Rättsfallssamlingen

DOMSTOLENS DOM (stora avdelningen)

den 20 september 2022 *

”Begäran om förhandsavgörande – Den inre marknaden för finansiella tjänster – Marknadsmissbruk – Insiderhandel – Direktiv 2003/6/EG – Artikel 12.2 a och d – Förordning (EU) nr 596/2014 – Artikel 23.2 g och h – Finansmarknadsmyndighetens tillsyns- och utredningsbefogenheter – Allmänt intresse av att skydda finansmarknadens integritet i Europeiska unionen och allmänhetens förtroende för finansiella instrument – Möjlighet för finansmarknadsmyndigheten att begära in trafikuppgifter som innehas av en operatör som tillhandahåller elektroniska kommunikationstjänster – Behandling av personuppgifter inom sektorn för elektroniska kommunikationstjänster – Direktiv 2002/58/EG – Artikel 15.1 – Europeiska unionens stadga om de grundläggande rättigheterna – Artiklarna 7, 8, 11 och 52.1 – Konfidentialitet vid kommunikation – Begränsningar – Lagstiftning som innebär att operatörer som tillhandahåller elektroniska kommunikationstjänster generellt och odifferentierat ska lagra trafikuppgifter – Möjlighet för en nationell domstol att begränsa verkningarna i tiden av en fastställelse av att nationell lagstiftning som strider mot unionsrätten är ogiltig – Saknas”

I de förenade målen C-339/20 och C-397/20,

angående två beslut att begära förhandsavgörande enligt artikel 267 FEUF, från Cour de cassation (Högsta domstolen, Frankrike), av den 1 april 2020, som inkom till domstolen den 24 juli 2020 respektive den 20 augusti 2020, i brottmålen mot

VD (C-339/20),

SR (C-397/20),

meddelar

DOMSTOLEN (stora avdelningen),

sammansatt av ordföranden K. Lenaerts, avdelningsordförandena A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis och I. Ziemele, samt domarna T. von Danwitz, M. Safjan, F. Biltgen, P. G. Xuereb (referent), N. Piçarra, L. S. Rossi och A. Kumin,

generaladvokat: M. Campos Sánchez-Bordona,

justitiesekreterare: handläggaren R. Şereş,

efter det skriftliga förfarandet och förhandlingen den 14 september 2021,

* Rättegångsspråk: franska.

med beaktande av de yttranden som avgetts av:

– VD, genom D. Foussard och F. Peltier, avocats,

– SR, genom M. Chavannes och P. Spinosi, avocats,

– Frankrikes regering, genom A. Daniel, E. de Moustier, D. Dubois, J. Illouz och T. Stéhelin, samtliga i egenskap av ombud,

– Danmarks regering, genom N. Holst-Christensen, N. Lykkegaard och M. Søndahl Wolff, samtliga i egenskap av ombud,

– Estlands regering, genom A. Kalbus och M. Kriisa, båda i egenskap av ombud,

– Irland, genom M. Browne, A. Joyce och J. Quaney, samtliga i egenskap av ombud, biträdda av D. Fennelly, BL,

– Spaniens regering, genom L. Aguilera Ruiz, i egenskap av ombud,

– Polens regering, genom B. Majczyna, i egenskap av ombud,

– Portugals regering, genom P. Barros da Costa, L. Inez Fernandes, L. Medeiros och I. Oliveira, samtliga i egenskap av ombud,

– Europeiska kommissionen, genom S. L. Kalėda, H. Kranenborg, T. Scharf och F. Wilman, samtliga i egenskap av ombud,

– Europeiska datatillsynsmannen, genom A. Buchta, M. Guglielmetti, C.-A. Mamier och D. Nardi, samtliga i egenskap av ombud,

och efter att den 18 november 2021 ha hört generaladvokatens förslag till avgörande,

följande

Dom

1 Respektive begäran om förhandsavgörande avser tolkningen av artikel 12.2 a och d i Europaparlamentets och rådets direktiv 2003/6/EG av den 28 januari 2003 om insiderhandel och otillbörlig marknadspåverkan (marknadsmissbruk) (EGT L 96, 2003, s. 16), samt artikel 23.2 g och h i Europaparlamentets och rådets förordning (EU) nr 596/2014 av den 16 april 2014 om marknadsmissbruk (marknadsmissbruksförordning) och om upphävande av Europaparlamentets och rådets direktiv 2003/6/EG och kommissionens direktiv 2003/124/EG, 2003/125/EG och 2004/72/EG (EUT L 173, 2014, s. 1), jämförda med artikel 15.1 i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT 201, 2002, s. 37), i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 (EUT L 337, 2009, s. 11) (nedan kallat direktiv 2002/58), jämte artiklarna 7, 8, 11 och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad stadgan).

2 Respektive begäran har framställts i brottmål mot VD och SR, där de anklagas för att ha gjort sig skyldiga till insider- och häleribrott, medhjälp till dylika brott, mutbrott samt penningtvättsbrott.

Tillämpliga bestämmelser

Unionsrätt

Direktiv 2002/58

3 I skäl 2, 6, 7 och 11 i direktiv 2002/58 anges följande:

”(2) I detta direktiv eftersträvas respekt för de grundläggande rättigheterna och iakttagande av de principer som erkänns i synnerhet i [stadgan]. I synnerhet eftersträvas i detta direktiv att säkerställa full respekt för rättigheterna i artiklarna 7 och 8 i … stadgan.

…

(6) Internet bryter upp traditionella marknadsstrukturer genom att tillhandahålla en gemensam, global infrastruktur för leverans av en mängd olika elektroniska kommunikationstjänster. Allmänt tillgängliga kommunikationstjänster via Internet öppnar nya möjligheter för användarna, men för även med sig nya risker för deras personuppgifter och integritet.

(7) När det gäller allmänna kommunikationsnät bör särskilda rättsliga och tekniska bestämmelser antas för att skydda fysiska personers grundläggande fri- och rättigheter samt juridiska personers berättigade intressen, särskilt med hänsyn till den ökade kapaciteten för automatisk lagring och behandling av uppgifter om abonnenter och användare.

…

(11) I likhet med [Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 1995, s.31)] omfattar det här direktivet inte sådana frågor om skydd av grundläggande fri- och rättigheter som rör verksamhet som inte regleras av gemenskapslagstiftningen. Det ändrar därför inte den befintliga jämvikten mellan den enskildes rätt till integritet och medlemsstaternas möjligheter att vidta sådana åtgärder, enligt artikel 15.1 i det här direktivet, som krävs för att skydda allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när verksamheten rör statens säkerhet) och brottsbekämpning. Det här direktivet påverkar följaktligen inte medlemsstaternas möjlighet att utföra laglig avlyssning av elektronisk kommunikation eller att vidta andra åtgärder om det är nödvändigt för något av dessa ändamål och sker i enlighet med Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna [undertecknad i Rom den 4 november 1950] i den tolkning dessa fått i rättspraxis från Europeiska domstolen för de mänskliga rättigheterna. Sådana åtgärder måste vara lämpliga, i strikt proportion till det avsedda ändamålet och nödvändiga i ett demokratiskt samhälle. De bör omfattas av lämpliga skyddsmekanismer i överensstämmelse med Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.”

4 I artikel 1 i direktiv 2002/58, med rubriken ”Tillämpningsområde och syfte”, föreskrivs följande:

”1. Genom detta direktiv möjliggörs en harmonisering av nationella bestämmelser för att säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, särskilt rätten till integritet och konfidentialitet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation, samt för att säkerställa fri rörlighet för sådana uppgifter samt för utrustning och tjänster avseende elektronisk kommunikation inom gemenskapen.”

2. Bestämmelserna i detta direktiv skall precisera och komplettera direktiv [95/46] för de ändamål som avses i punkt 1. Bestämmelserna är vidare avsedda att skydda berättigade intressen för de abonnenter som är juridiska personer.

3. Detta direktiv skall inte tillämpas på verksamheter som faller utanför tillämpningsområdet för [EUF-fördraget], t.ex. de som omfattas av avdelningarna V och VI i [EU-fördraget], och inte i något fall på verksamheter som avser allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när verksamheten rör statens säkerhet) och statens verksamhet på straffrättens område.”

5 I artikel 2 i nämnda direktiv, med rubriken ”Definitioner”, föreskrivs följande i andra stycket b:

”… följande definitioner [skall] gälla:

…

b) *trafikuppgifter*: alla uppgifter som behandlas i syfte att överföra en kommunikation via ett elektroniskt kommunikationsnät eller för att fakturera den.”

6 Artikel 5 i detta direktiv, med rubriken ”Konfidentialitet vid kommunikation”, har följande lydelse:

”1. Medlemsstaterna skall genom nationell lagstiftning säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. De skall särskilt förbjuda avlyssning, uppfångande med tekniskt hjälpmedel, lagring eller andra metoder som innebär att kommunikationen och de därmed förbundna trafikuppgifterna kan fångas upp eller övervakas av andra personer än användarna utan de berörda användarnas samtycke, utom när de har laglig rätt att göra detta i enlighet med artikel 15.1. Denna punkt får inte förhindra teknisk lagring som är nödvändig för överföring av kommunikationen utan att det påverkar principen om konfidentialitet.

2. Punkt 1 får inte påverka sådan inspelning av kommunikation och därmed förbundna trafikuppgifter som är tillåten enligt lag när den utförs i samband med laglig affärsverksamhet för att tillhandahålla bevis på en affärstransaktion eller annan affärskommunikation.

3. Medlemsstaterna ska se till att lagring av information eller tillgång till information som redan är lagrad i en abonnents eller användares terminalutrustning endast är tillåten på villkor att abonnenten eller användaren i fråga har gett sitt samtycke efter att ha fått tillgång till tydlig och fullständig information, i enlighet med direktiv [95/46], bland annat om ändamålen med behandlingen av uppgifterna. Detta får inte förhindra någon teknisk lagring eller åtkomst som endast sker för att utföra överföringen av en kommunikation via ett elektroniskt kommunikationsnät eller det som är absolut nödvändigt för att leverantören ska kunna

tillhandahålla en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt.”

7 I artikel 6 i direktiv 2002/58, med rubriken ”Trafikuppgifter”, föreskrivs följande:

”1. Trafikuppgifter om abonnenter och användare som behandlas och lagras av leverantören av ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst skall utplånas eller avidentifieras när de inte längre behövs för sitt syfte att överföra en kommunikation, utan att det påverkar tillämpningen av punkterna 2, 3 och 5 i den här artikeln samt artikel 15.1.

2. Trafikuppgifter som krävs för abonnentfakturering och betalning av samtrafikavgifter får behandlas. Sådan behandling är tillåten endast fram till utgången av den period under vilken det lagligen går att göra invändningar mot fakturan eller kräva betalning.

3. I syfte att saluföra elektroniska kommunikationstjänster eller i syfte att tillhandahålla mervärdestjänster får en leverantör av en allmänt tillgänglig elektronisk kommunikationstjänst behandla de uppgifter som avses i punkt 1 i den utsträckning och under den tidsperiod som är nödvändig för sådana tjänster eller sådan marknadsföring, om den abonnent eller användare som uppgifterna gäller i förväg har samtyckt till detta. Användare eller abonnenter ska ha möjlighet att när som helst dra tillbaka sitt samtycke till behandling av trafikuppgifter.

…

5. Behandlingen av trafikuppgifter skall, i enlighet med punkterna 1, 2, 3 och 4, begränsas till sådana personer som av leverantören av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster getts i uppdrag att sköta fakturering, trafikstyrning, kundförfrågningar, spårning av bedrägerier, marknadsföring av elektroniska kommunikationstjänster eller tillhandahållande av en mervärdestjänst, och behandlingen skall begränsas till sådant som är nödvändigt för dessa verksamheter.

