



Navigazione



Documenti

- [C-339/20 - Conclusioni](#)
- [C-339/20 - Domanda \(GU\)](#)
- [C-339/20 - Domanda di pronuncia pregiudiziale](#)



1 / 1

[Pagina iniziale](#) > [Formulario di ricerca](#) > [Elenco dei risultati](#) > **Documenti**



[Avvia la stampa](#)

Lingua del documento :

ECLI:EU:C:2021:940

CONCLUSIONS DE L'AVOCAT GÉNÉRAL

M. MANUEL CAMPOS SÁNCHEZ-BORDONA

présentées le 18 novembre 2021 ([1](#))

Affaires jointes C-339/20 et C-397/20

VD (C-339/20)

SR (C-397/20)

[demande de décision préjudicielle formée par la Cour de cassation (France)]

« Renvoi préjudiciel – Opérations d’initiés et manipulation de marché – Directive 2003/6 – Article 12, paragraphe 2, sous a) et d) – Règlement no 596/2014 – Article 23, paragraphe 2, sous g) et h) – Directive 2002/58 – Article 15, paragraphe 1 – Pouvoirs de surveillance et d’enquête des autorités compétentes – Faculté des autorités compétentes d’exiger les enregistrements téléphoniques et des données échangées existants – Réglementation nationale imposant aux

opérateurs de communications électroniques une conservation temporaire mais généralisée des données de connexion »

1. Les demandes de décision préjudicielle en cause dans la présente procédure ont un lien étroit avec les renvois préjudiciels introduits dans les affaires C-793/19, SpaceNet, C-794/19, Telekom Deutschland, et C-140/20, Commissioner of the Garda Síochána e.a.(2), dans lesquelles je présente également des conclusions ce jour.

2. Dans les conclusions SpaceNet et Telekom Deutschland et dans les conclusions Commissioner of the Garda Síochána, j'expose les raisons qui m'incitent à suggérer à la Cour de répondre au Bundesverwaltungsgericht (Cour administrative fédérale, Allemagne) et à la Supreme Court (Cour suprême, Irlande) dans la ligne de la jurisprudence relative à la directive 2002/58/CE (3), « récapitulée » dans l'arrêt La Quadrature du Net (4).

3. Les deux demandes de décision préjudicielle de la Cour de cassation (France) en cause en l'espèce n'ont certes pas pour objet immédiat la directive 2002/58, mais la directive 2003/6/CE (5) et le règlement (UE) n° 596/2014 (6).

4. Cela étant, la question qui se pose dans les deux procédures jointes en l'espèce est, en substance, la même que dans les autres procédures préjudicielles précitées, à savoir si les États membres peuvent imposer l'obligation de conserver de manière généralisée et indifférenciée les données relatives au trafic des communications électroniques (7).

5. C'est pourquoi, bien que, en l'occurrence, les réglementations en jeu soient la directive 2003/6 et le règlement n° 596/2014 (visant à lutter contre les opérations pouvant être qualifiées d'abus de marché) (8), j'estime que la jurisprudence de la Cour condensée dans l'arrêt La Quadrature du Net s'applique en l'espèce.

I. Le cadre juridique

A. Le droit de l'Union

1. La directive 2002/58

6. Aux termes de l'article 1^{er} (« Champ d'application et objectif ») de la directive 2002/58 :

« 1. La présente directive prévoit l'harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et services de communications électroniques dans [l'Union].

2. Les dispositions de la présente directive précisent et complètent la directive 95/46/CE [du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces

données (JO 1995, L 281, p. 31)] aux fins énoncées au paragraphe 1. En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales.

3. La présente directive ne s'applique pas aux activités qui ne relèvent pas du [TFUE], telles que celles visées dans les titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal. »

7. L'article 2 (« Définitions ») de la directive 2002/58 dispose :

« Sauf disposition contraire, les définitions figurant dans la directive 95/46/CE et dans la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques (directive "cadre") [(JO 2002, L 108, p. 33),] s'appliquent aux fins de la présente directive.

Les définitions suivantes sont aussi applicables :

[...]

b) "données relatives au trafic" : toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation ;

c) "données de localisation" : toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public ;

[...] »

8. L'article 15 de la directive 2002/58 précise, à son paragraphe 1 :

« Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne. »

2. *La directive 2003/6*

9. Conformément à l'article 11 de la directive 2003/6 :

« Sans préjudice des compétences des autorités judiciaires, chaque État membre désigne une autorité administrative unique compétente en vue d'assurer l'application des dispositions adoptées conformément à la présente directive.

[...] »

10. L'article 12 de la directive 2003/6 prévoit :

« 1. L'autorité compétente est investie de tous les pouvoirs de surveillance et d'enquête nécessaires à l'exercice de ses fonctions. [...]

2. Sans préjudice de l'article 6, paragraphe 7, les pouvoirs visés au paragraphe 1 du présent article sont exercés en conformité avec la législation nationale et incluent au moins le droit :

a) d'avoir accès à tout document sous quelque forme que ce soit et d'en recevoir copie ;

[...]

d) d'exiger des enregistrements téléphoniques et des données échangées existants ;

[...] »

3. ***Le règlement n° 596/2014***

11. Le règlement contient les considérants suivants :

« (1) Un véritable marché intérieur des services financiers est essentiel à la croissance économique et à la création d'emplois dans l'Union.

(2) Pour qu'un marché financier puisse être intégré, efficace et transparent, l'intégrité du marché est nécessaire. Le bon fonctionnement des marchés des valeurs mobilières et la confiance du public en ces marchés sont des préalables indispensables à la croissance économique et à la prospérité. Les abus de marché nuisent à l'intégrité des marchés financiers et ébranlent la confiance du public dans les valeurs mobilières et les instruments dérivés.

[...]

(62) L'efficacité de la surveillance est assurée si les autorités compétentes de chaque État membre sont dotées d'un ensemble d'outils, de compétences et de ressources adéquats. Par conséquent, le présent règlement prévoit en particulier un ensemble minimal de pouvoirs de surveillance et d'enquête que les autorités compétentes des États membres devraient se voir conférer au titre du droit national. Ces pouvoirs devraient s'exercer, lorsque le droit national l'exige, sur demande auprès des autorités judiciaires compétentes. [...]

[...]

