administrative authority, for accessing connection data.

36. According to the referring court:

– given that the effects of the declaration as to the unconstitutionality of the first paragraph of Article L. 621-10 of the CMF – in force at the time of the events at issue in the main sets of proceedings – were postponed, that provision cannot be held to be invalid; [10]

– nonetheless, such a provision, in so far as it did not make access to connection data subject to prior review by a court or an independent administrative authority, 'was not consistent with the requirements laid down in Articles 7, 8 and 11 of the Charter …, as interpreted by the [Court of Justice]'. [11]

37. On that basis, the Cour de cassation (Court of Cassation) concludes that the 'only question that arises is whether the consequences of the incompatibility of Article L. 621-10 of the [CMF] may be postponed'. [12]

38. The referring court, therefore, is not asking whether Article L. 621-10 of the CMF is compatible with EU law but, on the basis of its incompatibility with several provisions of the Charter, only whether, as was the case under domestic law with the effects of the declaration as to the unconstitutionality of that provision, the legal effects attendant upon its inconsistency with EU law may also be delayed. This forms the subject of the third question.

2. Judgment of 21 April 2021 of the Conseil d'État (Council of State, France)

39. Following the submission of these two requests for a preliminary ruling, the Conseil d'État (Council of State) gave judgment, on 21 April 2021, [13] in the proceedings which had led to the raising of the request for a preliminary ruling culminating in the judgment in *La Quadrature du Net*.

40. In that judgment, the Conseil d'État (Council of State) decided to disapply Article L. 34-1 of the CPCE and to order the government to repeal Article R. 10-13 of the CPCE within six months, on the ground that those provisions do not properly limit the purposes of the obligation to retain traffic and location data on a general and indiscriminate basis. [14]

[10] Paragraph 28 of the order for reference in Case C-339/20 and paragraph 43 of the order for reference in Case C-397/20.

[11] Cited above.

[12] Paragraphs 29 and 44 of the respective orders for reference.

[13] Judgment No 393099 (ECLI:FR:CEASS:2021:393099.20210421). I cannot of course comment in the course of this case on the content of that judgment from the point of view of the consistency with EU law of the passages or findings contained in it (in particular, those relating to access for other purposes to data retained on national security grounds) or from the point of view of its interpretation of the judgment in *La Quadrature du Net*. At the hearing, the Commission stated that it was considering whether any kind of response in opposition to that judgment was called for, although it had not as yet come to any decision in that regard.

[14] The Court gave the parties the opportunity to comment on that judgment at the hearing.

41. The Conseil d'État (Council of State) referred to the consistency of the national provisions at issue here with Directive 2002/58. In its view, the answer given by the Court in the judgment in *La Quadrature du Net* supports the inference that they should either be disapplied (*écarter*) in the main proceedings (namely, Article L. 34-1 of the CPCE), [15] or repealed (namely, Article R. 10-13 of the CPCE). [16]

42. The relevance of the judgment in *La Quadrature du Net* to the answer to be given to the first question raised in these references is particularly acute given that that judgment had already taken into account, among other provisions, Article R. 10-13 of the CPCE, [17] which, together with Article L. 34-I of the CPCE, is key to the application of Article L. 621-10 of the CMF.

43. I would recall that, in order to collect data relating to the use of the telephone lines used by the persons suspected of having committed the breaches forming the subject of the investigation into possible market abuse, the officials from the administrative authority relied specifically on Article L. 621-10 of the CMF.

3. Whether the requests for a preliminary ruling have become devoid of purpose

44. As I have already said, the referring court wishes to ascertain whether the national legislation at issue is compatible with Directive 2003/6 and Regulation No 596/2014, in so far as both of those texts may provide a specific basis for the obligation to retain data that is separate from that contained in Directive 2002/58.

45. If that is the case, it is my view that the requests for a preliminary ruling have not become devoid of purpose, notwithstanding the impact which the judgments of the French courts mentioned above might have on that national legislation:

– First, the possibility cannot be ruled out that, under domestic law, Article R. 10-13 of the CPCE may have some effect on the main proceedings, a question which it is for the referring court to answer.

