ARRÊT DE LA COUR (grande chambre)

20 septembre 2022 (*)

« Renvoi préjudiciel – Marché unique pour les services financiers – Abus de marché – Opérations d'initiés – Directive 2003/6/CE – Article 12, paragraphe 2, sous a) et d) – Règlement (UE) no 596/2014 – Article 23, paragraphe 2, sous g) et h) – Pouvoirs de surveillance et d'enquête de l'Autorité des marchés financiers (AMF) – Objectif d'intérêt général visant à protéger l'intégrité des marchés financiers de l'Union européenne et la confiance du public dans les instruments financiers – Possibilité pour l'AMF de se faire remettre les enregistrements de données relatives au trafic détenus par un opérateur de services de communications électroniques – Traitement des données à caractère personnel dans le secteur des communications électroniques – Directive 2002/58/CE – Article 15, paragraphe 1 – Charte des droits fondamentaux de l'Union européenne – Articles 7, 8 et 11 ainsi que article 52, paragraphe 1 – Confidentialité des communications – Limitations – Législation prévoyant la conservation généralisée et indifférenciée des données relatives au trafic par les opérateurs de services de communications électroniques – Possibilité, pour une juridiction nationale, de limiter les effets dans le temps d'une déclaration d'invalidité concernant des dispositions législatives nationales incompatibles avec le droit de l'Union – Exclusion »

Dans les affaires jointes C-339/20 et C-397/20,

ayant pour objet des demandes de décision préjudicielle au titre de l'article 267 TFUE, introduites par la Cour de cassation (France), par décisions du 1er avril 2020, parvenues à la Cour, respectivement, le 24 juillet 2020 et le 20 août 2020, dans les procédures pénales contre

VD (C-339/20),

SR (C-397/20),

LA COUR (grande chambre),

composée de M. K. Lenaerts, président, M. A. Arabadjiev, Mme A. Prechal, MM. S. Rodin, I. Jarukaitis et Mme I. Ziemele, présidents de chambre, MM. T. von Danwitz, M. Safjan, F. Biltgen, P. G. Xuereb (rapporteur), N. Piçarra, Mme L. S. Rossi et M. A. Kumin, juges,

avocat général : M. M. Campos Sánchez-Bordona,

greffier : Mme R. Şereş, administratrice,

vu la procédure écrite et à la suite de l'audience du 14 septembre 2021,

considérant les observations présentées :

– pour VD, par Mes D. Foussard et F. Peltier, avocats,

– pour SR, par Mes M. Chavannes et P. Spinosi, avocats,

– pour le gouvernement français, par Mmes A. Daniel et E. de Moustier, MM. D. Dubois, J. Illouz et T. Stéhelin, en qualité d'agents,

– pour le gouvernement danois, par Mmes N. Holst-Christensen, N. Lykkegaard et M. Søndahl Wolff, en qualité d'agents,

– pour le gouvernement estonien, par Mmes A. Kalbus et M. Kriisa, en qualité d'agents,

– pour l'Irlande, par M^me^ M. Browne, M. A. Joyce et M^me^ J. Quaney, en qualité d'agents, assistés de M. D. Fennelly, BL,

– pour le gouvernement espagnol, par M. L. Aguilera Ruiz, en qualité d'agent,

– pour le gouvernement polonais, par M. B. Majczyna, en qualité d'agent,

– pour le gouvernement portugais, par M^me^ P. Barros da Costa, M. L. Inez Fernandes, M^mes^ L. Medeiros et I. Oliveira, en qualité d'agents,

– pour la Commission européenne, par MM. S. L. Kalėda, H. Kranenborg, T. Scharf et F. Wilman, en qualité d'agents,

– pour le Contrôleur européen de la protection des données, par M^me^ A. Buchta, M. M. Guglielmetti, M^me^ C.-A. Mamier et M. D. Nardi, en qualité d'agents,

ayant entendu l'avocat général en ses conclusions à l'audience du 18 novembre 2021,

rend le présent

Arrêt

1 Les demandes de décision préjudicielle portent, en substance, sur l'interprétation de 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) (JO 2003, L 96, p. 16), ainsi que de l'article 23, paragraphe 2, sous g) et h), du règlement (UE) n^o^ 596/2014 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 et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission (JO 2014, L 173, p. 1), lus en combinaison 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) (JO 2002, L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11) (ci-après la « directive 2002/58 »), et lus 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 (ci-après la « Charte »).

2 Ces demandes ont été présentées dans le cadre des procédures pénales engagées contre VD et SR des chefs de délits d'initié, de recel de délits d'initié, de complicité, de corruption et de blanchiment.

Le cadre juridique

Le droit de l'Union

La directive 2002/58

3 Les considérants 2, 6, 7 et 11 de la directive 2002/58 énoncent :

« (2) La présente directive vise à respecter les droits fondamentaux et observe les principes reconnus notamment par la [Charte]. En particulier, elle vise à garantir le plein respect des droits exposés aux articles 7 et 8 de [celle-ci].

[...]

(6) L'Internet bouleverse les structures commerciales traditionnelles en offrant une infrastructure mondiale commune pour la fourniture de toute une série de services de communications

électroniques. Les services de communications électroniques accessibles au public sur l'Internet ouvrent de nouvelles possibilités aux utilisateurs, mais présentent aussi de nouveaux dangers pour leurs données à caractère personnel et leur vie privée.

(7) Dans le cas des réseaux publics de communications, il convient d'adopter des dispositions législatives, réglementaires et techniques spécifiques afin de protéger les droits et les libertés fondamentaux des personnes physiques et les intérêts légitimes des personnes morales, notamment eu égard à la capacité accrue de stockage et de traitement automatisés de données relatives aux abonnés et aux utilisateurs.

[...]

(11) À l'instar de 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)], la présente directive ne traite pas des questions de protection des droits et libertés fondamentaux liées à des activités qui ne sont pas régies par le droit communautaire. Elle ne modifie donc pas l'équilibre existant entre le droit des personnes à une vie privée et la possibilité dont disposent les États membres de prendre des mesures telles que celles visées à l'article 15, paragraphe 1, de la présente directive, nécessaires pour la protection de la sécurité publique, de la défense, de 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) et de l'application du droit pénal. Par conséquent, la présente directive ne porte pas atteinte à la faculté des États membres de procéder aux interceptions légales des communications électroniques ou d'arrêter d'autres mesures si cela s'avère nécessaire pour atteindre l'un quelconque des buts précités, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, [signée à Rome le 4 novembre 1950], telle qu'interprétée par la Cour européenne des droits de l'homme dans ses arrêts. Lesdites mesures doivent être appropriées, rigoureusement proportionnées au but poursuivi et nécessaires dans une société démocratique. Elles devraient également être subordonnées à des garanties appropriées, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. »

4 L'article 1er de la directive 2002/58, intitulé « Champ d'application et objectif », dispose :

« 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 la Communauté.

2. Les dispositions de la présente directive précisent et complètent la directive [95/46] 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 [traité FUE], telles que celles visées dans les titres V et VI du traité [UE], 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. »

5 L'article 2 de ladite directive, intitulé « Définitions », dispose, à son second alinéa, sous b) :

« Les définitions suivantes sont [...] 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 ».

6 Aux termes de l'article 5 de la même directive, intitulé « Confidentialité des communications » :

« 1. Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité.

2. Le paragraphe 1 n'affecte pas l'enregistrement légalement autorisé de communications et des données relatives au trafic y afférentes, lorsqu'il est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale.

3. Les États membres garantissent que le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive [95/46], une information claire et complète, entre autres sur les finalités du traitement. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur. »

7 L'article 6 de la directive 2002/58, intitulé « Données relatives au trafic », dispose :

« 1. Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5 du présent article ainsi que de l'article 15, paragraphe 1.

2. Les données relatives au trafic qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion peuvent être traitées. Un tel traitement n'est autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement.

3. Afin de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée, le fournisseur d'un service de communications électroniques accessible au public peut traiter les données visées au paragraphe 1 dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de ces services, pour autant que l'abonné ou l'utilisateur que concernent ces données ait donné son consentement préalable. Les utilisateurs ou abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données relatives au trafic.

[...]

5. Le traitement des données relatives au trafic effectué conformément aux dispositions des paragraphes 1, 2, 3 et 4 doit être restreint aux personnes agissant sous l'autorité des fournisseurs de réseaux publics de communications et de services de communications électroniques accessibles au public qui sont chargées d'assurer la facturation ou la gestion du trafic, de répondre aux demandes de la clientèle, de détecter les fraudes et de commercialiser les services de communications électroniques ou de fournir un service à valeur ajoutée ; ce traitement doit se limiter à ce qui est nécessaire à de telles activités.