(65) Les enregistrements existants des conversations téléphoniques et des données relatives au trafic des entreprises d'investissement, des établissements de crédit et des établissements financiers qui exécutent et documentent l'exécution de transactions, ainsi que les enregistrements téléphoniques et les enregistrements des données relatives au trafic existants des opérateurs de télécommunications, constituent une preuve essentielle, et parfois la seule, permettant de détecter et

de démontrer l'existence d'une opération d'initié ou d'une manipulation de marché. Les enregistrements téléphoniques et des données relatives au trafic peuvent établir l'identité de la personne à l'origine de la diffusion d'une information fausse ou trompeuse, ou prouver que des personnes ont été en contact à un moment donné et démontrer l'existence d'une relation entre deux ou plusieurs personnes. Par conséquent, les autorités compétentes devraient être en mesure d'exiger des enregistrements existants des conversations téléphoniques, des communications électroniques et des données relatives au trafic détenus par une entreprise d'investissement, un établissement de crédit ou un établissement financier conformément à la directive 2014/65/UE. L'accès aux enregistrements téléphoniques et aux enregistrements de données est nécessaire pour fournir des preuves et enquêter sur des pistes d'éventuelles opérations d'initiés ou manipulations de marché et, partant, pour détecter et infliger des sanctions pour les abus de marché. [...] L'accès aux enregistrements téléphoniques et aux enregistrements de données relatives au trafic détenus par un opérateur de télécommunications n'inclut pas l'accès au contenu vocal des communications téléphoniques.

(66) Si le présent règlement précise un ensemble minimal de pouvoirs qui devraient être conférés aux autorités compétentes, ces pouvoirs doivent être exercés dans le cadre d'un système de droit national complet qui garantit le respect des droits fondamentaux, y compris le droit à la vie privée. Aux fins de l'exercice de ces pouvoirs, qui peuvent entrer en grave conflit avec le droit au respect de la vie privée et familiale, du domicile et des communications, les États membres devraient prévoir des garanties appropriées et efficaces contre tout abus, comme, le cas échéant, une exigence d'obtenir une autorisation préalable de la part des autorités judiciaires d'un État membre concerné. Les États membres ne devraient prévoir la possibilité pour les autorités compétentes d'exercer de tels pouvoirs intrusifs que dans la mesure où ils sont nécessaires à la conduite correcte d'une enquête sur des cas graves pour lesquels ils ne disposent pas de moyens équivalents leur permettant de parvenir efficacement au même résultat.

[...]

(77) Le présent règlement respecte les droits fondamentaux et observe les principes consacrés par la charte des droits fondamentaux de l'Union européenne (ci-après [la "C]harte"). En conséquence, le présent règlement devrait être interprété et appliqué conformément à ces droits et principes. [...]

[...] »

12. Aux termes de l'article 1^{er} (« Objet ») du règlement n° 596/2014 :

« Le présent règlement établit un cadre réglementaire commun sur les opérations d'initiés, la divulgation illicite d'informations privilégiées et les manipulations de marché (ci-après dénommés "abus de marché"), ainsi que des mesures visant à empêcher les abus de marché afin de garantir l'intégrité des marchés financiers de l'Union et d'accroître la protection des investisseurs et leur confiance dans ces marchés. »

13. L'article 3 (« Définitions ») du règlement n° 596/2014, dispose, à son point 27, que, aux fins dudit règlement, on entend par « enregistrements de données relatives au trafic » « les enregistrements de données relatives au trafic tels qu'ils sont définis à l'article 2, deuxième alinéa, point b), de la directive 2002/58[...] ».

14. Conformément à l'article 22 (« Autorités compétentes ») du règlement n° 596/2014 :

« Sans préjudice des compétences des autorités judiciaires, chaque État membre désigne une autorité administrative compétente unique aux fins du présent règlement. [...] ».

15. L'article 23 (« Pouvoirs des autorités compétentes ») du règlement n° 596/2014 prévoit :

« [...] »

2. Afin de mener à bien leurs missions au titre du présent règlement, les autorités compétentes sont dotées, conformément au droit national, au moins des pouvoirs de surveillance et d'enquête suivants :

a) avoir accès à tout document et à toute donnée, sous quelle que forme que ce soit, et en recevoir ou en prendre une copie ;

[...]

g) se faire remettre les enregistrements des conversations téléphoniques, des communications électroniques ou des enregistrements de données relatives au trafic détenus par des entreprises d'investissement, des établissements de crédit ou des institutions financières ;

h) se faire remettre, dans la mesure où le droit national l'autorise, les enregistrements existants de données relatives au trafic détenus par un opérateur de télécommunications, lorsqu'il existe des raisons de suspecter une violation et que de tels enregistrements peuvent se révéler pertinents pour l'enquête relative à la violation de l'article 14, point a) ou b), ou de l'article 15 ;

[...]

3. Les États membres veillent à mettre en place des mesures appropriées pour que les autorités compétentes disposent de tous les pouvoirs de surveillance et d'enquête nécessaires à l'exercice de leurs missions.

[...]

4. Toute personne qui met des informations à la disposition de l'autorité compétente conformément au présent règlement n'est pas considérée comme violant une quelconque restriction à la divulgation d'informations requise en vertu d'un contrat ou d'une disposition législative, réglementaire ou administrative, et cela n'entraîne, pour la personne concernée, aucune responsabilité quelle qu'elle soit relative à cette notification ».

16. Aux termes de l'article 28 ("Protection des données") du règlement n° 596/2014 :

« En ce qui concerne le traitement de données à caractère personnel dans le cadre du présent règlement, les autorités compétentes exécutent leurs tâches aux fins du présent règlement conformément aux dispositions législatives, réglementaires et administratives nationales transposant la directive 95/46/CE. En ce qui concerne le traitement de données à caractère personnel qu'elle effectue dans le cadre du présent règlement, l'[Autorité européenne des marchés financiers] respecte les dispositions du règlement (CE) n° 45/2001 [du Parlement européen et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO 2001, L 8, p. 1)].

Les données à caractère personnel sont conservées pendant une durée maximale de cinq ans. »

B. Le droit national

1. *Le code monétaire et financier (ci-après le « CMF »)*

17. L'article L. 621-10, premier alinéa, du CMF, dans sa version en vigueur à l'époque des faits, disposait :

« Les enquêteurs et les contrôleurs peuvent, pour les nécessités de l'enquête ou du contrôle, se faire communiquer tous documents, quel qu'en soit le support. Les enquêteurs peuvent également se faire communiquer les données conservées et traitées par les opérateurs de télécommunications dans le cadre de l'article L. 34-1 du code des postes et des communications électroniques [ci-après le "CPCE"] et les prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [ci-après la "loi n° 2004-575"] et en obtenir la copie. »

18. L'article L. 621-10-2 du CMF était libellé comme suit :

« Pour la recherche des abus de marché [...], les enquêteurs peuvent se faire communiquer les données conservées et traitées par les opérateurs de télécommunication, dans les conditions et sous les limites prévues à l'article L. 34-1 du [CPCE], et par les prestataires mentionnés aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 [...].

La communication des données mentionnées au premier alinéa du présent article fait l'objet d'une autorisation préalable par un contrôleur des demandes de données de connexion.

