

Quelle: <http://curia.europa.eu/>

URTEIL DES GERICHTSHOFS (Große Kammer)

20. September 2022(*)

„Vorlage zur Vorabentscheidung – Binnenmarkt für Finanzdienstleistungen – Marktmissbrauch – Insidergeschäfte – Richtlinie 2003/6/EG – Art. 12 Abs. 2 Buchst. a und d – Verordnung (EU) Nr. 596/2014 – Art. 23 Abs. 2 Buchst. g und h – Aufsichts- und Ermittlungsbefugnisse der Finanzaufsichtsbehörde (Autorité des marchés financiers, AMF) – Im Allgemeininteresse liegendes Ziel des Schutzes der Integrität der Finanzmärkte in der Europäischen Union und des Vertrauens der Öffentlichkeit in die Finanzinstrumente – Möglichkeit der AMF, Datenverkehrsaufzeichnungen im Besitz eines Anbieters von Diensten der elektronischen Kommunikation anzufordern – Verarbeitung personenbezogener Daten in der elektronischen Kommunikation – Richtlinie 2002/58/EG – Art. 15 Abs. 1 – Charta der Grundrechte der Europäischen Union – Art. 7, 8, 11 und 52 Abs. 1 – Vertraulichkeit der Kommunikation – Einschränkungen – Regelung, die die allgemeine und unterschiedslose Speicherung der Verkehrsdaten durch die Anbieter von Diensten der elektronischen Kommunikation vorsieht – Möglichkeit eines nationalen Gerichts, eine Entscheidung, mit der die Unionsrechtswidrigkeit innerstaatlicher Rechtsvorschriften festgestellt wird, in ihren zeitlichen Wirkungen zu beschränken – Ausschluss“

In den verbundenen Rechtssachen C-339/20 und C-397/20

betreffend Vorabentscheidungsersuchen nach Art. 267 AEUV, eingereicht von der Cour de cassation (Kassationsgerichtshof, Frankreich) mit Entscheidungen vom 1. April 2020, beim Gerichtshof eingegangen am 24. Juli 2020 bzw. 20. August 2020, in den Strafverfahren gegen

VD (C-339/20),

SR (C-397/20),

erlässt

DER GERICHTSHOF (Große Kammer)

unter Mitwirkung des Präsidenten K. Lenaerts, des Kammerpräsidenten A. Arabadjiev, der Kammerpräsidentin A. Prechal, der Kammerpräsidenten S. Rodin und I. Jarukaitis, der Kammerpräsidentin I. Ziemele, der Richter T. von Danwitz, M. Safjan, F. Biltgen, P. G. Xuereb (Berichterstatter) und N. Piçarra, der Richterin L. S. Rossi und des Richters A. Kumin,

Generalanwalt: M. Campos Sánchez-Bordona,

Kanzler: R. Şereş, Verwaltungsrätin,

aufgrund des schriftlichen Verfahrens und auf die mündliche Verhandlung vom 14. September 2021,

unter Berücksichtigung der Erklärungen

- von VD, vertreten durch D. Foussard und F. Peltier, Avocats,
- von SR, vertreten durch M. Chavannes und P. Spinosi, Avocats,
- der französischen Regierung, vertreten durch A. Daniel, E. de Moustier, D. Dubois, J. Illouz und T. Stéhelin als Bevollmächtigte,
- der dänischen Regierung, vertreten durch N. Holst-Christensen, N. Lykkegaard und M. Søndahl Wolff als Bevollmächtigte,
- der estnischen Regierung, vertreten durch A. Kalbus und M. Kriisa als Bevollmächtigte,
- Irlands, vertreten durch M. Browne, A. Joyce und J. Quaney als Bevollmächtigte im Beistand von D. Fennelly, BL,
- der spanischen Regierung, vertreten durch L. Aguilera Ruiz als Bevollmächtigten,
- der polnischen Regierung, vertreten durch B. Majczyna als Bevollmächtigten,
- der portugiesischen Regierung, vertreten durch P. Barros da Costa, L. Inez Fernandes, L. Medeiros und I. Oliveira als Bevollmächtigte,
- der Europäischen Kommission, vertreten durch S. L. Kalèda, H. Kranenborg, T. Scharf und F. Wilman als Bevollmächtigte,
- des Europäischen Datenschutzbeauftragten, vertreten durch A. Buchta, M. Guglielmetti, C.-A. Mamier und D. Nardi als Bevollmächtigte,

nach Anhörung der Schlussanträge des Generalanwalts in der Sitzung vom 18. November 2021

folgendes

Urteil

- 1 Die Vorabentscheidungsersuchen betreffen im Wesentlichen die Auslegung von Art. 12 Abs. 2 Buchst. a und d der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates vom 28. Januar 2003 über Insider-Geschäfte und Marktmanipulation (Marktmissbrauch) (ABl. 2003, L 96, S. 16) und von Art. 23 Abs. 2 Buchst. g und h der Verordnung (EU) Nr. 596/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über Marktmissbrauch (Marktmissbrauchsverordnung) und zur Aufhebung der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates und der Richtlinien 2003/124/EG, 2003/125/EG und 2004/72/EG der Kommission (ABl. 2014, L 173, S. 1) in Verbindung mit Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) (ABl. 2002, L 201, S. 37) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 (ABl. 2009, L 337, S. 11) geänderten Fassung (im Folgenden: Richtlinie 2002/58) im Licht der Art. 7, 8, 11 und 52 Abs. 1 der Charta der Grundrechte der Europäischen Union (im Folgenden: Charta).
- 2 Sie ergeben im Rahmen von gegen VD und SR wegen Insiderhandels, Hehlerei im Zusammenhang mit Insiderhandel, Beihilfe, Bestechung und Geldwäsche eingeleiteter Strafverfahren.

Rechtlicher Rahmen

Unionsrecht

Richtlinie 2002/58

- 3 In den Erwägungsgründen 2, 6, 7 und 11 der Richtlinie 2002/58 heißt es:

„(2) Ziel dieser Richtlinie ist die Achtung der Grundrechte; sie steht insbesondere im Einklang mit den durch die Charta ... anerkannten Grundsätzen. Insbesondere soll mit dieser Richtlinie gewährleistet werden, dass die in den Artikeln 7 und 8 [der] Charta niedergelegten Rechte uneingeschränkt geachtet werden.

...

(6) Das Internet revolutioniert die herkömmlichen Marktstrukturen, indem es eine gemeinsame, weltweite Infrastruktur für die Bereitstellung eines breiten Spektrums elektronischer Kommunikationsdienste bietet. Öffentlich zugängliche elektronische Kommunikationsdienste über das Internet eröffnen neue Möglichkeiten für die Nutzer, bilden aber auch neue Risiken in Bezug auf ihre personenbezogenen Daten und ihre Privatsphäre.

- (7) Für öffentliche Kommunikationsnetze sollten besondere rechtliche, ordnungspolitische und technische Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und der berechtigten Interessen juristischer Personen erlassen werden, insbesondere im Hinblick auf die zunehmenden Fähigkeiten zur automatischen Speicherung und Verarbeitung personenbezogener Daten über Teilnehmer und Nutzer.

...

- (11) Wie die Richtlinie 95/46/EG [des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. 1995, L 281, S. 31)] gilt auch die vorliegende Richtlinie nicht für Fragen des Schutzes der Grundrechte und Grundfreiheiten in Bereichen, die nicht unter das Gemeinschaftsrecht fallen. Deshalb hat sie keine Auswirkungen auf das bestehende Gleichgewicht zwischen dem Recht des Einzelnen auf Privatsphäre und der Möglichkeit der Mitgliedstaaten, Maßnahmen nach Artikel 15 Absatz 1 dieser Richtlinie zu ergreifen, die für den Schutz der öffentlichen Sicherheit, für die Landesverteidigung, für die Sicherheit des Staates (einschließlich des wirtschaftlichen Wohls des Staates, soweit die Tätigkeiten die Sicherheit des Staates berühren) und für die Durchsetzung strafrechtlicher Bestimmungen erforderlich sind. Folglich betrifft diese Richtlinie nicht die Möglichkeit der Mitgliedstaaten zum rechtmäßigen Abfangen elektronischer Nachrichten oder zum Ergreifen anderer Maßnahmen, sofern dies erforderlich ist, um einen dieser Zwecke zu erreichen, und sofern dies im Einklang mit der [am 4. November 1950 in Rom unterzeichneten] Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten in ihrer Auslegung durch die Urteile des Europäischen Gerichtshofs für Menschenrechte erfolgt. Diese Maßnahmen müssen sowohl geeignet sein als auch in einem strikt angemessenen Verhältnis zum intendierten Zweck stehen und ferner innerhalb einer demokratischen Gesellschaft notwendig sein sowie angemessenen Garantien gemäß der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten entsprechen.“

4 Art. 1 („Geltungsbereich und Zielsetzung“) der Richtlinie 2002/58 bestimmt:

„(1) Diese Richtlinie sieht die Harmonisierung der Vorschriften der Mitgliedstaaten vor, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten.“

(2) Die Bestimmungen dieser Richtlinie stellen eine Detaillierung und Ergänzung der Richtlinie [95/46] im Hinblick auf die in Absatz 1 genannten Zwecke dar. Darüber hinaus regeln sie den Schutz der berechtigten Interessen von Teilnehmern, bei denen es sich um juristische Personen handelt.

(3) Diese Richtlinie gilt nicht für Tätigkeiten, die nicht in den Anwendungsbereich des [AEU-Vertrags] fallen, beispielsweise Tätigkeiten gemäß den Titeln V und VI des [EU-Vertrags], und auf keinen Fall für Tätigkeiten betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Tätigkeit die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich.“

5 Art. 2 („Begriffsbestimmungen“) der Richtlinie 2002/58 bestimmt in Abs. 2 Buchst. b:

„[I]m Sinne dieser Richtlinie [bezeichnet] der Ausdruck

...

b) ‚Verkehrsdaten‘ Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden“.

6 Art. 5 („Vertraulichkeit der Kommunikation“) der Richtlinie 2002/58 bestimmt:

„(1) Die Mitgliedstaaten stellen die Vertraulichkeit der mit öffentlichen Kommunikationsnetzen und öffentlich zugänglichen Kommunikationsdiensten übertragenen Nachrichten und der damit verbundenen Verkehrsdaten durch innerstaatliche Vorschriften sicher. Insbesondere untersagen sie das Mithören, Abhören und Speichern sowie andere Arten des Abfangens oder Überwachens von Nachrichten und der damit verbundenen Verkehrsdaten durch andere Personen als die Nutzer, wenn keine Einwilligung der betroffenen Nutzer vorliegt, es sei denn, dass diese Personen gemäß Artikel 15 Absatz 1 gesetzlich dazu ermächtigt sind. Diese Bestimmung steht – unbeschadet des Grundsatzes der Vertraulichkeit – der für die Weiterleitung einer Nachricht erforderlichen technischen Speicherung nicht entgegen.

(2) Absatz 1 betrifft nicht das rechtlich zulässige Aufzeichnen von Nachrichten und der damit verbundenen Verkehrsdaten, wenn dies im Rahmen einer rechtmäßigen Geschäftspraxis zum Nachweis einer kommerziellen Transaktion oder einer sonstigen geschäftlichen Nachricht geschieht.

(3) Die Mitgliedstaaten stellen sicher, dass die Speicherung von Informationen oder der Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind, nur gestattet ist, wenn der

betreffende Teilnehmer oder Nutzer auf der Grundlage von klaren und umfassenden Informationen, die er gemäß der Richtlinie [95/46] u. a. über die Zwecke der Verarbeitung erhält, seine Einwilligung gegeben hat. Dies steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz ist oder wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Nutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann.“

7 Art. 6 („Verkehrsdaten“) der Richtlinie 2002/58 bestimmt:

„(1) Verkehrsdaten, die sich auf Teilnehmer und Nutzer beziehen und vom Betreiber eines öffentlichen Kommunikationsnetzes oder eines öffentlich zugänglichen Kommunikationsdienstes verarbeitet und gespeichert werden, sind unbeschadet der Absätze 2, 3 und 5 des vorliegenden Artikels und des Artikels 15 Absatz 1 zu löschen oder zu anonymisieren, sobald sie für die Übertragung einer Nachricht nicht mehr benötigt werden.

(2) Verkehrsdaten, die zum Zwecke der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen erforderlich sind, dürfen verarbeitet werden. Diese Verarbeitung ist nur bis zum Ablauf der Frist zulässig, innerhalb deren die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann.

(3) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes kann die in Absatz 1 genannten Daten zum Zwecke der Vermarktung elektronischer Kommunikationsdienste oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und innerhalb des dazu oder zur Vermarktung erforderlichen Zeitraums verarbeiten, sofern der Teilnehmer oder der Nutzer, auf den sich die Daten beziehen, zuvor seine Einwilligung gegeben hat. Der Nutzer oder der Teilnehmer hat die Möglichkeit, seine Einwilligung zur Verarbeitung der Verkehrsdaten jederzeit zu widerrufen.

...

(5) Die Verarbeitung von Verkehrsdaten gemäß den Absätzen 1, 2, 3 und 4 darf nur durch Personen erfolgen, die auf Weisung der Betreiber öffentlicher Kommunikationsnetze und öffentlich zugänglicher Kommunikationsdienste handeln und die für Gebührenabrechnungen oder Verkehrsabwicklung, Kundenanfragen, Betrugsermittlung, die Vermarktung der elektronischen Kommunikationsdienste oder für die Bereitstellung eines Dienstes mit Zusatznutzen zuständig sind; ferner ist sie auf das für diese Tätigkeiten erforderliche Maß zu beschränken.