– Secondly, the instruction given to the government by the Conseil d'État (Council of State) not only imposes an obligation formally to repeal that provision but also contains a number of guidelines on the conditions that must be met by any legislation enacted to replace the legislation to be repealed. [18]

15 Paragraph 58 of the judgment of the Conseil d'État (Council of State).

16 Article 2 of the operative part of the judgment of the Conseil d'État (Council of State).

17 Judgment in *La Quadrature du Net*, paragraph 70: 'As regards Article R. 10-13 of the CPCE and the obligation of general and indiscriminate retention of communications data laid down therein, the referring court … observes that such retention allows a judicial authority to access data relating to communications made by an individual before being suspected of having committed a criminal offence, with the result that such retention is of unparalleled usefulness for the investigation, detection and prosecution of criminal offences.'

18 At the hearing, the French Government reported on the adoption of Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement (Law No 2021-998 of 30 July 2021 on the prevention of acts of terrorism and the intelligence services) (JORF No 176 of 31 July 2021). Article 17 thereof amends Article L. 34-1 of the CPCE. It is for a subsequent decree to determine, 'on the basis of the activities of the operators and the nature of the communications, the information and categories of data retained under [paragraphs] IIa and III, as amended', of Article L. 34 of the CPCE.

46. Thus, the Conseil d'État (Council of State) does not confine itself to imposing on the government an obligation to repeal Article R. 10-13 of the CPCE within a period of six months, but explicitly requires it to 'limit the purposes pursued by these articles and to adapt the regulatory framework relating to the retention of connection data'. [19]

47. Consequently, the Court's ruling on the merits may be of use to the referring court, since:

– Directive 2003/6 and Regulation No 596/2014 might, hypothetically, offer an independent basis separate from that available under Directive 2002/58 for the retention of traffic data.

– Directive 2003/6 and Regulation No 596/2014 might contain particular and specific conditions in connection with the purposes of data retention.

B. First question referred

48. The first question concerns Article 12(2)(a) and (d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014.

49. Those provisions allow competent administrative authorities to require electronic communications undertakings (and, where appropriate, investment firms, credit institutions or financial institutions) to provide existing data traffic and telephone data records [20] where there is a reasonable suspicion that an infringement constituting market abuse has been committed and those records may be relevant to their investigation.

50. The premiss from which the referring court starts is that access to those records presupposes that 'the national legislature … require[s] electronic communications operators to retain connection data on a temporary but general basis in order to enable the administrative authority … to require the operator to surrender existing records of traffic data …, to the extent, in particular, that they offer a means of tracing the contacts established by the persons concerned before the suspicions emerged'.

51. Now, as regards the obligation to retain connection data on a general and indiscriminate basis in fields other than national security (for the purposes of this case, in the field of combating market abuse), the Court's case-law as *summarised* in the judgment in *La Quadrature du Net* is fully valid.

1. Where there is an independent legal basis for the obligation to retain data in Directive 2003/6 and Regulation No 596/2014

52. It is true that the case-law in the judgment in *La Quadrature du Net* was established in relation to Directive 2002/58, whereas the provisions referred to by the Cour de cassation (Court of Cassation) are Directive 2003/6 and Regulation No 596/2014.

[19] Paragraph 59 of the judgment of the Conseil d'État (Council of State). In particular, and as is clear from Article 1 of the operative part of that judgment, the adaptation required must include 'a periodic review of the existence of a serious, genuine and present or foreseeable threat to national security'.

[20] According to Article 3 of Regulation No 596/2014, 'traffic data records' means records of traffic data as defined in point (b) of the second paragraph of Article 2 of Directive 2002/58, that is to say 'any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof'.

53. However, Directive 2002/58 is the provision of reference in matters relating, as its title states, to 'the processing of personal data and the protection of privacy in the electronic communications sector'.