[...] »

2. *Le CPCE*

19. Conformément à l'article L. 34-1 du CPCE en vigueur au moment des faits :

« [...]

II. Les opérateurs de communications électroniques [...] effacent ou rendent anonymes toute donnée relative au trafic, sous réserve des dispositions des III[...].

[...]

III. Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales [...], il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. [...]

[...]

VI. Les données conservées et traitées dans les conditions définies aux III, IV et V portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux.

Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications.

[...] »

20. L'article R. 10-13 du CPCE prévoyait :

« I. En application du III de l'article L. 34-1 les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :

- a) Les informations permettant d'identifier l'utilisateur ;
- b) Les données relatives aux équipements terminaux de communication utilisés ;
- c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
- d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
- e) Les données permettant d'identifier le ou les destinataires de la communication.

II. Pour les activités de téléphonie l'opérateur conserve les données mentionnées au II et, en outre, celles permettant d'identifier l'origine et la localisation de la communication.

III. La durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement.

[...] »

21. La juridiction de renvoi précise que ces données de connexion sont celles, générées ou traitées par suite d'une communication, qui sont relatives aux circonstances de celle-ci et aux utilisateurs du service à l'exclusion de toute indication sur le contenu des messages.

II. Les faits, la procédure et les questions préjudicielles

22. Les faits qui sont à l'origine des deux renvois préjudiciels faisant l'objet de la présente procédure coïncident en substance.

23. Par un réquisitoire introductif du 22 mai 2014, une information judiciaire a été ouverte concernant des faits qualifiés de délit d'initié et recel.

24. Les 23 et 25 septembre 2015, l'Autorité française des marchés financiers (ci-après l'« AMF ») a adressé au ministère public une communication à laquelle étaient annexées des pièces provenant d'une enquête menée par elle et comportant, notamment, des données à caractère personnel relatives à l'utilisation de lignes téléphoniques.

25. Pour recueillir les données relatives à l'utilisation de ces lignes téléphoniques, les agents de l'AMF se sont fondés sur l'article L. 621-10 du CMF.

26. À la suite de cette communication, par trois réquisitoires supplétifs des 29 septembre 2015, 22 décembre 2015 et 23 novembre 2016, l'instruction a été étendue à certains titres et instruments financiers qui leur seraient liés, sous les mêmes qualifications et celles de complicité, corruption et blanchiment.

27. Mis en examen pour des faits relatifs à ces titres des chefs de délit d'initié et blanchiment, VD et SR ont présenté une requête en nullité visant à l'annulation d'actes de la procédure pour violation, notamment, des articles 7, 8, 11 et 52 de la Charte ainsi que de l'article 15 de la directive 2002/58.

28. Leurs demandes ayant été rejetés par deux arrêts, du 20 décembre 2018 et du 7 mars 2019, de la chambre de l'instruction de la cour d'appel de Paris, 2^e section (France), les prévenus ont formé un pourvoi contre ces arrêts devant la Cour de cassation, qui pose à la Cour les questions préjudicielles suivantes :

« 1) L'article 12, [paragraphe] 2, [sous] a) et d), de la directive 2003/6[...], de même que l'article 23, [paragraphe] 2, [sous] g) et h), du règlement (UE) 596/2014 [...], lu à la lumière du considérant 65 de ce règlement, n'impliquent-ils pas, compte tenu du caractère occulte des informations échangées et de la généralité du public susceptible d'être mis en cause, la possibilité, pour le législateur national, d'imposer aux opérateurs de communications électroniques une conservation temporaire mais généralisée des données de connexion pour permettre à l'autorité administrative mentionnée aux articles 11 de la directive et 22 du règlement, lorsqu'apparaissent à l'encontre de certaines personnes des raisons de soupçonner qu'elles sont impliquées dans une opération d'initié ou une manipulation de marché, de se faire remettre, par l'opérateur, les enregistrements existants de données de trafic dans les cas où il existe des raisons de suspecter que ces enregistrements liés à l'objet de l'enquête peuvent se révéler pertinents pour la preuve de la réalité du manquement, en permettant notamment de retracer les contacts noués par les intéressés avant l'apparition des soupçons ?

2) Dans le cas où la réponse de la Cour [...] serait telle qu'elle conduirait la Cour de cassation à considérer que la législation française sur la conservation des données de connexion n'est pas conforme au droit de l'Union, les effets de cette législation pourraient-ils être maintenus provisoirement afin d'éviter une insécurité juridique et de permettre que les données collectées et conservées précédemment soient utilisées dans l'un des buts visés par cette législation ?

3) Une juridiction nationale peut-elle maintenir provisoirement les effets d'une législation permettant aux agents d'une autorité administrative indépendante chargée de mener des enquêtes en matière d'abus de marché d'obtenir, sans contrôle préalable d'une juridiction ou d'une autre autorité administrative indépendante, la communication de données de connexion ? »

III. La procédure devant la Cour

29. Les demandes de décision préjudicielle ont été enregistrées au greffe de la Cour respectivement le 24 juillet 2020 et le 20 août 2020.

30. Des observations écrites ont été déposées par VD, SR, les gouvernements français, estonien, irlandais, espagnol, polonais et portugais ainsi que par la Commission européenne.

31. VD, SR, les gouvernements français, danois, estonien, irlandais et espagnol, la Commission et le Contrôleur européen de la protection des données ont pris part à l'audience qui s'est tenue le 14 septembre 2021.

IV. Analyse

A. Considérations liminaires

32. La réglementation nationale pertinente dans les deux procédures jointes en l'espèce a fait l'objet de décisions de justice nationales qu'il convient de mentionner.

1. *L'arrêt du Conseil constitutionnel (France) du 21 juillet 2017*

33. La juridiction de renvoi a indiqué que le premier alinéa de l'article L. 621-10 du CMF a été déclaré inconstitutionnel par arrêt du Conseil constitutionnel du 21 juillet 2017 (9).

34. Le Conseil constitutionnel a toutefois reporté les effets de la déclaration d'inconstitutionnalité au 31 décembre 2018.

35. Entretemps, le législateur national a introduit dans le CMF l'article L. 621-10-2, par lequel il a instauré un régime d'autorisation préalable, par une autorité administrative indépendante, de l'accès aux données de connexion.

36. Selon la juridiction de renvoi :

– compte tenu du report dans le temps des effets de la déclaration d'inconstitutionnalité du premier alinéa de l'article L. 621-10 du CMF – en vigueur au moment des faits litigieux dans les procédures en cause en l'espèce –, la nullité de cette disposition ne saurait être constatée (10) ;

– toutefois, cette disposition, en ce qu'elle ne subordonnait pas l'accès aux données de connexion à un contrôle préalable par une juridiction ou une autorité administrative indépendante, « n'était pas conforme aux exigences posées par les articles 7, 8 et 11 de la Charte [...], tels qu'interprétés par la [Cour] » (11).