...“

- 8 Art. 9 („Andere Standortdaten als Verkehrsdaten“) der Richtlinie 2002/58 bestimmt in Abs. 1:

„(1) Können andere Standortdaten als Verkehrsdaten in Bezug auf die Nutzer oder Teilnehmer von öffentlichen Kommunikationsnetzen oder öffentlich zugänglichen Kommunikationsdiensten verarbeitet werden, so dürfen diese Daten nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn die Nutzer oder Teilnehmer ihre Einwilligung gegeben haben. Der Diensteanbieter muss den Nutzern oder Teilnehmern vor Einholung ihrer Einwilligung mitteilen, welche Arten anderer Standortdaten als Verkehrsdaten verarbeitet werden, für welche Zwecke und wie lange das geschieht, und ob die Daten zum Zwecke der Bereitstellung des Dienstes mit Zusatznutzen an einen Dritten weitergegeben werden. ...“

- 9 Art. 15 („Anwendung einzelner Bestimmungen der Richtlinie [95/46]“) der Richtlinie 2002/58 bestimmt in Abs. 1:

„(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie [95/46] für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit sowie die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem durch Rechtsvorschriften vorsehen, dass Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit aufbewahrt werden. Alle in diesem Absatz genannten Maßnahmen müssen den allgemeinen Grundsätzen des Gemeinschaftsrechts einschließlich den in Artikel 6 Absätze 1 und 2 [EUV] niedergelegten Grundsätzen entsprechen.“

Richtlinie 2003/6

- 10 In den Erwägungsgründen 1, 2, 12, 37, 41 und 44 der Richtlinie 2003/6 heißt es:

„(1) Ein echter Binnenmarkt für Finanzdienstleistungen ist für das Wirtschaftswachstum und die Schaffung von Arbeitsplätzen in der Gemeinschaft von entscheidender Bedeutung.

(2) Ein integrierter und effizienter Finanzmarkt setzt Marktintegrität voraus. Das reibungslose Funktionieren der Wertpapiermärkte und das Vertrauen der Öffentlichkeit in die Märkte sind Voraussetzungen für Wirtschaftswachstum und Wohlstand. Marktmissbrauch verletzt die

Integrität der Finanzmärkte und untergräbt das Vertrauen der Öffentlichkeit in Wertpapiere und Derivate.

...

- (12) Marktmissbrauch beinhaltet Insider-Geschäfte und Marktmanipulation. Vorschriften zur Bekämpfung von Insider-Geschäften haben dasselbe Ziel wie Vorschriften zur Bekämpfung von Marktmanipulation, nämlich die Integrität der Finanzmärkte der Gemeinschaft sicherzustellen und das Vertrauen der Anleger in diese Märkte zu stärken. ...

...

- (37) Ein gemeinsames Mindestmaß an wirksamen Mitteln und Befugnissen der zuständigen Behörden der Mitgliedstaaten ist notwendig, um eine wirksame Aufsicht sicherzustellen. Auch die Marktteilnehmer und alle Wirtschaftsakteure sollten in ihrem Bereich einen Beitrag zur Marktintegrität leisten. ...

...

- (41) Da das Ziel der vorgeschlagenen Maßnahmen, nämlich die Verhütung von Marktmissbrauch in Form von Insider-Geschäften und Marktmanipulationen, auf Ebene der Mitgliedstaaten nicht ausreichend erreicht werden kann und daher wegen des Umfangs und der Wirkung der Maßnahmen besser auf Gemeinschaftsebene zu erreichen ist, kann die Gemeinschaft im Einklang mit dem in Artikel 5 [EUV] niedergelegten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Verhältnismäßigkeitsprinzip geht diese Richtlinie nicht über das für die Erreichung dieses Ziels erforderliche Maß hinaus.

- (44) Diese Richtlinie steht im Einklang mit den Grundrechten und Grundsätzen, die insbesondere mit der Charta ..., insbesondere Artikel 11, sowie mit Artikel 10 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten anerkannt wurden. ...“

11 Art. 11 der Richtlinie 2003/6 bestimmt:

„Unbeschadet der Zuständigkeiten der Justizbehörden benennen die Mitgliedstaaten eine einzige Behörde, die für die Überwachung der Anwendung der nach dieser Richtlinie erlassenen Vorschriften zuständig ist.

...“

12 Art. 12 der Richtlinie 2003/6 bestimmt:

„(1) Die zuständige Behörde ist mit allen Aufsichts- und Ermittlungsbefugnissen auszustatten, die zur Ausübung ihrer Tätigkeit erforderlich sind. ...

(2) Unbeschadet des Artikels 6 Absatz 7 werden die in Absatz 1 des vorliegenden Artikels genannten Befugnisse im Einklang mit dem innerstaatlichen Recht ausgeübt und beinhalten zumindest das Recht,

a) Unterlagen aller Art einzusehen und Kopien von ihnen zu erhalten,

...

d) bereits existierende Aufzeichnungen von Telefongesprächen und Datenübermittlungen anzufordern,

...“

Verordnung Nr. 596/2014

13 Die Richtlinie 2003/6 wurde durch die Verordnung Nr. 596/2014 mit Wirkung ab dem 3. Juli 2016 aufgehoben und ersetzt.

14 In den Erwägungsgründen 1, 2, 7, 24, 44, 62, 65, 66, 77 und 86 der Verordnung Nr. 596/2014 heißt es:

„(1) Ein echter Binnenmarkt für Finanzdienstleistungen ist für das Wirtschaftswachstum und die Schaffung von Arbeitsplätzen in der Union von entscheidender Bedeutung.

(2) Ein integrierter, effizienter und transparenter Finanzmarkt setzt Marktintegrität voraus. Das reibungslose Funktionieren der Wertpapiermärkte und das Vertrauen der Öffentlichkeit in die Märkte sind Voraussetzungen für Wirtschaftswachstum und Wohlstand. Marktmissbrauch verletzt die Integrität der Finanzmärkte und untergräbt das Vertrauen der Öffentlichkeit in Wertpapiere und Derivate.

...

(7) Marktmissbrauch ist ein Oberbegriff für unrechtmäßige Handlungen an den Finanzmärkten und sollte für die Zwecke dieser Verordnung Insidergeschäfte oder die unrechtmäßige Offenlegung von Insiderinformationen und Marktmanipulation umfassen. Solche Handlungen verhindern vollständige und ordnungsgemäße Markttransparenz, die eine Voraussetzung dafür ist, dass alle Wirtschaftsakteure an integrierten Finanzmärkten teilnehmen können.

...

(24) Wenn eine juristische oder natürliche Personen im Besitz von Insiderinformationen für eigene Rechnung oder für Rechnung Dritter, sei es unmittelbar oder mittelbar, Finanzinstrumente, auf die sich diese Informationen beziehen, erwirbt oder veräußert bzw. zu erwerben oder zu veräußern versucht, sollte unterstellt werden, dass diese Person diese Informationen genutzt hat. Diese Annahme lässt die Verteidigungsrechte unberührt. Ob eine Person gegen das Verbot von Insidergeschäften verstoßen hat oder versucht hat, Insidergeschäfte durchzuführen, sollte im Hinblick auf den Zweck dieser Verordnung untersucht werden, der darin besteht, die Integrität des Finanzmarkts zu schützen und das Vertrauen der Investoren zu stärken, das wiederum auf der Gewissheit beruht, dass die Investoren gleichbehandelt und vor der missbräuchlichen Verwendung von Insiderinformationen geschützt werden.

...

(44) Der Preis vieler Finanzinstrumente wird durch Bezugnahme auf Referenzwerte festgesetzt. Eine tatsächliche oder versuchte Manipulation von Referenzwerte[n], einschließlich der Angebotssätze im Interbankengeschäft, kann das Marktvertrauen erheblich beeinträchtigen und zu beträchtlichen Verlusten für die Anleger wie auch zu realwirtschaftlichen Verzerrungen führen. ...

(62) Eine wirkungsvolle Aufsicht wird durch eine Reihe wirksamer Instrumente und Befugnisse sowie von Ressourcen für die zuständigen Behörden der Mitgliedstaaten sichergestellt. Diese Verordnung sieht daher insbesondere ein Mindestmaß an Aufsichts- und Untersuchungsbefugnissen vor, die den zuständigen Behörden der Mitgliedstaaten gemäß nationalem Recht übertragen werden sollten. Wenn es die nationalen Rechtsvorschriften erfordern, sollten diese Befugnisse durch Antrag bei den zuständigen Justizbehörden ausgeübt werden. ...

...

(65) Bereits vorhandene Aufzeichnungen von Telefongesprächen und Datenverkehrsaufzeichnungen von Wertpapierfirmen, Kreditinstituten und anderen Finanzinstituten, die Geschäfte ausführen und diese Ausführung dokumentieren, sowie bereits vorhandene Telefon- und Datenverkehrsaufzeichnungen von Telekommunikationsgesellschaften stellen entscheidende und manchmal die einzigen Belege für die Aufdeckung und den Nachweis des Bestehens von Insiderhandel und Marktmanipulation dar. Mit Telefon- und Datenverkehrsaufzeichnungen kann die Identität einer für die Verbreitung falscher oder irreführender Informationen verantwortlichen Person ermittelt oder festgestellt werden, dass Personen zu einer bestimmten Zeit Kontakt hatten und dass eine Beziehung zwischen zwei oder mehr Personen besteht. Die zuständigen

Behörden sollten daher befugt sein, bestehende Aufzeichnungen von Telefongesprächen, elektronischer Kommunikation und Datenverkehrsaufzeichnungen anzufordern, die sich gemäß der Richtlinie 2014/65/EU [des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU (ABl. 2014, L 173, S. 349)] im Besitz einer Wertpapierfirma, eines Kreditinstituts oder eines Finanzinstituts befinden. Der Zugang zu Telefon- und Datenverkehrsaufzeichnungen ist erforderlich, um Beweise und Ermittlungsansätze in Bezug auf Insidergeschäfte und Marktmanipulation und mithin zur Aufdeckung von Marktmissbrauch und zum Verhängen von Sanktionen dagegen zu erlangen. Zur Schaffung einheitlicher Bedingungen in der Union in Bezug auf den Zugang zu Telefon- und bestehenden Datenverkehrsaufzeichnungen im Besitz einer Telekommunikationsgesellschaft oder zu bestehenden Aufzeichnungen von Telefongesprächen und Datenverkehr im Besitz einer Wertpapierfirma, eines Kreditinstituts oder eines Finanzinstituts sollten die zuständigen Behörden im Einklang mit den nationalen Rechtsvorschriften befugt sein, bestehende Telefon- und Datenverkehrsaufzeichnungen, die sich, soweit die nationalen Rechtsvorschriften dies gestatten, im Besitz einer Telekommunikationsgesellschaft befinden, und bestehende Aufzeichnungen von Telefongesprächen und Datenverkehr im Besitz einer Wertpapierfirma anzufordern, wenn es sich um Fälle handelt, in denen der begründete Verdacht besteht, dass diese Aufzeichnungen mit Bezug zum Gegenstand der Überprüfung oder Untersuchung für den Nachweis von Insidergeschäften oder Marktmanipulation unter Verstoß gegen diese Verordnung relevant sein können. Der Zugang zu Telefon- und Datenverkehrsaufzeichnungen im Besitz von Telekommunikationsgesellschaften umfasst nicht den Zugang zu Inhalten von Telefongesprächen.

- (66) Obgleich in dieser Verordnung ein Mindestmaß an Befugnissen festgelegt wird, die die zuständigen Behörden haben sollten[,] müssen diese Befugnisse im Rahmen eines Gesamtsystems nationaler Rechtsvorschriften ausgeübt werden, in denen die Einhaltung der Grundrechte unter Einschluss des Rechts auf Schutz der Privatsphäre garantiert wird. Für den Zweck der Ausübung dieser Befugnisse, durch die es zu gravierenden Eingriffen in Bezug auf das Recht auf Achtung des Privat- und Familienlebens, der Wohnung sowie der Kommunikation kommen kann, sollten in den Mitgliedstaaten angemessene und wirksame Schutzvorkehrungen gegen jegliche Form des Missbrauchs bestehen, beispielsweise, falls erforderlich, das Erfordernis zur Einholung einer vorherigen Genehmigung der Justizbehörden eines betroffenen Mitgliedstaats. Die Mitgliedstaaten sollten die Möglichkeit vorsehen, dass die zuständigen Behörden derartige Eingriffsbefugnisse in dem Umfang

ausüben, in dem dies für die ordnungsgemäße Untersuchung schwerwiegender Fälle erforderlich ist, sofern keine gleichwertigen Mittel zur Verfügung stehen, mit denen wirksam dasselbe Ergebnis erzielt werden kann.

...

(77) Diese Verordnung steht im Einklang mit den Grundrechten und Grundsätzen, die mit der Charta ... anerkannt wurden. Diese Verordnung sollte daher im Einklang mit diesen Rechten und Grundsätzen ausgelegt und angewandt werden. ...

...

(86) Da das Ziel dieser Verordnung, nämlich die Verhütung von Marktmissbrauch in Form von Insidergeschäften, unrechtmäßiger Offenlegung von Insiderinformationen und Marktmanipulation, von den Mitgliedstaaten nicht ausreichend erreicht werden kann, sondern vielmehr wegen ihres Umfangs und ihrer Wirkung auf Unionsebene besser zu verwirklichen ist, kann die Union im Einklang mit dem in Artikel 5 [EUV] verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.“

15 Art. 1 der Verordnung Nr. 596/2014 bestimmt:

„Mit dieser Verordnung wird ein gemeinsamer Rechtsrahmen für Insidergeschäfte, die unrechtmäßige Offenlegung von Insiderinformationen und Marktmanipulation (Marktmissbrauch) sowie für Maßnahmen zur Verhinderung von Marktmissbrauch geschaffen, um die Integrität der Finanzmärkte in der Union sicherzustellen und den Anlegerschutz und das Vertrauen der Anleger in diese Märkte zu stärken.“

16 Art. 3 („Begriffsbestimmungen“) der Verordnung Nr. 596/2014 bestimmt in Abs. 1 Nr. 27:

„Für die Zwecke dieser Verordnung gelten folgende Begriffsbestimmungen:

...

27. ‚Datenverkehrsaufzeichnungen‘ bezeichnet die Aufzeichnungen von Verkehrsdaten im Sinne von Artikel 2 Buchstabe b Unterabsatz 2 der Richtlinie [2002/58]“.