54. Both Directive 2003/6 (which is specifically concerned with insider dealing and market manipulation) and Regulation No 596/2014 (which deals with market abuse) include provisions which, like those listed in the first question raised in these references, relate to the *processing* of data traffic records.

55. They are, therefore, provisions which, in that particular regard, and purely by virtue of their purpose and subject matter, must be interpreted within the context of the regime established by Directive 2002/58.

56. This follows, in my opinion, from Article 12(2)(d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014:

– the first of those provisions concerns the right to 'require … *existing* data traffic records'; [21]

– Article 23(2)(g) of Regulation No 596/2014 concerns '*existing* recordings of telephone conversations, electronic communications or data traffic records *held* by investment firms, credit institutions or financial institutions'; [22]

– finally, Article 23(2)(h) also speaks of '*existing* data traffic records *held* by a telecommunications operator …'. [23]

57. To my mind, none of those provisions grants specific powers – separate from those provided for in Directive 2002/58 – to *retain* data. They are confined to authorising competent authorities to *access* (*existing*) retained data in accordance with the legislation that generally governs the processing of such personal data in the electronic communications sector, that is to say, Directive 2002/58.

58. Neither could Article 28 of Regulation No 596/2014 (an interpretation of which, moreover, the referring court does not ask for) be claimed to be an independent legal basis for imposing an obligation to retain data in this field.

59. That provision, under the heading 'Data protection' and in connection once again with the 'processing of personal data':

– reaffirms the right, and at the same time the duty, of competent authorities to carry out 'their tasks for the purposes of this Regulation in accordance with the national laws, regulations or administrative provisions transposing Directive 95/46/EC';

21 Emphasis added.

22 Emphasis added.

23 Emphasis added.

– does not mention the obligation to retain data [24] imposed on electronic communications undertakings, but simply makes a reference to Directive 95/46 [25] when it comes to data protection.

60. The fact that Directive 2003/6 and Regulation No 596/2014 are silent on the matter of the data retention requirement imposed on electronic communications operators is understandable given their proximity in time to Directive 2002/58. The European legislature already had the latter directive as an exhaustive reference framework for outlining the features of (and exceptions to) that obligation and there was therefore no need to create a retention regime specifically aimed at combating market abuse.

61. It follows that the Court's interpretation of Directive 2002/58 must naturally be extended to the data retention tools which, although in the possession of electronic communications operators, may be used by investigating authorities in the course of combating market abuse.

62. The 'existing records' referred to in Directive 2003/6 and Regulation No 596/2014 can only be '*lawfully* existing records', that is to say those compiled in accordance with Directive 2002/58. It is that directive which, in EU law, 'provides, inter alia, for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communications sector'. [26]

63. The 'existing records' can be shown to be *lawful* only where their existence is covered by the provisions of Directive 2002/58.

64. The French Government is opposed to that proposition. It submits that the Court's reply must be confined to an interpretation of Directive 2003/6 and Regulation No 596/2014. In its contention, both of those texts implicitly authorise Member States to lay down an obligation of general and indiscriminate retention. Their effectiveness would otherwise be seriously undermined.

65. I do not share the French Government's views but, even if I were to accept them, the fact remains that the alleged 'implicit authorisation' would still be subject to the conditions which, in accordance with the Court's case-law, apply to Member States when they take up the option to impose an obligation of general and indiscriminate data retention under Directive 2002/58.

66. In other words, if it were to be accepted, hypothetically, that Directive 2003/6 and Regulation No 596/2014 provide an independent basis for data retention (*quod non*), such retention would be subject to the same conditions as would necessarily apply if it were based on any other EU legislative provision.

[24] It does, however, lay down a data retention period of five years.

[25] Directive repealed by 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, and repealing Directive 95/46 (General Data Protection Regulation) (OJ 2016 L 119, p. 1). I should recall that, in the judgment in *La Quadrature du Net*, paragraph 210, the Court held that, '… as is the case for Article 15(1) of Directive 2002/58, the power conferred on Member States by Article 23(1) of Regulation 2016/679 may be exercised only in accordance with the requirement of proportionality, according to which derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary (see, by analogy, with regard to Directive 95/46, judgment of 7 November 2013, *IPI*, C-473/12, EU:C:2013:715, paragraph 39 and the case-law cited)'.