37. Dans ces conditions, la Cour de cassation conclut que la « seule question qui se pose porte sur la possibilité de reporter dans le temps les conséquences de l'inconventionnalité de l'article L. 621-10 du [CMF] » (12).

38. La juridiction de renvoi ne s'interroge donc pas sur la conformité au droit de l'Union de l'article L. 621-10 du CMF, mais, partant du principe de son incompatibilité avec plusieurs dispositions de la Charte, elle souhaite seulement savoir si, à l'instar de ce qui s'est passé en droit national avec les effets de la déclaration d'inconstitutionnalité de cette disposition, il est également possible de retarder les effets juridiques découlant de sa non-conformité au droit de l'Union. Tel est l'objet de la troisième question préjudicielle.

2. *L'arrêt du Conseil d'État (France) du 21 avril 2021*

39. Après l'introduction des deux demandes de décision préjudicielle en cause en l'espèce, le Conseil d'État a rendu, le 21 avril 2021 (13), un arrêt dans le cadre de la procédure au cours de laquelle la demande de décision préjudicielle ayant donné lieu à l'arrêt La Quadrature du Net a été introduite.

40. Dans cet arrêt, le Conseil d'État a décidé d'écarter l'application de l'article L. 34-1 du CPCE et d'enjoindre au gouvernement d'abroger, dans un délai de six mois, l'article R. 10-13 du CPCE,

dans la mesure où ces dispositions ne limitent pas dûment les finalités de l'obligation de conservation généralisée et indifférenciée des données de trafic et de localisation (14).

41. Le Conseil d'État s'est prononcé sur la conformité des règles nationales litigieuses en l'espèce avec la directive 2002/58. Selon lui, il ressort de la réponse donnée par la Cour dans l'arrêt *La Quadrature du Net* que ces règles auraient dû soit être écartées dans la procédure au principal (article L. 34-1 du CPCE) (15), soit être abrogées (article R. 10-13 du CPCE) (16).

42. La pertinence de l'arrêt *La Quadrature du Net* pour répondre à la première question préjudicielle des renvois faisant l'objet de la présente procédure est d'autant plus forte que, dans cet arrêt, il a été tenu compte, entre autres dispositions, de l'article R. 10-13 du CPCE (17), qui, avec l'article L. 34-I du même code, constitue une disposition-clef d'application de l'article L. 621-10 du CMF.

43. Je rappellerai que, pour recueillir les données relatives à l'utilisation des lignes téléphoniques par les personnes suspectées d'avoir commis les infractions sur lesquelles portait l'enquête relative à un éventuel abus de marché, les agents de l'autorité administrative se sont précisément fondés sur l'article L. 621-10 du CMF.

3. *La perte d'objet des demandes de décision préjudicielle ?*

44. Comme je l'ai déjà indiqué, la juridiction de renvoi souhaite savoir si la réglementation nationale litigieuse est conforme à la directive 2003/6 et au règlement n° 596/2014, dans la mesure où l'une et l'autre peuvent offrir un fondement spécifique à l'obligation de conservation des données distinct de celui contenu dans la directive 2002/58.

45. Si tel est le cas, j'estime que les demandes de décision préjudicielle n'ont pas perdu leur objet, malgré l'incidence que les arrêts des juridictions françaises précités pourraient avoir sur cette réglementation nationale :

– d'une part, on ne saurait exclure que, en droit national, l'article R. 10-13 du CPCE puisse produire un effet sur les procédures au principal, ce qu'il appartient à la juridiction de renvoi de déterminer ;

– d'autre part, le mandat adressé au gouvernement par le Conseil d'État, outre l'obligation d'abroger formellement cette disposition, comporte également une série de lignes directrices quant aux conditions devant être remplies par la réglementation qui sera adoptée en remplacement de celle devant être abrogée (18).

46. En effet, le Conseil d'État ne s'est pas contenté d'imposer au gouvernement l'obligation d'abroger l'article R. 10-13 du CPCE dans un délai de six mois ; il lui a explicitement enjoint de « limiter les finalités poursuivies par ces articles et adapter le cadre réglementaire relatif à la conservation des données de connexion » (19).

47. En conséquence, la décision de la Cour sur le fond peut être utile à la juridiction de renvoi, car :

– la conservation des données relatives au trafic pourrait, en théorie, trouver un fondement autonome dans la directive 2003/6 et dans le règlement n° 596/2014 distinct de celui offert par la directive 2002/58 ;

– il pourrait découler de la directive 2003/6 et du règlement n° 596/2014 des conditions particulières et spécifiques en ce qui concerne les finalités de la conservation des données.

B. Sur la première question préjudicielle

48. La première question préjudicielle concerne l'article 12, paragraphe 2, sous a) et d), de la directive 2003/6 et l'article 23, paragraphe 2, sous g) et h), du règlement n° 596/2014.

49. Ces dispositions permettent aux autorités administratives compétentes de demander aux opérateurs de communications électroniques (et, le cas échéant, aux entreprises d'investissement, aux établissements de crédit ou aux institutions financières) les enregistrements téléphoniques et les enregistrements de données relatives au trafic (20) existants, lorsqu'il existe des raisons de suspecter une infraction d'abus de marché et que de tels enregistrements peuvent se révéler pertinents pour l'enquête relative à la violation.

50. La juridiction de renvoi se fonde sur la prémisse que l'accès à ces enregistrements présuppose que « le législateur national [impose] aux opérateurs de communications électroniques une conservation temporaire mais généralisée des données de connexion pour permettre à l'autorité administrative [...] de se faire remettre, par l'opérateur, les enregistrements existants de données de trafic [...] en permettant notamment de retracer les contacts noués par les intéressés avant l'apparition des soupçons ».

51. Or, concernant l'obligation de conserver de manière généralisée et indifférenciée les données de connexion dans des domaines autres que la sécurité nationale (pour ce qui importe ici, dans le domaine de la lutte contre l'abus de marché), la jurisprudence de la Cour, *récapitulée* dans l'arrêt *La Quadrature du Net*, est pleinement applicable.

1. *Un fondement juridique autonome de l'obligation de conservation de données dans la directive 2003/6 et dans le règlement n° 596/2014 ?*

52. La jurisprudence de l'arrêt *La Quadrature du Net* a certes été établie relativement à la directive 2002/58, alors que les règles visées en l'espèce par la Cour de cassation sont la directive 2003/6 et le règlement n° 596/2014.

53. Toutefois, la directive 2002/58 constitue la norme de référence en ce qui concerne, ainsi que l'indique son intitulé, le « traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques ».