17 Art. 14 („Verbot von Insidergeschäften und unrechtmäßiger Offenlegung von Insiderinformationen“) der Verordnung Nr. 596/2014 bestimmt:

„Folgende Handlungen sind verboten:

- a) das Tätigen von Insidergeschäften und der Versuch hierzu,
- b) Dritten zu empfehlen, Insidergeschäfte zu tätigen, oder Dritte dazu zu verleiten, Insidergeschäfte zu tätigen, oder
- c) die unrechtmäßige Offenlegung von Insiderinformationen.“

18 Art. 22 der Verordnung Nr. 596/2014 bestimmt:

„Unbeschadet der Zuständigkeiten der Justizbehörden benennen die Mitgliedstaaten eine einzige Behörde, die für die Zwecke dieser Verordnung zuständig ist. ...“

19 Art. 23 („Befugnisse der zuständigen Behörden“) der Verordnung Nr. 596/2014 bestimmt in den Abs. 2 und 3:

„(2) Zur Wahrnehmung ihrer Aufgaben gemäß dieser Verordnung müssen die zuständigen Behörden nach nationalem Recht zumindest über die folgenden Aufsichts- und Ermittlungsbefugnisse verfügen:

- a) Zugang zu jedweden Unterlagen und Daten in jeder Form zu haben und Kopien von ihnen zu erhalten oder anzufertigen;

...

- g) bestehende Aufzeichnungen von Telefongesprächen oder elektronischen Mitteilungen oder Datenverkehrsaufzeichnungen im Besitz von Wertpapierfirmen, Kreditinstituten oder Finanzinstituten anzufordern;

- h) bestehende Datenverkehrsaufzeichnungen im Besitz einer Telekommunikationsgesellschaft anzufordern, wenn der begründete Verdacht eines Verstoßes besteht und wenn diese Aufzeichnungen für die Untersuchung eines Verstoßes gegen Artikel 14 Buchstaben a oder b oder Artikel 15 relevant sein können, soweit dies nach nationalem Recht zulässig ist;

...

(3) Die Mitgliedstaaten stellen durch geeignete Maßnahmen sicher, dass die zuständigen Behörden alle zur Wahrnehmung ihrer Aufgaben erforderlichen Aufsichts- und Ermittlungsbefugnisse haben.

...“

Französisches Recht

CPCE

20 Das Gesetzbuch betreffend das Postwesen und die elektronische Kommunikation (Code des postes et des communications électroniques) in der auf die Ausgangsverfahren anwendbaren Fassung (im Folgenden: CPCE) bestimmte in Art. L. 34-1:

„I. – Dieser Artikel gilt für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung von öffentlich zugänglichen Diensten der elektronischen Kommunikation; er gilt insbesondere für Netze, die Datenerfassungs- und Identifizierungsgeräte unterstützen.

II. – Anbieter von Diensten der elektronischen Kommunikation, insbesondere Personen, deren Tätigkeit darin besteht, öffentlich zugängliche Dienste der Kommunikation online bereitzustellen, löschen oder anonymisieren sämtliche Verkehrsdaten; die Bestimmungen in den Absätzen III, IV, V und VI bleiben unberührt.

Personen, die öffentlich zugängliche Dienste der elektronischen Kommunikation bereitstellen, führen unter Beachtung der Bestimmungen des vorstehenden Unterabsatzes interne Verfahren ein, um Ersuchen der zuständigen Behörden nachkommen zu können.

Personen, die im Rahmen einer haupt- oder nebenberuflichen Tätigkeit eine öffentlich zugängliche Verbindung bereitstellen, die über einen Netzzugang eine Online-Kommunikation ermöglicht, müssen die Bestimmungen beachten, die nach dem vorliegenden Artikel für die Anbieter von Diensten der elektronischen Kommunikation gelten; dies gilt auch, wenn die Verbindung kostenlos bereitgestellt wird.

III. – Zum Zweck der Ermittlung, Feststellung und Verfolgung von Straftaten oder eines Verstoßes gegen die Verpflichtung gemäß Artikel L. 336-3 des Gesetzbuchs über geistiges Eigentum [(Code de la propriété intellectuelle)] oder zum Zweck der Verhinderung von Beeinträchtigungen der Systeme zur automatisierten Verarbeitung von Daten, die nach den Artikeln 323-1 bis 323-3-1 des Strafgesetzbuchs [(Code pénal)] strafbar sind, können Maßnahmen zur Löschung oder Anonymisierung bestimmter Arten von technischen Daten bis zu einem Jahr aufgeschoben werden, aber nur, um diese Daten, soweit erforderlich, der Justizbehörde oder der in Artikel L. 331-12 des Gesetzbuchs über geistiges Eigentum genannten Hohen Behörde [(Haute Autorité)] oder der in Artikel L. 2321-1 des Verteidigungsgesetzbuchs [(Code de la défense)] genannten Nationalen Behörde für die Sicherheit der Informationssysteme [(Autorité nationale de sécurité des systèmes d'information)] zur Verfügung zu stellen. Diese Arten von Daten und die Dauer ihrer Speicherung, je nach der Tätigkeit der Anbieter und der Art der Kommunikationen, sowie die Modalitäten des etwaigen Ausgleichs der ermittelbaren spezifischen Mehrkosten für die von den Anbietern insoweit auf Ersuchen des Staates erbrachten Leistungen werden innerhalb der in Absatz VI festgelegten Grenzen in einem nach Anhörung des Conseil d'État [(Staatsrat)] und nach

Stellungnahme der Nationalen Kommission für Informatik und Freiheiten [(Commission nationale de l'informatique et des libertés)] zu erlassenden Dekret bestimmt.

...

VI. – Die Daten, die unter den in den Absätzen III, IV und V festgelegten Voraussetzungen auf Vorrat gespeichert und verarbeitet werden, beziehen sich ausschließlich auf die Identifizierung der Nutzer der von den Anbietern bereitgestellten Dienste, die technischen Merkmale der von den Anbietern ermöglichten Kommunikationen und den Standort der Endgeräte.

Sie dürfen sich auf keinen Fall auf den Inhalt der ausgetauschten Nachrichten oder auf die Informationen beziehen, die, in welcher Form auch immer, im Rahmen dieser Kommunikationen abgerufen wurden.

Bei der Vorratsspeicherung und Verarbeitung dieser Daten sind die Bestimmungen des Gesetzes Nr. 78-17 vom 6. Januar 1978 über Informatik, Dateien und Freiheiten [(Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)] zu beachten.

Die Anbieter ergreifen alle Maßnahmen, um eine Verwendung dieser Daten zu anderen als den in diesem Artikel vorgesehenen Zwecken zu verhindern.“

- 21 Art. L. 34-1 des Gesetzbuchs betreffend das Postwesen und die elektronische Kommunikation in der Fassung des Gesetzes Nr. 2021-998 vom 30. Juli 2021 betreffend die Terrorismusbekämpfung und die nachrichtendienstliche Aufklärung (Loi n° 2021-998, du 30 juillet 2021, relative à la prévention d'actes de terrorisme et au renseignement, JORF vom 31. Juli 2021, Text Nr. 1) bestimmt in den Absätzen IIa bis IIIa:

„IIa. – Die Anbieter von Diensten der elektronischen Kommunikation sind verpflichtet, auf Vorrat zu speichern:

1. für die Zwecke der Strafverfolgung, der Abwehr von Gefahren für die öffentliche Sicherheit und des Schutzes der nationalen Sicherheit die Informationen über die Identität des Nutzers bis zum Ablauf von fünf Jahren ab dem Ende der Gültigkeit des Vertrags;

2. für die in Nummer 1 genannten Zwecke die übrigen Angaben, die der Nutzer beim Abschluss eines Vertrags oder der Einrichtung eines Kontos macht, und die Informationen über die Zahlung bis zum Ablauf von einem Jahr ab dem Ende der Laufzeit des Vertrags bzw. dem Zeitpunkt, zu dem das Konto geschlossen wird;

3. für die Zwecke der Bekämpfung schwerer Kriminalität, der Abwehr schwerer Gefahren für die öffentliche Sicherheit und des Schutzes der nationalen Sicherheit die technischen Daten, anhand derer sich die Quelle der

Verbindung feststellen lässt, oder die technischen Daten betreffend die verwendeten Endgeräte bis zum Ablauf von einem Jahr ab der Verbindung oder der Verwendung der Endgeräte.

III. – Wird eine schwere, gegenwärtige oder vorhersehbare Gefahr für die nationale Sicherheit festgestellt, kann der Premierminister den Anbietern von Diensten der elektronischen Kommunikation aus Gründen des Schutzes der nationalen Sicherheit durch ein Dekret die Verpflichtung auferlegen, für die Dauer eines Jahres bestimmte Arten von Verkehrsdaten, zusätzlich zu den in Absatz IIa Nummer 3 genannten, und von Lokalisierungsdaten auf Vorrat zu speichern; diese Arten von Daten werden nach Anhörung des Conseil d'État [(Staatsrat)] durch ein Dekret bestimmt.

Die Anordnung des Premierministers, die nur bis zu einem Jahr gelten kann, kann verlängert werden, wenn die Voraussetzungen, aufgrund derer sie getroffen wurde, weiter erfüllt sind. Das Auslaufen der Anordnung hat keinen Einfluss auf die Dauer der Speicherung der in Unterabsatz 1 genannten Daten.

IIIa. – Die Behörden, die nach dem Gesetz zum Zweck der Bekämpfung und Verfolgung von Verbrechen, schweren Vergehen und anderen schweren Verstößen gegen die Vorschriften, für deren Einhaltung sie zu sorgen haben, Zugang zu den Daten der elektronischen Kommunikation haben, können anordnen, dass die Daten, die von den Anbietern gemäß diesem Artikel auf Vorrat gespeichert werden, umgehend zu sichern sind, damit sie Zugang zu diesen Daten haben.“

22 Art. R. 10-13 CPCE bestimmt:

„I. – Die Anbieter von Diensten der elektronischen Kommunikation speichern für die Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten gemäß Artikel L. 34-1 Absatz III auf Vorrat:

- a) die Informationen, anhand derer sich der Nutzer identifizieren lässt;
- b) die Daten über die verwendeten Kommunikationsendgeräte;
- c) die technischen Merkmale sowie Datum, Uhrzeit und Dauer jeder Kommunikation;
- d) die Daten über bestellte oder in Anspruch genommene Zusatzleistungen und deren Anbieter;
- e) die Daten, anhand derer sich die Identität des oder der Adressaten der Kommunikation feststellen lässt.

II. – Bei Telefondiensten speichert der Anbieter die in Absatz II genannten Daten sowie die Daten, anhand derer sich der Ausgangspunkt und der Standort der Kommunikation bestimmen lassen, auf Vorrat.

III. – Die in diesem Artikel genannten Daten werden für die Dauer eines Jahres ab dem Tag der Speicherung gespeichert.

...“

LCEN

23 Art. 6 des Gesetzes Nr. 2004-575 vom 21. Juni 2004 für das Vertrauen in die digitale Wirtschaft (Loi n° 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique, JORF vom 22. Juni 2004, S. 11168) in der auf die Ausgangsverfahren anwendbaren Fassung (im Folgenden: LCEN) bestimmte:

„I. – 1. Personen, deren Tätigkeit darin besteht, online öffentlich zugängliche Dienste der Kommunikation bereitzustellen, informieren ihre Kunden darüber, dass es technische Mittel gibt, mit denen der Zugang zu bestimmten Diensten beschränkt werden kann oder bestimmte Dienste ausgewählt werden können, und bieten ihnen mindestens eines dieser Mittel an.

...

2. Natürliche oder juristische Personen, die, sei es auch kostenlos, zur Bereitstellung für die Öffentlichkeit durch öffentlich zugängliche Online-Kommunikationsdienste die Speicherung der von den Adressaten dieser Dienste gelieferten Signale, Schriftstücke, Bilder, Töne oder Nachrichten jeder Art gewährleisten, können für Tätigkeiten oder für Informationen, die auf Verlangen eines Adressaten dieser Dienste gespeichert wurden, nicht zivilrechtlich verantwortlich gemacht werden, wenn sie nicht tatsächlich Kenntnis von ihrem rechtswidrigen Charakter oder von Tatsachen und Umständen, aus denen sich dieser Charakter ergab, hatten oder wenn sie, sobald sie davon Kenntnis erlangten, unverzüglich tätig wurden, um diese Daten zu entfernen oder den Zugang zu ihnen unmöglich zu machen.

...

II. – Die in Absatz I Unterabsätze 1 und 2 genannten Personen erheben und speichern die Daten in einer Weise auf Vorrat, die die Identifizierung jeder Person ermöglicht, die zur Schaffung des Inhalts oder eines der Inhalte der von ihnen erbrachten Dienste beigetragen hat.

Sie stellen den Personen, die einen öffentlich zugänglichen Online-Kommunikationsdienst betreiben, die technischen Mittel zur Verfügung, mit denen sie die in Absatz III vorgesehenen Voraussetzungen für die Identifizierung erfüllen können.

Die Justizbehörde kann von den in Absatz I Absätze 1 und 2 genannten Anbietern die Übermittlung der in Unterabsatz 1 genannten Daten verlangen.

Für die Verarbeitung dieser Daten gelten die Bestimmungen der Artikel 226-17, 226-21 und 226-22 des Strafgesetzbuchs.

Die in Unterabsatz 1 genannten Daten sowie die Dauer und die Modalitäten ihrer Vorratsspeicherung werden in einem nach Anhörung des Conseil d'État [(Staatsrat)] und nach Stellungnahme der Nationalen Kommission für Informatik und Freiheiten zu erlassenden Dekret bestimmt.

...“

CMF

- 24 Art. L. 621-10 des Code monétaire et financier (Gesetzbuch über das Währungs- und Finanzwesen) in der auf die Ausgangsverfahren anwendbaren Fassung (im Folgenden: CMF) bestimmte in Abs. 1:

„Die Ermittler und die Kontrolleure können, soweit dies für die Untersuchung oder die Kontrolle erforderlich ist, alle Dokumente anfordern, gleich in welcher Form. Die Ermittler können auch die von den Telekommunikationsanbietern gemäß Artikel L. 34-1 [CPCE] oder den in Artikel 6 Absatz 1 Unterabsätze 1 und 2 [LCEN] genannten Dienstleistungserbringern auf Vorrat gespeicherten und verarbeiteten Daten oder eine Kopie davon anfordern.