[...] »

8 L'article 9 de cette directive, intitulé « Données de localisation autres que les données relatives au trafic », prévoit, à son paragraphe 1 :

« Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée. [...] »

9 L'article 15 de la directive 2002/58, intitulé « Application de certaines dispositions de la directive [95/46] », énonce, 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]. 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, [TUE]. »

La directive 2003/6

10 Les considérants 1, 2, 12, 37, 41 et 44 de la directive 2003/6 sont libellés comme suit :

« (1) Un véritable marché unique pour les services financiers est essentiel à la croissance économique et à la création d'emplois dans la Communauté.

(2) Un marché financier intégré et efficace exige l'intégrité du marché. 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.

[...]

(12) La notion d'abus de marché recouvre les opérations d'initiés et les manipulations de marché. La législation visant à lutter contre les opérations d'initiés et celle visant les manipulations de marché poursuivent le même objectif : assurer l'intégrité des marchés financiers communautaires et renforcer la confiance des investisseurs en ces marchés. [...]

[...]

(37) L'efficacité de la surveillance sera garantie par un ensemble commun minimal de compétences et de moyens d'action puissants dont sera dotée l'autorité compétente de chaque État membre. Les entreprises de marché et tous les opérateurs économiques devraient également contribuer, à leur niveau, à l'intégrité du marché. [...]

[...]

(41) Étant donné que l'objectif de l'action envisagée, à savoir la prévention des abus de marché sous la forme d'opérations d'initiés et de manipulations de marché, ne peut être réalisé de manière

suffisante par les États membres et peut donc, en raison des dimensions et des effets de l'action, être mieux réalisé au niveau communautaire, la Communauté peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 [TUE]. Conformément au principe de proportionnalité tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre cet objectif.

(44) La présente directive respecte les droits fondamentaux et observe les principes reconnus en particulier par la [Charte], notamment par l'article 11 de celle-ci, et par l'article 10 de la convention européenne [de sauvegarde] des droits de l'homme [et des libertés fondamentales]. [...] »

11 L'article 11 de cette directive dispose :

« 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.

[...] »

12 Aux termes de l'article 12 de ladite directive :

« 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 ;

[...] »

Le règlement n^{o} 596/2014

13 Le règlement n^{o} 596/2014 a abrogé et remplacé la directive 2003/6 avec effet au 3 juillet 2016.

14 Les considérants 1, 2, 7, 24, 44, 62, 65, 66, 77 et 86 de ce règlement sont libellés comme suit :

« (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.

[...]

(7) La notion d'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. Ces comportements empêchent une transparence intégrale et adéquate du marché, qui est un préalable aux négociations sur des marchés financiers intégrés pour tous les acteurs économiques.

[...]

(24) Lorsqu'une personne physique ou morale en possession d'informations privilégiées acquiert ou cède, ou tente d'acquérir ou de céder, pour son propre compte ou pour le compte d'un tiers, que ce soit directement ou indirectement, des instruments financiers auxquels se rapportent ces informations, il devrait être supposé que cette personne a utilisé ces informations. Cette présomption s'entend sans préjudice des droits de la défense. La question de savoir si une personne a enfreint l'interdiction des opérations d'initiés ou a tenté d'effectuer une telle opération devrait être analysée à la lumière de l'objectif du présent règlement, qui est de protéger l'intégrité du marché financier et de renforcer la confiance des investisseurs, laquelle se fonde à son tour sur l'assurance que les investisseurs bénéficieront des mêmes conditions et seront protégés contre l'utilisation abusive d'informations privilégiées.

[...]

(44) Les prix de nombreux instruments financiers sont établis à partir d'indices de référence. La manipulation ou tentative de manipulation d'indices de référence, y compris les taux interbancaires offerts, est susceptible d'avoir de graves répercussions sur la confiance des marchés et peut entraîner des pertes importantes pour les investisseurs ou des distorsions de l'économie réelle. [...]

(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 [du Parlement européen et du Conseil, du 15 mai 2014, concernant les marchés d'instruments financiers et modifiant la directive 2002/92/CE et la directive 2011/61/UE (JO 2014, L 173, p. 349)]. 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. Pour assurer des conditions de concurrence homogènes dans l'Union en ce qui concerne l'accès aux enregistrements téléphoniques et aux enregistrements des données relatives au trafic existants détenus par un opérateur de télécommunications ou aux enregistrements existants des conversations téléphoniques et des données relatives au trafic détenus par une entreprise d'investissement, un établissement de crédit ou un établissement financier, les autorités compétentes devraient, conformément au droit national, être en mesure d'exiger des enregistrements téléphoniques et des données relatives au trafic existants détenus par un opérateur de télécommunications dans la mesure où le droit national l'autorise, ainsi que les enregistrements existants des conversations téléphoniques et des données relatives au trafic détenus par une entreprise d'investissement, dans les cas où il existe des raisons de suspecter que ces enregistrements liés à l'objet de l'inspection ou de l'enquête peuvent se révéler pertinents pour apporter la preuve d'un cas d'opération d'initié ou de manipulation de marché, en violation

du présent règlement. 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]. En conséquence, le présent règlement devrait être interprété et appliqué conformément à ces droits et principes. [...]

[...]

(86) Étant donné que l'objectif du présent règlement, à savoir la prévention des abus de marché sous la forme d'opérations d'initiés, de la divulgation illicite d'informations privilégiées et des manipulations de marché, ne peut pas être atteint de manière suffisante par les États membres mais peut, en raison de ses dimensions et de ses effets, l'être mieux au niveau de l'Union, celle-ci peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 [TUE]. Conformément au principe de proportionnalité tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre cet objectif. »

15 Aux termes de l'article 1 dudit règlement :

« 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. »

16 Sous l'intitulé « Définitions », l'article 3 du même règlement dispose, à son paragraphe 1, point 27 :

« Aux fins du présent règlement, on entend par :

[...]

27) "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] ».

17 Aux termes de l'article 14 du règlement n^{o} 596/2014, intitulé « Interdiction des opérations d'initiés et de la divulgation illicite d'informations privilégiées » :

« Une personne ne doit pas :

a) effectuer ou tenter d'effectuer des opérations d'initiés ;

b) recommander à une autre personne d'effectuer des opérations d'initiés ou inciter une autre personne à effectuer des opérations d'initiés ; ou

c) divulguer illicitement des informations privilégiées. »

18 L'article 22 de ce règlement prévoit :

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

19 L'article 23 dudit règlement, intitulé « Pouvoirs des autorités compétentes », dispose, à ses paragraphes 2 et 3 :

« 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 [quelque] 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.

[...] »

Le droit français

Le CPCE

20 Le code des postes et des communications électroniques, dans sa version applicable aux litiges au principal (ci-après le « CPCE »), disposait, à son article L. 34-1 :

« I. – Le présent article s'applique au traitement des données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques ; il s'applique notamment aux réseaux qui prennent en charge les dispositifs de collecte de données et d'identification.

II. – Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des III, IV, V et VI.

Les personnes qui fournissent au public des services de communications électroniques établissent, dans le respect des dispositions de l'alinéa précédent, des procédures internes permettant de répondre aux demandes des autorités compétentes.

Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.

III. – Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, 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. Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le VI, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'État, par les opérateurs.

[...]

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.

La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Les opérateurs prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article. »

21 L'article L. 34-1 du code des postes et des communications électroniques, dans sa version issue de la loi n° 2021-998, du 30 juillet 2021, relative à la prévention d'actes de terrorisme et au renseignement (JORF du 31 juillet 2021, texte n° 1), prévoit, à ses paragraphes II bis à III bis :

« II bis. – Les opérateurs de communications électroniques sont tenus de conserver :

1° Pour les besoins des procédures pénales, de la prévention des menaces contre la sécurité publique et de la sauvegarde de la sécurité nationale, les informations relatives à l'identité civile de l'utilisateur, jusqu'à l'expiration d'un délai de cinq ans à compter de la fin de validité de son contrat ;

2° Pour les mêmes finalités que celles énoncées au 1° du présent II bis, les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte ainsi que les informations relatives au paiement, jusqu'à l'expiration d'un délai d'un an à compter de la fin de validité de son contrat ou de la clôture de son compte ;

3° Pour les besoins de la lutte contre la criminalité et la délinquance grave, de la prévention des menaces graves contre la sécurité publique et de la sauvegarde de la sécurité nationale, les données techniques permettant d'identifier la source de la connexion ou celles relatives aux équipements terminaux utilisés, jusqu'à l'expiration d'un délai d'un an à compter de la connexion ou de l'utilisation des équipements terminaux.

III. – Pour des motifs tenant à la sauvegarde de la sécurité nationale, lorsqu'est constatée une menace grave, actuelle ou prévisible, contre cette dernière, le Premier ministre peut enjoindre par décret aux opérateurs de communications électroniques de conserver, pour une durée d'un an, certaines catégories de données de trafic, en complément de celles mentionnées au 3° du II bis, et de données de localisation précisées par décret en Conseil d'État.