[26] The judgment in *La Quadrature du Net*, paragraph 91.

67. The reason for this is that those conditions derive ultimately from the need to safeguard the fundamental rights guaranteed by the Charter, respect for which is referred to in Directive 2003/6 and Regulation No 596/2014. Those are the very rights which the Court invoked in the case-law in *La Quadrature du Net*.

68. Not even the French Government – or indeed any of the other parties that have intervened in these proceedings – was able to avoid making reference to the case-law contained in that judgment. Some parties (such as the Portuguese Government and the Commission) have emphasised that that case-law serves as a guide for answering the questions referred for a preliminary ruling in this case; others (such as, in particular, Ireland) have explicitly requested that it be revised.

69. The debate prompted by these proceedings has therefore focused on whether to endorse or revise the Court's case-law on the lawfulness of the general and indiscriminate retention of traffic and location data in the field of electronic communications.

2. Prohibition of the general and indiscriminate retention of traffic data and legislative measures to protect national security or to combat serious crime

70. As I argued in my Opinions in *Commissioner of the Garda Síochána* and in *SpaceNet and Telekom Deutschland*, delivered today, I do not consider it appropriate to revise the Court's case-law on Article 15(1) of Directive 2002/58.

71. In that context, the essential components of the answer to be given to the referring court flow directly, in my view, from the Court's case-law as *summarised* in the judgment in *La Quadrature du Net*.

72. I should therefore begin by recalling the case-law established by the Court in that judgment, paragraph 168 of which sums it up as follows:

'Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding legislative measures which, for the purposes laid down in Article 15(1), provide, as a preventive measure, for the general and indiscriminate retention of traffic and location data. By contrast, Article 15(1), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, does 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 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;

— provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of IP addresses assigned to the source of an Internet connection for a period that is limited in time to what is strictly necessary;

— provide, for the purposes of safeguarding national security, combating crime and safeguarding public security, for the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems;

— 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,

provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.'

73. At the heart of the Court's case-law in relation to Directive 2002/58 is the idea that users of electronic communications systems are entitled to expect that, in principle, their communications and data relating to them will remain anonymous and may not be recorded, unless they have agreed otherwise. [27]

74. Article 15(1) of Directive 2002/58 permits exceptions to the obligation to guarantee confidentiality. The judgment in *La Quadrature du Net* examines at length how those exceptions can be reconciled with the fundamental rights the exercise of which may be affected. [28]

75. According to the Court, the general and indiscriminate retention of traffic data could be justified only by the objective of safeguarding national security, the importance of which 'goes beyond that of the other objectives referred to in Article 15(1) of Directive 2002/58'. [29]

76. In that case (national security), the Court held that that provision, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, 'does not, in principle, preclude *a legislative measure which permits the competent authorities to order* providers of electronic communications services *to retain* traffic and location data of all users of electronic communications systems *for a limited period of time*, as long as there are sufficiently solid grounds for considering that the Member State concerned is confronted with a serious threat … which is shown to be genuine and present or foreseeable'. [30]

[27] The judgment in *La Quadrature du Net*, paragraph 109.

[28] *Ibidem*, paragraphs 111 to 133.

[29] *Ibidem*, paragraph 136.

[30] *Ibidem*, paragraph 137 (emphasis added). This is true, the Court goes on, 'even if such a measure is applied indiscriminately to all users of electronic communications systems, without there being at first sight any connection … with a threat to the national security of that Member State', in which case it must be 'considered that the existence of that threat is, in itself, capable of establishing that connection' (cited above).

77. In particular, the Court takes the view that the 'objective of safeguarding national security' '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'. [31]

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).