...“

- 25 Nachdem der Conseil constitutionnel (Verfassungsrat, Frankreich) mit Entscheidung vom 21. Juli 2017 die Verfassungswidrigkeit von Art. L. 621-10 Abs. 1 Satz 2 CMF festgestellt hatte, wurde mit dem Gesetz Nr. 2018-898 vom 23. Oktober 2018 über die Betrugsbekämpfung (Loi n° 2018-898, du 23 octobre 2018, relative à la lutte contre la fraude, JORF vom 24. Oktober 2018, Text Nr. 1) folgender Art. L. 621-10-2 in den CMF eingefügt:

„Zur Aufdeckung von Marktmissbrauch im Sinne der Verordnung [Nr. 596/2014] können die Ermittler unter den Voraussetzungen und in den Grenzen des Artikels L. 34-1 [CPCE] die von den Telekommunikationsanbietern auf Vorrat gespeicherten und verarbeiteten Daten anfordern; sie können zu diesem Zweck auch die von den in Artikel 6 Absätze 1 und 2 [LCEN] genannten Dienstleistungserbringern auf Vorrat gespeicherten und verarbeiteten Daten anfordern.

Die Übermittlung der in Absatz 1 genannten Daten unterliegt der vorherigen Genehmigung durch eine Person, die für die Überprüfung von Anträgen auf Zugang zu Verbindungsdaten zuständig ist.

Für die Überprüfung von Anträgen auf Zugang zu Verbindungsdaten sind abwechselnd zuständig ein Mitglied oder Mitglied außer Dienst des Conseil d'État [(Staatsrat)], das von der Generalversammlung des Conseil d'État [(Staatsrat)] bestimmt wird, und ein Richter oder Richter außer Dienst der Cour

de cassation [(Kassationsgerichtshof)], der von der Generalversammlung der Cour de cassation [(Kassationsgerichtshof)] bestimmt wird. Der jeweilige Stellvertreter, der von dem jeweils anderen Gericht stammt, wird nach denselben Modalitäten bestimmt. Die Person, die für die Überprüfung von Anträgen auf Zugang zu Verbindungsdaten zuständig ist, und ihr Stellvertreter werden für eine Dauer von vier Jahren gewählt; sie können nicht wiedergewählt werden.

...

Die Person, die für die Überprüfung von Anträgen auf Zugang zu Verbindungsdaten zuständig ist, erhält bei der Ausübung ihres Amtes keine Weisungen von der Finanzaufsichtsbehörde oder einer anderen Behörde und ersucht auch nicht um solche Weisungen. Sie ist gemäß Artikel L. 621-4 dieses Gesetzbuchs zur Verschwiegenheit verpflichtet.

Sie wird auf begründeten Antrag des Generalsekretärs oder des stellvertretenden Generalsekretärs der Finanzaufsichtsbehörde tätig. Der Antrag ist zu begründen.

Die Genehmigung wird in die Ermittlungsakten aufgenommen.

Die Ermittler verwenden die ihnen von den Telekommunikationsanbietern und den in Absatz 1 genannten Dienstleistungserbringern übermittelten Daten ausschließlich für die Ermittlungen, auf die sich die erteilte Genehmigung bezieht.

Verbindungsdaten, die sich auf Sachverhalte beziehen, in Bezug auf die vom Kollegium der Finanzaufsichtsbehörde Rügen erhoben worden sind, werden sechs Monate nach der endgültigen Entscheidung des Sanktionsausschusses oder der Gerichte, die über eingelegte Rechtsmittel zu entscheiden haben, vernichtet. Bei einer Verständigung im Verwaltungsverfahren läuft die Frist von sechs Monaten ab der Durchführung der Vereinbarung.

Verbindungsdaten, die sich auf Sachverhalte beziehen, in Bezug auf die vom Kollegium der Finanzaufsichtsbehörde keine Rügen erhoben worden sind, werden einen Monat nach der Entscheidung des Kollegiums vernichtet.

Wird der Ermittlungsbericht dem für Finanzsachen zuständigen Staatsanwalt vorgelegt oder erhebt dieser ... die öffentliche Klage werden die Verbindungsdaten dem für Finanzsachen zuständigen Staatsanwalt übermittelt und von der Finanzaufsichtsbehörde nicht weiter gespeichert.

Die Modalitäten der Anwendung dieses Artikels werden durch ein nach Anhörung des Conseil d'État [(Staatsrat)] zu erlassendes Dekret festgelegt.“

Ausgangsverfahren, Vorlagefragen und Verfahren vor dem Gerichtshof

- 26 Mit Anklageschrift vom 22. Mai 2014 wurde gegen VD und SR ein gerichtliches Ermittlungsverfahren wegen Insiderhandels und Hehlerei im Zusammenhang mit Insiderhandel eingeleitet. Das Verfahren wurde mit einer ersten ergänzenden Anklageschrift vom 14. November 2014 auf Beihilfe ausgedehnt.
- 27 Am 23. und 25. September 2015 wurden dem Ermittlungsrichter von der Finanzaufsichtsbehörde (Autorité des marchés financiers, AMF, Frankreich) bestimmte Beweise vorgelegt. Die AMF hatte diese im Rahmen von Ermittlungen gemäß Art. L. 621-10 CMF erlangt. Es handelt sich insbesondere um personenbezogene Daten betreffend Telefongespräche von VD und SR, die die Ermittler der AMF auf der Grundlage von Art. L. 34-1 CPCE bei Anbietern von Diensten der elektronischen Kommunikation angefordert hatten.
- 28 Daraufhin wurde das Ermittlungsverfahren mit drei ergänzenden Anklageschriften vom 29. September 2015, vom 22. Dezember 2015 und vom 23. November 2016 auf Bestechung und Geldwäsche ausgedehnt.
- 29 Gegen VD wurde am 10. März 2017 wegen Insiderhandels und Geldwäsche das Hauptverfahren eröffnet, gegen SR am 29. Mai 2017 wegen Insiderhandels.
- 30 Da bei den Entscheidungen über die Eröffnung des Hauptverfahrens von der AMF vorgelegte Verkehrsdaten verwertet wurden, legten VD und SR dagegen bei der Cour d'appel de Paris (Berufungsgericht Paris, Frankreich) jeweils ein Rechtsmittel ein. Sie rügten im Kern insbesondere einen Verstoß gegen Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8, 11 und 52 Abs. 1 der Charta. Sie beriefen sich insbesondere auf die durch das Urteil vom 21. Dezember 2016, Tele2 Sverige und Watson u. a. (C-203/15 und C-698/15, EU:C:2016:970), begründete Rechtsprechung. Die AMF habe sich bei der Erhebung der Daten zu Unrecht auf Art. L. 621-10 CMF und auf Art. L. 34-1 CPCE gestützt. Diese Vorschriften seien, soweit sie eine allgemeine und unterschiedslose Vorratsspeicherung der Verbindungsdaten vorsähen, unionsrechtswidrig. Zudem werde in ihnen die Befugnis der Ermittler der AMF, gespeicherte Daten anzufordern, nicht begrenzt.
- 31 Die Rechtsmittel von VD und SR wurden von der Cour d'appel de Paris (Berufungsgericht Paris) mit Urteilen vom 20. Dezember 2018 bzw. 7. März 2019 zurückgewiesen. Wie aus den Vorlageentscheidungen hervorgeht, hat die Cour d'appel de Paris (Berufungsgericht Paris) die Rüge eines Verstoßes gegen Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8, 11 und Art. 52 Abs. 1 der Charta hauptsächlich mit der Begründung zurückgewiesen, dass die zuständigen Behörden nach Art. 23 Abs. 2 Buchst. h der Verordnung Nr. 596/2014 über Marktmissbrauch bestehende Datenverkehrsaufzeichnungen im Besitz eines Anbieters von Diensten der elektronischen Kommunikation anfordern können, wenn der begründete Verdacht eines Verstoßes gegen das Verbot von Insidergeschäften im Sinne von Art. 14 Buchst. a und b bestehe und

wenn diese Aufzeichnungen für die Untersuchung eines solchen Verstoßes relevant sein könnten, soweit dies nach nationalem Recht zulässig sei.

- 32 VD und SR haben gegen diese Urteile beim vorlegenden Gericht jeweils Kassationsbeschwerde eingelegt. Sie rügen insbesondere einen Verstoß gegen die in der vorstehenden Randnummer genannten Bestimmungen der Charta und der Richtlinie 2002/58.
- 33 Was den Zugang zu den Verbindungsdaten angeht, nimmt das vorlegende Gericht Bezug auf eine Entscheidung des Conseil constitutionnel (Staatsrat) vom 21. Juli 2017. Danach sei das im französischen Recht für den Zugang der Ermittler der AMF zu auf Vorrat gespeicherten personenbezogenen Daten vorgesehene Verfahren nicht mit dem durch Art. 2 der Erklärung der Menschen- und Bürgerrechte (Déclaration des droits de l'homme et du citoyen) von 1789 verbürgten Recht auf Achtung des Privatlebens vereinbar. Zwar habe der nationale Gesetzgeber die Befugnis, solche Daten im Rahmen von Ermittlungen anzufordern, hierzu eigens ermächtigten und zur Verschwiegenheit verpflichteten Personen vorbehalten und diesen Personen keine Befugnis zur Zwangsvollstreckung übertragen. Er habe das Verfahren aber nicht mit Garantien versehen, mit denen ein angemessener Ausgleich zwischen dem Recht auf Achtung des Privatlebens einerseits und dem Schutz der öffentlichen Ordnung und der Strafverfolgung andererseits gewährleistet wäre. Deshalb sei festzustellen, dass Art. L. 621-10 Abs. 1 Satz 2 CMF nicht mit der französischen Verfassung (Constitution française) vereinbar sei.
- 34 Wegen der „offensichtlich übermäßigen“ Auswirkungen, die eine sofortige Aufhebung von Art. L. 621-10 Abs. 1 Satz 2 CMF auf laufende Verfahren haben würde, sei der Conseil constitutionnel aber zu der Einschätzung gelangt, dass der Zeitpunkt der Aufhebung auf den 31. Dezember 2018 zu verschieben sei. Der nationale Gesetzgeber habe, nachdem Art. L. 621-10 Abs. 1 CMF für verfassungswidrig erklärt worden sei, Art. L. 621-10-2 in den CMF aufgenommen.
- 35 Das vorlegende Gericht weist auf Rn. 125 des Urteils vom 21. Dezember 2016, *Tele2 Sverige und Watson u. a.* (C-203/15 und C-698/15, EU:C:2016:970), hin und führt aus, dass sich die Nichtigkeit von Art. L. 621-10 Abs. 1 Satz 2 CMF, der zum Zeitpunkt der Begehung der Taten, die Gegenstand der Ausgangsverfahren seien, anwendbar gewesen sei, nicht aus der Feststellung der Verfassungswidrigkeit dieser Vorschrift ergeben könne, da die Wirkungen der Aufhebung der Vorschrift aufgeschoben worden seien. Die den Ermittlern der AMF nach dieser Vorschrift zustehende Befugnis, Verbindungsdaten ohne vorherige Kontrolle durch ein Gericht oder eine unabhängige Behörde anzufordern, genüge aber nicht den Anforderungen der Art. 7, 8 und 11 der Charta, wie sie vom Gerichtshof ausgelegt würden.

- 36 Insoweit stelle sich daher lediglich die Frage, ob die Wirkungen der Aufhebung von Art. L. 621-10 CMF aufgeschoben werden könnten, obwohl diese Bestimmung nicht mit der Charta vereinbar sei.
- 37 Was die Vorratsspeicherung der Verbindungsdaten angeht, weist das vorliegende Gericht zunächst darauf hin, dass die Anbieter von Diensten der elektronischen Kommunikation nach Art. L. 34-1 Abs. II CPCE zwar grundsätzlich verpflichtet seien, Verkehrsdaten zu löschen oder zu anonymisieren. Für diese Verpflichtung gälten aber eine ganze Reihe von Ausnahmen, u. a. die Ausnahme betreffend die „Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten“, die in Art. L. 34-1 Abs. III CPCE vorgesehen sei. Für diese besonderen Zwecke würden die Vorgänge der Löschung oder Anonymisierung bestimmter Daten um ein Jahr aufgeschoben.
- 38 Die fünf Arten von Daten, für die u. a. die Voraussetzungen von Art. L. 34-1 Abs. III CPCE gälten, seien in Art. R. 10-13 CPCE aufgezählt. Diese Verbindungsdaten, die nach einer Kommunikation erhoben oder verarbeitet würden, beträfen die Umstände der Kommunikation und die Nutzer der Dienstleistungen, enthielten aber keine Angaben zum Inhalt der betreffenden Kommunikationen.
- 39 Unter Verweis auf Rn. 112 des Urteils vom 21. Dezember 2016, *Tele2 Sverige und Watson u. a.* (C-203/15 und C-698/15, EU:C:2016:970), wonach Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8, 11 und Art. 52 Abs. 1 der Charta dahin auszulegen ist, dass er einer nationalen Regelung entgegensteht, die für Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle Mittel der elektronischen Kommunikation vorsieht, führt das vorliegende Gericht weiter aus, dass die AMF in den Ausgangsverfahren wegen des Verdachts von Insidergeschäften und Marktmissbrauch, die mehrere schwere Straftatbestände erfüllen könnten, Zugang zu den von den Anbietern von Diensten der elektronischen Kommunikation auf Vorrat gespeicherten Daten gehabt habe. Der Zugang sei dadurch gerechtfertigt gewesen, dass diese Behörde, um die Wirksamkeit ihrer Ermittlungen zu gewährleisten, verschiedene Daten, die in einem bestimmten Zeitraum gespeichert worden seien, hätte abgleichen müssen, um Insiderinformationen aufzudecken, die zwischen mehreren Personen ausgetauscht worden seien. Auf diese Weise seien entsprechende Straftaten aufgedeckt worden.
- 40 Mit den Ermittlungen der AMF werde den Verpflichtungen nachgekommen, die Art. 12 Abs. 2 Buchst. d der Richtlinie 2003/6 und Art. 23 Abs. 2 Buchst. g und h der Verordnung Nr. 596/2014 in Verbindung mit deren Art. 1 den Mitgliedstaaten auferlegten, u. a. der Verpflichtung, bereits existierende Datenverkehrsaufzeichnungen, die sich im Besitz der Anbieter von Diensten der elektronischen Kommunikation befinden, anzufordern.

