



Judikatūras krājums

TIESAS SPRIEDUMS (virspalāta)

2022. gada 20. septembrī*

Lūgums sniegt prejudiciālu nolēmumu – Vienotais finanšu pakalpojumu tirgus –
Tirgus ļaunprātīga izmantošana – Iekšējās informācijas ļaunprātīga izmantošana –
Direktīva 2003/6/EK – 12. panta 2. punkta a) un d) apakšpunkts – Regula (ES) Nr. 596/2014 –
23. panta 2. punkta g) un h) apakšpunkts – *Autorité des marchés financiers (AMF)* uzraudzības un
izmeklēšanas pilnvaras – Vispārējo interešu mērķis aizsargāt Eiropas Savienības finanšu tirgu
integritāti un sabiedrības uzticēšanos finanšu instrumentiem – Iespēja *AMF* panākt, ka tai tiek
nosūtīti elektronisko komunikāciju operatora rīcībā esošie datu plūsmas ieraksti – Personas datu
apstrāde elektronisko komunikāciju nozarē – Direktīva 2002/58/EK – 15. panta 1. punkts –
Eiropas Savienības Pamattiesību harta – 7., 8. un 11. pants, kā arī 52. panta 1. punkts –
Komunikāciju konfidencialitāte – Ierobežojumi – Tiesību akti, kuros ir noteikts, ka elektronisko
komunikāciju operatori visaptveroši un nediferencēti glabā informāciju par datu plūsmu –
Iespēja valsts tiesai ierobežot ar Savienības tiesībām nesaderīgu valsts tiesību normu atzīšanas par
spēkā neesošām sekas laikā – Izslēgšana

Apvienotajās lietās C-339/20 un C-397/20

par lūgumiem sniegt prejudiciālu nolēmumu atbilstoši LESD 267. pantam, ko *Cour de cassation*
(Kasācijas tiesa, Francija) iesniegusi ar 2020. gada 1. aprīļa lēmumiem un kas Tiesā reģistrēti
attiecīgi 2020. gada 24. jūlijā un 2020. gada 20. augustā, kriminālprocesos pret

VD (C-339/20),

SR (C-397/20),

TIESA (virspalāta)

šādā sastāvā: Tiesas priekšsēdētājs K. Lēnartss [*K. Lenaerts*], palātu priekšsēdētāji A. Arabadžijevs
[*A. Arabadjiev*], A. Prehala [*A. Prechal*], S. Rodins [*S. Rodin*], I. Jarukaitis [*I. Jarukaitis*] un
I. Ziemele, tiesneši T. fon Danvics [*T. von Danwitz*], M. Safjans [*M. Safjan*], F. Biltšens
[*F. Biltgen*], P. Dž. Švirebs [*P. G. Xuereb*] (referents), N. Pisarra [*N. Piçarra*], L. S. Rosi [*L. S. Rossi*]
un A. Kumins [*A. Kumin*],

ģenerālvokāts: M. Kampos Sančess-Bordona [*M. Campos Sánchez-Bordona*],

sekretāre: R. Šereša [*R. Şereş*], administratore,

ņemot vērā rakstveida procesu un 2021. gada 14. septembra tiesas sēdi,

* Tiesvedības valoda – franču.

nemot vērā apsvērumus, ko sniedza:

- VD vārdā – *D. Foussard* un *F. Peltier, avocats*,
- SR vārdā – *M. Chavannes* un *P. Spinosi, avocats*,
- Francijas valdības vārdā – *A. Daniel* un *E. de Moustier, D. Dubois, J. Illouz* un *T. Stéhelin*, pārstāvji,
- Dānijas valdības vārdā – *N. Holst-Christensen, N. Lykkegaard* un *M. Søndahl Wolff*, pārstāves,
- Igaunijas valdības vārdā – *A. Kalbus* un *M. Kriisa*, pārstāves,
- Īrijas vārdā – *M. Browne, A. Joyce* un *J. Quaney*, pārstāvji, kam palīdz *D. Fennelly, BL*,
- Spānijas valdības vārdā – *L. Aguilera Ruiz*, pārstāvis,
- Polijas valdības vārdā – *B. Majczyna*, pārstāvis,
- Portugāles valdības vārdā – *P. Barros da Costa, L. Inez Fernandes, L. Medeiros* un *I. Oliveira*, pārstāvji,
- Eiropas Komisijas vārdā – *S. L. Kalèda, H. Kranenborg, T. Scharf* un *F. Wilman*, pārstāvji,
- Eiropas Datu aizsardzības uzraudzītāja vārdā – *A. Buchta, M. Guglielmetti, C.-A. Mamier* un *D. Nardi*, pārstāvji,

noklausījusies ģenerālvokāta secinājumus 2021. gada 18. novembra tiesas sēdē,

pasludina šo spriedumu.