…”

8 I artikel 9 i direktivet, med rubriken ”Andra lokaliseringsuppgifter än trafikuppgifter”, föreskrivs följande i punkt 1:

”Om andra lokaliseringsuppgifter än trafikuppgifter som rör användare eller abonnenter av allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster kan behandlas, får dessa uppgifter endast behandlas sedan de har avidentifierats eller om användarna eller abonnenterna givit sitt samtycke, i den utsträckning och för den tid som krävs för tillhandahållandet av en mervärdestjänst. Innan användaren eller abonnenten ger sitt samtycke skall tjänsteleverantören informera denne om vilken typ av andra lokaliseringsuppgifter än trafikuppgifter som kommer att behandlas, behandlingens syfte och varaktighet samt om uppgifterna kommer att vidarebefordras till tredje part för tillhandahållande av mervärdestjänsten. …”

9 I artikel 15 i direktiv 2002/58, med rubriken ”Tillämpningen av vissa bestämmelser i direktiv [95/46]”, anges följande i punkt 1:

”Medlemsstaterna får genom lagstiftning vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges i artikel 5, artikel 6, artikel 8.1, 8.2, 8.3 och 8.4 och artikel 9 i detta direktiv när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och

proportionell för att skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem enligt artikel 13.1 i direktiv [95/46]. Medlemsstaterna får för detta ändamål bland annat vidta lagstiftningsåtgärder som innebär att uppgifter får bevaras under en begränsad period som motiveras av de skäl som fastställs i denna punkt. Alla åtgärder som avses i denna punkt skall vara i enlighet med de allmänna principerna i gemenskapslagstiftningen, inklusive principerna i artikel 6.1 och 6.2 i [EU-fördraget]. ”

Direktiv 2003/6

10 Skäl 1, 2, 12, 37, 41 och 44 i direktiv 2003/6 har följande lydelse:

”(1) En verklig inre marknad för finansiella tjänster är avgörande för ekonomisk tillväxt och skapande av arbetstillfällen i gemenskapen.

(2) För en integrerad och effektiv finansmarknad krävs marknadsintegritet. Att värdepappersmarknaderna fungerar väl och att allmänheten har förtroende för dem är förutsättningar för ekonomisk tillväxt och välstånd. Marknadsmissbruk skadar finansmarknadernas integritet och allmänhetens förtroende för värdepapper och derivatinstrument.

…

(12) Marknadsmissbruk består av insiderhandel och otillbörlig marknadspåverkan. Lagstiftning mot insiderhandel och mot otillbörlig marknadspåverkan har samma syfte: att garantera finansmarknadernas integritet i gemenskapen och höja investerarnas förtroende för dem. …

…

(37) En gemensam minimiuppsättning av kraftfulla verktyg och befogenheter för den behöriga myndigheten i varje medlemsstat kommer att garantera effektivitet i övervakningen. Marknadsföretag och alla finansiella aktörer bör också på sin nivå bidra till marknadens integritet. …

…

(41) Eftersom målet för den föreslagna åtgärden, nämligen att förhindra marknadsmissbruk i form av insiderhandel och otillbörlig marknadspåverkan, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna och de därför, på grund av åtgärdens omfattning och verkningar, bättre kan uppnås på gemenskapsnivå, kan gemenskapen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i [EU-fördraget]. I enlighet med proportionalitetsprincipen i samma artikel går detta direktiv inte utöver vad som är nödvändigt för att uppnå dessa mål.

(44) Detta direktiv respekterar de grundläggande rättigheter och iakttar de principer som bland annat erkänns i [stadgan], särskilt artikel 11 i densamma, och artikel 10 i Europeiska konventionen om skydd för de mänskliga rättigheterna [och de grundläggande friheterna]. …”

11 I artikel 11 i detta direktiv föreskrivs följande:

”Utan att de rättsliga myndigheternas befogenheter åsidosätts skall varje medlemsstat utse en enda administrativ myndighet med befogenhet att se till att de bestämmelser som antas enligt detta direktiv tillämpas.

…”

12 I artikel 12 i direktivet anges följande:

”1. Den behöriga myndigheten skall få alla tillsyns- och utredningsbefogenheter som den behöver för att utföra sina uppgifter. …

2. Utan att det påverkar tillämpningen av artikel 6.7 skall de befogenheter som avses i punkt 1 i den här artikeln utövas i enlighet med nationell rätt och omfatta åtminstone rätten att

a) få tillgång till varje dokument i vilken form som helst och få en kopia på det,

…

d) infordra befintliga uppgifter om tele- och datatrafik,

…”

Förordning nr 596/2014

13 Från och med den 3 juli 2016 upphävdes och ersattes direktiv 2003/6 av förordning nr 596/2014.

14 Skäl 1, 2, 7, 24, 44, 62, 65, 66, 77 och 86 i denna förordning har följande lydelse:

”(1) En verklig inre marknad för finansiella tjänster är avgörande för ekonomisk tillväxt och skapande av arbetstillfällen i unionen.

(2) För en integrerad, effektiv och öppen finansmarknad krävs marknadsintegritet. Väl fungerande värdepappersmarknader som har allmänhetens förtroende är en förutsättning för ekonomisk tillväxt och välstånd. Marknadsmissbruk skadar finansmarknadernas integritet och allmänhetens förtroende för värdepapper och derivatinstrument.

…

(7) Marknadsmissbruk är ett begrepp som omfattar olagliga beteenden på finansmarknaderna, och vid tillämpning av denna förordning bör begreppet anses omfatta insiderhandel, olagligt röjande av insiderinformation och marknadsmanipulation. Sådant beteende hindrar fullständig öppenhet på marknaden som är en förutsättning för handel för alla ekonomiska aktörer på integrerade finansmarknader.

…

(24) När en juridisk eller fysisk person som förfogar över insiderinformation förvärvar eller avyttrar, eller försöker förvärva eller avyttra, finansiella instrument som omfattas av den informationen, för egen eller annans räkning, direkt eller indirekt, bör det underförstås att den personen har utnyttjat den informationen. Det antagandet påverkar inte rätten till försvar. Frågan huruvida en person har överträtt förbudet mot insiderhandel eller har försökt utöva insiderhandel bör bedömas mot bakgrund av syftet med denna förordning, vilket är att skydda finansmarknadernas integritet och höja investerarnas förtroende för dem. Detta förtroende bygger i sin tur på att investerarna har tillförsäkrats likabehandling och skydd mot otillbörligt utnyttjande av insiderinformation.

…

(44) Många finansiella instrument prissätts i förhållande till referensvärden. Faktisk manipulation eller försök till manipulation av referensvärden, inbegripet interbankräntor, kan ha allvarliga konsekvenser för marknadens förtroende och kan leda till betydande förluster för investerare eller snedvrida den reala ekonomin. …

(62) Tillsynens effektivitet garanteras genom en uppsättning effektiva verktyg, befogenheter och resurser för den behöriga myndigheten i varje medlemsstat. I denna förordning fastställs följaktligen särskilt den minimiuppsättning av tillsyns- och utredningsbefogenheter som medlemsstaternas behöriga myndigheter bör ges enligt nationell rätt. De befogenheterna bör, när nationell rätt så kräver, utövas genom ansökan hos de behöriga rättsliga myndigheterna. …

…

(65) Befintliga inspelningar av telefonsamtal och trafikuppgifter från värdepappersföretag, kreditinstitut och finansiella institut som verkställer och dokumenterar verkställandet av transaktioner samt befintliga uppgifter om tele- och datatrafik från teleoperatörer utgör ett avgörande bevis, och ibland det enda beviset, när det gäller att upptäcka och styrka förekomsten av insiderhandel och otillbörligt marknadsmissbruk. Uppgifter om tele- och datatrafik kan göra det möjligt att fastställa identiteten på en person som ansvarar för spridningen av falsk eller vilseledande information eller fastställa att personer varit i kontakt med varandra vid en viss tidpunkt och att det finns en koppling mellan två eller fler personer. De behöriga myndigheterna bör därför kunna kräva befintliga inspelningar av telefonsamtal, elektronisk kommunikation och trafikuppgifter som innehas av ett värdepappersföretag, ett kreditinstitut eller ett finansiellt institut i enlighet med [Europaparlamentets och rådets direktiv 2014/65/EU av den 15 maj 2014 om marknader för finansiella instrument och om ändring av direktiv 2002/92/EG och av direktiv 2011/61/EU (EUT L 173, 2014, s. 349)]. Tillgång till uppgifter om data- och teletrafik är nödvändig för att få fram bevis och för att utreda eventuell insiderhandel eller marknadsmanipulation, och därmed för upptäckt och beslut om att påföra sanktioner när det gäller marknadsmissbruk. För att införa samma spelregler i hela unionen när det gäller tillgång till befintliga uppgifter om tele- och datatrafik som innehas av en teleoperatör eller befintliga inspelningar av telefonsamtal och datatrafik som innehas av ett värdepappersföretag, ett kreditinstitut eller ett annat finansiellt institut, bör de behöriga myndigheterna, i enlighet med nationell rätt, kunna kräva befintliga uppgifter om tele- och datatrafik som innehas av en teleoperatör, i den mån detta tillåts enligt nationell rätt, och befintliga inspelningar av telefonsamtal och datatrafik som innehas av ett värdepappersföretag, i fall när det finns en rimlig misstanke om att sådana uppgifter

relaterade till föremålet för inspektionen eller utredningen kan vara relevanta för att bevisa insiderhandel eller marknadsmanipulation i strid med denna förordning. Tillgång till uppgifter om tele- och datatrafik som innehas av en teleoperatör omfattar inte tillgång till innehållet i telefonsamtal.

(66) Samtidigt som denna förordning specificerar en minimiuppsättning befogenheter som de behöriga myndigheterna bör ha, bör de befogenheterna utövas inom ramen för ett komplett system av nationell rätt som garanterar respekt för grundläggande rättigheter, inbegripet rätten till personlig integritet. För utövandet av dessa befogenheter, som kan utgöra allvarliga intrång i rätten till respekt för privatliv och familjeliv, bostad och kommunikationer, bör medlemsstaterna ha infört adekvata och effektiva garantier mot alla former av missbruk, exempelvis, när det är lämpligt, ett krav att erhålla förhandsgodkännande från den berörda medlemsstatens behöriga rättsliga myndigheter. Medlemsstaterna bör ge de behöriga myndigheterna möjlighet att utöva sådana inkräktande befogenheter i den utsträckning som de är nödvändiga för en korrekt utredning av allvarliga fall där det saknas likvärdiga medel för att nå samma resultat.

…

(77) Denna förordning står i överensstämmelse med de grundläggande rättigheter och principer som erkänns i [stadgan]. Denna förordning bör således tolkas och tillämpas i överensstämmelse med dessa rättigheter och principer. …

…

(86) Eftersom målet för denna förordning, nämligen att förhindra marknadsmissbruk i form av insiderhandel, olagligt röjande av insiderinformation och marknadsmanipulation, inte i tillräcklig utsträckning kan uppnås av medlemsstaterna utan snarare, på grund av åtgärdens omfattning och verkningar, kan uppnås bättre på unionsnivå, kan unionen vidta åtgärder i enlighet med subsidiaritetsprincipen i artikel 5 i [EU-fördraget]. I enlighet med proportionalitetsprincipen i samma artikel går denna förordning inte utöver vad som är nödvändigt för att uppnå detta mål.”

15 I artikel 1 i denna förordning föreskrivs följande:

”Genom den här förordningen fastställs ett gemensamt regelverk om insiderhandel, olagligt röjande av insiderinformation och marknadsmanipulation (marknadsmissbruk) samt åtgärder för att förhindra marknadsmissbruk för att säkerställa de finansiella marknadernas integritet i unionen och förbättra investerares skydd på och förtroende för de marknaderna.”

16 I artikel 3 i förordningen, med rubriken ”Definitioner”, anges följande i punkt 1 led 27:

”I denna förordning avses med

…

27. *trafikuppgifter*: trafikuppgifter såsom det definieras i artikel 2 andra stycket b i [direktiv 2002/58].”