- 41 Wie im 65. Erwägungsgrund der Verordnung Nr. 596/2014 erläutert werde, seien Verbindungsdaten entscheidende und manchmal die einzigen Belege, mit denen sich Insiderhandel aufdecken und nachweisen lasse, da mit ihnen die Identität einer für die Verbreitung falscher oder irreführender Informationen verantwortlichen Person ermittelt oder festgestellt werden könne, dass Personen zu einer bestimmten Zeit Kontakt gehabt hätten.
- 42 Im 66. Erwägungsgrund der Verordnung Nr. 596/2014 werde allerdings darauf hingewiesen, dass es durch die Ausübung der den zuständigen Finanzaufsichtsbehörden übertragenen Befugnisse zu Eingriffen in das Recht auf Achtung des Privat- und Familienlebens, der Wohnung sowie der Kommunikation kommen könne und in den Mitgliedstaaten deshalb angemessene und wirksame Schutzvorkehrungen gegen jegliche Form des Missbrauchs bestehen sollten, indem die Befugnisse auf Fälle beschränkt würden, in denen sie für die ordnungsgemäße Untersuchung schwerwiegender Fälle erforderlich seien, sofern keine gleichwertigen Mittel zur Verfügung stünden, mit denen wirksam dasselbe Ergebnis erzielt werden könne. Demnach seien bestimmte Fälle von Marktmissbrauch als schwere Straftaten anzusehen.
- 43 In den Ausgangsverfahren seien die Insiderinformationen, die geeignet gewesen seien, den objektiven Tatbestand von unrechtmäßigen Handlungen an den Finanzmärkten zu erfüllen, naturgemäß mündlich und geheim gewesen.
- 44 Es sei daher fraglich, ob Art. 15 Abs. 1 der Richtlinie 2002/58 in Verbindung mit den Art. 7, 8, 11 und Art. 52 Abs. 1 der Charta mit den Anforderungen von Art. 12 Abs. 2 Buchst. d der Richtlinie 2003/6 und Art. 23 Abs. 2 Buchst. g und h der Verordnung Nr. 596/2014 vereinbar sei.
- 45 Sollte der Gerichtshof zu der Einschätzung gelangen, dass die Regelung über die Vorratsspeicherung der Verbindungsdaten, um die es in den Ausgangsverfahren gehe, unionsrechtswidrig sei, stelle sich außerdem die Frage, ob die Wirkungen dieser Regelung vorläufig aufrechtzuerhalten seien, um Rechtsunsicherheit zu vermeiden und es zu ermöglichen, dass die zuvor erhobenen und auf Vorrat gespeicherten Daten zur Aufdeckung und Verfolgung von Insidergeschäften verwendet würden.
- 46 Die Cour de cassation (Kassationsgerichtshof) hat deshalb beschlossen, das Verfahren auszusetzen und dem Gerichtshof folgende, in den Rechtssachen C-339/20 und C-397/20 gleichlautende Fragen zur Vorabentscheidung vorzulegen:
1. Ermächtigen Art. 12 Abs. 2 Buchst. a und d der Richtlinie 2003/6 und Art. 23 Abs. 2 Buchst. g und h der Verordnung Nr. 596/2014, der die erstgenannte Vorschrift ab dem 3. Juli 2016 ersetzt hat, im Licht des 65. Erwägungsgrundes der Verordnung Nr. 596/2014 den nationalen Gesetzgeber, weil die Informationen im Verborgenen ausgetauscht

werden und alle potenziellen Anleger als Verdächtige in Betracht kommen, nicht, die Telekommunikationsgesellschaften zu verpflichten, die Verbindungsdaten für eine bestimmte Zeit generell auf Vorrat zu speichern, um es der Behörde im Sinne von Art. 11 der Richtlinie 2003/6 und Art. 22 der Verordnung Nr. 596/2014 zu ermöglichen, bei dem Verdacht, dass bestimmte Personen an einem Insidergeschäft oder einer Marktmanipulation beteiligt sind, bestehende Datenverkehrsaufzeichnungen im Besitz einer Telekommunikationsgesellschaft anzufordern, wenn Grund zu der Annahme besteht, dass diese Aufzeichnungen, die einen Bezug zum Gegenstand der Ermittlungen aufweisen, für den Beweis des Verstoßes relevant sein könnten, indem insbesondere ermöglicht wird, die Kontakte zurückzuverfolgen, die von den betroffenen Personen vor dem Auftreten des Verdachts geknüpft worden sind?

2. Für den Fall, dass die Antwort des Gerichtshofs auf Frage 1 so ausfallen sollte, dass die Cour de cassation (Kassationsgerichtshof) annehmen müsste, dass die französischen Rechtsvorschriften über die Vorratsspeicherung von Verbindungsdaten nicht mit dem Unionsrecht vereinbar sind: Können die Wirkungen dieser Rechtsvorschriften vorläufig aufrechterhalten werden, um Rechtsunsicherheit zu vermeiden und es zu ermöglichen, dass die zuvor erhobenen und auf Vorrat gespeicherten Daten zu einem mit diesen Rechtsvorschriften verfolgten Ziel verwendet werden?
3. Kann ein nationales Gericht die Wirkungen von Rechtsvorschriften, mit denen die Bediensteten einer unabhängigen Behörde, die dafür zuständig ist, Ermittlungen auf dem Gebiet des Marktmissbrauchs durchzuführen, ermächtigt werden, ohne vorherige Kontrolle durch ein Gericht oder eine andere unabhängige Behörde, Verbindungsdaten anzufordern, vorläufig aufrechterhalten?

47 Mit Entscheidung des Präsidenten des Gerichtshofs vom 17. September 2020 sind die Rechtssachen C-339/20 und C-397/20 zu gemeinsamem schriftlichen und mündlichen Verfahren und zu gemeinsamem Endurteil verbunden worden.

48 Am 21. April 2021 erging das Urteil French Data Network u. a. (Nrn. 393099, 394922, 397844, 397851, 424717 und 424718) des Conseil d'État (Staatsrat), mit dem insbesondere über die Frage entschieden wurde, ob bestimmte nationale Rechtsvorschriften, die in den Ausgangsverfahren einschlägig sind, nämlich Art. L. 34-1 CPCE und Art. R. 10-13 CPC, mit dem Unionsrecht vereinbar sind.

49 Der Gerichtshof hat den Beteiligten, die in den vorliegenden Rechtssachen an der mündlichen Verhandlung teilgenommen haben, Gelegenheit gegeben, sich

zu der Frage zu äußern, welche Auswirkungen das Urteil des Conseil d'État (Staatsrat) auf die vorliegenden Vorabentscheidungsersuchen hat.

- 50 Der Vertreter der französischen Regierung hat in der mündlichen Verhandlung erläutert, dass mit dem Urteil des Conseil d'État (Staatsrat) im Wesentlichen die Vorschriften für rechtswidrig erklärt worden seien, die die allgemeine und unterschiedslose Vorratsspeicherung der Verbindungsdaten – mit Ausnahme der IP-Adressen und der Daten über die Identität der Nutzer der Netze der elektronischen Kommunikation – zum Zwecke der Bekämpfung von Kriminalität ermöglichen. Der Conseil d'État (Staatsrat) habe damit dem Urteil vom 6. Oktober 2020, *La Quadrature du Net* u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), Rechnung getragen. In der streitigen Verhandlung habe sich der Conseil d'État (Staatsrat) aber mit dem Vorbringen der französischen Regierung auseinandersetzen müssen, dass diese Auslegung des Unionsrechts nicht mit Vorschriften vereinbar sei, die Verfassungsrang hätten, nämlich den Vorschriften, die dem Schutz der öffentlichen Ordnung, insbesondere der Sicherheit von Personen und Gütern, und der Strafverfolgung dienen.
- 51 Der Conseil d'État (Staatsrat) habe dieses Vorbringen, in zwei Schritten zurückgewiesen. Er habe zwar eingeräumt, dass die allgemeine und unterschiedslose Vorratsspeicherung der Verbindungsdaten für den Erfolg der strafrechtlichen Ermittlungen von entscheidender Bedeutung sei und durch keine andere Methode wirksam ersetzt werden könne. Unter Verweis auf Rn. 164 des Urteils vom 6. Oktober 2020, *La Quadrature du Net* u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), habe er aber angenommen, dass die umgehende Sicherung der Daten unionsrechtlich zulässig sei, und zwar auch dann, wenn sie Daten betreffe, die ursprünglich zum Zweck des Schutzes der nationalen Sicherheit gespeichert worden seien.
- 52 Nachdem das Urteil des Conseil d'État (Staatsrat) vom 21. April 2021, *French Data Network* u. a. (Nrn. 393099, 394922, 397844, 397851, 424717 und 424718), ergangen sei, habe der nationale Gesetzgeber in Art. L. 34-1 des Gesetzbuchs betreffend das Postwesen und die elektronische Kommunikation Art. IIIa eingefügt (siehe oben, Rn. 21).

Zu den Vorlagefragen

Vorbemerkungen

- 53 Als Erstes ist festzustellen, dass nach der Einreichung der vorliegenden Vorabentscheidungsersuchen das Urteil des Conseil d'État (Staatsrat) vom 21. April 2021, *French Data Network* u. a. (Nrn. 393099, 394922, 397844, 397851, 424717 und 424718), erging, das insbesondere die Vereinbarkeit von Art. L. 34-1 CPCE und Art. R. 10-13 CPCE mit dem Unionsrecht betrifft.

- 54 Wie der Generalanwalt in Nr. 42 seiner Schlussanträge ausgeführt hat und wie sich auch aus den Ausführungen des vorlegenden Gerichts ergibt (siehe oben, Rn. 27, 37 und 38), handelt es sich bei diesen Vorschriften um „Schlüsselvorschriften“ für die Anwendung des in den Ausgangsverfahren einschlägigen Art. 621-10 CMF.
- 55 In der mündlichen Verhandlung hat der Vertreter der französischen Regierung, nachdem er darauf hingewiesen hat, welche Änderungen Art. 34-1 CPCE nach dem Urteil des Gerichtshofs vom 6. Oktober 2020, *La Quadrature du Net* u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), erfahren hat (siehe oben, Rn. 21), im Wesentlichen geltend gemacht, dass das vorlegende Gericht in den Ausgangsverfahren bei seinen Entscheidungen nach dem in den Art. 7 und 8 der Erklärung der Menschen- und Bürgerrechte von 1789 verankerten Grundsatz der zeitlichen Anwendung des Gesetzes die nationalen Vorschriften in der Fassung zugrunde zu legen habe, die zum Zeitpunkt der Begehung der Taten, die Gegenstand der Ausgangsverfahren seien, gegolten habe. Da diese Taten in den Jahren 2014 und 2015 begangen worden seien, könne das Urteil des Conseil d’État (Staatsrat) vom 21. April 2021, *French Data Network* u. a. (Nrn. 393099, 394922, 397844, 397851, 424717 und 424718), für die Prüfung der vorliegenden Vorabentscheidungsersuchen überhaupt nicht maßgeblich sein.
- 56 Nach ständiger Rechtsprechung ist es im Rahmen des durch Art. 267 AEUV geschaffenen Verfahrens ausschließlich Sache des mit dem Rechtsstreit befassten nationalen Richters, in dessen Verantwortungsbereich die zu erlassende gerichtliche Entscheidung fällt, im Hinblick auf die Besonderheiten des Einzelfalls sowohl die Erforderlichkeit einer Vorabentscheidung für den Erlass seines Urteils als auch die Erheblichkeit der dem Gerichtshof vorgelegten Fragen zu beurteilen. Solange diese Fragen die Auslegung des Unionsrechts betreffen, ist der Gerichtshof daher grundsätzlich gehalten, über sie zu befinden (vgl. in diesem Sinne Urteil vom 8. September 2010, *Winner Wetten*, C-409/06, EU:C:2010:503, Rn. 36 und die dort angeführte Rechtsprechung).
- 57 Die Entscheidung über eine Vorlagefrage eines nationalen Gerichts kann nur dann abgelehnt werden, wenn die Auslegung des Unionsrechts, um die der Gerichtshof ersucht wird, offensichtlich in keinem Zusammenhang mit den Gegebenheiten oder dem Gegenstand des Ausgangsrechtsstreits steht, wenn das Problem hypothetischer Natur ist oder wenn der Gerichtshof nicht über die tatsächlichen und rechtlichen Angaben verfügt, die für eine sachdienliche Beantwortung der ihm vorgelegten Fragen erforderlich sind (vgl. in diesem Sinne Urteil vom 19. November 2009, *Filipiak*, C-314/08, EU:C:2009:719, Rn. 42 und die dort angeführte Rechtsprechung).
- 58 In den vorliegenden Fällen ergibt sich aus den Vorlageentscheidungen, dass die Fragen 1 und 3 unmittelbar nicht Art. L. 34-1 CPCE und Art. R. 10-13

CPCE betreffen, sondern Art. L. 621-10 CMF. Die Verkehrsdaten zu Telefongesprächen von VD und SR, auf deren Grundlage gegen VD und SR das Hauptverfahren eröffnet wurde und deren Zulässigkeit als Beweismittel in den Ausgangsverfahren in Zweifel gezogen wird, waren von der AMF bei den Anbietern von Diensten der elektronischen Kommunikation gemäß dieser letztgenannten Vorschrift angefordert worden.