Spriedums

- 1 Lūgumi sniegt prejudiciālu nolēmumu būtībā ir par to, kā jāinterpretē Eiropas Parlamenta un Padomes Direktīvas 2003/6/EK (2003. gada 28. janvāris) par iekšējās informācijas ļaunprātīgu izmantošanu un tirgus manipulācijām (tirgus ļaunprātīgu izmantošanu) (OV 2003, L 96, 16. lpp.) 12. panta 2. punkta a) un d) apakšpunkts, kā arī Eiropas Parlamenta un Padomes Regulas (ES) Nr. 596/2014 (2014. gada 16. aprīlis) par tirgus ļaunprātīgu izmantošanu (tirgus ļaunprātīgas izmantošanas regula) un ar ko atceļ Eiropas Parlamenta un Padomes Direktīvu 2003/6/EK un Komisijas Direktīvas 2003/124/EK, 2003/125/EK un 2004/72/EK (OV 2014, L 173, 1. lpp.) 23. panta 2. punkta g) un h) apakšpunkts, lasot tos kopsakarā ar Eiropas Parlamenta un Padomes Direktīvas 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju) (OV 2002, L 201, 37. lpp.), redakcijā ar grozījumiem, kas izdarīti ar Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīvu 2009/136/EK (OV 2009, L 337, 11. lpp.) (turpmāk tekstā – “Direktīva 2002/58”), 15. panta 1. punktu un lasot tos Eiropas Savienības Pamattiesību hartas (turpmāk tekstā – “Harta”) 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā.

- 2 Šie lūgumi ir iesniegti saistībā ar kriminālprocesiem pret VD un SR par šādiem noziedzīgiem nodarījumiem: iekšējās informācijas ļaunprātīga izmantošana, iekšējās informācijas ļaunprātīgas izmantošanas slēpšana, līdzdalība, korupcija un nelikumīgi iegūtu līdzekļu legalizēšana.

Atbilstošās tiesību normas

Savienības tiesības

Direktīva 2002/58

- 3 Direktīvas 2002/58 2., 6., 7. un 11. apsvērumā ir teikts:

“(2) Šī direktīva respektē pamattiesības un ievēro principus, kas jo īpaši ir atzīti [Hartā]. Šī direktīva jo īpaši nodrošina pilnībā tiesības, kas izklāstītas [tās] 7. un 8. pantā.

[..]

(6) Internets maina tradicionālās tirgus struktūras, nodrošinot kopēju, globālu infrastruktūru plaša elektronisko komunikāciju pakalpojumu klāsta piedāvājumam. Publiski pieejami elektronisko telekomunikāciju pakalpojumi internetā atklāj jaunas iespējas lietotājiem, taču rada jaunu risku to personas datiem un privātajai dzīvei.

(7) Attiecībā uz publisko komunikāciju tīklu jāizstrādā īpaši normatīvi un tehniskie noteikumi, lai aizsargātu fizisku personu pamattiesības un pamatbrīvības, kā arī juridisku personu likumīgās intereses, jo īpaši ņemot vērā arvien lielāku jaudu abonentu un lietotāju datu automatizētai glabāšanai un apstrādei.

[..]

(11) Tāpat kā [Eiropas Parlamenta un Padomes] Direktīva 95/46/EK [(1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV 1995, L 281, 31. lpp.)], arī šī direktīva neattiecas uz pamattiesību un pamatbrīvību aizsardzības jautājumiem, kas saistīti ar darbībām, kuras neregulē Kopienas tiesību akti. Tāpēc tā nemaina esošo līdzsvaru starp fizisku personu tiesībām uz privāto dzīvi un iespēju dalībvalstīm pieņemt šīs direktīvas 15. panta 1. punktā minētos pasākumus, kas nepieciešami sabiedrības drošībai, aizsardzībai, valsts drošībai (tostarp valsts ekonomisko labklājību, ja darbības attiecas uz valsts drošības jautājumiem) un krimināltiesību aktu piemērošanai. Tādējādi šī direktīva neietekmē dalībvalstu iespēju veikt komunikāciju likumīgu pārtraukšanu vai pieņemt citus pasākumus, ja tie nepieciešami jebkuram no šiem nolūkiem un ir saskaņā ar [Romā 1950. gada 4. novembrī parakstīto] Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvenciju, kā skaidrots Eiropas Cilvēktiesību tiesas nolēmumos. Šādiem pasākumiem jābūt atbilstošiem, stingri samērīgiem ar paredzēto nolūku un nepieciešamiem demokrātiskā sabiedrībā, un tiem jāatbilst attiecīgajiem drošības pasākumiem saskaņā ar Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvenciju.”