17 Artikel 14 i förordning nr 596/2014, med rubriken ”Förbud mot insiderhandel och olagligt röjande av insiderinformation”, har följande lydelse:

”En person får inte

a) ägna sig åt eller försöka ägna sig åt insiderhandel,

b) rekommendera att någon annan person ägnar sig åt insiderhandel eller förmå någon annan person att ägna sig åt insiderhandel, eller

c) olagligen röja insiderinformation.”

18 I artikel 22 i denna förordning föreskrivs följande:

”Utan att de rättsliga myndigheternas befogenheter åsidosätts ska varje medlemsstat utse en enda behörig administrativ myndighet för tillämpningen av denna förordning. …”

19 I artikel 23 i förordningen, med rubriken ”De behöriga myndigheternas befogenheter”, föreskrivs följande i punkterna 2 och 3:

”2. För att utföra sina uppgifter enligt denna förordning ska behöriga myndigheter i enlighet med nationell rätt ha minst följande tillsyns- och utredningsbefogenheter:

a) Få tillgång till varje dokument och uppgifter i vilken form som helst eller ta kopia på det.

…

g) Begära in inspelningar av telefonsamtal, elektronisk kommunikation och datatrafik som innehas av ett värdepappersföretag, kreditinstitut eller finansiellt institut.

h) I den mån det är tillåtet enligt nationell rätt, begära in befintliga trafikuppgifter som innehas av en teleoperatör om det finns en rimlig misstanke om överträdelse och om sådana uppgifter kan vara av betydelse för att undersöka en överträdelse av artikel 14 a eller b eller artikel 15 a eller b.

…

3. Medlemsstaterna ska se till att lämpliga åtgärder vidtagits så att behöriga myndigheter förfogar över de tillsyns- och övervakningsbefogenheter som behövs för att de ska kunna uppfylla sina åtaganden.

…”

Fransk rätt

CPCE

20 I artikel L. 34-1 i Code des postes et des communications électroniques (lag om elektronisk post och kommunikation), i den lydelse som är tillämplig i de nationella målen (nedan kallad CPCE), föreskrevs följande:

”I. – Denna artikel ska tillämpas på behandling av personuppgifter i samband med tillhandahållande av elektroniska kommunikationstjänster till allmänheten. Artikeln ska i synnerhet tillämpas på nät som stöder insamling av uppgifter och identifiering.

II. – Operatörer som tillhandahåller elektronisk kommunikation, i synnerhet sådana vars verksamhet består i att erbjuda allmänheten tillgång till kommunikationstjänster på internet, ska utplåna eller avidentifiera alla trafikuppgifter, med förbehåll för vad som anges i punkterna III, IV, V och VI.

Aktörer som tillhandahåller elektroniska kommunikationstjänster till allmänheten ska, med iakttagande av bestämmelserna i föregående stycke, upprätta interna förfaranden som gör det möjligt att besvara en begäran från behöriga myndigheter.

Aktörer som i en yrkesmässig huvud- eller sidoverksamhet erbjuder allmänheten en uppkoppling som möjliggör kommunikation på internet med hjälp av en nätanslutning ska, även om detta görs kostnadsfritt, iaktta de bestämmelser som gäller för operatörer som tillhandahåller elektronisk kommunikation enligt denna artikel.

III. – När det behövs för att utreda, avslöja och lagföra brott eller åsidosättanden av den skyldighet som föreskrivs i artikel L. 336-3 i code de la propriété intellectuelle (immaterialrättslagen) eller för att förhindra sådant intrång i automatiserade databehandlingssystem som är straffbelagt enligt artiklarna 323-1–323-3-1 i code pénal (strafflagen), och i det enda syftet att vid behov låta den rättsliga myndighet eller den höga myndighet som avses i artikel L. 331-12 i immaterialrättslagen eller den nationella säkerhetsmyndighet för informationssystem som avses i artikel L. 2321-1 i code de la défense (försvarslagen) ta del av uppgifterna, får uppskov i högst ett år meddelas för åtgärder avsedda att utplåna eller avidentifiera vissa kategorier av tekniska uppgifter. Conseil d’État (Högsta förvaltningsdomstolen) ska, efter att ha inhämtat yttrande från Commission nationale de l’informatique et des libertés (Nationella kommissionen för informationsteknik och friheter), genom dekret och med iakttagande av de begränsningar som anges i punkt VI, fastställa dessa kategorier av uppgifter jämte lagringstider utifrån operatörernas verksamhet och kommunikationstyp samt, i förekommande fall, förutsättningarna för eventuell ersättning för identifierbara och specifika merkostnader för de tjänster som operatörerna således tillhandahåller på statens begäran.

…

VI. – Uppgifter som lagras eller behandlas enligt de villkor som anges i punkterna III, IV och V får enbart avse identifiering av användarna av de tjänster som operatörerna tillhandahåller, de tekniska egenskaperna hos de kommunikationer som operatörerna tillhandahåller, samt terminalutrustningens lokalisering.

De får under inga omständigheter avse innehållet i den korrespondens som utbytts eller den information som sökts, i någon form, inom ramen för dessa kommunikationer.

Lagringen och behandlingen av uppgifterna ska ske med iakttagande av bestämmelserna i loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (lag nr 78-17 av den 6 januari 1978 om informationsteknik, register och friheter).

Operatörerna ska vidta alla åtgärder som krävs för att förhindra att dessa uppgifter används för andra ändamål än de som föreskrivs i denna artikel."

21 I artikel L. 34-1 i code des postes et des communications électroniques (lag om elektronisk post och kommunikation), i dess lydelse enligt loi nº 2021-998, du 30 juillet 2021, relative à la prévention d'actes de terrorisme et au renseignement (lag nr 2021-998 av den 30 juli 2021 om förebyggande av terroristhandlingar och om underrättelseverksamhet) (JORF av den 31 juli 2021, text nr 1), föreskrivs följande i punkterna II bis–III bis:

"II bis. – Operatörer som tillhandahåller elektronisk kommunikation är skyldiga att lagra:

1. information om användarens fysiska identitet, upp till fem år efter det att vederbörandes avtal har upphört att gälla, för att kunna genomföra straffrättsliga förfaranden, förebygga hot mot den allmänna säkerheten, samt skydda den nationella säkerheten,

2. annan information som användaren lämnat i samband med tecknandet av ett avtal eller skapandet av ett konto samt betalningsinformation, upp till ett år efter det att vederbörandes avtal har upphört att gälla eller dennes konto har avslutats, för samma ändamål som de som avses i punkt 1 i denna bestämmelse,

3. tekniska uppgifter som gör det möjligt att identifiera uppkopplingskällan eller den terminalutrustning som använts, upp till ett år efter uppkopplingen eller användningen av terminalutrustningen, för att bekämpa grov brottslighet, förebygga allvarliga hot mot den allmänna säkerheten, samt skydda den nationella säkerheten.

III. – Om det föreligger ett allvarligt, nära förestående eller förutsägbart hot mot den nationella säkerheten får premiärministern, för att skydda densamma, genom dekret ålägga operatörer som tillhandahåller elektronisk kommunikation att under ett år lagra vissa kategorier av trafikuppgifter, utöver de som avses i punkt II bis nr 3, samt sådana lokaliseringsuppgifter som definierats i dekret av Högsta förvaltningsdomstolen.

Premiärministerns åläggande, vars giltighetstid inte får överskrida ett år, kan förlängas om villkoren för utfärdande fortfarande är uppfyllda. Att denna frist löper ut påverkar inte lagringstiden för de uppgifter som avses i första stycket i denna punkt III.

III bis. – De uppgifter som operatörer lagrar i enlighet med denna artikel kan bli föremål för ett föreläggande om skyndsam lagring från myndigheter som har lagstadgad tillgång till uppgifter om elektronisk kommunikation i syfte att förebygga och bekämpa kriminalitet, grov brottslighet och andra grova överträdelser av de regler som de ansvarar för efterlevnaden av, för att dessa myndigheter ska få tillgång till nyssnämnda uppgifter."

22 Artikel R. 10-13 CPCE har följande lydelse:

”I. – För att utreda, avslöja och lagföra brott ska operatörer som tillhandahåller elektronisk kommunikation, i enlighet med artikel L. 34–1 III, lagra följande:

a) Information som gör det möjligt att identifiera användaren.

b) Uppgifter om den terminalutrustning som använts.

c) Tekniska egenskaper, samt datum, klockslag och varaktighet för varje kommunikation.

d) Uppgifter om kompletterande tjänster som har efterfrågats eller använts och om leverantörerna av dessa tjänster.

e) Uppgifter som gör det möjligt att identifiera den eller de som kommunikationen riktade sig till.

II. – I fråga om telefoniverksamhet ska operatören lagra de uppgifter som avses i II, inklusive sådana uppgifter som gör det möjligt att identifiera kommunikationens ursprung och lokalisering.

III. Lagringstiden för de uppgifter som avses i denna artikel är ett år från och med dagen för registreringen.

… ”

LCEN

23 I artikel 6 i loi nº 2004-575, du 21 juin 2004, pour la confiance dans l’économie numérique (lag nr 2004-575 av den 21 juni 2004 om förtroende för den digitala ekonomin) (JORF av den 22 juni 2004, s. 11168), i den lydelse som är tillämplig i de nationella målen (nedan kallad LCEN), föreskrevs följande:

”I – 1. Personer vars verksamhet består i att erbjuda allmänheten tillgång till elektroniska kommunikationstjänster på internet ska informera sina abonnenter om att det finns tekniska hjälpmedel som gör det möjligt att begränsa tillgången till vissa tjänster eller att utesluta vissa tjänster, samt erbjuda dem åtminstone ett av dessa hjälpmedel.

…

2. Fysiska eller juridiska personer som, även kostnadsfritt, på internet tillhandahåller allmänheten elektroniska kommunikationstjänster för lagring av signaler, skrivna meddelanden, bilder, ljud eller andra former av meddelanden som tillhandahålls av tjänstemottagarna, kan inte ådra sig civilrättsligt ansvar för verksamhet eller information som lagrats på begäran av en tjänstemottagare, om de inte har haft faktisk kännedom om att verksamheten eller informationen var olaglig, eller om fakta och omständigheter som tydde på att så var fallet, eller om de – så snart de har fått sådan kännedom – inte har agerat skyndsamt för att radera dessa uppgifter eller omöjliggöra tillgång till dem.

…

II. De personer som avses i I punkterna 1 och 2 ska inneha och lagra uppgifter som gör det möjligt att identifiera var och en som har bidragit till skapandet av innehållet eller en del av innehållet i de tjänster som de tillhandahåller.

De ska tillhandahålla personer som driver en elektronisk kommunikationstjänst på internet sådana tekniska hjälpmedel som gör det möjligt för dem att uppfylla de identifieringsvillkor som föreskrivs i III.

Den rättsliga myndigheten kan begära att få tillgång till de uppgifter som avses i första stycket från de tjänsteleverantörer som nämns i I punkterna 1 och 2.

Bestämmelserna i artiklarna 226-17, 226-21 och 226-22 i strafflagen är tillämpliga på behandling av dessa uppgifter.

Vilka uppgifter som avses i första stycket, hur länge lagringen får pågå och hur uppgifterna ska lagras, fastställs genom dekret från Högsta förvaltningsdomstolen, efter yttrande från Nationella kommissionen för informationsteknik och friheter.

…”

CMF

24 I artikel L. 621-10 i code monétaire et financier (lag om penning- och finansmarknaden), i den lydelse som är tillämplig i de nationella målen (nedan kallad CMF), föreskrevs följande i första stycket:

”Utredare och kontrollanter får begära in varjehanda handlingar, oavsett lagringsmedium, för att kunna fullgöra sina utrednings- och tillsynsuppdrag. Utredare får även begära in, och ta kopia av, uppgifter som har lagrats och behandlats av teleoperatörer med stöd av artikel L. 34-1 [CPCE] eller av sådana tjänsteleverantörer som avses i artikel 6 I.1 och 6 I.2 [LCEN].

…”.