- 59 Mit den Fragen 2 und 3, die jeweils an Frage 1 anknüpfen, möchte das vorlegende Gericht für den Fall, dass die die Vorratsspeicherung und Vorlage von Verbindungsdaten betreffende nationale Regelung, um die es in den Ausgangsverfahren geht, unionsrechtswidrig sein sollte, jeweils im Wesentlichen wissen, ob die Wirkungen dieser Regelung dennoch vorläufig aufrechterhalten werden können, um Rechtsunsicherheit zu vermeiden und es zu ermöglichen, dass die auf der Grundlage der Regelung gespeicherten Daten zur Aufdeckung und Verfolgung von Insidergeschäften verwendet werden können.
- 60 In Anbetracht der vorstehenden Ausführungen und in Anbetracht der Ausführungen, die der Generalanwalt in den Nrn. 44 bis 47 seiner Schlussanträge gemacht hat, ist festzustellen, dass eine Antwort des Gerichtshofs auf die Vorlagefragen für die Entscheidung der Ausgangsverfahren nach wie vor erforderlich ist – unabhängig von dem Urteil des Conseil d'État (Staatsrat) vom 21. April 2021, French Data Network u. a. (Nrn. 393099, 394922, 397844, 397851, 424717 und 424718), und der Entscheidung des Conseil constitutionnel (Verfassungsrat) vom 25. Februar 2022 (Nr. 2021-976/977), mit der Art. L. 34-1 CPCE in der oben in Rn. 20 wiedergegebenen Fassung teilweise für verfassungswidrig erklärt wurde.
- 61 Als Zweites ist festzustellen, dass der Vertreter von VD in der mündlichen Verhandlung vor dem Gerichtshof die Auffassung vertreten hat, dass die Verordnung Nr. 596/2014 in zeitlicher Hinsicht nicht anwendbar sei. Er hat im Wesentlichen geltend gemacht, dass die Taten, die Gegenstand der Ausgangsverfahren seien, vor dem Inkrafttreten dieser Verordnung begangen worden seien. Für die Prüfung der Vorlagefragen seien daher allein die Bestimmungen der Richtlinie 2003/6 maßgeblich.
- 62 Nach ständiger Rechtsprechung ist eine neue Rechtsnorm ab dem Inkrafttreten des Rechtsakts anwendbar, mit dem sie eingeführt wird; sie ist zwar nicht auf unter dem alten Recht entstandene und endgültig erworbene Rechtspositionen anwendbar, doch findet sie auf deren künftige Wirkungen sowie auf neue Rechtspositionen Anwendung. Etwas anderes gilt – vorbehaltlich des Verbots der Rückwirkung von Rechtsakten – nur, wenn zusammen mit der Neuregelung besondere Vorschriften getroffen werden, die speziell die Voraussetzungen für die zeitliche Geltung der Neuregelung regeln (vgl. in diesem Sinne Urteile vom 15. Januar 2019, E. B., C-258/17, EU:C:2019:17, Rn. 50 und die dort

angeführte Rechtsprechung, und vom 14. Mai 2020, Azienda Municipale Ambiente, C-15/19, EU:C:2020:371, Rn. 57).

- 63 Wie bereits ausgeführt (siehe oben, Rn. 26 bis 29), sind die Rechtspositionen, um die es in den Ausgangsverfahren geht, vor dem Inkrafttreten der Verordnung Nr. 596/2014 entstanden, mit der die Richtlinie 2003/6 mit Wirkung ab dem 3. Juli 2016 aufgehoben und ersetzt wurde. Die Ausgangsverfahren wurden aber nach dem 3. Juli 2016 weiter durchgeführt. Ab diesem Zeitpunkt findet auf die künftigen Wirkungen der Rechtspositionen, um die es in den Ausgangsverfahren geht, nach dem in der vorstehenden Randnummer dargestellten Grundsatz daher die Verordnung Nr. 596/2014 Anwendung.
- 64 Die Vorschriften der Verordnung Nr. 596/2014 sind in den vorliegenden Fällen also anwendbar. Im Übrigen ist nicht zwischen den vom vorlegenden Gericht angeführten Vorschriften der Richtlinie 2003/6 und der Verordnung Nr. 596/2014 zu unterscheiden. Diese haben nämlich, was die Auslegung angeht, die der Gerichtshof im Rahmen der vorliegenden Rechtssachen vornehmen wird, im Wesentlichen dieselbe Tragweite.

Zu Frage 1

- 65 Mit Frage 1 möchte das vorlegende Gericht jeweils im Wesentlichen wissen, ob Art. 12 Abs. 2 Buchst. a und d der Richtlinie 2003/6 und Art. 23 Abs. 2 Buchst. g und h der Verordnung Nr. 596/2014 in Verbindung mit Art. 15 Abs. 1 der Richtlinie 2002/58 und im Licht der Art. 7, 8, 11 und Art. 52 Abs. 1 der Charta dahin auszulegen sind, dass sie einer gesetzlichen Regelung wie der, um die es in den Ausgangsverfahren geht, entgegenstehen, die zur Bekämpfung von Straftaten des Marktmissbrauchs, u. a. von Insidergeschäften, präventiv eine allgemeine und unterschiedslose Vorratsspeicherung der Verkehrsdaten für ein Jahr ab dem Zeitpunkt der Speicherung vorsieht.
- 66 Die Parteien des Ausgangsverfahrens und die Beteiligten, die schriftliche Erklärungen beim Gerichtshof eingereicht haben, vertreten insoweit unterschiedliche Auffassungen. Die estnische Regierung, Irland und die spanische und die französische Regierung sind der Auffassung, dass Art. 12 Abs. 2 Buchst. a und d der Richtlinie 2003/6 und Art. 23 Abs. 2 Buchst. g und h der Verordnung Nr. 596/2014 den nationalen Gesetzgeber zwar nicht ausdrücklich, aber zwingend ermächtigten, die Anbieter von Diensten der elektronischen Kommunikation zu einer allgemeinen und unterschiedslosen Vorratsspeicherung der Daten zu verpflichten, um es der zuständigen Finanzaufsichtsbehörde zu ermöglichen, Insidergeschäfte aufzudecken und zu ahnden. Wie sich aus dem 65. Erwägungsgrund der Verordnung Nr. 596/2014 ergebe, stellten solche Aufzeichnungen entscheidende und manchmal die einzigen Belege für die Aufdeckung und den Nachweis des Bestehens von Insiderhandel dar. Die Verpflichtung der Anbieter von Diensten der

elektronischen Kommunikation zu einer allgemeinen und unterschiedslosen Vorratsspeicherung der Daten sei daher sowohl unerlässlich, um die Wirksamkeit der Ermittlungen und der Verfolgungsmaßnahmen der zuständigen Finanzaufsichtsbehörde und damit die praktische Wirksamkeit von Art. 12 Abs. 2 Buchst. a und d der Richtlinie 2003/6 und Art. 23 Abs. 2 Buchst. h der Verordnung Nr. 596/2014 zu gewährleisten, als auch, um den Zielen von allgemeinem Interesse, die mit diesen Rechtsakten verfolgt würden, nämlich der Gewährleistung der Integrität der Finanzmärkte der Union und der Stärkung des Vertrauens der Investoren in diese Märkte, Rechnung zu tragen.

- 67 VD, SR, die polnische Regierung und die Europäische Kommission vertreten hingegen die Auffassung, dass in den genannten Bestimmungen lediglich die Befugnis, von den Anbietern von Diensten der elektronischen Kommunikation „bestehende“ Datenverkehrsaufzeichnungen, die sich in deren Besitz befänden, anzufordern, geregelt werde, also lediglich die Frage des Zugangs zu diesen Daten.
- 68 Als Erstes ist festzustellen, dass bei der Auslegung einer Vorschrift des Unionsrechts nach ständiger Rechtsprechung neben dem Wortlaut auch der Kontext der Vorschrift und die Ziele zu berücksichtigen sind, die mit der Regelung verfolgt werden, zu der die Vorschrift gehört, insbesondere auch die Entstehungsgeschichte dieser Regelung (vgl. in diesem Sinne Urteil vom 17. April 2018, Egenberger, C-414/16, EU:C:2018:257, Rn. 44).
- 69 Was den Wortlaut der Vorschriften angeht, auf die in den Vorabentscheidungsersuchen jeweils in Frage 1 Bezug genommen wird, ist festzustellen, dass in Art. 12 Abs. 2 Buchst. d der Richtlinie 2003/6 von der Befugnis der zuständigen Finanzaufsichtsbehörde die Rede ist, „bereits existierende Aufzeichnungen von Telefongesprächen und Datenübermittlungen anzufordern“, und in Art. 23 Abs. 2 Buchst. g und h der Verordnung Nr. 596/2014 von der Befugnis dieser Behörde, „Datenverkehrsaufzeichnungen im Besitz von Wertpapierfirmen, Kreditinstituten oder Finanzinstituten“ bzw. „bestehende Datenverkehrsaufzeichnungen im Besitz einer Telekommunikationsgesellschaft ..., soweit dies nach nationalem Recht zulässig ist“, anzufordern.
- 70 Aus dem Wortlaut der Bestimmungen ergibt sich eindeutig, dass lediglich die Befugnis der Behörde geregelt ist, die Daten, über die die betreffenden Anbieter verfügen, „anzufordern“, was einem Zugang zu diesen Daten entspricht. Auch, dass von „bestehenden“ Aufzeichnungen die Rede ist, die sich „im Besitz“ der betreffenden Anbieter befinden, deutet darauf hin, dass der Unionsgesetzgeber nicht die Möglichkeit des nationalen Gesetzgebers regeln wollte, eine Verpflichtung zur Vorratsspeicherung solcher Aufzeichnungen einzuführen.
- 71 Nach ständiger Rechtsprechung darf eine Auslegung einer Bestimmung des Unionsrechts nicht dazu führen, dem klaren und unmissverständlichen Wortlaut

der Bestimmung jede praktische Wirksamkeit zu nehmen. Somit kann der Gerichtshof, wenn sich der Sinn einer Bestimmung des Unionsrechts eindeutig aus ihrem Wortlaut ergibt, nicht von dieser Auslegung abweichen (Urteil vom 25. Januar 2022, VYSOČINA WIND, C-181/20, EU:C:2022:51, Rn. 39 und die dort angeführte Rechtsprechung).

- 72 Die oben in Rn. 70 angedachte Auslegung wird sowohl durch den Kontext von Art. 12 Abs. 2 Buchst. a und d der Richtlinie 2003/6 und Art. 23 Abs. 2 Buchst. g und h der Verordnung Nr. 596/2014 als auch durch die Ziele, die mit der Regelung verfolgt werden, zu der diese Bestimmungen gehören, gestützt.
- 73 Zum Kontext der genannten Bestimmungen ist festzustellen, dass der Unionsgesetzgeber nach dem Wortlaut von Art. 12 Abs. 1 der Richtlinie 2003/6 und von Art. 23 Abs. 3 der Verordnung Nr. 596/2014 im Licht des 62. Erwägungsgrundes dieser Verordnung die Mitgliedstaaten zwar verpflichten wollte, die erforderlichen Maßnahmen zu ergreifen, damit die zuständigen Finanzaufsichtsbehörden über eine Reihe wirksamer Instrumente, Befugnisse und Ressourcen und über die erforderlichen Aufsichts- und Untersuchungsbefugnisse verfügen, damit sie ihre Aufgaben wirksam erledigen können. In den genannten Bestimmungen sind aber weder eine Möglichkeit der Mitgliedstaaten, den Anbietern von Diensten der elektronischen Kommunikation zu diesem Zweck eine Verpflichtung zur allgemeinen und unterschiedslosen Vorratsspeicherung der Verkehrsdaten aufzuerlegen, noch die Bedingungen, unter denen die Daten von den Anbietern von Diensten der elektronischen Kommunikation auf Vorrat gespeichert werden müssten, um gegebenenfalls den zuständigen Behörden übermittelt zu werden, geregelt.
- 74 Mit Art. 12 Abs. 2 der Richtlinie 2003/6 und Art. 23 Abs. 2 der Verordnung Nr. 596/2014 wollte der Unionsgesetzgeber die zuständige Finanzaufsichtsbehörde, um die Wirksamkeit ihrer Aufsichts- und Ermittlungstätigkeiten zu gewährleisten, lediglich mit klassischen Ermittlungsbefugnissen ausstatten, etwa wie denen, die es ihr ermöglichen, Zugang zu Dokumenten zu erhalten, Ermittlungen und Durchsuchungen durchzuführen oder Anordnungen oder Verbote gegen Personen zu erlassen, bei denen der Verdacht besteht, dass sie Straftaten des Marktmissbrauchs, u. a. Insidergeschäfte, begangen haben.
- 75 Die Bestimmungen der Verordnung Nr. 596/2014, in denen speziell die Frage der Vorratsspeicherung von Daten geregelt ist (Art. 11 Abs. 5 Unterabs. 2, Abs. 6 Unterabs. 2, Abs. 8 und Abs. 11 Buchst. c, Art. 17 Abs. 1 Unterabs. 1, Art. 18 Abs. 5 und Art. 28), enthalten eine solche Verpflichtung zur Vorratsspeicherung lediglich für die in Art. 23 Abs. 2 Buchst. g der Verordnung aufgezählten Finanzakteure und betreffen daher lediglich die Daten zu Finanztransaktionen und Dienstleistungen, die speziell von solchen Anbietern erbracht werden.