L'injonction du Premier ministre, dont la durée d'application ne peut excéder un an, peut être renouvelée si les conditions prévues pour son édiction continuent d'être réunies. Son expiration est sans incidence sur la durée de conservation des données mentionnées au premier alinéa du présent III.

III bis. – Les données conservées par les opérateurs en application du présent article peuvent faire l'objet d'une injonction de conservation rapide par les autorités disposant, en application de la loi, d'un accès aux données relatives aux communications électroniques à des fins de prévention et de répression de la criminalité, de la délinquance grave et des autres manquements graves aux règles dont elles ont la charge d'assurer le respect, afin d'accéder à ces données. »

22 L'article R. 10-13 du CPCE est libellé comme suit :

« 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.

[...] »

La LCEN

23 L'article 6 de la loi n^{o} 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique (JORF du 22 juin 2004, p. 11168), dans sa version applicable aux litiges au principal (ci-après la « LCEN »), prévoyait :

« I. – 1. Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens.

[...]

2. Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible.

[...]

II. – Les personnes mentionnées aux 1 et 2 du I détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.

Elles fournissent aux personnes qui éditent un service de communication au public en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues au III.

L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des données mentionnées au premier alinéa.

Les dispositions des articles 226-17, 226-21 et 226-22 du code pénal sont applicables au traitement de ces données.

Un décret en Conseil d'État, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation.

[...] »

Le CMF

24 L'article L. 621-10 du code monétaire et financier, dans sa version applicable aux litiges au principal (ci-après le « CMF »), disposait, à son premier alinéa :

« 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 [CPCE] et les prestataires mentionnés aux 1 et 2 du I de l'article 6 de la [LCEN] et en obtenir la copie.

[...] »

25 Tirant les conséquences de la déclaration d'inconstitutionnalité de la seconde phrase du premier alinéa de l'article L. 621-10 du CMF par le Conseil constitutionnel (France) dans sa décision du 21 juillet 2017, le législateur a, par la loi n^{o} 2018-898, du 23 octobre 2018, relative à la lutte contre la fraude (JORF du 24 octobre 2018, texte n^{o} 1), inséré l'article L. 621-10-2 dans le code monétaire et financier, lequel prévoit :

« Pour la recherche des abus de marché définis par le règlement [n^{o} 596/2014], 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 [LCEN].

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.

Le contrôleur des demandes de données de connexion est, en alternance, un membre du Conseil d'État, en activité ou honoraire, élu par l'assemblée générale du Conseil d'État, puis un magistrat de la Cour de cassation, en activité ou honoraire, élu par l'assemblée générale de ladite Cour. Son suppléant, issu de l'autre juridiction, est désigné selon les mêmes modalités. Le contrôleur des demandes de données de connexion et son suppléant sont élus pour une durée de quatre ans non renouvelable.

[...]

Le contrôleur des demandes de données de connexion ne peut recevoir ou solliciter aucune instruction de l'Autorité des marchés financiers ni d'aucune autre autorité dans l'exercice de sa mission. Il est tenu au secret professionnel dans les conditions prévues à l'article L. 621-4 du présent code.

Il est saisi par demande motivée du secrétaire général ou du secrétaire général adjoint de l'Autorité des marchés financiers. Cette demande comporte les éléments de nature à en justifier le bien-fondé.

L'autorisation est versée au dossier d'enquête.

Les enquêteurs utilisent les données communiquées par les opérateurs de télécommunication et les prestataires mentionnés au premier alinéa du présent article exclusivement dans le cadre de l'enquête au titre de laquelle ils ont reçu l'autorisation.

Les données de connexion relatives aux faits faisant l'objet de notifications de griefs par le collège de l'Autorité des marchés financiers sont détruites à l'expiration d'un délai de six mois à compter de la décision définitive de la commission des sanctions ou des juridictions de recours. En cas de composition administrative, le délai de six mois court à compter de l'exécution de l'accord.

Les données de connexion relatives à des faits n'ayant pas fait l'objet d'une notification de griefs par le collège de l'Autorité des marchés financiers sont détruites à l'expiration d'un délai d'un mois à compter de la décision du collège.

En cas de transmission du rapport d'enquête au procureur de la République financier ou en cas de mise en mouvement de l'action publique par le procureur de la République financier [...], les données de connexion sont remises au procureur de la République financier et ne sont pas conservées par l'Autorité des marchés financiers.

Les modalités d'application du présent article sont fixées par décret en Conseil d'État. »

Les litiges au principal, les questions préjudicielles et la procédure devant la Cour

26 Par un réquisitoire introductif du 22 mai 2014, une information judiciaire a été ouverte à l'encontre de VD et de SR, portant sur des faits qualifiés de délit d'initié et de recel de délits d'initié. Cette information a par la suite été étendue, par un premier réquisitoire supplétif du 14 novembre 2014, sous la qualification de délit de complicité.

27 Les 23 et 25 septembre 2015, l'Autorité des marchés financiers (AMF) (France) a communiqué au juge d'instruction certains éléments dont elle disposait dans le cadre d'une enquête qu'elle avait diligentée au titre de l'article L. 621-10 du CMF, notamment des données à caractère personnel issues d'appels téléphoniques effectués par VD et SR que les enquêteurs de l'AMF avaient recueillies, sur le fondement de l'article L. 34-1 du CPCE, auprès d'opérateurs de services de communications électroniques.

28 À la suite du signalement ainsi effectué par l'AMF, l'instruction a été étendue, par trois réquisitoires supplétifs du 29 septembre 2015, du 22 décembre 2015 et du 23 novembre 2016, sous les qualifications de corruption et de blanchiment.

29 VD et SR ont été mis en examen, respectivement, les 10 mars et 29 mai 2017, des chefs de délits d'initié et de blanchiment pour le premier et de délit d'initié pour le second.

30 Dans la mesure où leur mise en examen respective était fondée sur les données de trafic fournies par l'AMF, VD et SR ont chacun saisi la cour d'appel de Paris (France) d'un recours, en invoquant, notamment, un moyen tiré, en substance, de la 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. Plus particulièrement, en prenant appui sur la jurisprudence issue de l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970), VD et SR contestaient le fait que cette autorité se soit fondée, pour procéder à la collecte desdites données, sur l'article L. 621-10 du CMF et l'article L. 34-1 du CPCE, alors que ces dispositions, d'une part, n'étaient pas conformes au droit de l'Union, pour autant qu'elles prévoyaient une conservation généralisée et indifférenciée des données de connexion et, d'autre part, ne fixaient aucune limite au pouvoir pour les enquêteurs de l'AMF de se faire communiquer les données conservées.

31 Par deux arrêts de la cour d'appel de Paris du 20 décembre 2018 et du 7 mars 2019, cette juridiction a rejeté les recours de VD et de SR. Il ressort des indications figurant dans les demandes de décision préjudicielle que, pour écarter le moyen tiré, en substance, de la 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, les juges de fond ont pris appui, notamment, sur le fait que l'article 23, paragraphe 2, sous h),

du règlement n° 596/2014, relatif aux abus de marché, permet aux autorités compétentes de se faire remettre, dans la mesure où le droit national l'autorise, les enregistrements existants des données relatives au trafic détenus par les opérateurs de services de communications électroniques, lorsqu'il existe des raisons de suspecter une violation de l'interdiction des opérations d'initiés, au titre de l'article 14, sous a) et b), de ce règlement et que de tels enregistrements peuvent se révéler pertinents pour l'enquête relative à cette violation.

32 VD et SR ont formé un pourvoi contre ces arrêts devant la juridiction de renvoi, en soulevant un moyen pris de la violation, notamment, des dispositions de la Charte et de la directive 2002/58 visées au point précédent.

33 S'agissant de l'accès aux données de connexion, la juridiction de renvoi se réfère à une décision du Conseil constitutionnel du 21 juillet 2017, dont il ressortirait que la procédure d'accès aux données personnelles conservées par les enquêteurs de l'AMF, telle que prévue par le droit français, ne serait pas conforme au droit au respect de la vie privée, tel que protégé par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789, soulignant que, si le législateur national avait réservé à des agents habilités et soumis au respect du secret professionnel le pouvoir d'obtenir ces données dans le cadre d'une enquête et ne leur avait pas conféré un pouvoir d'exécution forcée, il n'avait toutefois assorti ladite procédure d'aucune autre garantie de nature à assurer une conciliation équilibrée entre, d'une part, le droit au respect de la vie privée et, d'autre part, la prévention des atteintes à l'ordre public et la recherche des auteurs d'infractions, de telle sorte que la seconde phrase du premier alinéa de l'article L. 621-10 du CMF devait être déclarée contraire à la Constitution française.