54. Tant la directive 2003/6 (ayant pour objet propre les opérations d'initiés et les manipulations de marché) que le règlement n° 596/2014 (consacré à l'abus de marché) comportent des dispositions qui, telles que celles énoncées dans la première question des renvois préjudiciels faisant l'objet de la présente procédure, concernent le *traitement* des enregistrements de données relatives au trafic.

55. Il s'agit donc de règles qui, à cet égard spécifique, purement instrumentales de leur finalité et de leur objet, doivent être interprétées dans le cadre du régime instauré par la directive 2002/58.

56. Cela découle, selon moi, de l'article 12, paragraphe 2, sous d), de la directive 2003/6 et de l'article 23, paragraphe 2, sous g) et h), du règlement n° 596/2014 :

– la première disposition porte sur le droit d'« exiger des enregistrements [...] des données échangées *existants* » (21) ;

– la lettre g) de l’article 23, paragraphe 2, du règlement n° 596/2014 concerne les « enregistrements des conversations téléphoniques, des communications électroniques ou des enregistrements de données relatives au trafic *détenus* par des entreprises d’investissement, des établissements de crédit ou des institutions financières » (22) ;

– enfin, la lettre h) de cette même disposition se rapporte également aux « enregistrements *existants* de données relatives au trafic *détenus* par un opérateur de télécommunications » (23).

57. À mon avis, aucune de ces dispositions ne confère des compétences spécifiques – autres que celles prévues par la directive 2002/58 – pour *conserver* des données. Elles se bornent à autoriser les administrations compétentes à *accéder* aux données conservées (*existantes*) conformément à la réglementation qui régit, de manière générale, le traitement de ces données à caractère personnel dans le secteur des communications électroniques, à savoir la directive 2002/58.

58. L’article 28 du règlement n° 596/2014 (dont l’interprétation n’est du reste pas demandée par la juridiction de renvoi) ne pourrait pas non plus être invoqué en tant que prétendu fondement juridique autonome de l’obligation de conservation de données dans ce domaine.

59. Cet article, intitulé « Protection des données » et, une fois encore, concernant le « traitement de données à caractère personnel » :

– confirme le droit, et en même temps le devoir, pour les autorités compétentes d’exercer les « tâches aux fins du présent règlement conformément aux dispositions législatives, réglementaires et administratives nationales transposant la directive 95/46/CE » ;

– ne mentionne pas l’obligation de conservation des données (24) requise des opérateurs de communications électroniques, se contentant de renvoyer à la directive 95/46 (25) en ce qui concerne la protection de celles-ci.

60. Le silence de la directive 2003/6 et du règlement n° 596/2014 quant à la conservation des données imposée aux opérateurs de communications électroniques est compréhensible, eu égard à la proximité temporelle de ces réglementations avec la directive 2002/58. Le législateur européen disposait déjà de cette dernière en tant que cadre de référence exhaustif pour tracer les contours de cette obligation (ainsi que ses dérogations), ce qui rendait inutile un régime propre de conservation afin de lutter contre les abus de marché.

61. Il s’ensuit que l’interprétation faite par la Cour de la directive 2002/58 doit, tout naturellement, s’étendre à la conservation des données qui, détenues par les opérateurs de communications électroniques, peuvent être utilisées par les autorités chargées des enquêtes dans le cadre de la lutte contre les abus de marché.

62. Les « enregistrements existants » visés par la directive 2003/6 et le règlement n° 596/2014 ne peuvent être que les « enregistrements *légalement* existants », c’est-à-dire ceux effectués conformément à la directive 2002/58. C’est cette directive qui, dans le droit de l’Union, « prévoit, notamment, l’harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et des libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques » (26).

63. La *légalité* des « enregistrements existants » ne peut être justifiée que si, en définitive, leur existence est couverte par les dispositions de la directive 2002/58.

64. Le gouvernement français s'oppose à cette approche. Il fait valoir que la réponse de la Cour doit être limitée à l'interprétation de la directive 2003/6 et du règlement n° 596/2014. L'une et l'autre autoriseraient implicitement les États membres à instituer une obligation de conservation généralisée et indifférenciée. Dans le cas contraire, leur effet utile serait sérieusement compromis.

65. Je ne partage pas les allégations du gouvernement français ; toutefois, même s'il y avait lieu de les accueillir, cette prétendue « habilitation implicite » n'en serait pas moins soumise aux conditions auxquelles, conformément à la jurisprudence de la Cour, les États membres doivent satisfaire lorsqu'ils utilisent la possibilité d'imposer une conservation généralisée et indifférenciée des données conformément à la directive 2002/58.

66. En d'autres termes, s'il était hypothétiquement admis que la directive 2003/6 et le règlement n° 596/2014 offrent un fondement autonome à la conservation des données (quod non), cette conservation serait soumise aux mêmes conditions que celles qui devraient la régir si elle était fondée sur n'importe quelle autre disposition du droit de l'Union.

67. Il en va ainsi car, en définitive, ces conditions découlent de la sauvegarde des droits fondamentaux garantis par la Charte, au respect desquels la directive 2003/6 et le règlement n° 596/2014 renvoient. Ce sont précisément ces droits que la Cour a invoqués dans la jurisprudence *La Quadrature du Net*.

68. Le gouvernement français lui-même ainsi que tous ceux qui sont intervenus dans les procédures au principal n'ont pas pu éviter de se référer à la jurisprudence reproduite dans ce dernier arrêt, certains (comme le gouvernement portugais ou la Commission) soulignant que cette jurisprudence fournit la ligne directrice pour répondre aux questions préjudicielles et d'autres (comme, notamment, le gouvernement irlandais) demandant explicitement sa révision.

69. Le débat suscité par la présente procédure a donc porté sur le point de savoir s'il convenait de confirmer ou de modifier la jurisprudence de la Cour relative à la légalité de la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation dans le domaine des communications électroniques.

2. L'interdiction de la conservation généralisée et indifférenciée des données relatives au trafic et les mesures législatives visant à protéger la sécurité nationale ou à lutter contre la criminalité grave

70. Ainsi que je l'ai défendu dans les conclusions *Commissioner of the Garda Síochána* et dans les conclusions *SpaceNet et Telekom Deutschland*, que je présente également ce jour, il ne me semble pas pertinent de modifier la jurisprudence de la Cour relative à l'article 15, paragraphe 1, de la directive 2002/58.

71. Dans ce contexte, les éléments indispensables pour répondre à la juridiction de renvoi découlent, selon moi, directement de la jurisprudence de la Cour telle que *récapitulée* dans l'arrêt *La Quadrature du Net*.