- 76 Was die Ziele angeht, die mit der in Rede stehenden Regelung verfolgt werden, ist festzustellen, dass aus den Erwägungsgründen 2 und 12 der Richtlinie 2003/6 und Art. 1 der Verordnung Nr. 596/2014 im Licht der Erwägungsgründe 2 und 24 dieser Verordnung hervorgeht, dass mit diesen Rechtsakten die Integrität der Finanzmärkte in der Union sichergestellt und das Vertrauen der Anleger in diese Märkte gestärkt werden soll, das insbesondere darauf beruht, dass die Anleger gleich behandelt werden und gegen die unzulässige Verwendung von Insiderinformationen geschützt werden. Das in Art. 2 Abs. 1 der Richtlinie 2003/6 und Art. 8 Abs. 1 der Verordnung Nr. 596/2014 normierte Verbot von Insidergeschäften soll somit die Gleichheit der Vertragspartner bei einem Börsengeschäft gewährleisten, indem es verhindert, dass einer von ihnen, der über eine Insiderinformation verfügt und deshalb einen Vorteil gegenüber den anderen Anlegern hat, daraus zum Nachteil der anderen, die diese Information nicht haben, einen Nutzen zieht (vgl. in diesem Sinne Urteil vom 15. März 2022, *Autorité des marchés financiers*, C-302/20, EU:C:2022:190, Rn. 43, 65 und 77 sowie die dort angeführte Rechtsprechung).
- 77 Zwar stellen Aufzeichnungen von Verbindungsdaten dem 65. Erwägungsgrund der Verordnung Nr. 596/2014 zufolge entscheidende und manchmal die einzigen Belege für die Aufdeckung und den Nachweis des Bestehens von Insiderhandel und Marktmanipulation dar. Dieser Erwägungsgrund bezieht sich aber lediglich auf die Aufzeichnungen, die „im Besitz“ der Anbieter von Diensten der elektronischen Kommunikation sind, und auf die Befugnis der zuständigen Finanzaufsichtsbehörde, von den Anbietern von Diensten der elektronischen Kommunikation „bestehende“ Daten „anzufordern“. Aus ihm kann daher nicht abgeleitet werden, dass der Unionsgesetzgeber den Mitgliedstaaten mit der Verordnung Nr. 596/2014 die Befugnis hätte einräumen wollen, den Anbietern von Diensten der elektronischen Kommunikation eine allgemeine Verpflichtung zur Vorratsspeicherung der Daten aufzuerlegen.
- 78 Somit ist festzustellen, dass weder die Richtlinie 2003/6 noch die Verordnung Nr. 596/2014 dahin ausgelegt werden können, dass sie im Hinblick auf die Ausübung der der zuständigen Finanzaufsichtsbehörde durch die Richtlinie 2003/6 und die Verordnung Nr. 596/2014 übertragenen Befugnisse eine Rechtsgrundlage für eine allgemeine Verpflichtung zur Aufbewahrung der Datenverkehrsaufzeichnungen im Besitz der Anbieter von Diensten der elektronischen Kommunikation bildeten.
- 79 Als Zweites ist festzustellen, dass es sich bei der Richtlinie 2002/58, wie der Generalanwalt im Wesentlichen in den Nrn. 53 und 61 seiner Schlussanträge ausgeführt hat, um den Referenzrechtsakt im Bereich der Speicherung und allgemein der Verarbeitung personenbezogener Daten in der elektronischen Kommunikation handelt. Die Auslegung dieser Richtlinie durch den Gerichtshof ist daher auch für die Datenverkehrsaufzeichnungen im Besitz der

Anbieter von Diensten der elektronischen Kommunikation maßgeblich, die die zuständigen Finanzaufsichtsbehörden im Sinne von Art. 11 der Richtlinie 2003/6 und Art. 22 der Verordnung Nr. 596/2014 bei Letzteren anfordern können.

- 80 Nach ihrem Art. 1 Abs. 1 sieht die Richtlinie 2002/58 nämlich u. a. die Harmonisierung der Vorschriften der Mitgliedstaaten vor, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre und Vertraulichkeit, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation, zu dem auch der Bereich der Telekommunikation gehört, zu gewährleisten (der Richtlinie).
- 81 Zudem gilt die Richtlinie 2002/58 nach ihrem Art. 3 für die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union, einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen. Folglich ist davon auszugehen, dass sie die Tätigkeiten der Anbieter solcher Dienste, u. a. der Anbieter von Telekommunikationsdiensten, regelt (vgl. in diesem Sinne Urteil vom 6. Oktober 2020, *La Quadrature du Net* u. a., C-511/18, C-512/18 und C-520/18, EU:C:2020:791, Rn. 93 und die dort angeführte Rechtsprechung).
- 82 Wie der Generalanwalt im Wesentlichen in den Nrn. 62 und 63 seiner Schlussanträge ausgeführt hat, sind für die Beurteilung der Frage, ob die Verarbeitung der Aufzeichnungen im Besitz der Anbieter von Diensten der elektronischen Kommunikation im Sinne von Art. 12 Abs. 2 Buchst. d der Richtlinie 2003/6 und Art. 23 Abs. 2 Buchst. g und h der Verordnung Nr. 596/2014 zulässig ist, mithin die Voraussetzungen gemäß der Richtlinie 2002/58 und die Auslegung dieser Richtlinie durch die Rechtsprechung des Gerichtshofs maßgeblich.
- 83 Diese Auslegung findet eine Stütze in Art. 3 Abs. 1 Nr. 27 der Verordnung Nr. 596/2014. Dort heißt es nämlich, dass mit Datenverkehrsaufzeichnungen für die Zwecke dieser Verordnung die Aufzeichnungen von Verkehrsdaten im Sinne von Art. 2 Unterabs. 2 Buchst. b der Richtlinie 2002/58 gemeint sind.
- 84 Außerdem sind nach dem 44. Erwägungsgrund der Richtlinie 2003/6 und den Erwägungsgründen 66 und 77 der Verordnung Nr. 596/2014 bei der Verfolgung der Ziele dieser Rechtsakte die in der Charta verbürgten Grundrechte und Grundsätze zu wahren, u. a. das Recht auf Privatsphäre. Insoweit hat der Unionsgesetzgeber im 66. Erwägungsgrund der Verordnung Nr. 596/2014 ausdrücklich darauf hingewiesen, dass in den Mitgliedstaaten für den Zweck der Ausübung der der zuständigen Finanzaufsichtsbehörde eingeräumten Befugnisse, durch die es zu gravierenden Eingriffen in Bezug auf

das Recht auf Achtung des Privat- und Familienlebens, der Wohnung sowie der Kommunikation kommen kann, angemessene und wirksame Schutzvorkehrungen gegen jegliche Form des Missbrauchs bestehen sollten, beispielsweise, falls erforderlich, das Erfordernis zur Einholung einer vorherigen Genehmigung der Justizbehörden eines betroffenen Mitgliedstaats. Die Mitgliedstaaten sollten die Möglichkeit vorsehen, dass die zuständigen Behörden derartige Eingriffsbefugnisse in dem Umfang ausüben, in dem dies für die ordnungsgemäße Untersuchung schwerwiegender Fälle erforderlich ist, sofern keine gleichwertigen Mittel zur Verfügung stehen, mit denen wirksam dasselbe Ergebnis erzielt werden kann. Die Anwendung der Maßnahmen gemäß der Richtlinie 2003/6 und der Verordnung Nr. 596/2014 darf daher in keinem Fall den Schutz der personenbezogenen Daten, den die Richtlinie 2002/58 gewährt, beeinträchtigen (vgl. entsprechend Urteile vom 29. Januar 2008, *Promusicae*, C-275/06, EU:C:2008:54, Rn. 57, und vom 17. Juni 2021, *M.I.C.M.*, C-597/19, EU:C:2021:492, Rn. 124 und die dort angeführte Rechtsprechung).

- 85 Art. 12 Abs. 2 Buchst. a und d der Richtlinie 2003/6 und Art. 23 Abs. 2 Buchst. g und h der Verordnung Nr. 596/2014 sind mithin dahin auszulegen, dass nach ihnen eine allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten zur Bekämpfung von Straftaten des Marktmissbrauchs, insbesondere von Insidergeschäften, nicht zulässig ist. Für die Beurteilung der Frage, ob eine nationale Regelung, die eine solche Vorratsspeicherung vorsieht, mit dem Unionsrecht vereinbar ist, ist Art. 15 Abs. 1 der Richtlinie 2002/58 maßgeblich, und zwar im Licht der Art. 7, 8, 11 und Art. 52 Abs. 1 der Charta und in der Auslegung durch die Rechtsprechung des Gerichtshofs.
- 86 Insoweit ist darauf hinzuweisen, dass es in den vorliegenden Vorabentscheidungsersuchen, wie sich im Wesentlichen aus einer Gesamtschau der Rn. 53, 54 und 58 des vorliegenden Urteils ergibt, zwar hauptsächlich um Art. L. 621-10 CMF geht, nach dem die AMF bei den Anbietern von Diensten der elektronischen Kommunikation Verkehrsdaten zu Telefongesprächen von VD und SR angefordert hatte, auf deren Grundlage gegen VD und SR das Hauptverfahren eröffnet wurde. Wie der Generalanwalt in Nr. 42 seiner Schlussanträge ausgeführt hat, handelt es sich bei Art. L. 34-1 CPCE und Art. R. 10-13 CPCE aber um „Schlüsselvorschriften“ für die Anwendung von Art. 621-10 CMF.
- 87 Aus den Ausführungen des vorlegenden Gerichts, wie sie oben in den Rn. 27, 37 und 38 zusammengefasst sind, ergibt sich nämlich, dass die Ermittler der AMF die betreffenden Verkehrsdaten auf der Grundlage von Art. L. 34-1 CPCE in der auf die Ausgangsverfahren anwendbaren Fassung erhoben hatten, in dem die grundsätzliche Verpflichtung der Anbieter von Diensten der elektronischen Kommunikation gemäß Abs. II, Daten zu Verbindungen zu löschen oder zu anonymisieren, in Abs. III mit einer Reihe von Ausnahmen

versehen war, u. a. mit der Ausnahme betreffend die „Zwecke der Ermittlung, Feststellung und Verfolgung von Straftaten“. Für diese besonderen Zwecke wurden die Vorgänge der Löschung oder Anonymisierung bestimmter Daten um ein Jahr aufgeschoben.

- 88 Das vorliegende Gericht weist ferner darauf hin, dass die fünf Kategorien von Daten, auf die sich Art. L. 34-1 Abs. III CPCE in der auf die Ausgangsverfahren anwendbaren Fassung bezogen habe, in Art. R. 10-13 CPCE aufgezählt gewesen seien. Es handelt sich dabei um die Informationen, anhand derer sich der Nutzer identifizieren lassen, die Daten über die verwendeten Kommunikationsendgeräte, die technischen Merkmale sowie Datum, Uhrzeit und Dauer jeder Kommunikation, die Daten über beantragte oder in Anspruch genommene Zusatzleistungen und deren Anbieter sowie die Daten, anhand derer sich die Identität des oder der Adressaten der Kommunikation feststellen lässt. Nach Art. R. 10-13 Abs. II CPCE in der auf die Ausgangsverfahren anwendbaren Fassung durften die betreffenden Anbieter bei Telefondiensten auch die Daten auf Vorrat speichern, anhand derer sich der Ausgangspunkt und der Standort der Kommunikation bestimmen lassen.
- 89 Die Regelung, um die es in den Ausgangsverfahren geht, gilt mithin unterschieds- und ausnahmslos für sämtliche Mittel der telefonischen Kommunikation und für sämtliche Nutzer. Außerdem handelt es sich bei den Daten, die nach der Regelung, um die es in den Ausgangsverfahren geht, von den Anbietern von Diensten der elektronischen Kommunikation auf Vorrat zu speichern sind, insbesondere um die Daten, die erforderlich sind, um den Ausgangs- und den Endpunkt einer Kommunikation aufzuspüren, Datum, Uhrzeit, Dauer und Art der Kommunikation zu ermitteln, die verwendeten Kommunikationsgeräte zu identifizieren sowie den Standort der Endgeräte und der Kommunikationen zu bestimmen. Zu diesen Daten gehören u. a. Name und Adresse des Nutzers und die Telefonnummern des Anrufers und des Angerufenen.
- 90 Somit lässt sich anhand der Daten, die nach der nationalen Regelung, um die es in den Ausgangsverfahren geht, ein Jahr lang zu speichern sind – auch wenn sie nicht den Inhalt der Kommunikationen betreffen –, u. a. ermitteln, mit welcher Person der Nutzer eines Mittels der telefonischen Kommunikation kommuniziert hat und mit welchem Mittel die Kommunikation erfolgt ist, an welchem Tag und zu welcher Uhrzeit die Kommunikationen erfolgt sind und wie lange sie gedauert haben, von welchem Ort aus die Kommunikationen erfolgt sind und an welchem Ort sich die Endgeräte befunden haben, ohne dass eine Kommunikation unbedingt weitergeleitet worden sein muss. Anhand der Daten lässt sich ferner ermitteln, wie häufig der Nutzer in einem bestimmten Zeitraum mit bestimmten Personen kommuniziert hat. Aus der Gesamtheit der Daten können mithin sehr genaue Schlüsse auf das Privatleben der Personen, deren Daten gespeichert wurden, gezogen werden, etwa auf Gewohnheiten des

täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte, tägliche oder in anderem Rhythmus erfolgende Ortsveränderungen, ausgeübte Tätigkeiten und soziale Beziehungen dieser Personen sowie das soziale Umfeld, in dem sie verkehren. Die Daten ermöglichen insbesondere die Erstellung eines Profils der Betroffenen, das im Hinblick auf das Recht auf Achtung des Privatlebens eine ebenso sensible Information darstellt wie der Inhalt der Kommunikationen selbst (vgl. in diesem Sinne Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 45 und die dort angeführte Rechtsprechung).

- 91 Was die Ziele angeht, die mit der Regelung, um die es in den Ausgangsverfahren geht, verfolgt werden, ist festzustellen, dass eines dieser Ziele die Ermittlung, Feststellung und Verfolgung von Straftaten, u. a. von Straftaten des Marktmissbrauchs, ist, zu denen Insidergeschäfte gehören.
- 92 In Anbetracht der Ausführungen oben in den Rn. 86 bis 91 ist festzustellen, dass der nationale Gesetzgeber in der Regelung, um die es in den Ausgangsverfahren geht, zur Ermittlung, Feststellung und Verfolgung von Straftaten und zur Verbrechensbekämpfung eine allgemeine und unterschiedslose Vorratsspeicherung der Verkehrsdaten für ein Jahr ab dem Zeitpunkt der Speicherung vorgesehen hat.
- 93 Wie sich insbesondere aus den Rn. 140 bis 168 des Urteils vom 6. Oktober 2020, La Quadrature du Net u. a. (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), und aus den Rn. 59 bis 101 des Urteils vom 5. April 2022, Commissioner of An Garda Síochána u. a. (C-140/20, EU:C:2022:258), ergibt, kann eine solche Vorratsspeicherung der Verkehrsdaten durch solche Ziele aber nicht gemäß Art. 15 Abs. 1 der Richtlinie 2002/58 gerechtfertigt werden.
- 94 Eine nationale Regelung wie die, um die es in den Ausgangsverfahren geht, mit der den Anbietern von Diensten der elektronischen Kommunikation unterschieds- und ausnahmslos die Verpflichtung auferlegt wird, zur Bekämpfung von Straftaten des Marktmissbrauchs, u. a. von Insidergeschäften, die Verkehrsdaten sämtlicher Nutzer elektronischer Kommunikationsmittel präventiv allgemein und unterschiedslos auf Vorrat zu speichern, ohne dass erwiesen wäre, dass zwischen den auf Vorrat zu speichernden Daten und dem verfolgten Ziel das nach der in der vorstehenden Randnummer dargestellten Rechtsprechung erforderliche Verhältnis besteht, überschreitet somit die Grenzen des absolut Notwendigen und kann nicht als in einer demokratischen Gesellschaft gerechtfertigt angesehen werden, wie es Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht von Art. 7, 8, 11 und Art. 52 Abs. 1 der Charta verlangt (vgl. in diesem Sinne entsprechend Urteil vom 6. Oktober 2020, Privacy International, C-623/17, EU:C:2020:790, Rn. 81).
- 95 Nach alledem ist in den Rechtssachen C-339/20 und C-397/20 auf Frage 1 jeweils zu antworten, dass Art. 12 Abs. 2 Buchst. a und d der Richtlinie 2003/6

und Art. 23 Abs. 2 Buchst. g und h der Verordnung Nr. 596/2014 in Verbindung mit Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8, 11 und Art. 52 Abs. 1 der Charta dahin auszulegen sind, dass sie einer gesetzlichen Regelung, die zur Bekämpfung von Straftaten des Marktmissbrauchs, u. a. von Insidergeschäften, präventiv eine allgemeine und unterschiedslose Vorratsspeicherung der Verkehrsdaten für ein Jahr ab dem Zeitpunkt der Speicherung vorsieht, entgegenstehen.