34 La juridiction de renvoi relève en outre, d'une part, que le Conseil constitutionnel a estimé que, compte tenu des conséquences « manifestement excessives » qu'une abrogation immédiate de cette disposition pourrait avoir sur les procédures en cours, il y avait lieu de différer la date de cette abrogation au 31 décembre 2018 et, d'autre part, que le législateur national, tirant les conséquences de la déclaration d'inconstitutionnalité du premier alinéa de l'article L. 621-10 du CMF, a inséré dans ce code l'article L. 621-10-2.

35 La juridiction de renvoi, tout en rappelant les considérations ressortant du point 125 de l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970), estime que la nullité de la seconde phrase du premier alinéa de l'article L. 621-10 du CMF, applicable à l'époque des faits au principal, ne saurait résulter de cette déclaration d'inconstitutionnalité, compte tenu du report des effets de l'abrogation de cette disposition. Elle estime toutefois que la faculté dont disposent les enquêteurs de l'AMF au titre de cette disposition, d'obtenir des données de connexion sans contrôle préalable par une juridiction ou une autorité administrative indépendante, n'est pas conforme aux exigences ressortant des articles 7, 8 et 11 de la Charte, tels qu'interprétés par la Cour.

36 Dans ces conditions, seule se poserait à cet égard la question de la possibilité de reporter dans le temps les effets de l'abrogation de l'article L. 621-10 du CMF, alors même que celui-ci n'est pas conforme à la Charte.

37 S'agissant de la conservation des données de connexion, la juridiction de renvoi indique tout d'abord que, bien que le paragraphe II de l'article L. 34-1 du CPCE énonce une obligation de principe, selon laquelle les opérateurs de services de communications électroniques doivent effacer ou rendre anonyme toute donnée relative au trafic, cette obligation serait toutefois assortie d'un certain nombre d'exceptions, dont celle prévue au paragraphe III de cette disposition, relative aux « besoins de la recherche, de la constatation et de la poursuite des infractions pénales ». Pour ces besoins spécifiques, les opérations d'effacement ou d'anonymisation d'un certain nombre de données seraient différées d'un an.

38 Elle précise, à cet égard, que les cinq catégories de données concernées notamment par les conditions définies au paragraphe III de l'article L. 34-1 du CPCE sont celles énumérées à l'article R. 10-13 du CPCE. Ces données de connexion seraient générées ou traitées à la suite d'une communication, et seraient relatives aux circonstances de cette communication et aux utilisateurs du service, mais ne fourniraient aucune indication sur le contenu des communications concernées.

39 Ensuite, tout en rappelant le point 112 de l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970), aux termes duquel 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 une législation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique, la juridiction de renvoi relève que, dans le cadre des affaires au principal, l'AMF a eu accès aux données conservées par les opérateurs de services de communications électroniques en raison des soupçons portant sur des opérations d'initiés et des abus de marché susceptibles de relever de plusieurs qualifications pénales graves. Cet accès aurait été justifié par la nécessité pour cette autorité, aux fins d'assurer l'efficacité de son enquête, de croiser différentes données conservées sur un certain laps de temps, en vue de mettre à jour des informations privilégiées circulant entre plusieurs interlocuteurs, qui ont révélé l'existence de pratiques illicites en la matière.

40 Selon la juridiction de renvoi, les enquêtes menées par l'AMF répondraient aux obligations mises à la charge des États membres par l'article 12, paragraphe 2, sous d), de la directive 2003/6 et par l'article 23, paragraphe 2, sous g) et h), du règlement n° 596/2014, lu à la lumière de l'article 1er de ce règlement, dont, notamment, celle d'exiger la communication des enregistrements existants des données relatives au trafic, détenus par les opérateurs de services de communications électroniques.

41 En outre, cette juridiction souligne, d'une part, en se référant au considérant 65 dudit règlement, que ces données de connexion constituent une preuve essentielle, et parfois la seule, permettant de détecter et de démontrer l'existence d'une opération d'initié, dès lors qu'elles permettent d'établir l'identité de la personne à l'origine de la diffusion d'une information fausse ou trompeuse, ou de prouver que des personnes ont été en contact à un moment donné.

42 D'autre part, la juridiction de renvoi cite le considérant 66 du même règlement, duquel il ressort que l'exercice des pouvoirs conférés aux autorités compétentes en matière financière peut entrer en conflit avec le droit au respect de la vie privée et familiale, du domicile et des communications, et que, partant, les États membres devraient prévoir des garanties appropriées et efficaces contre tout abus en limitant lesdits pouvoirs aux seuls cas où ils sont nécessaires à la conduite correcte d'une enquête sur des cas graves pour lesquels ces États ne disposent pas de moyens équivalents leur permettant de parvenir efficacement au même résultat. Selon elle, il résulterait de ce considérant que certains cas d'abus de marché doivent être considérés comme étant des infractions graves.

43 Cette juridiction souligne par ailleurs que, dans le cadre des affaires au principal, les informations privilégiées susceptibles de caractériser l'élément matériel de pratiques illicites en matière de marché étaient, par essence, orales et secrètes.

44 Au vu des considérations qui précèdent, la juridiction de renvoi s'interroge sur la conciliation 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, avec les exigences ressortant 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.

45 Enfin, pour le cas où la Cour considérerait que la législation portant sur la conservation des données de connexion en cause au principal n'est pas conforme au droit de l'Union, se poserait la question du maintien provisoire des effets de cette législation, en vue d'éviter une insécurité juridique et de permettre que les données précédemment collectées et conservées soient utilisées aux fins de la détection et de la poursuite des opérations d'initiés.

46 C'est dans ces conditions que la Cour de cassation a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes, lesquelles sont formulées en des termes identiques dans les affaires C-339/20 et C-397/20 :

« 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 [n° 596/2014], qui s'est substitué au premier à compter du 3 juillet 2016, 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 [à l'article] 11 de la directive [2003/6] et [à l'article] 22 du règlement [n° 596/2014], 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 apporter 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 [...] [à la première question] 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 des données de connexion ? »

47 Par décision du président de la Cour du 17 septembre 2020, les affaires C-339/20 et C-397/20 ont été jointes aux fins des phases écrite et orale de la procédure ainsi que de l'arrêt.

48 Le 21 avril 2021, le Conseil d'État (France) a rendu l'arrêt French Data Network et autres (n° 393099, 394922, 397844, 397851, 424717, 424718), par lequel il s'est notamment prononcé sur la conformité au droit de l'Union de certaines dispositions législatives nationales qui sont pertinentes dans le cadre des litiges au principal, à savoir l'article L. 34-1 du CPCE et l'article R. 10-13 du CPCE.

49 Sur invitation de la Cour, les participants à l'audience dans les présentes affaires ont eu l'opportunité de se prononcer sur l'éventuelle incidence, pour les présents renvois préjudiciels, de cet arrêt du Conseil d'État.

50 Le représentant du gouvernement français a indiqué, lors de cette audience, que, par ledit arrêt, le Conseil d'État a, en substance, déclaré illégales les dispositions permettant de mettre en œuvre la conservation généralisée et indifférenciée des données de connexion à des fins de lutte contre la criminalité à l'exception de la conservation des adresses IP et des données relatives à l'identité civile des usagers des réseaux de communications électroniques, en tirant ainsi les conséquences de l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791). Il a toutefois précisé que, dans le cadre du débat contentieux, le Conseil d'État devait aussi répondre à l'objection du gouvernement français selon laquelle cette interprétation du droit de l'Union entrait en contradiction avec des règles de rang constitutionnel, à savoir celles visant la prévention des atteintes à l'ordre public, notamment à la sécurité des personnes et des biens, et la recherche des auteurs d'infractions pénales.

51 À cet égard, le représentant du gouvernement français a expliqué que le Conseil d'État avait écarté cette objection en deux temps. D'une part, il aurait certes reconnu que la conservation généralisée et indifférenciée des données de connexion était une condition déterminante du succès des enquêtes pénales et qu'aucune autre méthode ne pouvait utilement s'y substituer. D'autre part, néanmoins, le Conseil d'État aurait considéré, en prenant appui, notamment, sur le point 164 de l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), que la conservation rapide des données serait autorisée par le droit de l'Union y compris lorsque cette conservation rapide portait sur des données initialement conservées aux fins de la sauvegarde de la sécurité nationale.

52 Par ailleurs, le représentant du gouvernement français a précisé que, à la suite de l'arrêt du Conseil d'État, du 21 avril 2021, French Data Network et autres (n° 393099, 394922, 397844, 397851, 424717, 424718), le législateur national avait inséré le paragraphe III bis à l'article L. 34-1 du code des postes et des communications électroniques, ainsi qu'il est mentionné au point 21 du présent arrêt.