72. Je rappelle, tout d'abord, la jurisprudence de la Cour dans cet arrêt, que le point 168 résume comme suit :

« [L]'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une

conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En revanche, ledit article 15, paragraphe 1, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à des mesures législatives :

- permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues, et ladite injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace ;
- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ;
- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;
- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et
- permettant, aux fins de la lutte contre la criminalité grave et, a fortiori, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services,

dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus ».

73. L'idée qui est au cœur de la jurisprudence de la Cour concernant la directive 2002/58 est que les utilisateurs des moyens de communication électronique sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes restent anonymes et ne puissent pas faire l'objet d'un enregistrement, sauf s'ils y consentent (27).

74. L'article 15, paragraphe 1, de la directive 2002/58 admet des exceptions à l'obligation de garantir la confidentialité. Dans l'arrêt *La Quadrature du Net*, la Cour procède à l'examen approfondi de la conciliation de ces dérogations avec les droits fondamentaux dont l'exercice est susceptible d'être affecté (28).

75. La conservation généralisée et indifférenciée des données relatives au trafic ne pourrait être justifiée, selon la Cour, que par l'objectif de sauvegarde de la sécurité nationale, dont l'importance « dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58 » (29).

76. Dans un tel cas (sécurité nationale), la Cour a jugé que cette disposition, lue à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, « ne s'oppose pas, en principe, à *une mesure législative qui autorise les autorités compétentes à enjoindre* aux fournisseurs de services de communications électroniques de procéder à la *conservation* des données relatives au trafic et des données de localisation de l'ensemble des utilisateurs des moyens de communications électroniques *pendant une période limitée*, dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave [...] pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible » (30).

77. La Cour considère notamment que l'« objectif de sauvegarde de la sécurité nationale » « inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel » (31).

78. Or, le sens de l'arrêt La Quadrature du Net ne serait pas respecté si les considérations qu'il contient concernant la sécurité nationale pouvaient être étendues aux infractions, même graves, qui ne portent pas atteinte à celle-ci, mais à la sécurité publique ou à d'autres intérêts juridiquement protégés.

79. La Cour a donc soigneusement distingué les mesures législatives nationales prévoyant la conservation préventive, généralisée et indifférenciée des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité nationale (points 134 à 139 de l'arrêt La Quadrature du Net) de celles ayant trait à la lutte contre la criminalité et à la sauvegarde de la sécurité publique (points 140 à 151 du même arrêt). Les unes et les autres ne sauraient avoir la même portée, sous peine de priver cette distinction de tout sens.

80. Les instruments de conservation des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave sont indiqués, je le répète, aux points 140 à 151 de l'arrêt La Quadrature du Net. Il convient d'y ajouter ceux qui autorisent, avec la même finalité, la conservation préventive des adresses IP et des données relatives à l'identité civile de la personne (points 152 à 159 de cet arrêt) ainsi que la « conservation rapide » des données relatives au trafic et des données de localisation (points 160 à 166 dudit arrêt).

81. Les abus de marché sont sans aucun doute hautement répréhensibles, car ils « nuisent à l'intégrité des marchés financiers et ébranlent la confiance du public dans les valeurs mobilières et les instruments dérivés ». Dans la même mesure, ils peuvent être qualifiés, selon le cas, d'infractions punissables et, dans les cas les plus sévères, d'infractions graves (32).

82. C'est pourquoi, lorsque l'annexe I du règlement (UE) 2016/794 (33) se réfère à la coopération mutuelle entre les autorités compétentes des États membres dans la prévention de la criminalité grave affectant deux ou plusieurs États membres ou portant atteinte à un intérêt commun qui fait l'objet d'une politique de l'Union ainsi que dans la lutte contre ladite criminalité, elle englobe dans cette notion, outre d'autres comportements répréhensibles, les « délits d'initiés et manipulation des marchés financiers ».

83. Cela étant, le caractère infractionnel de ces derniers, y compris lorsqu'il est grave, est le même que celui que pourraient avoir de nombreuses autres infractions portant atteinte à des intérêts publics importants et à des politiques de l'Union. L'annexe I du règlement 2016/794 énumère, entre autres exemples de criminalité grave, le trafic de stupéfiants ; les activités de blanchiment d'argent ; la filière d'immigration ; la traite des êtres humains ; les enlèvements, séquestrations et prises d'otage ; les infractions portant atteinte aux intérêts financiers de l'Union ; la contrefaçon et le piratage de produits ; la criminalité informatique ; la corruption ; et la criminalité au détriment de l'environnement, y compris la pollution causée par les navires.

84. Les intérêts publics protégés par l'incrimination pénale de certains de ces comportements peuvent avoir autant ou plus d'importance que les intérêts défendus lors de la répression des abus de marché. Cela ne signifie cependant pas que de tels comportements constituent une menace pour la sécurité nationale, au sens de l'arrêt *La Quadrature du Net* (34).

85. Ainsi que la Commission l'a soutenu lors de l'audience, les objectifs de la directive 2003/6 et du règlement n° 596/2014 tendent à la réalisation d'un marché intérieur (notamment dans le secteur des marchés financiers), et non à la préservation de la sécurité nationale (35).

86. Étendre la notion de « menace contre la sécurité nationale » aux infractions d'abus de marché ouvrirait la porte à faire de même pour beaucoup d'autres atteintes à des intérêts publics non moins importants, mais qu'une juridiction pénale considérerait difficilement comme relevant de cette notion, bien plus restrictive. Si la Cour acceptait d'ouvrir cette porte, l'équilibre soigneux qui sous-tend l'arrêt *La Quadrature du Net* aurait été inutile.

87. En définitive, les enregistrements « existants » visés à l'article 12, paragraphe 2, point d), de la directive 2003/6 et à l'article 23, paragraphe 2, sous g) et h), du règlement n° 596/2014 ne peuvent être que ceux que la directive 2002/58, telle qu'interprétée par la Cour, permet de conserver afin de lutter contre la criminalité grave et de sauvegarder la sécurité publique. Ils ne sauraient en aucun cas être assimilés à ceux conservés de manière préventive, généralisée et indifférenciée afin de défendre la sécurité nationale.

3. *Sur la deuxième question préjudicielle*

88. Par la deuxième question préjudicielle, la juridiction de renvoi souhaite savoir si, dans l'hypothèse où la réglementation française relative à la conservation des données de connexion ne serait pas conforme au droit de l'Union, ses effets pourraient être maintenus provisoirement.

89. Compte tenu de la date de ses renvois préjudiciels, la juridiction de renvoi n'a pas pu tenir compte du fait que la réponse à ses doutes se trouve dans l'arrêt (du 6 octobre 2020) *La Quadrature du Net* (notamment aux points 213 à 228), qui, à cet égard, s'est conformé à la jurisprudence traditionnelle.