4 Direktīvas 2002/58 1. pantā “Darbības joma un mērķis” ir noteikts:

“1. Šajā direktīvā paredzēta dalībvalstu to noteikumu saskaņošana, ar kuriem jānodrošina pamattiesību un pamatbrīvību līdzvērtīgs aizsardzības līmenis, un jo īpaši tiesības uz privāto dzīvi un konfidencialitāti saistībā ar personas datu apstrādi elektronisko komunikāciju nozarē, kā arī jānodrošina šo datu un elektronisko komunikāciju iekārtu un pakalpojumu brīva aprīte Kopienā.

2. Šīs direktīvas noteikumi precizē un papildina [Direktīvu 95/46 šā panta] 1. punktā minētajam nolūkam. Turklāt ar tiem paredz to abonentu likumīgo interešu aizsardzību, kuri ir juridiskas personas.

3. Šī direktīva neattiecas uz darbībām, uz kurām neattiecas [LESD], tādām kā tās, kas iekļautas [LES] V un VI sadaļā, un jebkurā gadījumā uz darbībām, kas attiecas uz sabiedrības drošību, aizsardzību, valsts drošību (tostarp valsts ekonomisko labklājību, ja darbības attiecas uz valsts drošības jautājumiem) un uz valsts darbībām krimināltiesību jomā.”

5 Minētās direktīvas 2. panta “Definīcijas” otrās daļas b) punktā ir noteikts:

“Piemēro [..] šādas definīcijas:

[..]

b) “informācija par datu plūsmu” ir jebkuri dati, kas apstrādāti ar nolūku pārsūtīt komunikāciju elektronisko komunikāciju tīklā vai ar nolūku sagatavot rēķinu.”

6 Saskaņā ar šīs pašas direktīvas 5. pantu “Komunikāciju konfidencialitāte”:

“1. Dalībvalstis nodrošina komunikāciju un saistītās informācijas par datu plūsmu konfidencialitāti ar publisko komunikāciju tīkla un publiski pieejamu elektronisko komunikāciju pakalpojumiem, ievērojot valsts tiesību aktus. Īpaši tās aizliedz komunikāciju un saistītās informācijas par datu plūsmu noklausīšanos, ierakstīšanu, uzglabāšanu vai cita veida aizturēšanu vai pārraudzību personām, kas nav lietotāji, bez attiecīgo lietotāju piekrišanas, izņemot gadījumus, kad to darīt ir ar likumu atļauts saskaņā ar 15. panta 1. punktu. Šis punkts neliedz tehnisko uzglabāšanu, kas nepieciešama komunikāciju pārsūtīšanai, neierobežojot konfidencialitātes principu.

2. [Šā panta] 1. punkts neietekmē ar likumu atļautu komunikāciju un saistītās informācijas par datu plūsmu reģistrēšanu, ja to veic likumīgas uzņēmējdarbības prakses sakarā, lai sniegtu pierādījumu par komerciālu darījumu vai par jebkuru citu uzņēmējdarbības komunikāciju.

3. Dalībvalstis nodrošina, ka informācijas uzglabāšana abonenta vai lietotāja gala iekārtā vai piekļuves iegūšana šādā iekārtā jau uzglabātai informācijai ir atļauta tikai ar nosacījumu, ka attiecīgais abonents vai lietotājs ir devis savu piekrišanu un saskaņā ar Direktīvu [95/46] nodrošināts ar skaidru un visaptverošu informāciju, tostarp par apstrādes nolūku. Tas neliedz jebkādu tehnisku uzglabāšanu vai piekļuvi, kas paredzēta vienīgi, lai veiktu saziņas pārraidīšanu elektronisko sakaru tīklā, vai kas noteikti nepieciešama tā informācijas sabiedrības pakalpojuma sniedzējam, kuru skaidri pieprasījis abonents vai lietotājs.”

7 Direktīvas 2002/58 6. pantā “Informācija par datu plūsmu” ir noteikts:

“1. Informācija par datu plūsmu, kas attiecas uz abonentiem un lietotājiem un ko publisko komunikāciju tīkla pakalpojumu sniedzējs vai publiski pieejamu elektronisko komunikāciju pakalpojuma sniedzējs apstrādā vai uzglabā, ir jādzēš vai jāpadara anonīma, kad tā vairs nav nepieciešama komunikāciju pārraidīšanai, neierobežojot šā panta 2., 3. un 5. [punktu] un 15. panta 1. punktu.

2. Var apstrādāt informāciju par datu plūsmu, kas nepieciešama, lai abonentam sagatavotu rēķinu un veiktu norēķinus par starpsavienojumiem. Šāda apstrāde ir pieļaujama tikai tik ilgi, kamēr nav beidzies termiņš, kura laikā var likumīgi apstrīdēt rēķinu vai saņemt maksājumu.