Sur les questions préjudicielles

Observations liminaires

53 En premier lieu, il convient de rappeler que, postérieurement à l'introduction des présentes demandes de décision préjudicielle, le Conseil d'État a prononcé l'arrêt du 21 avril 2021, French Data Network et autres (n° 393099, 394922, 397844, 397851, 424717, 424718), portant, notamment, sur la conformité au droit de l'Union de l'article L. 34-1 du CPCE et de l'article R. 10-13 du CPCE.

54 Or, ainsi que l'a relevé M. l'avocat général au point 42 de ses conclusions, et comme il ressort également des explications fournies par la juridiction de renvoi, telles qu'exposées aux points 27, 37 et 38 du présent arrêt, ces articles constituent des « dispositions clés » dans le cadre de l'application de l'article L. 621-10 du CMF, qui est en cause dans les affaires au principal.

55 Lors de l'audience devant la Cour, le représentant du gouvernement français, après avoir mis en exergue l'évolution législative dont l'article L. 34-1 du CPCE a fait l'objet à la suite des précisions apportées par la Cour dans l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), telle que mentionnée au point 21 du présent arrêt, a indiqué, en substance, que, pour trancher les litiges au principal, la juridiction de renvoi serait amenée, conformément au principe d'application de la loi dans le temps consacré aux articles 7 et 8 de la Déclaration des droits de l'homme et du citoyen de 1789, à tenir compte des dispositions nationales dans leur version applicable aux faits en cause au principal, qui remontent aux années 2014 et 2015, de sorte que l'arrêt du Conseil d'État, du 21 avril 2021, French Data Network et autres (n° 393099, 394922, 397844, 397851, 424717, 424718), ne saurait, en tout état de cause, être pris en considération pour l'analyse des présentes demandes de décision préjudicielle.

56 Selon une jurisprudence constante, dans le cadre de la procédure instituée par l'article 267 TFUE, il appartient au seul juge national, qui est saisi du litige et qui doit assumer la responsabilité de la décision juridictionnelle à intervenir, d'apprécier, au regard des particularités de l'affaire, tant la nécessité d'une décision préjudicielle pour être en mesure de rendre son jugement que la pertinence des questions qu'il pose à la Cour. En conséquence, dès lors que les questions posées portent sur l'interprétation du droit de l'Union, la Cour est, en principe, tenue de statuer (voir, en ce sens, arrêt du 8 septembre 2010, Winner Wetten, C-409/06, EU:C:2010:503, point 36 et jurisprudence citée).

57 Le refus de statuer sur une question préjudicielle posée par une juridiction nationale n'est possible que lorsqu'il apparaît de manière manifeste que l'interprétation du droit de l'Union sollicitée n'a aucun rapport avec la réalité ou l'objet du litige au principal, lorsque le problème est de nature hypothétique ou encore lorsque la Cour ne dispose pas des éléments de fait et de droit nécessaires pour répondre de façon utile aux questions qui lui sont posées (voir, en ce sens, arrêt du 19 novembre 2009, Filipiak, C-314/08, EU:C:2009:719, point 42 et jurisprudence citée).

58 En l'occurrence, il ressort des décisions de renvoi que les premières et troisièmes questions concernent directement non pas l'article L. 34-1 du CPCE et l'article R. 10-13 du CPCE, mais l'article L. 621-10 du CMF, au titre duquel l'AMF a demandé aux opérateurs de services de communications électroniques la communication des données relatives au trafic afférentes à des appels téléphoniques effectués par VD et SR, sur le fondement desquelles ces derniers ont été mis en examen et dont la recevabilité comme éléments de preuve est contestée dans le cadre des procédures au principal.

59 En outre, il convient de relever que, par les deuxièmes et troisièmes questions posées dans les présentes affaires, qui s'inscrivent dans le prolongement des premières, la juridiction de renvoi demande, en substance, si, dans l'hypothèse où la législation nationale en cause portant sur la conservation et l'accès des données de connexion devait s'avérer non-conforme au droit de l'Union, ses

effets ne pourraient toutefois pas être maintenus provisoirement, de sorte à éviter une insécurité juridique et à permettre que les données conservées sur le fondement de cette législation puissent être utilisées aux fins de la détection et de la poursuite des opérations d'initiés.

60 Au vu des éléments qui précèdent, ainsi que de ceux relevés par M. l'avocat général aux points 44 à 47 de ses conclusions, il y a lieu de considérer que, indépendamment de l'arrêt du Conseil d'État, du 21 avril 2021, French Data Network et autres (n° 393099, 394922, 397844, 397851, 424717, 424718), ainsi que de la décision du Conseil constitutionnel du 25 février 2022 (n° 2021-976/977), ayant partiellement déclaré inconstitutionnel l'article L. 34-1 du CPCE dans sa version visée au point 20 du présent arrêt, une réponse de la Cour aux questions posées demeure nécessaire pour la solution des litiges au principal.

61 En second lieu, il convient de relever que, lors de l'audience devant la Cour, le représentant de VD a contesté l'applicabilité ratione temporis du règlement n° 596/2014, en faisant valoir, en substance, que les faits en cause au principal étaient intervenus antérieurement à l'entrée en vigueur de ce règlement. Partant, seules les dispositions de la directive 2003/6 seraient pertinentes aux fins de l'examen des questions posées par la juridiction de renvoi.

62 À cet égard, il y a lieu de rappeler que, selon une jurisprudence constante, une règle de droit nouvelle s'applique à compter de l'entrée en vigueur de l'acte qui l'instaure et si elle ne s'applique pas aux situations juridiques nées et définitivement acquises sous l'empire de la loi ancienne, elle s'applique aux effets futurs de celles-ci, ainsi qu'aux situations juridiques nouvelles. Il n'en va autrement, et sous réserve du principe de non-rétroactivité des actes juridiques, que si la règle nouvelle est accompagnée de dispositions particulières qui déterminent spécialement ses conditions d'application dans le temps (voir, en ce sens, arrêts du 15 janvier 2019, E.B., C-258/17, EU:C:2019:17, point 50 et jurisprudence citée, ainsi que du 14 mai 2020, Azienda Municipale Ambiente, C-15/19, EU:C:2020:371, point 57).

63 Or, ainsi qu'il a été relevé aux points 26 à 29 du présent arrêt, si les situations juridiques concernées par les affaires au principal sont, en effet, nées avant l'entrée en vigueur du règlement n° 596/2014, lequel a abrogé et remplacé la directive 2003/6 avec effet au 3 juillet 2016, les procédures au principal ont suivi leur cours après cette date, de telle sorte que, à compter de celle-ci, les effets futurs de ces situations sont, conformément au principe rappelé au point précédent, régis par le règlement n° 596/2014.

64 Il s'ensuit que les dispositions du règlement n° 596/2014 sont en l'occurrence applicables. Par ailleurs, il n'y a pas lieu d'opérer de distinction entre les dispositions évoquées par la juridiction de renvoi résultant de la directive 2003/6 et du règlement n° 596/2014, ces dernières revêtant une portée en substance similaire pour les besoins de l'interprétation que la Cour sera amenée à donner dans le cadre des présentes affaires.

Sur les premières questions

65 Par ses premières questions, la juridiction de renvoi demande, en substance, si 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, lus en combinaison avec l'article 15, paragraphe 1, de la directive 2002/58, et à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doivent être interprétés en ce sens qu'ils s'opposent à des mesures législatives telles que celle en cause au principal prévoyant, à titre préventif, aux fins de la lutte contre les infractions d'abus de marché, dont font partie les opérations d'initiés, une conservation généralisée et indifférenciée des données de trafic pendant un an à compter du jour de l'enregistrement.

66 Les parties au principal et les intéressés ayant soumis des observations écrites à la Cour ont exprimé des avis divergents à cet égard. Pour le gouvernement estonien, pour l'Irlande ainsi que pour les gouvernements espagnol et français, l'article 12, paragraphe 2, sous a) et d), de la directive 2003/6 ainsi que l'article 23, paragraphe 2, sous g) et h), du règlement n° 596/2014 habilitent implicitement mais nécessairement le législateur national à instituer, dans le chef des opérateurs de services de

communications électroniques, une obligation de conservation généralisée et indifférenciée des données, afin de permettre à l'autorité compétente en matière financière de détecter et de sanctionner les opérations d'initiés. Dès lors que, ainsi qu'il ressort du considérant 65 du règlement nº 596/2014, lesdits enregistrements constituent une preuve essentielle, et parfois la seule, permettant de détecter et de démontrer l'existence d'une opération d'initié, une telle obligation de conservation serait indispensable tant pour assurer l'efficacité des enquêtes et des poursuites effectuées par ladite autorité, et par là même, l'effet utile de l'article 12, paragraphe 2, sous a) et d), de la directive 2003/6 ainsi que de l'article 23, paragraphe 2, sous h), du règlement nº 596/2014, que pour répondre aux objectifs d'intérêt général poursuivis par ces instruments, visant à garantir l'intégrité des marchés financiers de l'Union et à renforcer la confiance des investisseurs en ces marchés.