90. Selon la Cour, lorsqu'une violation de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, est constatée, « la juridiction de renvoi ne saurait faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, de la législation nationale en cause au principal » (36).

91. Il en va ainsi, car « seule la Cour peut, à titre exceptionnel et pour des considérations impérieuses de sécurité juridique, accorder une suspension provisoire de l'effet d'éviction exercé par une règle du droit de l'Union à l'égard du droit national contraire à celle-ci » (37), « limitation

dans le temps des effets de l'interprétation de ce droit donnée par la Cour [qui] ne peut être accordée que dans l'arrêt même qui statue sur l'interprétation sollicitée » (38), ce qui n'a pas été le cas dans l'arrêt du 8 avril 2014, *Digital Rights Ireland e.a.* (39).

92. Par conséquent, si la Cour n'a pas jugé pertinent de limiter dans le temps les effets de son interprétation de la directive 2002/58, la juridiction de renvoi ne saurait décider de prolonger l'effet utile d'une réglementation nationale incompatible avec les règles du droit de l'Union qui, comme la directive 2003/6 et le règlement n° 596/2014, doivent être interprétées à la lumière de la directive 2002/58.

4. *Sur la troisième question préjudicielle*

93. Dans la même ligne que pour la question précédente, par sa troisième question préjudicielle, la juridiction de renvoi souhaite savoir si une juridiction nationale peut maintenir provisoirement les effets d'une législation « permettant aux agents d'une autorité administrative indépendante chargée de mener des enquêtes en matière d'abus de marché d'obtenir, sans contrôle préalable d'une juridiction ou d'une autre autorité administrative indépendante, la communication de données de connexion ».

94. La prémisse de cette question est, à nouveau, l'incompatibilité de cette législation, en tant que telle, avec le droit de l'Union (40). En effet, la juridiction de renvoi indique elle-même que, bien que l'AMF soit une autorité administrative indépendante, « la faculté offerte à ses enquêteurs d'obtenir des données de connexion sans contrôle préalable par une juridiction ou une autre autorité administrative indépendante n'était pas conforme aux exigences posées par les articles 7, 8 et 11 de la Charte [...], tels qu'interprétés par la [Cour] » (41).

95. La Cour parvient à la même conclusion dans l'arrêt du 2 mars 2021, *Prokuratuur* (Conditions d'accès aux données relatives aux communications électroniques) (42), aux points 51 et suivants duquel elle indique que l'accès des autorités nationales compétentes aux données conservées doit être subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante ayant la qualité de « tiers » par rapport à celle qui demande l'accès à ces données.

96. Dans ces conditions, la réponse à la troisième question préjudicielle doit être la même que la réponse à la deuxième question.

V. **Conclusion**

97. Eu égard à ce qui précède, je suggère à la Cour de répondre à la Cour de cassation (France) dans les termes suivants :

1) L'article 12, paragraphe 2, sous a) et d), de la directive 2003/6/CE du Parlement européen et du Conseil, du 28 janvier 2003, sur les opérations d'initiés et les manipulations de marché (abus de marché), et l'article 23, paragraphe 2, sous g) et h), du règlement (UE) n° 596/2014 du Parlement européen et du Conseil, du 16 avril 2014, relatif à l'abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission, doivent être interprétés en ce sens qu'ils s'opposent à une réglementation nationale qui impose aux opérateurs de communications électroniques l'obligation de conserver de manière généralisée et indifférenciée les données relatives au trafic dans le cadre d'une enquête concernant des opérations d'initiés ou des manipulations et abus de marché.

2) Une juridiction nationale ne saurait limiter dans le temps les effets de la non-conformité au droit de l'Union d'une réglementation nationale qui impose aux fournisseurs de services de communications électroniques une obligation de conservation généralisée et indifférenciée des données relatives au trafic incompatible avec l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, et qui permet à l'autorité administrative chargée de mener des enquêtes en matière d'abus de marché d'obtenir, sans contrôle préalable d'une juridiction ou d'une autre autorité administrative indépendante, la communication de données de connexion.

[1](#) Langue originale : l'espagnol.

[2](#) Ci-après, respectivement, les « conclusions SpaceNet et Telekom Deutschland » et les « conclusions Commissioner of the Garda Síochána ».

[3](#) Directive du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37).

[4](#) Arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, ci-après l'« arrêt La Quadrature du Net », EU:C:2020:791).

[5](#) Directive du Parlement européen et du Conseil du 28 janvier 2003 sur les opérations d'initiés et les manipulations de marché (abus de marché) (JO 2003, L 96, p. 16).

[6](#) Règlement du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché (règlement relatif aux abus de marché) et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission (JO 2014, L 173, p. 1).

[7](#) En l'espèce, les données de localisation semblent être exclues, bien que la frontière entre celles-ci et les données relatives au trafic ne soit pas tout à fait claire.

[8](#) Dans son acception large, que j'adopterai dans les présentes conclusions, l'abus de marché recouvre « tout comportement illicite sur un marché financier, et, aux fins du présent règlement, il convient d'entendre par cette notion les opérations d'initiés, la divulgation illicite d'informations privilégiées et les manipulations de marché » (considérant 7 du règlement n° 596/2014).

[9](#) Le Conseil constitutionnel aurait constaté l'incompatibilité de la procédure d'accès de l'AMF aux données de connexion avec le droit au respect de la vie privée, protégé par l'article 2 de la Déclaration des droits de l'homme et du citoyen.

[10](#) Point 28 de la décision de renvoi dans l'affaire C-339/20 et point 43 de la décision de renvoi dans l'affaire C-397/20.

[11](#) Point 28 de la décision de renvoi dans l'affaire C-339/20 et point 43 de la décision de renvoi dans l'affaire C-397/20.

[12](#) Point 29 de la décision de renvoi dans l'affaire C-339/20 et point 44 de la décision de renvoi dans l'affaire C-397/20.

[13](#) Arrêt n° 393099 (ECLI:FR:CEASS :2021:393099.20210421). En toute logique, dans le cadre de la présente procédure, je ne peux pas me prononcer sur le contenu de cet arrêt en ce qui concerne la conformité au droit de l'Union de l'un de ses passages ou prononcés (notamment ceux relatifs à l'accès, à d'autres fins, aux données conservées pour des raisons de sécurité nationale) ou l'interprétation qu'il donne de l'arrêt La Quadrature du Net. Lors de l'audience, la Commission a déclaré qu'elle évaluait s'il convenait de réagir d'une quelconque manière à cet arrêt et qu'elle n'avait pas encore pris de décision à cet égard.

[14](#) À la demande de la Cour, les parties ont eu l'occasion de se prononcer sur cet arrêt au cours de l'audience.

[15](#) Point 58 de l'arrêt du Conseil d'État.