25 Sedan Conseil constitutionnel (Författningsdomstolen, Frankrike), genom ett beslut av den 21 juli 2017, fastställt att artikel L. 621-10 första stycket andra meningen CMF var grundlagsstridig, införde den nationella lagstiftaren, genom loi n° 2018-898, du 23 octobre 2018, relative à la lutte contre la fraude (lag nr 2018-898 av den 23 oktober 2018 om bedrägeribekämpning) (JORF av den 24 oktober 2018, text nr 1), artikel L. 621-10-2 CMF. Denna bestämmelse har följande lydelse:

”Vid utredningar avseende marknadsmissbruk, i den mening som avses i förordning [nr 596/2014], får utredarna begära in uppgifter som har lagrats och behandlats av teleoperatörerna, på de villkor och inom de gränser som föreskrivs i artikel L. 34-1 [CPCE], och av de tjänsteleverantörer som avses i artikel 6 I.1 och 6 I.2 [LCEN].

För att sådana uppgifter som avses i första stycket i denna artikel ska få lämnas ut krävs förhandstillstånd från en granskare av ansökningar om tillgång till uppkopplingsuppgifter.

Granskaren av ansökningar om tillgång till uppkopplingsuppgifter ska växelvis vara en aktiv ledamot eller hedersledamot av Högsta förvaltningsdomstolen, utnämnd av dess generalförsamling, respektive en aktiv ledamot eller hedersledamot av Författningsdomstolen, utnämnd av dess generalförsamling. Granskarens suppleant, vald av den instans granskaren inte tillhör, ska utses på samma sätt. Granskaren av ansökningar om tillgång till uppkopplingsuppgifter och dennes suppleant väljs för en period på fyra år som inte kan förnyas.

…

Vid utövandet av sitt uppdrag får granskaren av ansökningar om tillgång till uppkopplingsuppgifter inte ta emot eller begära instruktioner från finansmarknadsmyndigheten eller någon annan myndighet. Granskaren ska iaktta tystnadsplikt i enlighet med de villkor som anges i artikel L. 621-4 i denna lag.

Ett ärende hänskjuts till granskaren genom en motiverad begäran från finansmarknadsmyndighetens generalsekreterare eller ställföreträdande generalsekreterare. Begäran ska innehålla sådana omständigheter av vilka det framgår att den är välgrundad.

Tillståndet ska tillfogas utredningsakten.

Uppgifter som tillhandahålls av teleoperatörer och sådana tjänsteleverantörer som avses i första stycket i denna artikel får utredarna använda endast inom ramen för den utredning för vilken tillstånd har beviljats.

Uppkopplingsuppgifter beträffande omständigheter som finansmarknadsmyndighetens styrelse avser vidta åtgärder mot ska förstöras inom sex månader från det att sanktionskommittén eller överklagandeinstanserna har meddelat sitt slutliga beslut. Vid förlikning ska sexmånadersperioden räknas från och med förlikningsavtalets fullgörelse.

Uppkopplingsuppgifter beträffande omständigheter som finansmarknadsmyndighetens styrelse inte avser vidta några åtgärder mot ska förstöras inom en månad från det att styrelsen meddelat sitt beslut.

Om utredningsrapporten överlämnas till finansmarknadsåklagaren eller denne beslutar att väcka allmänt åtal …, ska uppkopplingsuppgifterna överlämnas till finansmarknadsåklagaren och inte lagras av finansmarknadsmyndigheten.

Tillämpningsföreskrifter för denna artikel ska fastställas i dekret från Högsta förvaltningsdomstolen.”

Målen vid den nationella domstolen, tolkningsfrågorna och förfarandet vid EU-domstolen

26 I enlighet med en ansökan av den 22 maj 2014 inleddes en förundersökning mot VD och SR, avseende gärningar som ansågs utgöra insiderbrott och häleri genom insiderbrott. Genom en första kompletterande ansökan av den 14 november 2014 utvidgades denna förundersökning till att även avse medhjälp till dylika brott.

27 Den 23 och den 25 september 2015 överlämnade finansmarknadsmyndigheten (Frankrike) vissa uppgifter till den ansvarige undersökningsdomaren, uppgifter som myndigheten hade fått tillgång till inom ramen för en utredning som den hade genomfört i enlighet med L. 621-10 CMF, däribland personuppgifter som förekommit i VD:s och SR:s telefonsamtal och som finansmarknadsmyndighetens utredare hade samlat in, med stöd av artikel L. 34–1 CPCE, från operatörer som tillhandahåller elektroniska kommunikationstjänster.

28 Till följd av finansmarknadsmyndighetens agerande utvidgades förundersökningen, genom ytterligare tre kompletterande ansökningar av den 29 september 2015, den 22 december 2015 respektive den 23 november 2016, till att även avse mutbrott och penningtvättsbrott.

29 Den 10 mars respektive den 29 maj 2017 åtalades VD för insiderbrott och penningtvättsbrott, medan SR åtalades för insiderbrott.

30 I den mån åtalen grundade sig på de trafikuppgifter som finansmarknadsmyndigheten hade lämnat ut, väckte både VD och SR talan vid Cour d'appel de Paris (Appellationsdomstolen i Paris, Frankrike) och åberopade bland annat en grund avseende ett åsidosättande av artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och artikel 52.1 i stadgan. Med hänvisning till den rättspraxis som följer av domen av den 21 december 2016, Tele2 Sverige och Watson m.fl. (C-203/15 och C-698/15, EU:C:2016:970), invände VD och SR närmare bestämt mot den omständigheten att myndigheten hade samlat in dessa uppgifter med stöd av artikel L. 621-10 CMF och artikel L. 34-1 CPCE trots att dessa bestämmelser dels stred mot unionsrätten, eftersom de medförde en skyldighet att generellt och odifferentierat lagra uppkopplingsuppgifter, dels inte innehöll någon begränsning av befogenheten för finansmarknadsmyndighetens utredare att begära ut de lagrade uppgifterna.

31 Genom två domar av den 20 december 2018 respektive den 7 mars 2019 ogillade Appellationsdomstolen i Paris deras talan. Det framgår av uppgifterna i respektive begäran om förhandsavgörande att de instanser som prövat målen i sak, grundade sin slutsats att det inte förelåg något åsidosättande av artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och artikel 52.1 i stadgan, bland annat på den omständigheten att enligt artikel 23.2 h i förordning nr 596/2014, avseende marknadsmissbruk, får de behöriga myndigheterna, i den mån det är tillåtet enligt nationell rätt, begära in befintliga trafikuppgifter som innehas av teleoperatörer om det finns en rimlig misstanke om överträdelse av förbudet mot insiderhandel enligt artikel 14 a och b i samma förordning och om sådana uppgifter kan vara av betydelse för att undersöka denna överträdelse.

32 VD och SR överklagade dessa domar till den hänskjutande domstolen och åberopade en grund avseende ett åsidosättande av bland annat de bestämmelser i stadgan och i direktiv 2002/58 som omnämnts i föregående punkt.

33 När det gäller tillgången till uppkopplingsuppgifterna har den hänskjutande domstolen hänvisat till Conseil constitutionnels (Författningsdomstolen) beslut av den 21 juli 2017, där det fastställts att det förfarande som enligt fransk rätt skulle tillämpas avseende en begäran om tillgång till personuppgifter som lagrats av finansmarknadsmyndighetens utredare inte var förenligt med rätten till respekt för privatlivet, såsom denna rättighet skyddas genom artikel 2 i 1789 års människo- och medborgarrättsförklaring. Conseil constitutionnel (Författningsdomstolen) underströk härvidlag att även om den nationella lagstiftaren endast hade givit behöriga tjänstemän som ålagts tystnadsplikt befogenhet att begära ut sådana uppgifter inom ramen för en utredning, och inte tilldelat dem tvingande verkställighetsbefogenheter, hade den inte vidtagit

några andra åtgärder för att garantera att ett dylikt förfarande innehöll en lämplig avvägning mellan rätten till respekt för privatlivet å ena sidan, och intresset av att avvärja hot mot den allmänna ordningen och lagföra lagöverträdare å den andra, med följden att artikel L. 621-10 första stycket andra meningen CMF ansågs strida mot den franska konstitutionen.

34 Den hänskjutande domstolen har även påpekat att Conseil constitutionnel (Författningsdomstolen) ansåg att det skulle medföra ”uppenbart orimliga” följder för pågående förfaranden att omedelbart upphäva denna bestämmelse och att upphävandet därför inte skulle ske förrän den 31 december 2018. Eftersom artikel L. 621-10 första stycket CMF ansågs vara grundlagsstridig införde den nationella lagstiftaren således artikel L. 621-10-2 i denna lag.

35 Den hänskjutande domstolen har visserligen erinrat om övervägandena i punkt 125 i domen av den 21 december 2016, Tele2 Sverige och Watson m.fl. (C-203/15 och C-698/15, EU:C:2016:970), men anser likväl att den omständigheten att artikel L. 621-10 första stycket andra meningen CMF, som var tillämplig vid tidpunkten för omständigheterna i de nationella målen, konstaterats vara författningsstridig inte kan resultera i att den ska anses vara ogiltig, eftersom verkningarna av upphävandet av denna bestämmelse skjutits upp. Den hänskjutande domstolen anser emellertid att den befogenhet som finansmarknadsmyndighetens utredare har enligt denna bestämmelse, att inhämta trafikuppgifter utan någon föregående kontroll av en domstol eller oberoende myndighet, inte är förenlig med de krav som följer av artiklarna 7, 8 och 11 i stadgan, såsom dessa har tolkats av EU-domstolen.

36 Under dessa omständigheter uppkommer endast frågan huruvida det är möjligt att skjuta upp verkningarna i tiden av upphävandet av artikel L. 621-10 CMF, trots att denna bestämmelse inte är förenlig med stadgan.

37 När det gäller lagring av uppkopplingsuppgifter har den hänskjutande domstolen först och främst påpekat att, även om artikel L. 34-1.II CPCE inför en principiell skyldighet för operatörer som tillhandahåller elektroniska kommunikationstjänster att utplåna eller anonymisera alla trafikuppgifter, är denna skyldighet emellertid förenad med ett antal undantag, däribland det undantag som föreskrivs i punkt III i denna bestämmelse, avseende behovet av att ”utreda, avslöja och lagföra brott”. För detta särskilda behov ska utplåning och anonymisering av ett visst antal uppgifter inte ske förrän efter ett år.

38 Den hänskjutande domstolen har härvidlag preciserat att de fem kategorier av uppgifter som omfattas av de villkor som anges i artikel L. 34-1.III CPCE räknas upp i artikel R. 10-13 CPCE. Dessa uppkopplingsuppgifter genereras eller behandlas till följd av en kommunikation och avser omständigheterna kring kommunikationen och användarna av tjänsten, men de innefattar ingen information om innehållet i den aktuella kommunikationen.

39 Den hänskjutande domstolen har även erinrat om punkt 112 i domen av den 21 december 2016, Tele2 Sverige och Watson m.fl. (C-203/15 och C-698/15, EU:C:2016:970), där det framgår att artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, ska tolkas så, att den utgör hinder mot nationell lagstiftning som i brottsbekämpande syfte föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel, men har samtidigt påpekat att i de nationella målen har finansmarknadsmyndigheten fått tillgång till uppgifter som lagrats av operatörer av elektroniska kommunikationstjänster på grund av misstankar om insiderhandel och marknadsmissbruk som kan utgöra ett flertal allvarliga brott. Finansmarknadsmyndigheten har fått sådan tillgång för att

kunna säkerställa utredningens effektivitet, genom att samköra olika uppgifter som lagrats under en viss tid för att avslöja insiderinformation som cirkulerat mellan flera samtalspartner, information som visar att det förekommit otillåten praxis på området.

40 Den hänskjutande domstolen anser att finansmarknadsmyndighetens utredningar uppfyller de skyldigheter som åligger medlemsstaterna enligt artikel 12.2 d i direktiv 2003/6 och enligt artikel 23.2 g och h i förordning nr 596/2014, jämförd med artikel 1 i samma förordning, däribland skyldigheten att begära in befintliga trafikuppgifter som innehas av operatörer som tillhandahåller elektroniska kommunikationstjänster.