67 VD, SR, le gouvernement polonais et la Commission européenne font valoir en revanche que ces dispositions, pour autant qu'elles se limitent à encadrer le pouvoir d'exiger, auprès des opérateurs de services de communications électroniques, la communication des enregistrements « existants » de données relatives au trafic détenus par ces opérateurs, ne régissent que la question de l'accès à ces données.

68 À cet égard, il convient de rappeler, en premier lieu, qu'il est de jurisprudence constante que, afin d'interpréter une disposition du droit de l'Union, il convient non seulement de se référer aux termes de celle-ci, mais également de tenir compte de son contexte et des objectifs poursuivis par la réglementation dont elle fait partie ainsi que de prendre en considération, notamment, la genèse de cette réglementation (voir, en ce sens, arrêt du 17 avril 2018, Egenberger, C-414/16, EU:C:2018:257, point 44).

69 S'agissant du libellé des dispositions visées dans les premières questions, il convient de constater que, tandis que l' article 12, paragraphe 2, sous d), de la directive 2003/6 se réfère au pouvoir de l'autorité compétente en matière financière « d'exiger des enregistrements téléphoniques et des données échangées existants », l'article 23, paragraphe 2, sous g) et h), du règlement nº 596/2014 renvoie au pouvoir de cette autorité de se faire remettre, d'une part, les « enregistrements [...] de données relatives au trafic détenus par des entreprises d'investissement, des établissements de crédit ou des institutions financières » et, d'autre part, « dans la mesure où le droit national l'autorise, les enregistrements existants de données relatives au trafic détenus par un opérateur de télécommunications ».

70 Or, il ressort sans ambigüité du libellé de ces dispositions que celles-ci se bornent à encadrer le pouvoir de ladite autorité d'« exiger », ou encore, de « se faire remettre » les données dont disposent ces opérateurs, ce qui correspond à un accès à ces données. En outre, la référence faite aux enregistrements « existants », tels que « détenus » par lesdits opérateurs, laisse entendre que le législateur de l'Union n'a pas entendu régir la possibilité, pour le législateur national, d'instaurer une obligation de conservation de tels enregistrements.

71 À cet égard, il importe de rappeler que, selon une jurisprudence constante, une interprétation d'une disposition du droit de l'Union ne saurait avoir pour résultat de retirer tout effet utile au libellé clair et précis de cette disposition. Ainsi, dès lors que le sens d'une disposition du droit de l'Union ressort sans ambiguïté du libellé même de celle-ci, la Cour ne saurait se départir de cette interprétation (arrêt du 25 janvier 2022, VYSOČINA WIND, C-181/20, EU:C:2022:51, point 39 et jurisprudence citée).

72 L'interprétation esquissée au point 70 du présent arrêt est corroborée tant par le contexte dans lequel s'inscrivent 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 nº 596/2014 que par les objectifs poursuivis par la réglementation dont ces dispositions font partie.

73 S'agissant du contexte dans lequel s'inscrivent ces dispositions, il convient d'observer que, si, aux termes de l'article 12, paragraphe 1, de la directive 2003/6 et de l'article 23, paragraphe 3, du règlement no 596/2014, lu à la lumière du considérant 62 de ce règlement, le législateur de l'Union a entendu imposer aux États membres de prendre les mesures requises pour que les autorités compétentes en matière financière disposent d'un ensemble d'outils, de compétences et de ressources adéquates, ainsi que des pouvoirs de surveillance et d'enquête nécessaires pour assurer l'efficacité de leurs missions,

ces dispositions ne se prononcent ni sur l'éventuelle possibilité pour les États membres d'instituer, à ces fins, à la charge des opérateurs de services de communications électroniques, une obligation de conservation généralisée et indifférenciée des données de trafic ni sur les conditions dans lesquelles ces données doivent être conservées par lesdits opérateurs aux fins de leur remise, le cas échéant, aux autorités compétentes.

74 Par l'article 12, paragraphe 2, de la directive 2003/6 et l'article 23, paragraphe 2, du règlement n° 596/2014, le législateur de l'Union a seulement entendu investir l'autorité compétente en matière financière, afin d'assurer l'efficacité de ses missions d'enquête et de surveillance, de pouvoirs classiques d'investigation, tels que ceux permettant à cette autorité d'avoir accès à des documents, de procéder à des inspections et à des perquisitions, ou encore, de prononcer des injonctions ou des interdictions contre des personnes soupçonnées d'avoir commis des infractions d'abus de marché, dont font partie, notamment, les opérations d'initiés.

75 Par ailleurs, force est de constater que les dispositions du règlement no 596/2014 qui régissent spécifiquement la question de la conservation des données, à savoir l'article 11, paragraphe 5, dernier alinéa, paragraphe 6, second alinéa, paragraphe 8 et paragraphe 11, sous c), l'article 17, paragraphe 1, premier alinéa, l'article 18, paragraphe 5, ainsi que l'article 28 de ce règlement, ne comportent une telle obligation de conservation que dans le chef des opérateurs financiers, tels qu'énumérés à l'article 23, paragraphe 2, sous g), dudit règlement, et concernent, dès lors, uniquement les données afférentes à des transactions financières et à des services fournis par ces opérateurs spécifiques.

76 S'agissant des objectifs poursuivis par la réglementation en cause, il convient d'observer qu'il ressort, d'une part, des considérants 2 et 12 de la directive 2003/6 ainsi que, d'autre part, de l'article 1er du règlement n° 596/2014, lu à la lumière des considérants 2 et 24 de celui-ci, que ces instruments ont pour finalité d'assurer l'intégrité des marchés financiers de l'Union et de renforcer la confiance des investisseurs en ces marchés, confiance qui repose, notamment, sur le fait qu'ils seront placés sur un pied d'égalité et protégés contre l'utilisation illicite d'informations privilégiées. L'interdiction des opérations d'initiés énoncée à l'article 2, paragraphe 1, de la directive 2003/6 et à l'article 8, paragraphe 1, du règlement n° 596/2014 vise ainsi à garantir l'égalité des cocontractants dans une transaction boursière en évitant que l'un d'eux, qui détient une information privilégiée et se trouve, de ce fait, dans une position avantageuse par rapport aux autres investisseurs, en tire profit au détriment de ceux qui l'ignorent (voir, en ce sens, arrêt du 15 mars 2022, Autorité des marchés financiers, C-302/20, EU:C:2022:190, points 43, 65 et 77 ainsi que jurisprudence citée).

77 Si, aux termes du considérant 65 du règlement n° 596/2014, les enregistrements des données de connexion 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, il n'en reste pas moins que ce considérant ne se réfère qu'aux enregistrements « détenus » par les opérateurs de services de communications électroniques, ainsi qu'au pouvoir de l'autorité compétente en matière financière d'« exiger », auprès de ces opérateurs, la communication des données « existantes ». Ainsi, il ne ressort nullement de ce considérant que le législateur de l'Union a, par ce règlement, entendu reconnaître aux États membres le pouvoir d'imposer aux opérateurs de services de communications électroniques une obligation générale de conservation des données.

78 Au vu des éléments qui précèdent, il y a lieu de considérer que ni la directive 2003/6 ni le règlement n° 596/2014 ne sauraient être interprétés comme pouvant constituer le fondement juridique d'une obligation générale de conservation des enregistrements de données relatives au trafic détenus par les opérateurs de services de communications électroniques aux fins de l'exercice des pouvoirs conférés à l'autorité compétente en matière financière au titre de la directive 2003/6 et du règlement n° 596/2014.

79 En second lieu, il convient de rappeler que, ainsi que l'a relevé, en substance, M. l'avocat général aux points 53 et 61 de ses conclusions, la directive 2002/58 constitue l'acte de référence en matière de conservation et, de manière plus générale, de traitement des données à caractère personnel dans le secteur des communications électroniques, de telle sorte que l'interprétation faite par la Cour au regard de cette directive régit également les enregistrements des données de trafic détenus par les opérateurs

de services de communications électroniques, que les autorités compétentes en matière financière, au sens de l'article 11 de la directive 2003/6 et de l'article 22 du règlement n° 596/2014, peuvent se faire remettre par ceux-ci.

80 En effet, aux termes de l'article 1er, paragraphe 1, de la directive 2002/58, celle-ci 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, ce dernier englobant également le secteur des télécommunications.