81. There is no doubt that market abuse is reprehensible, since it harms 'the integrity of financial markets and public confidence in securities [and] derivatives'. By the same token, such abuse may, depending on the case, constitute a punishable breach or, in the worst scenario, a serious criminal offence. [32]

82. Accordingly, when referring to mutual cooperation between the competent authorities of the Member States in preventing and combating serious crime affecting two or more Member States or a common interest protected by a Union policy, Annex I to Regulation (EU) 2016/794 [33] encompasses within that concept, along with other punishable conduct, 'insider dealing and financial market manipulation'.

83. However, its nature as a criminal offence, even a serious one in some cases, is no different from the potential criminal nature of many other breaches contrary to important public interests and EU policies. Annex I to Regulation 2016/794 lists, among other examples of serious crime, drug trafficking; money-laundering activities; immigrant smuggling; trafficking in human beings;

[31] The judgment in *La Quadrature du Net*, paragraph 135. It is true, as I note in point 39 of my Opinion in *SpaceNet and Telekom Deutschland*, that those stipulations give rise to a more rigorous and stricter regime than that which flows from the case-law of the European Court of Human Rights (ECtHR) concerning Article 8 of the European Convention on Human Rights and Fundamental Freedoms. This is of course allowed by Article 52(3), *in fine*, of the Charter. The fact remains, however, as I state in point 40 of that Opinion, that the case-law established by the ECtHR in its judgments of 25 May 2021, *Big Brother Watch and Others v. the United Kingdom* (CE:ECHR:2021:0525JUD005817013) and *Centrum för rättvisa v. Sweden* (CE:ECHR:2021:0525JUD003525208), as well as in the judgment of 4 December 2015, *Roman Zakharov v. Russia* (CE:ECHR:2015:1204JUD004714306), concerns situations which are not comparable with those at issue in these references for a preliminary ruling. In short, the solution must be found in the application of national legislation considered to be consistent with the *exhaustive* rules laid down in Directive 2002/58, as interpreted by the Court.

[32] See Directive 2014/57/EU of the European Parliament and of the Council of 16 April 2014 on criminal sanctions for market abuse (market abuse directive) (OJ 2014 L 173, p. 179).

[33] Regulation of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ 2016 L 135, p. 53).

kidnapping, illegal restraint and hostage-taking; crime against the financial interests of the European Union; counterfeiting and product piracy; computer crime; corruption; and environmental crime, including ship-source pollution.

84. The public interests protected through the criminalisation of some of the aforementioned behaviours may be as important as, or more important than, those protected through the punishment of market abuse. This does not mean, however, that such conduct entails a threat to national security within the meaning of the judgment in *La Quadrature du Net*.[34]

85. As the Commission maintained at the hearing, the objectives pursued by Directive 2003/6 and Regulation No 596/2014 are geared towards achieving an internal market (in particular, in the financial markets sector) but not towards preserving national security.[35]

86. Extending the concept of a 'threat to national security' to market abuse offences would open the door to the same approach being taken to many other infringements of public interests which are no less important but which a criminal court would struggle to bring within that far more restrictive concept. If the Court were to agree to open that door, the careful balance underlying the judgment in *La Quadrature du Net* would have been futile.

87. In short, the 'existing' records/recordings referred to in Article 12(2)(d) of Directive 2003/6 and Article 23(2)(g) and (h) of Regulation No 596/2014 must necessarily be those which Directive 2002/58, as interpreted by the Court, allows to be retained for the purposes of combating serious crime and safeguarding public security. Under no circumstances can they be considered to be the same as those retained on a preventive, general and indiscriminate basis for the purposes of safeguarding national security.

C. Second question referred

88. By the second question, the referring court wishes to ascertain whether, in the event that the French legislation on the retention of connection data is not compatible with EU law, its effects can be temporarily maintained.

89. Given the date of its references, the referring court could not have taken into account that the answer to its question is to be found in the judgment (of 6 October 2020) in *La Quadrature du Net* (in particular, in paragraphs 213 to 228 thereof), which has adhered to the traditional case-law in this regard.