41 Med hänvisning till skäl 65 i nyssnämnda förordning har den hänskjutande domstolen dessutom understrukit att dessa uppkopplingsuppgifter utgör ett avgörande bevis, och ibland det enda beviset, när det gäller att upptäcka och styrka förekomsten av insiderhandel, eftersom de gör det möjligt att fastställa identiteten på en person som ansvarar för spridningen av falsk eller vilseledande information eller fastställa att personer varit i kontakt med varandra vid en viss tidpunkt.

42 Vidare har den hänskjutande domstolen hänvisat till skäl 66 i samma förordning, där det anges att utövandet av de befogenheter som de behöriga finansmyndigheterna tilldelats kan utgöra intrång i rätten till respekt för privatliv och familjeliv, bostad och kommunikationer, och medlemsstaterna bör därför införa adekvata och effektiva garantier mot alla former av missbruk genom att föreskriva att de behöriga myndigheterna endast får utöva sådana befogenheter i den utsträckning det är nödvändigt för en korrekt utredning av allvarliga fall där det saknas likvärdiga medel för att nå samma resultat. Den hänskjutande domstolen anser att det följer av detta skäl att vissa fall av marknadsmissbruk ska anses utgöra allvarlig brottslighet.

43 Den hänskjutande domstolen har vidare understrukit att i de nationella målen var den insiderinformation som kunde tänkas uppfylla de objektiva rekvisiten för rättsstridiga marknadsbeteenden till sin natur muntlig och hemlig.

44 Mot bakgrund av det ovan anförda söker den hänskjutande domstolen klarhet i hur artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, ska förenas med de krav som följer av artikel 12.2 d i direktiv 2003/6, samt artikel 23.2 g och h i förordning nr 596/2014.

45 För det fall att EU-domstolen skulle finna att den aktuella lagstiftningen om lagring av uppkopplingsuppgifter inte är förenlig med unionsrätten, uppkommer frågan huruvida man kan låta verkningarna av denna lagstiftning bestå tillfälligt – för att undvika rättsosäkerhet och för att göra det möjligt att använda uppgifter som redan har samlats in och lagrats, i syfte att avslöja och beivra insiderhandel.

46 Mot denna bakgrund beslutade Cour de cassation (Högsta domstolen) att vilandeförklara målen och ställa följande frågor, vilka är identiska i målen C-339/20 och C-397/20, till EU-domstolen:

”1) Ska artikel 12.2 a och d i direktiv [2003/6], liksom artikel 23.2 g och h i förordning [nr 596/2014], som ersatt direktivet från och med den 3 juli 2016, jämförd med skäl 65 i denna förordning, tolkas så, att de – med beaktande av att de uppgifter som utväxlats är hemliga och att kretsen av personer som kan tänkas komma att åtalas för de aktuella brotten är så vidsträckt – ger den nationella lagstiftaren en möjlighet att ålägga operatörer som tillhandahåller elektronisk kommunikation en skyldighet att tillfälligt men generaliserat lagra uppkopplingsuppgifter, för att den förvaltningsmyndighet som avses i artikel 11 i

direktiv [2003/6] och i artikel 22 i förordning [nr 596/2014] ska ha möjlighet att, när det föreligger skäl att misstänka att vissa personer är inblandade i insiderhandel eller otillbörlig marknadspåverkan, från dessa operatörer begära in befintliga trafikuppgifter om det finns skäl att tro att dessa uppgifter, i den mån de rör föremålet för utredningen, kan vara relevanta för att styrka att en lagöverträdelse har skett, bland annat genom att spåra de kontakter som förekommit mellan de berörda personerna innan misstankarna uppstod?

2) För det fall att EU-domstolens svar [på den första frågan] föranleder Cour de cassation [Högsta domstolen] att göra bedömningen att den franska lagstiftningen om lagring av uppkopplingsuppgifter strider mot unionsrätten, kan verkningarna av denna lagstiftning då upprätthållas tillfälligt, för att undvika rättsosäkerhet och göra det möjligt att använda redan insamlade och lagrade uppgifter för något av de ändamål som eftersträvas genom denna lagstiftning?

3) Får en nationell domstol tillfälligt upprätthålla verkningarna av nationell lagstiftning som innebär att anställda vid en oberoende förvaltningsmyndighet med uppdraget att utreda misstankar om marknadsmissbruk har rätt att begära in uppkopplingsuppgifter, utan någon förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet?”

47 Domstolens ordförande beslutade den 17 september 2020 att förena målen C-339/20 och C-397/20 beträffande det skriftliga och det muntliga förfarandet samt domen.

48 Den 21 april 2021 meddelade Conseil d’État (Högsta förvaltningsdomstolen, Frankrike) dom i målet French Data Network m.fl. (nr 393099, 394922, 397844, 397851, 424717, 424718), där den bland annat uttalade sig om huruvida vissa nationella bestämmelser som är relevanta i de nationella målen, närmare bestämt artikel L. 34-1 CPCE och artikel R. 10-13 CPCE, ska anses vara förenliga med unionsrätten.

49 På EU-domstolens uppmaning ombads förhandlingsdeltagarna i förevarande mål att uttala sig om den eventuella betydelsen av nyssnämnda dom från Conseil d’État (Högsta förvaltningsdomstolen) för förevarande begäran om förhandsavgörande.

50 Vid förhandlingen uppgav den franska regeringens ombud genom domen i målet French Data Network m.fl. (nr 393099, 394922, 397844, 397851, 424717, 424718) följde Conseil d’État (Högsta förvaltningsdomstolen) domen av den 6 oktober 2020, La Quadrature du Net m.fl. (C-511/18, C-512/18 och C-520/18, EU:C:2020:791), och slog i huvudsak fast att bestämmelser som gjorde det möjligt att generellt och odifferentierat lagra trafikuppgifter i syfte att bekämpa brottslighet, med undantag för lagring av IP-adresser och uppgifter om den fysiska identiteten på användarna av elektroniska kommunikationsnät, inte var lagenliga. Han framhöll emellertid att inom ramen för det förfarandet borde Conseil d’État (Högsta förvaltningsdomstolen) också ha bemött den franska regeringens invändning att denna tolkning av unionsrätten strider mot konstitutionella bestämmelser, närmare bestämt bestämmelser som syftar till att förebygga hot mot den allmänna ordningen, särskilt mot säkerheten för personer och egendom, och till att eftersöka brottsmisstänkta.

51 Ombudet för den franska regeringen förklarade härvidlag att Conseil d’État (Högsta förvaltningsdomstolen) hade avfärdat denna invändning i två steg. Conseil d’État (Högsta förvaltningsdomstolen) medgav nämligen inledningsvis att generell och odifferentierad lagring av uppkopplingsuppgifter var av avgörande betydelse för framgångsrika brottsutredningar och att det inte fanns någon annan metod som kunde ersätta sådan lagring. Nyssnämnda domstol fann

emellertid, med stöd av bland annat punkt 164 i domen av den 6 oktober 2020, La Quadrature du Net m.fl. (C-511/18, C-512/18 och C-520/18, EU:C:2020:791), att ett skyndsamt säkrande av uppgifter var förenligt med unionsrätten, inklusive i de fall där ett sådant skyndsamt säkrande avsåg uppgifter som ursprungligen har lagrats i syfte att skydda den nationella säkerheten.

52 Den franska regeringens ombud preciserade dessutom att den nationella lagstiftaren hade infört punkt III bis i artikel L. 34-1 CPCE, såsom den återgivits i punkt 21 ovan, till följd av Conseil d'État (Högsta förvaltningsdomstolen) dom av den 21 april 2021, French Data Network m.fl. (nr 393099, 394922, 397844, 397851, 424717, 424718).

Prövning av tolkningsfrågorna

Inledande synpunkter

53 Inledningsvis ska det erinras om att efter det att respektive begäran om förhandsavgörande hade framställts i förevarande mål meddelade Conseil d'État (Högsta förvaltningsdomstolen) sin dom av den 21 april 2021, French Data Network m.fl. (nr 393099, 394922, 397844, 397851, 424717, 424718), angående bland annat huruvida artikel L. 34-1 CPCE och artikel R. 10-13 CPCE skaanses vara förenliga med unionsrätten.

54 Såsom generaladvokaten har påpekat i punkt 42 i sitt förslag till avgörande och såsom framgår av de förklaringar som den hänskjutande domstolen har lämnat, såsom dessa har redovisats i punkterna 27, 37 och 38 ovan, är dessa bestämmelser avgörande för tillämpningen av den nu aktuella artikel L. 621-10 CMF.

55 Vid förhandlingen vid domstolen hänvisade den franska regeringens ombud till de ändringar av artikel L. 34-1 CPCE som införts till följd av domstolens uttalanden i domen av den 6 oktober 2020, La Quadrature du Net m.fl. (C-511/18, C-512/18 och C-520/18, EU:C:2020:791), vilka det hänvisats till i punkt 21 ovan, och uppgav att för att kunna avgöra tvisterna i de nationella målen är den hänskjutande domstolen, i enlighet med den princip om tillämpning av lag i tiden som stadfästs i artiklarna 7 och 8 i 1789 års människo- och medborgarrättsförklaring, skyldig att tillämpa de nationella bestämmelserna i den version som var tillämplig på omständigheterna i de nationella målen, vilka inträffade under år 2014 och 2015, vilket innebär att Conseil d'États (Högsta förvaltningsdomstolen) dom av den 21 april 2021, French Data Network m.fl. (nr 393099, 394922, 397844, 397851, 424717, 424718), ändå inte kan tas i beaktande vid prövningen av förevarande begäran om förhandsavgörande.

56 Det framgår av fast rättspraxis att i ett förfarande enligt artikel 267 FEUF ankommer det uteslutande på den nationella domstol vid vilken tvisten har anhängiggjorts och som har ansvaret för det rättsliga avgörandet att mot bakgrund av de särskilda omständigheterna i målet bedöma såväl om ett förhandsavgörande är nödvändigt för att döma i saken som relevansen av de frågor som ställs till domstolen. Domstolen är följaktligen, i princip, skyldig att meddela ett förhandsavgörande när de frågor som ställts avser tolkningen av unionsrätten (se, för ett liknande resonemang, dom av den 8 september, C-409/06, Winner Wetten, EU:C:2010:503, punkt 36 och där angiven rättspraxis).

57 Domstolen får underlåta att besvara en tolkningsfråga som en nationell domstol har ställt endast då det är uppenbart att den begärda tolkningen av unionsrätten inte har något samband med de verkliga omständigheterna eller föremålet för tvisten i målet vid den nationella domstolen, eller

när frågan är hypotetisk, eller när domstolen inte har tillgång till sådana uppgifter om de faktiska och rättsliga förhållandena som är nödvändiga för att kunna ge ett användbart svar på de frågor som ställts till den (se, för ett liknande resonemang, dom av den 19 november 2009, C-314/08, Filipiak, EU:C:2009:719, punkt 42 och där angiven rättspraxis).

58 I förevarande fall framgår det av besluten om hänskjutande att den första och den tredje frågan inte direkt avser artikel L. 34-1 CPCE och artikel R. 10-13 CPCE utan artikel L. 621-10 CMF, som är den bestämmelse finansmarknadsmyndigheten lagt till grund för sin begäran att operatörer som tillhandahåller elektroniska kommunikationstjänster ska lämna ut trafikuppgifter avseende VD:s och SR:s telefonsamtal, uppgifter som utgör grunden för åtalen mot dem och vars tillåtlighet som bevisning har ifrågasatts inom ramen för de nationella målen.

59 Det ska dessutom noteras att den hänskjutande domstolen har ställt den andra och den tredje frågan, vilka utgör följdfrågor till den första, för att få klarhet i huruvida det är möjligt att låta verkningarna av den aktuella nationella lagstiftningen om lagring och tillgång till uppkopplingsuppgifter bestå tillfälligt, även om det visar sig att denna lagstiftning strider mot unionsrätten, för att undvika rättsosäkerhet och göra det möjligt att använda uppgifter som lagrats med stöd av denna lagstiftning i syfte att avslöja och lagföra insiderbrott.