81 Par ailleurs, il ressort de l'article 3 de cette directive que celle-ci s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics dans l'Union, y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification. Partant, ladite directive doit être regardée comme régissant les activités des fournisseurs de tels services, parmi lesquels figurent, notamment, les opérateurs de télécommunications (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 93 ainsi que jurisprudence citée).

82 Au vu des éléments qui précédent, il y a lieu de considérer que, ainsi que le fait valoir, en substance, M. l'avocat général aux points 62 et 63 de ses conclusions, l'appréciation de la licéité du traitement des enregistrements détenus par les opérateurs de services de communications électroniques, au sens 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, doit s'effectuer à la lumière des conditions prévues par la directive 2002/58, ainsi que de l'interprétation de cette directive dans la jurisprudence de la Cour.

83 Cette interprétation est corroborée par l'article 3, paragraphe 1, point 27, du règlement n° 596/2014, en ce qu'il prévoit que les enregistrements de données relatives au trafic aux fins de ce règlement sont ceux définis à l'article 2, second alinéa, sous b), de la directive 2002/58.

84 En outre, aux termes du considérant 44 de la directive 2003/6, ainsi que des considérants 66 et 77 du règlement n° 596/2014, les finalités visées par ces instruments sont à poursuivre dans le respect des droits fondamentaux et des principes consacrés par la Charte, y compris le droit à la vie privée. À cet égard, le législateur de l'Union a explicitement indiqué au considérant 66 du règlement n° 596/2014 que, aux fins de l'exercice des pouvoirs conférés à l'autorité compétente en matière financière, au titre de ce règlement, 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. Il s'ensuit que l'application des mesures régies par la directive 2003/6 et par le règlement n° 596/2014 ne saurait, en tout état de cause, porter atteinte à la protection des données à caractère personnel conférée au titre de la directive 2002/58 (voir, par analogie, arrêts du 29 janvier 2008, Promusicae, C-275/06, EU:C:2008:54, point 57, et du 17 juin 2021, M.I.C.M., C-597/19, EU:C:2021:492, point 124 ainsi que jurisprudence citée).

85 Par conséquent, 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 doivent être interprétés en ce sens qu'ils n'autorisent pas une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation aux fins de la lutte contre des infractions d'abus de marché et, notamment, contre les opérations d'initiés, la compatibilité avec le droit de l'Union d'une réglementation nationale prévoyant une telle conservation devant être appréciée au regard 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, tel qu'interprété par la jurisprudence de la Cour.

86 S’agissant de l’examen de la compatibilité d’une telle réglementation nationale avec ces dernières dispositions, il importe de rappeler que, ainsi qu’il résulte, en substance, d’une lecture combinée des points 53, 54 et 58 du présent arrêt, si la disposition au cœur des présents renvois préjudiciels est l’article L. 621-10 du CMF, au titre duquel l’AMF a demandé aux opérateurs de services de communications électroniques la transmission des données relatives au trafic afférentes à des appels téléphoniques effectués par VD et SR, sur le fondement desquelles ces derniers ont été mis en examen, il n’en reste pas moins que, comme l’a relevé M. l’avocat général au point 42 de ses conclusions, l’article L. 34-1 du CPCE et l’article R. 10-13 du CPCE constituent des « dispositions clés » dans le cadre de l’application de cet article L. 621-10 du CMF.

87 En effet, il ressort des explications fournies par la juridiction de renvoi, telles que résumées aux points 27, 37 et 38 du présent arrêt, que, d’une part, les enquêteurs de l’AMF avaient recueillies les données de trafic en cause sur le fondement de l’article L. 34-1 du CPCE, dans sa version applicable aux litiges au principal, dont le paragraphe III assortissait l’obligation de principe prévue au paragraphe II, selon laquelle les opérateurs de services de communications électroniques devaient effacer ou rendre anonyme toute donnée relative au trafic, d’un certain nombre d’exceptions, y compris celle relative aux « besoins de la recherche, de la constatation et de la poursuite des infractions pénales ». Pour ces besoins spécifiques, les opérations d’effacement ou d’anonymisation d’un certain nombre de données étaient différées d’un an.

88 D’autre part, cette juridiction précise que les cinq catégories de données concernées par le paragraphe III de l’article L. 34-1 du CPCE, dans sa version applicable aux litiges au principal, étaient celles énumérées à l’article R. 10-13 du CPCE, à savoir les informations permettant d’identifier l’utilisateur, les données relatives aux équipements terminaux de communication utilisés, les caractéristiques techniques ainsi que la date, l’horaire et la durée de chaque communication, les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs et, enfin, les données permettant d’identifier le ou les destinataires de la communication. Il ressort, en outre, du paragraphe II de l’article R. 10-13 du CPCE, dans sa version applicable aux litiges au principal, que, pour les activités de téléphonie, les opérateurs concernés pouvaient également conserver les données permettant d’identifier l’origine et la localisation de la communication.

89 Il s’ensuit que la réglementation en cause au principal couvre l’ensemble des moyens de communications téléphoniques et englobe l’ensemble des utilisateurs de ces moyens, sans qu’une différenciation ou une exception soit faite à cet égard. En outre, les données que cette réglementation impose aux opérateurs de services de communications électroniques de conserver sont, en particulier, celles qui sont nécessaires pour retrouver la source d’une communication et la destination de celle-ci, déterminer la date, l’heure, la durée et le type de la communication, identifier le matériel de communication utilisé ainsi que localiser les équipements terminaux et les communications, données au nombre desquelles figurent, notamment, le nom et l’adresse de l’utilisateur ainsi que les numéros de téléphone de l’appelant et de l’appelé.

90 Ainsi, les données qui doivent, en vertu de la réglementation nationale en cause, être conservées pendant un an, si elles ne couvrent pas le contenu des communications concernées, permettent, notamment, de savoir quelle est la personne avec laquelle l’utilisateur d’un moyen de communication téléphonique a communiqué et par quel moyen cette communication a eu lieu, de déterminer la date, l’heure et la durée des communications ainsi que l’endroit à partir duquel celles-ci ont eu lieu, et de connaître la localisation des équipements terminaux sans qu’une communication soit nécessairement acheminée. En outre, elles offrent la possibilité de déterminer la fréquence des communications de l’utilisateur avec certaines personnes pendant une période donnée. Dès lors, il y a lieu de considérer que ces données, prises dans leur ensemble, peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. En particulier, ces données fournissent les moyens d’établir le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications (voir, en ce sens, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 45 ainsi que jurisprudence citée).

91 Quant aux finalités poursuivies, il convient de relever que la réglementation en cause vise, entre autres finalités, la recherche, la constatation et la poursuite des infractions pénales, y compris celles relatives aux abus de marché dont font partie les opérations d'initiés.

92 Au vu des éléments exposés aux points 86 à 91 du présent arrêt, il y a lieu de constater que par la réglementation en cause, le législateur national a prévu, aux fins, notamment, de la recherche, de la constatation et de la poursuite des infractions pénales et de la lutte contre la criminalité, une conservation généralisée et indifférenciée des données de trafic pendant un an à compter du jour de l'enregistrement.

93 Or, il ressort en particulier des points 140 à 168 de l'arrêt du 6 octobre 2020, La Quadrature du Net e.a. (C–511/18, C–512/18 et C–520/18, EU:C:2020:791), ainsi que des points 59 à 101 de l'arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a. (C–140/20, EU:C:2022:258), qu'une telle conservation ne peut pas être justifiée par de tels objectifs au titre de l'article 15, paragraphe 1, de la directive 2002/58.

94 Il en résulte qu'une réglementation nationale, telle que celle en cause au principal, imposant aux opérateurs de services de communications électroniques de procéder, à titre préventif, aux fins de la lutte contre les infractions d'abus de marché, dont font partie les opérations d'initiés, une conservation généralisée et indifférenciée des données de trafic de l'ensemble des utilisateurs des moyens de communications électroniques, sans qu'aucune différenciation soit faite à cet égard ou que des exceptions soient prévues et sans que les rapports requis, au titre de la jurisprudence mentionnée au point précédent, entre les données à conserver et l'objectif poursuivi, soit établi, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique, ainsi que l'exige 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 (voir en ce sens, par analogie, arrêt du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790, point 81).

95 Au vu des éléments qui précèdent, il convient de répondre aux premières questions dans les affaires C-339/20 et C-397/20 que 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, lus en combinaison avec l'article 15, paragraphe 1, de la directive 2002/58, et à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doivent être interprétés en ce sens qu'ils s'opposent à des mesures législatives prévoyant, à titre préventif, aux fins de la lutte contre les infractions d'abus de marché, dont font partie les opérations d'initiés, une conservation généralisée et indifférenciée des données de trafic pendant un an à compter du jour de l'enregistrement.