Zu den Fragen 2 und 3

- 96 Es bietet sich an, die Fragen 2 und 3, die in den vorliegenden Rechtssachen jeweils gestellt werden, zusammen zu prüfen. Das vorlegende Gericht möchte im Wesentlichen wissen, ob das Unionsrecht dahin auszulegen ist, dass ein nationales Gericht die nach nationalem Recht zu treffende Feststellung, dass innerstaatliche Rechtsvorschriften, mit denen die Anbieter von Diensten der elektronischen Kommunikation zur allgemeinen und unterschiedslosen Vorratsspeicherung der Verkehrsdaten verpflichtet werden und nach denen solche Daten ohne vorherige Genehmigung durch ein Gericht oder eine unabhängige Behörde an die zuständige Finanzaufsichtsbehörde übermittelt werden können, wegen ihrer Unvereinbarkeit mit Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Charta ungültig sind, in ihren zeitlichen Wirkungen beschränken kann.
- 97 Hierzu ist zunächst festzustellen, dass der Grundsatz des Vorrangs des Unionsrechts besagt, dass das Unionsrecht dem Recht der Mitgliedstaaten vorgeht. Er verpflichtet daher alle mitgliedstaatlichen Stellen, den verschiedenen Bestimmungen des Unionsrechts volle Wirksamkeit zu verschaffen, wobei das Recht der Mitgliedstaaten die diesen Bestimmungen zuerkannte Wirkung im Hoheitsgebiet dieser Staaten nicht beeinträchtigen darf. Nach dem Grundsatz des Vorrangs des Unionsrechts ist ein nationales Gericht, das im Rahmen seiner Zuständigkeit die Bestimmungen des Unionsrechts anzuwenden hat und nationale Rechtsvorschriften nicht im Einklang mit den Anforderungen des Unionsrechts auslegen kann, verpflichtet, für die volle Wirksamkeit der Bestimmungen des Unionsrechts Sorge zu tragen, indem es erforderlichenfalls jede – auch spätere – entgegenstehende Bestimmung des nationalen Rechts aus eigener Entscheidungsbefugnis unangewendet lässt, ohne dass es die vorherige Beseitigung dieser Bestimmung auf gesetzgeberischem Weg oder durch irgendein anderes verfassungsrechtliches Verfahren beantragen oder abwarten müsste (vgl. in diesem Sinne Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 118 und die dort angeführte Rechtsprechung).
- 98 Nur der Gerichtshof kann in Ausnahmefällen und aus zwingenden Erwägungen der Rechtssicherheit eine vorübergehende Aussetzung der Verdrängungswirkung herbeiführen, die eine unionsrechtliche Vorschrift gegenüber mit ihr unvereinbarem nationalem Recht ausübt. Eine solche

zeitliche Beschränkung der Wirkungen einer Auslegung des Unionsrechts durch den Gerichtshof kann nur in dem Urteil vorgenommen werden, in dem über die begehrte Auslegung entschieden wird. Der Vorrang und die einheitliche Anwendung des Unionsrechts würden beeinträchtigt, wenn nationale Gerichte befugt wären, nationalen Bestimmungen, sei es auch nur vorübergehend, Vorrang vor dem Unionsrecht einzuräumen, gegen das sie verstoßen (Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 119 und die dort angeführte Rechtsprechung).

- 99 Zwar hat der Gerichtshof in einer Rechtssache betreffend die Rechtmäßigkeit von Maßnahmen, die unter Verstoß gegen die durch das Unionsrecht auferlegte Pflicht zur Durchführung einer vorherigen Prüfung der Umweltverträglichkeit eines Projekts und seiner Verträglichkeit mit einem geschützten Gebiet ergangen waren, entschieden, dass ein nationales Gericht, wenn das innerstaatliche Recht es gestattet, die Wirkungen solcher Maßnahmen ausnahmsweise aufrechterhalten kann, sofern dies durch zwingende Erwägungen gerechtfertigt ist, die im Zusammenhang mit der Notwendigkeit stehen, die tatsächliche und schwerwiegende Gefahr einer Unterbrechung der Stromversorgung im betreffenden Mitgliedstaat abzuwenden, der nicht mit anderen Mitteln und Alternativen, insbesondere im Rahmen des Binnenmarkts, entgegengetreten werden kann. Die Aufrechterhaltung der Wirkungen darf aber nur für den Zeitraum gelten, der absolut notwendig ist, um die Rechtswidrigkeit zu beseitigen (vgl. in diesem Sinne Urteil vom 29. Juli 2019, Inter-Environnement Wallonie und Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, Rn. 175, 176, 179 und 181).
- 100 Anders als das Versäumnis, einer Verfahrenspflicht wie der in dem speziellen Bereich des Umweltschutzes geltenden Pflicht zur vorherigen Prüfung der Auswirkungen eines Projekts nachzukommen, kann ein Verstoß gegen Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Art. 7, 8, 11 und Art. 52 Abs. 1 der Charta jedoch nicht durch ein Verfahren wie das in der vorstehenden Randnummer dargestellte geheilt werden (vgl. in diesem Sinne Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 121 und die dort angeführte Rechtsprechung).
- 101 Würden die Wirkungen nationaler Rechtsvorschriften wie derjenigen, um die es in den Ausgangsverfahren geht, aufrechterhalten, würde dies nämlich bedeuten, dass durch die betreffenden Rechtsvorschriften den Anbietern von Diensten der elektronischen Kommunikation weiterhin Verpflichtungen auferlegt würden, die gegen das Unionsrecht verstoßen und mit schwerwiegenden Eingriffen in die Grundrechte der Personen verbunden sind, deren Daten gespeichert wurden (vgl. entsprechend Urteil vom 5. April 2022, Commissioner of An Garda Síochána u. a., C-140/20, EU:C:2022:258, Rn. 122 und die dort angeführte Rechtsprechung).

- 102 Das vorlegende Gericht darf die Feststellung der Ungültigkeit der in den Ausgangsverfahren in Rede stehenden innerstaatlichen Rechtsvorschriften, die es nach nationalem Recht zu treffen hat, daher nicht in ihren zeitlichen Wirkungen beschränken (vgl. entsprechend Urteil vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, C-140/20, EU:C:2022:258, Rn. 123 und die dort angeführte Rechtsprechung).
- 103 In den Urteilen vom 21. Dezember 2016, *Tele2 Sverige und Watson u. a.* (C-203/15 und C-698/15, EU:C:2016:970), und vom 6. Oktober 2020, *La Quadrature du Net u. a.* (C-511/18, C-512/18 und C-520/18, EU:C:2020:791), wurden die Wirkungen der vorgenommenen Auslegung nicht zeitlich begrenzt. Nach der oben in Rn. 98 dargestellten Rechtsprechung kann dies in einem danach ergehenden Urteil des Gerichtshofs nicht mehr erfolgen.
- 104 Das vorlegende Gericht hat über Anträge zu entscheiden, auf der Grundlage von Verkehrsdaten erlangte Beweismittel für unverwertbar zu erklären, weil die betreffenden innerstaatlichen Rechtsvorschriften sowohl, was die Vorratsspeicherung der Daten, als auch, was den Zugang zu den Daten angeht, unionsrechtswidrig seien. Deshalb ist zu bestimmen, welche Auswirkungen die Feststellung einer etwaigen Unvereinbarkeit von Art. L. 621-10 CMF in der auf die Ausgangsverfahren anwendbaren Fassung mit Art. 15 Abs. 1 der Richtlinie 2002/58 in Verbindung mit den Art. 7, 8, 11 und Art. 52 Abs. 1 der Charta auf die Verwertbarkeit der in den Ausgangsverfahren gegen VD und SR beigebrachten Beweismittel hat.
- 105 Insoweit genügt ein Hinweis auf die Rechtsprechung des Gerichtshofs, insbesondere auf die Grundsätze, die in den Rn. 41 bis 44 des Urteils vom 2. März 2021, *Prokuratuur* (Voraussetzungen für den Zugang zu Daten über die elektronische Kommunikation) (C-746/18, EU:C:2021:152), dargestellt werden. Danach unterliegt die Verwertbarkeit solcher Beweise nach dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten – vorbehaltlich der Beachtung u. a. der Grundsätze der Äquivalenz und der Effektivität – dem nationalen Recht.
- 106 Der Effektivitätsgrundsatz verpflichtet ein nationales Strafgericht dazu, im Rahmen eines Strafverfahrens gegen Personen, die im Verdacht stehen, Straftaten begangen zu haben, Informationen und Beweise, die durch eine mit dem Unionsrecht unvereinbare allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten oder durch einen unionsrechtswidrigen Zugang der zuständigen Behörde zu den fraglichen Daten erlangt wurden, auszuschließen, sofern diese Personen nicht in der Lage sind, sachgerecht zu den Informationen und Beweisen Stellung zu nehmen, die einem Bereich entstammen, in dem das Gericht nicht über Sachkenntnis verfügt, und geeignet sind, die Würdigung der Tatsachen maßgeblich zu beeinflussen (vgl. in diesem Sinne Urteil vom 2. März 2021, *Prokuratuur* [Voraussetzungen für

den Zugang zu Daten über die elektronische Kommunikation], C-746/18, EU:C:2021:152, Rn. 44 und die dort angeführte Rechtsprechung).

- 107 Nach alledem ist in den vorliegenden Rechtssachen auf die Fragen 2 und 3 jeweils zu antworten, dass das Unionsrecht dahin auszulegen ist, dass es dem entgegensteht, dass ein nationales Gericht die nach nationalem Recht zu treffende Feststellung, dass innerstaatliche Rechtsvorschriften, mit denen die Anbieter von Diensten der elektronischen Kommunikation zur allgemeinen und unterschiedslosen Vorratsspeicherung der Verkehrsdaten verpflichtet werden und nach denen solche Daten ohne vorherige Genehmigung durch ein Gericht oder eine unabhängige Behörde an die zuständige Finanzaufsichtsbehörde übermittelt werden können, wegen ihrer Unvereinbarkeit mit Art. 15 Abs. 1 der Richtlinie 2002/58 im Licht der Charta ungültig sind, in ihren zeitlichen Wirkungen beschränkt. Die Verwertbarkeit von Beweismitteln, die gemäß innerstaatlichen Rechtsvorschriften erlangt wurden, die unionsrechtswidrig sind, unterliegt nach dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten – vorbehaltlich der Beachtung u. a. der Grundsätze der Äquivalenz und der Effektivität – dem nationalen Recht.

Kosten

- 108 Für die Beteiligten der Ausgangsverfahren ist das Verfahren Teil des bei dem vorliegenden Gericht anhängigen Verfahrens; die Kostenentscheidung ist daher Sache dieses Gerichts. Die Auslagen anderer Beteiligter für die Abgabe von Erklärungen vor dem Gerichtshof sind nicht erstattungsfähig.

Aus diesen Gründen hat der Gerichtshof (Große Kammer) für Recht erkannt:

- 1. Art. 12 Abs. 2 Buchst. a und d der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates vom 28. Januar 2003 über Insider-Geschäfte und Marktmanipulation (Marktmissbrauch) und Art. 23 Abs. 2 Buchst. g und h der Verordnung (EU) Nr. 596/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über Marktmissbrauch (Marktmissbrauchsverordnung) und zur Aufhebung der Richtlinie 2003/6/EG des Europäischen Parlaments und des Rates und der Richtlinien 2003/124/EG, 2003/125/EG und 2004/72/EG der Kommission in Verbindung mit Art. 15 Abs. 1 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) in der durch die Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 geänderten Fassung und im Licht der Art. 7, 8, 11 und Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union**

sind dahin auszulegen, dass

dass sie einer gesetzlichen Regelung, die zur Bekämpfung von Straftaten des Marktmissbrauchs, u. a. von Insidergeschäften, präventiv eine allgemeine und unterschiedslose Vorratsspeicherung der Verkehrsdaten für ein Jahr ab dem Zeitpunkt der Speicherung vorsieht, entgegenstehen.

2. Das Unionsrecht ist dahin auszulegen, dass es dem entgegensteht, dass ein nationales Gericht die nach nationalem Recht zu treffende Feststellung, dass innerstaatliche Rechtsvorschriften, mit denen die Anbieter von Diensten der elektronischen Kommunikation zur allgemeinen und unterschiedslosen Vorratsspeicherung der Verkehrsdaten verpflichtet werden und nach denen solche Daten ohne vorherige Genehmigung durch ein Gericht oder eine unabhängige Behörde an die zuständige Finanzaufsichtsbehörde übermittelt werden können, wegen ihrer Unvereinbarkeit mit Art. 15 Abs. 1 der Richtlinie 2002/58 in der durch die Richtlinie 2009/136 geänderten Fassung im Licht der Charta der Grundrechte der Europäischen Union ungültig sind, in ihren zeitlichen Wirkungen beschränkt. Die Verwertbarkeit von Beweismitteln, die gemäß innerstaatlichen Rechtsvorschriften erlangt wurden, die unionsrechtswidrig sind, unterliegt nach dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten – vorbehaltlich der Beachtung u. a. der Grundsätze der Äquivalenz und der Effektivität – dem nationalen Recht.