60 Mot bakgrund av det ovan anförda, jämte de omständigheter som generaladvokaten hänvisat till i punkterna 44–47 i sitt förslag till avgörande, finner EU-domstolen att den måste besvara de frågor som ställts för att det ska vara möjligt att lösa tvisterna i de nationella målen, oaktat Conseil d'État (Högsta förvaltningsdomstolen) dom av den 21 april 2021, French Data Network m.fl. (nr 393099, 394922, 397844, 397851, 424717, 424718), och Conseil constitutionnels (Författningsdomstolen) beslut av den 25 februari 2022 (nr 2021–976/977), varigenom artikel L. 34-1 CPCE – i den lydelse som avses i punkt 20 ovan – förklarats vara delvis oförenlig med konstitutionen.

61 Det ska vidare noteras att under förhandlingen vid EU-domstolen bestred VD:s ombud att förordning nr 596/2014 var tillämplig i tiden (*ratione temporis*), och gjorde gällande att omständigheterna i de nationella målen inträffade innan denna förordning trädde i kraft. Således är det endast bestämmelserna i direktiv 2003/6 som är relevanta vid prövningen av den hänskjutande domstolens frågor.

62 Härvidlag ska det erinras om att det följer av fast rättspraxis att en ny rättsregel ska tillämpas från och med den tidpunkt då den rättsakt i vilken den ingår träder i kraft och att en sådan rättsregel, även om den inte är tillämplig på rättsliga situationer som har uppkommit och blivit bestående under det äldre regelverkets giltighetstid, är tillämplig på framtida verkningar av dessa situationer liksom på nya situationer. Med förbehåll för principen om att rättsakter inte har retroaktiv verkan, förhåller det sig annorlunda endast när den nya bestämmelsen åtföljs av specialbestämmelser som reglerar dess tillämpning i tiden (se, för ett likande resonemang, dom av den 15 januari 2019, C-258/17, E.B, EU:C:2019:17, punkt 50 och där angiven rättspraxis, och dom av den 14 maj 2020, C-15/19, Azienda Municipale Ambiente, EU:C:2020:371, punkt 57).

63 Såsom framgår av punkterna 26–29 ovan uppkom visserligen de rättsliga förhållanden som är aktuella i de nationella målen innan förordning nr 596/2014 trädde i kraft, vilken upphävde och ersatte direktiv 2003/6 med verkan från och med den 3 juli 2016, men förfarandena i de nationella målen har genomförts därefter, vilket innebär att från och med detta datum ska de framtida verkningarna av dessa situationer regleras av förordning nr 596/2014, i enlighet med den princip som det erinrats om i föregående punkt.

64 Härav följer att bestämmelserna i förordning nr 596/2014 är tillämpliga i förevarande fall. Det finns inte heller anledning att göra någon åtskillnad mellan de bestämmelser som den hänskjutande domstolen har hänvisat till i direktiv 2003/6 respektive förordning nr 596/2014, eftersom sistnämnda bestämmelser har en i allt väsentligt likartad innebörd för den tolkning domstolen är ombedd att göra i förevarande mål.

Den första frågan i respektive mål

65 Den hänskjutande domstolen har ställt sina första frågor för att få klarhet i huruvida artikel 12.2 a och d i direktiv 2003/6 jämte artikel 23.2 g och h i förordning nr 596/2014, jämförda med artikel 15.1 i direktiv 2002/58 och mot bakgrund av artiklarna 7, 8, 11 och 52.1 i stadgan, ska tolkas så, att de utgör hinder mot sådana nationella lagstiftningsåtgärder som är aktuella i de nationella målen, vilka innebär att trafikuppgifter – i förebyggande syfte och för att bekämpa marknadsmissbruksbrott, inklusive insiderhandel – generellt och odifferentierat ska lagras i ett år från och med registreringsdagen.

66 Parterna i de nationella målen och de berörda parter som inkommit med skriftliga yttranden till EU-domstolen har uttryckt olika uppfattningar i detta avseende. Den estniska regeringen, Irland, samt den spanska och den franska regeringen anser att artikel 12.2 a och d i direktiv 2003/6, jämte artikel 23.2 g och h i förordning nr 596/2014, underförstått men definitivt ger den nationella lagstiftaren befogenhet att ålägga operatörer som tillhandahåller elektroniska kommunikationstjänster en skyldighet att generellt och odifferentierat lagra uppgifter, för att den behöriga finansmarknadsmyndigheten ska kunna avslöja och beivra insiderhandel. Såsom framgår av skäl 65 i förordning nr 596/2014 utgör sådana uppgifter ett avgörande bevis, och ibland det enda beviset, när det gäller att upptäcka och styrka förekomsten av insiderhandel, varför en sådan lagringsskyldighet är absolut nödvändig för att säkerställa effektiviteten i myndighetens utredningar och förfaranden, och i förlängningen den ändamålsenliga verkan av artikel 12.2 a och d i direktiv 2003/6 jämte artikel 23.2 h i förordning nr 596/2014, och för att uppnå de ändamål av allmänintresse som eftersträvas genom dessa rättsakter, det vill säga att garantera finansmarknadens integritet i unionen och att stärka investerarnas förtroende för denna marknad.

67 VD, SR, den polska regeringen och Europeiska kommissionen har däremot gjort gällande att i den mån dessa bestämmelser begränsar befogenheten att begära att operatörer som tillhandahåller elektroniska kommunikationstjänster ska lämna ut ”befintliga” trafikuppgifter som de förfogar över, reglerar de endast frågan om tillgång till sådana uppgifter.

68 Härvidlag erinrar domstolen inledningsvis om att det framgår av fast rättspraxis att vid tolkningen av en unionsbestämmelse ska inte bara lydelsen beaktas, utan också sammanhanget och de mål som eftersträvas med de föreskrifter som bestämmelsen ingår i. Därutöver ska bland annat förarbetena till bestämmelserna beaktas (se, för ett liknande resonemang, dom av den 17 april 2018, Egenberger, C-414/16, EU:C:2018:257, punkt 44)

69 Vad gäller lydelsen av de bestämmelser som avses i de första frågorna kan det konstateras att medan det i artikel 12.2 d i direktiv 2003/6 hänvisas till den behöriga finansmarknadsmyndighetens befogenhet att ”infordra befintliga uppgifter om tele- och datatrafik”, hänvisar artikel 23.2 g och h i förordning nr 596/2014 till myndighetens befogenhet att begära in dels ”inspelningar av … datatrafik som innehas av ett värdepappersföretag, kreditinstitut eller finansiellt institut”, dels ”[i] den mån det är tillåtet enligt nationell rätt, … befintliga trafikuppgifter som innehas av en teleoperatör”.

70 Det framgår otvetydigt av ordalydelsen i dessa bestämmelser att de endast avser att reglera den behöriga myndighetens befogenhet att ”infordra” eller ”begära in” sådana uppgifter som operatörerna förfogar över, vilket motsvarar tillgång till dessa uppgifter. Hänvisningen till ”befintliga” inspelningar som ”innehas” av dessa operatörer, visar också att unionslagstiftaren inte har haft för avsikt att reglera den nationella lagstiftarens möjlighet att införa en skyldighet att lagra sådana inspelningar.

71 Enligt fast rättspraxis får en tolkning av en unionsbestämmelse inte leda till att bestämmelsens klara och precisa lydelse förlorar all ändamålsenlig verkan. När innebörden av en unionsbestämmelse otvetydigt framgår av själva lydelsen av bestämmelsen, kan domstolen således inte avvika från denna tolkning (dom av den 25 januari 2022, VYSOČINA WIND, C-181/20, EU:C:2022:51, punkt 39 och där angiven praxis).

72 Den tolkning som förespråkas i punkt 70 ovan stöds såväl av det sammanhang som artikel 12.2 a och d i direktiv 2003/6 samt artikel 23.2 g och h i förordning nr 596/2014 ingår i, som av de mål som eftersträvas med de föreskrifter som dessa bestämmelser ingår i.

73 När det gäller det sammanhang som dessa bestämmelser ingår i, ska det noteras att det följer av artikel 12.1 i direktiv 2003/6 och artikel 23.3 i förordning nr 596/2014, jämförd med skäl 62 i denna förordning, att unionslagstiftaren har haft för avsikt att ålägga medlemsstaterna en skyldighet att vidta nödvändiga åtgärder så att de behöriga finansmarknadsmyndigheterna har tillgång till en uppsättning effektiva verktyg, befogenheter och resurser, samt sådana tillsyns- och utredningsbefogenheter som fordras för att de ska kunna fullgöra sitt uppdrag på ett tillfredsställande sätt. Det kan dock konstateras att dessa bestämmelser varken reglerar frågan huruvida medlemsstaterna, för detta ändamål, eventuellt har möjlighet att ålägga operatörer som tillhandahåller elektroniska kommunikationstjänster en skyldighet att generellt och odifferentierat lagra trafikuppgifter, och inte heller i enlighet med vilka villkor operatörerna ska lagra sådana uppgifter, för att i förekommande fall överlämna dem till de behöriga myndigheterna.

74 Genom artikel 12.2 i direktiv 2003/6 och artikel 23.2 i förordning nr 596/2014 har unionslagstiftaren önskat säkerställa att den behöriga finansmarknadsmyndighetens utrednings- och tillsynsuppdrag genomförs effektivt, varvid denna myndighet endast har tilldelats klassiska utredningsbefogenheter, såsom befogenheter som gör det möjligt för den att få tillgång till handlingar, genomföra inspektioner och husrannsakan, alternativt att utfärda förelägganden eller förbud mot personer som misstänks ha gjort sig skyldiga till marknadsmissbruksbrott, eventuellt i form av insiderhandel.

75 Det kan vidare konstateras att de bestämmelser i förordning nr 596/2014 som specifikt reglerar frågan om lagring av uppgifter, det vill säga artikel 11.5 sista stycket, 11.6 andra stycket, 11.8 och 11.11 c, artikel 17.1 första stycket, artikel 18.5 samt artikel 28 i denna förordning, endast medför en sådan lagringsskyldighet för finansiella aktörer, vilka räknas upp i artikel 23.2 g i samma förordning, och följaktligen endast avser uppgifter om sådana finansiella transaktioner och tjänster som dessa specifika operatörer tillhandahåller.

76 När det gäller de mål som eftersträvas med den aktuella lagstiftningen ska det framhållas att det framgår dels av skäl 2 och 12 i direktiv 2003/6, dels av artikel 1 i förordning nr 596/2014, jämförd med skäl 2 och 24 i denna förordning, att dessa rättsakter syftar till att säkerställa finansmarknadens integritet i unionen och öka investerarnas förtroende för denna marknad, ett förtroende som bland annat bygger på att investerare behandlas likvärdigt och skyddas mot otillåten användning av sekretessbelagda uppgifter. Förbudet mot insiderhandel i artikel 2.1 i

direktiv 2003/6 och artikel 8.1 i förordning nr 596/2014 syftar således till att säkerställa att avtalsparterna i en börstransaktion behandlas lika, genom att förhindra att en av dem, som förfogar över insiderinformation och som därigenom befinner sig i en fördelaktigare situation i jämförelse med andra investerare, drar nytta av informationen till nackdel för den som är ovetande om den (se, för ett liknande resonemang, dom av den 15 mars 2022, Autorité des marchés financiers, C-302/20, EU:C:2022:190, punkterna 43, 65 och 77 samt där angiven rättspraxis).