Sur les deuxièmes et troisièmes questions

96 Par ses deuxièmes et troisièmes questions dans les présentes affaires, qu'il convient d'examiner ensemble, la juridiction de renvoi cherche, en substance, à savoir si le droit de l'Union doit être interprété en ce sens qu'une juridiction nationale peut limiter dans le temps les effets d'une déclaration d'invalidité, en vertu du droit national, à l'égard des dispositions législatives nationales qui, d'une part, imposent aux opérateurs de services de communications électroniques une conservation généralisée et indifférenciée des données relatives au trafic et, d'autre part, permettent la communication de telles données à l'autorité compétente en matière financière, sans autorisation préalable d'une juridiction ou d'une autorité administrative indépendante, en raison de l'incompatibilité de cette législation avec l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière de la Charte.

97 Il convient de rappeler d'emblée que le principe de primauté du droit de l'Union consacre la prééminence du droit de l'Union sur le droit des États membres. Ce principe impose dès lors à toutes les instances des États membres de donner leur plein effet aux différentes dispositions du droit de l'Union, le droit des États membres ne pouvant affecter l'effet reconnu à ces dispositions sur le territoire desdits États. En vertu de ce principe, à défaut de pouvoir procéder à une interprétation de la législation nationale conforme aux exigences du droit de l'Union, le juge national chargé d'appliquer, dans le cadre de sa compétence, les dispositions du droit de l'Union a l'obligation d'assurer le plein effet de celles-ci en laissant au besoin inappliquée, de sa propre autorité, toute disposition contraire de la législation nationale, même postérieure, sans qu'il ait à demander ou à attendre l'élimination

préalable de celle-ci par voie législative ou par tout autre procédé constitutionnel (voir, en ce sens, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 118 ainsi que jurisprudence citée).

98 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. Une telle limitation dans le temps des effets de l'interprétation de ce droit donnée par la Cour ne peut être accordée que dans l'arrêt même qui statue sur l'interprétation sollicitée. Il serait porté atteinte à la primauté et à l'application uniforme du droit de l'Union si des juridictions nationales avaient le pouvoir de donner aux dispositions nationales la primauté par rapport au droit de l'Union auquel ces dispositions contreviennent, serait-ce même à titre provisoire (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 119 ainsi que jurisprudence citée).

99 Certes, la Cour a considéré, dans une affaire concernant la légalité de mesures adoptées en méconnaissance de l'obligation, édictée par le droit de l'Union, d'effectuer une évaluation préalable des incidences d'un projet sur l'environnement et sur un site protégé, qu'une juridiction nationale peut, si le droit interne le permet, maintenir exceptionnellement les effets de telles mesures lorsque ce maintien est justifié par des considérations impérieuses liées à la nécessité d'écarter une menace réelle et grave de rupture de l'approvisionnement en électricité de l'État membre concerné, à laquelle il ne pourrait être fait face par d'autres moyens et alternatives, notamment dans le cadre du marché intérieur, ledit maintien ne pouvant couvrir que le laps de temps strictement nécessaire pour remédier à cette illégalité (voir, en ce sens, arrêt du 29 juillet 2019, Inter-Environnement Wallonie et Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, points 175, 176, 179 et 181).

100 Cependant, contrairement à l'omission d'une obligation procédurale, telle que l'évaluation préalable des incidences d'un projet, qui s'inscrit dans le domaine spécifique de la protection de l'environnement, une méconnaissance 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, ne saurait faire l'objet d'une régularisation par voie d'une procédure comparable à celle mentionnée au point précédent (voir, en ce sens, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 121 ainsi que jurisprudence citée).

101 En effet, le maintien des effets d'une législation nationale telle que celle en cause au principal signifierait que cette législation continue à imposer aux opérateurs de services de communications électroniques des obligations qui sont contraires au droit de l'Union et qui comportent des ingérences graves dans les droits fondamentaux des personnes dont les données ont été conservées (voir, par analogie, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 122 ainsi que jurisprudence citée).

102 Partant, la juridiction de renvoi ne saurait limiter dans le temps les effets d'une déclaration d'invalidité lui incombant, en vertu du droit national, quant à la législation nationale en cause au principal (voir, par analogie, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 123 ainsi que jurisprudence citée).

103 Il convient, en outre, de préciser qu'une limitation dans le temps des effets de l'interprétation retenue n'a pas été opérée dans les arrêts du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970), ainsi que du 6 octobre 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 et C-520/18, EU:C:2020:791), de sorte que, conformément à la jurisprudence rappelée au point 98 du présent arrêt, elle ne saurait intervenir dans un arrêt de la Cour postérieur à ces arrêts.

104 Enfin, compte tenu du fait que la juridiction de renvoi est saisie de demandes de déclarer irrecevables des éléments de preuve obtenus à partir des données relatives au trafic, au motif que les dispositions nationales en cause seraient contraires au droit de l'Union, tant en ce qui concerne la conservation des données que l'accès à celles-ci, il convient de déterminer l'incidence du constat de l'éventuelle incompatibilité de l'article L. 621-10 du CMF, dans sa version applicable aux faits en cause au principal, avec 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, sur la recevabilité des preuves soulevées contre VD et SR dans le cadre des procédures au principal.

105 À cet égard, il suffit de renvoyer à la jurisprudence de la Cour, en particulier aux principes rappelés aux points 41 à 44 de l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152), dont il découle que cette recevabilité relève, conformément au principe d'autonomie procédurale des États membres, du droit national, sous réserve du respect notamment des principes d'équivalence et d'effectivité.

106 S'agissant de ce dernier principe, il convient de rappeler qu'il impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus au moyen d'une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union ou encore au moyen d'un accès de l'autorité compétente à ces données en violation de ce droit, dans le cadre d'une procédure pénale ouverte contre des personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits [voir, en ce sens, arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 44 et jurisprudence citée].

107 Eu égard aux considérations qui précèdent, il convient de répondre aux deuxièmes et troisièmes questions dans les présentes affaires que le droit de l'Union doit être interprété en ce sens qu'il s'oppose à ce qu'une juridiction nationale limite dans le temps les effets d'une déclaration d'invalidité qui lui incombe, en vertu du droit national, à l'égard des dispositions nationales qui, d'une part, imposent aux opérateurs de services de communications électroniques une conservation généralisée et indifférenciée des données relatives au trafic et, d'autre part, permettent la communication de telles données à l'autorité compétente en matière financière, sans autorisation préalable d'une juridiction ou d'une autorité administrative indépendante, en raison de l'incompatibilité de ces dispositions avec l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière de la Charte. L'admissibilité des éléments de preuve obtenus en application des dispositions législatives nationales incompatibles avec le droit de l'Union relève, conformément au principe d'autonomie procédurale des États membres, du droit national, sous réserve du respect, notamment, des principes d'équivalence et d'effectivité.

Sur les dépens

108 La procédure revêtant, à l'égard des parties au principal, le caractère d'un incident soulevé devant la juridiction de renvoi, il appartient à celle-ci de statuer sur les dépens. Les frais exposés pour soumettre des observations à la Cour, autres que ceux desdites parties, ne peuvent faire l'objet d'un remboursement.

Par ces motifs, la Cour (grande chambre) dit pour droit :

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^{o} 596/2014 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 et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission, lus en combinaison 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), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, et 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,

doivent être interprétés en ce sens que :

ils s'opposent à des mesures législatives prévoyant, à titre préventif, aux fins de la lutte contre les infractions d'abus de marché, dont font partie les opérations d'initiés, une

conservation généralisée et indifférenciée des données de trafic pendant un an à compter du jour de l'enregistrement.

2) **Le droit de l'Union doit être interprété en ce sens qu'il s'oppose à ce qu'une juridiction nationale limite dans le temps les effets d'une déclaration d'invalidité qui lui incombe, en vertu du droit national, à l'égard des dispositions nationales qui, d'une part, imposent aux opérateurs de services de communications électroniques une conservation généralisée et indifférenciée des données relatives au trafic et, d'autre part, permettent la communication de telles données à l'autorité compétente en matière financière, sans autorisation préalable d'une juridiction ou d'une autorité administrative indépendante, en raison de l'incompatibilité de ces dispositions avec l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière de la charte des droits fondamentaux de l'Union européenne. L'admissibilité des éléments de preuve obtenus en application des dispositions législatives nationales incompatibles avec le droit de l'Union relève, conformément au principe d'autonomie procédurale des États membres, du droit national, sous réserve du respect, notamment, des principes d'équivalence et d'effectivité.**

Lenaerts	Arabadjiev	Prechal
Rodin	Jarukaitis	Ziemele
von Danwitz	Safjan	Biltgen
Xuereb	Piçarra	Rossi
	Kumin	

Ainsi prononcé en audience publique à Luxembourg, le 20 septembre 2022.

Le greffier	Le président
A. Calot Escobar	K. Lenaerts

* Langue de procédure : le français.