90. According to the Court, once an infringement of Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, has been established, 'the referring court cannot apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality which it is bound to make under that law in respect of the national legislation at issue in the main proceedings'.[36]

[34] As regards the possibility of creating a *tertium genus* of criminal offence halfway between crimes against national security and serious crime, I refer to points 51 and 52 of my Opinion in *Commissioner of the Garda Síochána*.

[35] Taking a more critical stance, defence counsel for VD recalled in oral intervention that national security has been linked to numerous categories of criminal offence in totalitarian political systems, which find threats to State security at every turn.

[36] The judgment in *La Quadrature du Net*, paragraph 220.

91. The reason is that 'only the Court may, in exceptional cases, on the basis of overriding considerations of legal certainty, allow the temporary suspension of the ousting effect of a rule of EU law with respect to national law that is contrary thereto'. [37] 'Such a restriction on the temporal effects of the interpretation of that law, made by the Court, may be granted only in the actual judgment ruling upon the interpretation requested', [38] which was not the case in the judgment of 8 April 2014, *Digital Rights Ireland and Others*. [39]

92. Consequently, if the Court did not consider it appropriate to limit the temporal effects of its interpretation of Directive 2002/58, the referring court cannot decide to extend the effects of national legislation which is incompatible with provisions of EU law which, as in the case of Directive 2003/6 and Regulation No 596/2014, must be interpreted in the light of the former directive.

D. Third question referred

93. In the same vein as the previous question, the third question referred by the Cour de cassation (Court of Cassation) is intended to ascertain whether a national court may temporarily maintain the effects of legislation 'enabling the officials of an independent administrative authority responsible for investigating market abuse to obtain access to obtain connection data without prior review by a court or another independent administrative authority'.

94. The premiss for this question is, once again, that that legislation is intrinsically incompatible with EU law. [40] Moreover, it was found to be so by the referring court itself, which stated that, even though the AMF is an independent administrative authority, 'the power conferred on its investigators to obtain connection data without prior review by a court or another independent administrative authority was not consistent with the requirements laid down in Articles 7, 8 and 11 of the Charter … as interpreted by the [Court of Justice]'. [41]

95. The same outcome is arrived at in the judgment of the Court of Justice of 2 March 2021, *Prokuratuur (Conditions of access to data relating to electronic communications)*, [42] paragraph 51 et seq. of which emphasise that access by the competent national authorities to retained data must be made subject to a prior review carried out either by a court or by an independent administrative authority, which must be a third party in relation to the authority which requests access to those data.

96. In those circumstances, the answer to the third question must be identical to the answer to the second.

[37] *Ibidem*, paragraph 216.

[38] Cited above.

[39] C-293/12 and C-594/12, EU:C:2014:238.

[40] As I have already recalled, the Conseil Constitutionnel (Constitutional Council) annulled Article L. 621-10 of the CMF. The judgment of the Conseil d'État (Council of State) of 21 April 2021 recognises at various points that access to data must be preceded by review by a court or an independent authority vested with binding powers.

[41] Paragraph 28 and 43 of the orders for reference. The case-law to which it refers comes from the judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970, paragraph 120).

[42] Case C-746/18, EU:C:2021:152.

V. Conclusion

97. In the light of the foregoing, I suggest that the Court's answer to the Cour de cassation (Court of Cassation, France) should be as follows:

(1) Article 12(2)(a) and (d) of Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse), and Article 23(2)(g) and (h) of Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (market abuse regulation) and repealing Directive 2003/6/EC of the European Parliament and of the Council and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC, must be interpreted as meaning that they preclude national legislation which imposes on electronic communications undertakings an obligation to retain traffic data on a general and indiscriminate basis in the context of an investigation into insider dealing or market manipulation and abuse.

(2) A national court cannot limit in time the effects of the incompatibility with EU law of domestic legislation which imposes on providers of electronic communications services an obligation to retain traffic data on a general and indiscriminate basis which is incompatible with Article 15(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 (Directive on privacy and electronic communications), read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter of Fundamental Rights of the European Union, and which allows the administrative authority responsible for carrying out investigations into market abuse to secure the disclosure of connection data without prior review by a court or an independent administrative authority.