77 Det framgår visserligen av skäl 65 i förordning nr 596/2014 att uppkopplingsuppgifter utgör ett avgörande bevis, och ibland det enda beviset, när det gäller att upptäcka och styrka förekomsten av insiderhandel och otillbörlig marknadspåverkan, men det ska likväl noteras att detta skäl endast hänvisar till uppgifter som ”innehas” av operatörer som tillhandahåller elektroniska kommunikationstjänster och till den behöriga finansmarknadsmyndighetens befogenhet att ”kräva” att dessa operatörer lämnar ut ”befintliga” uppgifter. Följaktligen framgår det ingalunda av detta skäl att unionslagstiftaren genom denna förordning har haft för avsikt att ge medlemsstaterna befogenhet att ålägga operatörer som tillhandahåller elektroniska kommunikationstjänster en generell skyldighet att lagra uppgifter.

78 Mot bakgrund av det ovan anförda finner domstolen att varken direktiv 2003/6 eller förordning nr 596/2014 kan tolkas så, att de kan utgöra rättslig grund för att ålägga operatörer som tillhandahåller elektroniska kommunikationstjänster en generell skyldighet att lagra trafikuppgifter som de innehar, för att den behöriga finansmyndigheten ska kunna utöva sina befogenheter enligt detta direktiv och denna förordning.

79 Såsom generaladvokaten har påpekat i punkterna 53 och 61 i sitt förslag till avgörande ska det vidare erinras om att direktiv 2002/58 utgör det grundläggande regelverket för lagring och – mer allmänt – behandling av personuppgifter inom sektorn för elektronisk kommunikation, vilket innebär att domstolens tolkning av detta direktiv gör sig gällande även i fråga om lagring av trafikuppgifter som innehas av operatörer av elektroniska kommunikationstjänster och som de behöriga myndigheterna, i den mening som avses i artikel 11 i direktiv 2003/6 och i artikel 22 i förordning nr 596/2014, kan begära att få tillgång till.

80 Enligt artikel 1.1 i direktiv 2002/58 ska det direktivet bland annat möjliggöra en harmonisering av nationella bestämmelser för att säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, särskilt rätten till integritet och konfidentialitet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation, som även omfattar telekommunikationssektorn.

81 Det framgår dessutom av artikel 3 i detta direktiv att det ska tillämpas på behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät inom unionen, inbegripet allmänna kommunikationsnät som stöder datainsamling och identifieringsutrustning. Detta direktiv ska således anses reglera verksamheten för leverantörer av sådana tjänster, inklusive teleoperatörer (se, för ett liknande resonemang, dom av den 6 oktober 2020, La Quadrature du Net m.fl., C-511/18, C-512/18 och C-520/18, EU:C:2020:791, punkt 93 och där angiven rättspraxis).

82 Mot bakgrund av det ovan anförda finner domstolen, i likhet med vad generaladvokaten har påpekat i punkterna 62 och 63 i sitt förslag till avgörande, att bedömningen av huruvida det är tillåtet att behandla uppgifter som innehas av operatörer som tillhandahåller elektroniska kommunikationstjänster, i den mening som avses i artikel 12.2 d i direktiv 2003/6 och

artikel 23.2 g och h i förordning nr 596/2014, ska göras mot bakgrund av de villkor som föreskrivs i direktiv 2002/58, i enlighet med den tolkning av detta direktiv som etablerats genom domstolens rättspraxis.

83 Detta synsätt stöds av artikel 3.1 led 27 i förordning nr 596/2014, där det föreskrivs att trafikuppgifter i den mening som avses i förordningen utgörs av trafikuppgifter såsom de definieras i artikel 2 andra stycket led b i direktiv 2002/58.

84 Det framgår dessutom av skäl 44 i direktiv 2003/6, samt skäl 66 och 77 i förordning nr 596/2014, att de mål som eftersträvas med dessa rättsakter ska vara förenliga med de grundläggande rättigheter och principer som erkänns i stadgan, inklusive rätten till privatliv. Unionslagstiftaren har i detta avseende uttryckligen angett i skäl 66 i förordning nr 596/2014 att för utövandet av de befogenheter som den behöriga finansmarknadsmyndigheten förfogar över enligt denna förordning, vilka kan medföra allvarliga intrång i rätten till respekt för privatliv och familjeliv, bostad och kommunikationer, bör medlemsstaterna införa adekvata och effektiva garantier mot alla former av missbruk, exempelvis, när det är lämpligt, ett krav på att erhålla förhandsgodkännande från den berörda medlemsstatens behöriga rättsliga myndigheter. Medlemsstaterna bör ge de behöriga myndigheterna möjlighet att utöva sådana inkräktande befogenheter endast i den utsträckning de är nödvändiga för en korrekt utredning av allvarliga fall där det saknas likvärdiga medel för att nå samma resultat. Detta innebär att tillämpningen av sådana åtgärder som regleras av direktiv 2003/6 och förordning nr 596/2014 under alla omständigheter inte får undergräva det skydd av personuppgifter följer av direktiv 2002/58 (se, för ett liknande resonemang, dom av den 29 januari 2008, Promusicae, C-275/06, EU:C:2008:54, punkt 57, och dom av den 17 juni 2021, M.I.C.M., C-597/19, EU:C:2021:492, punkt 124 och där angiven rättspraxis).

85 Artikel 12.2 a och d i direktiv 2003/6, jämte artikel 23.2 g och h i förordning nr 596/2014, ska följaktligen tolkas så, att de inte tillåter en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter i syfte att bekämpa marknadsmissbruksbrott, däribland insiderhandel, varvid frågan huruvida nationell lagstiftning som föreskriver en sådan lagringsskyldighet är förenlig med unionsrätten ska bedömas mot bakgrund av artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, såsom dessa bestämmelser har tolkats i domstolens rättspraxis.

86 Vad gäller prövningen av huruvida sådan nationell lagstiftning är förenlig med sistnämnda bestämmelser, erinrar domstolen om att det följer av punkterna 53, 54 och 58 ovan att den centrala bestämmelsen i de nu aktuella begäran om förhandsavgörande visserligen utgörs av artikel L. 621-10 CMF, som finansmarknadsmyndigheten har lagt till grund för sin begäran att operatörer som tillhandahåller elektroniska kommunikationstjänster ska lämna ut trafikuppgifter avseende telefonsamtal som VD och SR genomfört och som ligger till grund för de åtal som väckts mot dem. Det kan inte desto mindre konstateras att artikel L. 34-1 CPCE och artikel 10-13 CPCE är avgörande vid tillämpningen av nyssnämnda artikel L. 621-10 CMF, vilket även generaladvokaten har påpekat i punkt 42 i sitt förslag till avgörande.

87 Det framgår nämligen av de förklaringar som lämnats av den hänskjutande domstolen, såsom dessa sammanfattats i punkterna 27, 37 och 38 ovan, att finansmarknadsmyndighetens utredare hade samlat in de aktuella trafikuppgifterna med stöd av artikel L.34-1 CPCE, i den lydelse som var tillämplig i de nationella målen. Genom punkt II i denna bestämmelse ålades operatörer som tillhandahåller elektroniska kommunikationstjänster en generell skyldighet att utplåna eller

anonymisera trafikuppgifter, men punkt III innehöll också ett antal undantag från denna skyldighet, bland annat ” för att utreda, avslöja och lagföra brott”. För dessa specifika behov skulle utplånandet eller anonymiseringen av vissa uppgifter skjutas upp i ett år.

88 Den hänskjutande domstolen har även uppgett att de fem kategorier av uppgifter som omfattades av punkt III i artikel L. 34-1 CPCE, i den lydelse som är tillämplig i de nationella målen, räknades upp i artikel R. 10-13 CPCE, närmare bestämt uppgifter som gör det möjligt att identifiera användaren, uppgifter om den terminalutrustning som använts, uppgifter om tekniska egenskaper, samt datum, klockslag och varaktighet för varje kommunikation, uppgifter om kompletterande tjänster som efterfrågats eller använts och om leverantörerna av dessa tjänster, samt uppgifter som gör det möjligt att identifiera den eller de som kommunikationen riktade sig till. Det framgår dessutom av artikel R. 10-13.II CPCE, i den lydelse som är tillämplig i de nationella målen, att i fråga om telefoniverksamhet kunde de berörda operatörerna även lagra uppgifter som gör det möjligt att identifiera kommunikationens ursprung och lokalisering.

89 Härav följer att den lagstiftning som är i fråga i de nationella målen omfattar samtliga telekommunikationsmedel och är tillämplig på samtliga användare av dessa kommunikationsmedel, utan att det görs någon åtskillnad eller att det föreskrivs något undantag i detta avseende. Dessutom utgörs de uppgifter som operatörer av elektroniska kommunikationstjänster åläggs att lagra enligt denna lagstiftning bland annat av sådana uppgifter som krävs för att spåra källan och mottagaren av en viss kommunikation, för att fastställa datum, tidpunkt, varaktighet och typ av kommunikation, för att identifiera den kommunikationsutrustning som använts, samt för att lokalisera terminalutrustning och kommunikationer. Bland dessa uppgifter återfinns bland annat användarens namn och adress, samt telefonnumret till den som ringt upp och mottagaren av samtalet.

90 De uppgifter som, enligt den aktuella nationella lagstiftningen, ska lagras under ett år, omfattar förvisso inte innehållet i den aktuella kommunikationen, men gör det möjligt att få kännedom om med vem en användare av ett telekommunikationsmedel har kommunicerat och vilket kommunikationsmedel som har använts, att fastställa datum, tidpunkt och varaktighet för kommunikationen, samt från vilken plats kommunikationen har ägt rum, och att få kännedom om terminalutrustningens lokalisering, utan att någon kommunikation nödvändigtvis har fullbordats. Dylika uppgifter gör det dessutom möjligt att fastställa hur ofta användaren har kommunicerat med vissa personer under en viss period. Det kan således konstateras att dessa uppgifter, gemensamt betraktade, kan göra det möjligt att dra mycket precisa slutsatser om privatlivet för personer vars uppgifter har lagrats, såsom deras vardagliga vanor, deras stadigvarande och tillfälliga uppehållsorter, deras dagliga förflyttningar och förflyttningar i övrigt, de aktiviteter de utövar, deras sociala relationer och de umgängeskretsar de rör sig i. Dessa uppgifter gör det möjligt att kartlägga de berörda personerna på ett sätt som är lika känsligt ur integritetssynpunkt som själva innehållet i kommunikationerna (se, för ett liknande resonemang, dom av den 5 april 2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, punkt 45 och där angiven rättspraxis).

91 När det gäller de mål som eftersträvas ska det noteras att den aktuella lagstiftningen bland annat syftar till att utreda, avslöja och lagföra brott, inklusive marknadsmissbruksbrott – som även omfattar insiderhandel.

92 Mot bakgrund av vad som anförts i punkterna 86–91 ovan konstaterar domstolen att genom den nu aktuella lagstiftningen har den nationella lagstiftaren infört en skyldighet att generellt och odifferentierat lagra trafikuppgifter i ett år från och med registreringsdagen, bland annat i syfte att utreda, avslöja och lagföra brott och för att bekämpa brottslighet.

93 Det framgår emellertid av punkterna 140–168 i domen av den 6 oktober 2020, La Quadrature du Net m.fl., (C-511/18, C-512/18 och C-520/18, EU:C:2020:791), och av punkterna 59–101 i domen av den 5 april 2022, Commissioner of An Garda Síochána m.fl., (C-140/20, EU:C:2022:258) att en dylik lagringsskyldighet inte kan grundas på sådana målsättningar med stöd av artikel 15.1 i direktiv 2002/58.

94 Sådan nationell lagstiftning som den som är aktuell i de nationella målen, vilken innebär att operatörer som tillhandahåller elektroniska kommunikationstjänster är skyldiga att – i förebyggande syfte och för att bekämpa marknadsmissbruksbrott, inklusive insiderhandel – är skyldiga att generellt och odifferentierat lagra trafikuppgifter för samtliga användare av elektroniska kommunikationsmedel, utan att det görs någon åtskillnad eller att det föreskrivs något undantag i detta avseende, och utan att det har styrkts att det föreligger en sådan koppling mellan de lagrade uppgifterna och det eftersträvade målet som krävs enligt den rättspraxis det hänvisats till i föregående punkt, går utöver vad som är strängt nödvändigt och kan därmed inte kan anses vara motiverad i ett demokratiskt samhälle, såsom krävs enligt artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan (se, för ett liknande resonemang och analogt, dom av den 6 oktober 2020, C-623/17, Privacy International, EU:C:2020:790, punkt 81).