[16](#) Article 2 du dispositif de l'arrêt du Conseil d'État.

[17](#) Arrêt La Quadrature du Net, point 70 : « S’agissant de l’article R. 10-13 du CPCE et de l’obligation de conservation généralisée et indifférenciée des données relatives aux communications qui y est prévue, la juridiction de renvoi [...] fait observer qu’une telle conservation permet à l’autorité judiciaire d’accéder aux données relatives aux communications qu’un individu a effectuées avant d’être suspecté d’avoir commis une infraction pénale, de telle sorte que cette conservation présente une utilité sans équivalent pour la recherche, la constatation et la poursuite des infractions pénales ».

[18](#) Lors de l’audience, le gouvernement français a fait part de l’adoption de la loi n° 2021-998, du 30 juin 2021, relative à la prévention d’actes de terrorisme et au renseignement (JORF n° 176, du 31 juillet 2021). L’article 17 de cette loi modifie l’article L. 34-1 du CPCE. Un décret ultérieur doit déterminer, « selon l’activité des opérateurs et la nature des communications, les informations et catégories de données conservées en application des II bis et III », tels que modifiés, de l’article L. 34 du CPCE.

[19](#) Point 59 de l’arrêt Conseil d’État. En particulier et ainsi qu’il ressort de l’article 1^{er} du dispositif de cet arrêt, l’adaptation requise doit inclure un « réexamen périodique de l’existence d’une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale ».

[20](#) Aux termes de l’article 3 du règlement n° 596/2004, on entend par « enregistrements de données relatives au trafic » ceux définis à l’article 2, deuxième alinéa, sous b), de la directive 2002/58, à savoir « toutes les données traitées en vue de l’acheminement d’une communication par un réseau de communications électroniques ou de sa facturation ».

[21](#) Mise en italique par mes soins.

[22](#) Mise en italique par mes soins.

[23](#) Mise en italique par mes soins.

[24](#) Il fixe toutefois une durée de cinq ans pour leur conservation.

[25](#) Directive abrogée par le règlement (UE) du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l’égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement

général sur la protection des données) (JO 2016, L 119, p. 1). Je rappelle que, au point 210 de l'arrêt La Quadrature du Net, la Cour a jugé que, « à l'instar de ce qui vaut pour l'article 15, paragraphe 1, de la directive 2002/58, le pouvoir que confère l'article 23, paragraphe 1, du règlement 2016/679 aux États membres ne saurait être exercé que dans le respect de l'exigence de proportionnalité, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celles-ci doivent s'opérer dans les limites du strict nécessaire (voir, par analogie, s'agissant de la directive 95/46, arrêt du 7 novembre 2013, IPI, C-473/12, EU:C:2013:715, point 39 et jurisprudence citée) ».

[26](#) Arrêt La Quadrature du Net, point 91.

[27](#) Arrêt La Quadrature du Net, point 109.

[28](#) Arrêt La Quadrature du Net, points 111 à 133.

[29](#) Arrêt La Quadrature du Net, point 136.

[30](#) Arrêt La Quadrature du Net, point 137 (mise en italique par mes soins). Il en est ainsi, poursuit la Cour, « [m]ême si une telle mesure vise, de manière indifférenciée, tous les utilisateurs de moyens de communications électroniques sans que ceux-ci paraissent, de prime abord, présenter de rapport [...] avec une menace pour la sécurité nationale de cet État membre », puisqu'il y a alors lieu de « considérer que l'existence d'une telle menace est de nature, par elle-même, à établir ce rapport » (arrêt La Quadrature du Net, point 137).

[31](#) Arrêt La Quadrature du Net, point 135. Il est vrai, ainsi que je l'ai souligné au point 39 des conclusions SpaceNet et Telekom Deutschland, que ces dispositions donnent lieu à un régime plus rigoureux et strict que celui découlant de la jurisprudence de la Cour européenne des droits de l'homme, lue en combinaison avec l'article 8 de la convention européenne des droits de l'homme. Cela est, bien entendu, conforme à l'article 52, paragraphe 3, in fine, de la Charte. Par ailleurs, comme je l'ai indiqué au point 40 des conclusions précitées, la jurisprudence de la Cour européenne des droits de l'homme dans ses arrêts du 25 mai 2021, Big Brother Watch e.a. c. Royaume-Uni (CE:ECHR:2021:0525JUD005817013) et Centrum för Rättvisa c. Suède (CE:ECHR:2021:0525JUD003525208), ainsi que dans l'arrêt du 4 décembre 2015, Zakharov c. Russie (CE:ECHR:2015:1204JUD004714306), concerne des cas de figure qui ne sont pas comparables à ceux qui sont débattus dans le cadre des renvois préjudiciels faisant l'objet de la présente procédure. En définitive, la solution doit être trouvée en appliquant des normes nationales réputées conformes à la réglementation *exhaustive* de la directive 2002/58, telle qu'interprétée par la Cour.

[32](#) Voir directive 2014/57/UE du Parlement européen et du Conseil, du 16 avril 2014, relative aux sanctions pénales applicables aux abus de marché (directive relative aux abus de marché) (JO 2014, L 173, p. 179).

[33](#) Règlement (UE) 2016/794 du Parlement européen et du Conseil, du 11 mai 2016, relatif à l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et remplaçant et abrogeant les décisions du Conseil 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI et 2009/968/JAI (JO 2016, L 135, p. 53).

[34](#) Quant à la possibilité d'établir un tertium genus d'infractions, à cheval entre la sécurité nationale et la criminalité grave, je renvoie aux points 51 et 52 de mes conclusions Commissioner of the Garda Síochána.

[35](#) Ayant une position plus critique, VD a rappelé, lors de son intervention orale, que la sécurité nationale a été liée à de nombreuses catégories d'infractions dans les systèmes politiques totalitaires, qui détectent partout des menaces à la sûreté de l'État.

[36](#) Arrêt La Quadrature du Net, point 220.

[37](#) Arrêt La Quadrature du Net, point 216.

[38](#) Arrêt La Quadrature du Net, point 216.

[39](#) Affaires jointes C-293/12 et C-594/12 (EU:C:2014:238).

[40](#) Ainsi que je l'ai rappelé, le Conseil constitutionnel a annulé l'article L. 621-10 du CMF. L'arrêt du Conseil d'État du 21 avril 2021 reconnaît, à divers endroits, que l'accès aux données doit être soumis à un contrôle préalable par une juridiction ou une autorité administrative indépendante.

[41](#) Point 28 de la décision de renvoi dans l'affaire C-339/20 et point 43 de la décision de renvoi dans l'affaire C-397/20. La jurisprudence à laquelle il est fait référence remonte à l'arrêt du

21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970, point 120).

[42](#) Affaire C-746/18, EU:C:2021:152.