95 Mot bakgrund av det ovan anförda ska den första frågan i målen C-339/20 och C-397/20 besvaras enligt följande. Artikel 12.2 a och d i direktiv 2003/6 jämte artikel 23.2 g och h i förordning nr 596/2014, jämförda med artikel 15.1 i direktiv 2002/58 och mot bakgrund av artiklarna 7, 8, 11 och 52.1 i stadgan, ska tolkas så, att de utgör hinder mot nationella lagstiftningsåtgärder som innebär att trafikuppgifter – i förebyggande syfte och för att bekämpa marknadsmissbruksbrott, inklusive insiderhandel – generellt och odifferentierat ska lagras i ett år från och med registreringsdagen.

Den andra och den tredje frågan i respektive mål

96 Den hänskjutande domstolen har ställt den andra och den tredje frågan i respektive mål, vilka ska prövas gemensamt, för att få klarhet i huruvida unionsrätten ska tolkas så, att en nationell domstol, med stöd av nationell rätt, får begränsa rättsverkningarna i tiden av en ogiltigförklaring av nationella bestämmelser som dels innebär att operatörer som tillhandahåller elektroniska kommunikationstjänster åläggs en skyldighet att generellt och odifferentierat lagra trafikuppgifter, dels tillåter att sådana uppgifter lämnas ut till den behöriga finansmarknadsmyndigheten utan föregående tillstånd från en domstol eller en oberoende förvaltningsmyndighet, när dessa bestämmelser har ansetts vara oförenliga med artikel 15.1 i direktiv 2002/58, tolkad mot bakgrund av stadgan.

97 Domstolen erinrar inledningsvis om att det följer av principen om unionsrättens företräde att unionsrätten har företräde framför respektive medlemsstats nationella rätt. Denna princip medför således en skyldighet för alla myndigheter i medlemsstaterna att säkerställa unionsbestämmelsernas fulla verkan, och medlemsstaternas lagstiftning kan inte påverka verkan av de unionsrättsliga bestämmelserna inom medlemsstaterna. Av denna princip följer att för det fall det inte är möjligt att tolka nationell rätt i enlighet med kraven i unionsrätten, är den

nationella domstol som inom ramen för sin behörighet ska tillämpa unionsbestämmelser skyldig att säkerställa att dessa bestämmelser ges full verkan genom att, med stöd av sin egen behörighet, vid behov, underlåta att tillämpa nationell lagstiftning som strider mot unionsbestämmelserna, även senare sådan, utan att vare sig begära eller avvakta ett föregående upphävande av denna genom ett lagstiftnings- eller annat konstitutionellt förfarande (se, för ett liknande resonemang, dom av den 5 april 2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, punkt 118 och där angiven rättspraxis).

98 Det är endast EU-domstolen som, undantagsvis och av tvingande rättssäkerhetshänsyn, får förordna om ett tillfälligt uppskjutande av en unionsbestämmelses företrädesrätt i förhållande till nationell rätt som strider mot den förstnämnda bestämmelsen. Det får endast förordnas om en sådan begränsning i tiden av verkningarna av domstolens tolkning av unionsrätten i den dom varigenom den begärda tolkningen meddelas. Om de nationella domstolarna hade kunnat ge nationella bestämmelser som strider mot unionsrätten, ens tillfälligt, företräde, skulle det äventyra unionsrättens företräde och den enhetliga tillämpningen av unionsrätten (se dom av den 5 april 2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, punkt 119 och där angiven rättspraxis).

99 EU-domstolen har visserligen, i ett mål där det var fråga om lagenligheten av åtgärder som vidtagits i strid med den skyldighet som föreskrivs i unionsrätten att göra en förhandsbedömning av ett projekts konsekvenser för miljön och för ett skyddat område, slagit fast att en nationell domstol, om detta är tillåtet enligt nationell rätt, undantagsvis får låta verkningarna av sådana åtgärder bestå när detta är motiverat av tvingande skäl hänförliga till behovet av att undanröja ett verkligt och allvarligt hot om avbrott i den berörda medlemsstatens elförsörjning, vilket inte skulle kunna avvärjas med andra medel och alternativ, särskilt inom ramen för den inre marknaden. Ett bibehållande av sådana åtgärders rättsverkningar får endast omfatta den tidsrymd som är strängt nödvändig för att avhjälpa rättsstridigheten (se, för ett liknande resonemang, dom av den 29 juli 2019, Inter-Environnement Wallonie och Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, punkterna 175, 176, 179 och 181).

100 Till skillnad från en underlåtenhet att uppfylla en formell skyldighet såsom att på miljöskyddsområdet göra en förhandsbedömning av ett projekts konsekvenser, kan ett åsidosättande av artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och artikel 52.1 i stadgan, emellertid inte avhjälpas genom ett förfarande som är jämförbart med det som nämnts i föregående punkt (se, för ett liknande resonemang, dom av den 5 april 2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, punkt 121 och där angiven rättspraxis).

101 Att låta verkningarna av sådan nationell lagstiftning som den nu aktuella bestå skulle innebära att operatörer som tillhandahåller elektroniska kommunikationstjänster fortsättningsvis åläggs skyldigheter som strider mot unionsrätten, och som medför allvarliga ingrepp i de grundläggande rättigheterna för de personer vars uppgifter har lagrats (se, analogt, dom av den 5 april 2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, punkt 122 och där angiven rättspraxis).

102 Den hänskjutande domstolen kan därför inte tidsbegränsa verkningarna av en ogiltigförklaring som den enligt nationell rätt ska utfärda med avseende på den nationella lagstiftning som är i fråga i det nationella målet (se, analogt, dom av den 5 april 2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, punkt 123 och där angiven rättspraxis).

103 Det ska även noteras att verkningarna av den tolkning som förordades i domen av den 21 december 2016, Tele2 Sverige och Watson m.fl., (C-203/15 och C-698/15, EU:C:2016:970), och domen av den 6 oktober, La Quadrature du Net m.fl., (C-511/18, C-512/18 och C-520/18, EU:C:2020:791) inte begränsades i tiden, vilket, i enlighet med den rättspraxis det erinrats om i punkt 98 ovan, innebär att domstolen inte kan besluta om en sådan begränsning i en dom som meddelats efter nyssnämnda domar.

104 Med hänsyn till att den hänskjutande domstolen har att pröva yrkanden om att inte tillåta bevisning som erhållits på grundval av trafikuppgifter, med motiveringen att de aktuella nationella bestämmelserna strider mot unionsrätten, såväl vad gäller lagringen av uppgifterna som tillgången till dem, ska det slutligen fastställas huruvida den omständigheten att artikel L. 621-10 CMF, i den lydelse som är tillämplig i de nationella målen, eventuellt strider mot artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, kan påverka tillåtligheten av den bevisning som åberopats gentemot VD och SR inom ramen för de nationella målen.

105 I detta avseende räcker det att hänvisa till EU-domstolens praxis på området, i synnerhet till de principer som det erinras om i punkterna 41–44 i domen av den 2 mars 2021, Prokuratuur (Villkor för att ge tillgång till uppgifter avseende elektronisk kommunikation) (C-746/18, EU:C:2021:152), av vilka det följer att frågan om sådan tillåtlighet, i enlighet med principen om medlemsstaternas processuella autonomi, omfattas av nationell rätt, under förutsättning att bland annat principerna om likvärdighet och effektivitet iakttas.

106 Vad gäller sistnämnda princip ska det erinras om att den kräver att en nationell brottmålsdomstol – inom ramen för ett straffrättsligt förfarande mot personer som är misstänkta för brott – bortser från information och bevisning som erhållits genom en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter som inte är förenlig med unionsrätten, eller genom att de nationella myndigheterna har fått tillgång till dessa uppgifter på ett sätt som strider mot unionsrätten, om dessa personer inte bereds tillfälle att på ett effektivt sätt yttra sig över denna information och bevisning, och denna hänför sig till ett område som domarna saknar sakkunskap om och som kan påverka bedömningen av omständigheterna på ett avgörande sätt (se, för ett liknande resonemang, dom av den 2 mars 2021, 2021, Prokuratuur (Villkor för att ge tillgång till uppgifter avseende elektronisk kommunikation), C-746/18, EU:C:2021:152, punkt 44 och där angiven rättspraxis).

107 Mot bakgrund av det ovan anförda ska den andra och tredje frågan i respektive mål besvaras enligt följande. Unionsrätten ska tolkas så att den utgör hinder mot att en nationell domstol, med stöd av nationell rätt, begränsar rättsverkningarna i tiden av en ogiltigförklaring av nationella bestämmelser som dels innebär att operatörer som tillhandahåller elektroniska kommunikationstjänster åläggs en skyldighet att generellt och odifferentierat lagra trafikuppgifter, dels tillåter att sådana uppgifter lämnas ut till den behöriga finansmarknadsmyndigheten utan föregående tillstånd från en domstol eller en oberoende förvaltningsmyndighet, när dessa bestämmelser har ansetts vara oförenliga med artikel 15.1 i direktiv 2002/58, tolkad mot bakgrund av stadgan. Tillåtligheten av bevisning som erhållits med stöd av nationell lagstiftning som strider mot unionsrätten regleras, i enlighet med principen om medlemsstaternas processuella autonomi, av nationell rätt, förutsatt att bland annat likvärdighetsprincipen och effektivitetsprincipen iakttas.

Rättegångskostnader

108 Eftersom förfarandet i förhållande till parterna i de nationella målen utgör ett led i beredningen av samma mål, ankommer det på den hänskjutande domstolen att besluta om rättegångskostnaderna. De kostnader för att avge yttrande till domstolen som andra än nämnda parter har haft är inte ersättningsgilla.

Mot denna bakgrund beslutar domstolen (stora avdelningen) följande:

1) **Artikel 12.2 a och d i Europaparlamentets och rådets direktiv 2003/6/EG av den 28 januari 2003 om insiderhandel och otillbörlig marknadspåverkan (marknadsmissbruk), jämte artikel 23.2 g och h i Europaparlamentets och rådets förordning (EU) nr 596/2014 av den 16 april 2014 om marknadsmissbruk (marknadsmissbruksförordning) och om upphävande av Europaparlamentets och rådets direktiv 2003/6/EG och kommissionens direktiv 2003/124/EG, 2003/125/EG och 2004/72/EG, jämförda med artikel 15.1 i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009, och mot bakgrund av artiklarna 7, 8, 11 och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna,**

   ska tolkas så,

   att de utgör hinder mot nationella lagstiftningsåtgärder som innebär att trafikuppgifter – i förebyggande syfte och för att bekämpa marknadsmissbruksbrott, inklusive insiderhandel – generellt och odifferentierat ska lagras i ett år från och med registreringsdagen.

2) **Unionsrätten ska tolkas så att den utgör hinder mot att en nationell domstol, med stöd av nationell rätt, begränsar rättsverkningarna i tiden av en ogiltigförklaring av nationella bestämmelser som dels innebär att operatörer som tillhandahåller elektroniska kommunikationstjänster åläggs en skyldighet att generellt och odifferentierat lagra trafikuppgifter, dels tillåter att sådana uppgifter lämnas ut till den behöriga finansmarknadsmyndigheten utan föregående tillstånd från en domstol eller en oberoende förvaltningsmyndighet, när dessa bestämmelser har ansetts vara oförenliga med artikel 15.1 i direktiv 2002/58, i dess lydelse enligt direktiv 2009/136, tolkad mot bakgrund av Europeiska unionens stadga om de grundläggande rättigheterna. Tillåtligheten av bevisning som erhållits med stöd av nationell lagstiftning som strider mot unionsrätten regleras, i enlighet med principen om medlemsstaternas processuella autonomi, av nationell rätt, förutsatt att bland annat likvärdighetsprincipen och effektivitetsprincipen iakttas.**

Underskrifter