3. Elektronisko komunikāciju pakalpojumu tirdzniecības nolūkā vai pievienotās vērtības pakalpojumu sniegšanas nolūkā publiski pieejamu elektronisko komunikāciju pakalpojuma sniedzējs var apstrādāt 1. punktā minēto informāciju līdz līmenim un tik ilgi, cik nepieciešams šādiem pakalpojumiem vai tirdzniecībai, ja abonents vai lietotājs, uz kuru šī informācija attiecas, pirms tam ir devis savu piekrišanu. Lietotājiem vai abonentiem dod iespēju jebkurā laikā atsaukt savu piekrišanu informācijas par datu plūsmu apstrādei.

[..]

5. Informācijas par datu plūsmu apstrāde, saskaņā ar 1., 2., 3. un 4. punktu, ir jāierobežo līdz personām, kas darbojas ar pilnvaru no publisko komunikāciju tīklu pakalpojumu sniedzējiem un tādu publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzējiem, kas apstrādā rēķinu sagatavošanas vai datu plūsmas pārvaldi, klientu pieprasījumus, pārkāpumu noteikšanu, elektronisko komunikāciju pakalpojumu tirdzniecību vai pievienotās vērtības pakalpojumu sniegšanu, un tā jāierobežo līdz līmenim, kas nepieciešams šādu darbību veikšanai.

[..]”

8 Šīs direktīvas 9. panta “Atrašanās vietas dati, kas nav informācija par datu plūsmu” 1. punktā ir paredzēts:

“Ja var apstrādāt atrašanās vietas datus, kas nav informācija par datu plūsmu, attiecībā uz publisko komunikāciju tīklu vai publiski pieejamu elektronisko komunikāciju pakalpojumu lietotājiem vai abonentiem, šādus datus var apstrādāt tikai tad, kad tie ir padarīti anonīmi, vai ar lietotāju vai abonentu piekrišanu, līdz tādām līmenim un tik ilgi, cik nepieciešams, lai sniegtu pievienotās vērtības pakalpojumus. Pakalpojuma sniedzējam ir jāinformē lietotāji vai abonentu pirms to piekrišanas saņemšanas par apstrādājamajiem atrašanās vietas datu veidiem, ja dati nav informācija par datu plūsmu, par apstrādes nolūku un ilgumu un par to, vai šos datus pārsūtīs trešajai personai ar nolūku sniegt pievienotās vērtības pakalpojumu. [..]”

9 Direktīvas 2002/58 15. panta “Direktīvas [95/46] dažu noteikumu piemērošana” 1. punktā ir noteikts:

“Dalībvalstis var pieņemt tiesību aktus, lai ierobežotu šīs direktīvas 5. un 6. pantā, 8. panta 1., 2., 3. un 4. punktā un 9. pantā minēto tiesību un pienākumu darbības jomu, ja šādi ierobežojumi ir vajadzīgi saskaņā ar nepieciešamiem, atbilstīgiem un samērīgiem pasākumiem demokrātiskā sabiedrībā, lai garantētu valsts drošību, aizsardzību, sabiedrības drošību un kriminālpārkāpumu [noziedzīgu nodarījumu] vai elektroniskās komunikāciju sistēmas nevēlamas izmantošanas novēršanu, izmeklēšanu, noteikšanu [atklāšanu] un kriminālvajāšanu, kā noteikts Direktīvas [95/46] 13. panta

1. punktā. Tālab dalībvalstis, cita starpā, var pieņemt tiesību aktus, paredzot datu saglabāšanu ierobežotā laikposmā, kas pamatots ar šajā punktā noteiktajiem iemesliem. Visi šajā punktā minētie pasākumi ir saskaņā ar Kopienas tiesību aktu vispārējiem principiem, tostarp tie[m], kas minēti [LES] 6. panta 1. un 2. punktā.”

Direktīva 2003/6

10 Direktīvas 2003/6 1., 2., 12., 37., 41. un 44. apsvērums ir formulēts šādi:

“(1) Patiesi vienots finanšu pakalpojumu tirgus ir izšķiroši nozīmīgs ekonomiskai izaugsmei un darba vietu izveidošanai Kopienā.

(2) Lai finanšu tirgus būtu vienots un efektīvs, ir vajadzīga tirgus integritāte. Ekonomiskā izaugsme un labklājība nebūs iespējama, ja vērtspapīru tirgu darbība nebūs vienmērīga un sabiedrība neuzticēsies šiem tirgiem. Tirgus ļaunprātīga izmantošana kaitē finanšu tirgu integritātei un vājina sabiedrības uzticību vērtspapīriem un atvasinātajiem instrumentiem.

[..]

(12) Tirgus ļaunprātīga izmantošana ietver iekšējās informācijas ļaunprātīgu izmantošanu un tirgus manipulācijas. Tiesību aktu mērķis attiecībā uz iekšējās informācijas ļaunprātīgas izmantošanas novēršanu ir tāds pats kā attiecībā uz tirgus manipulāciju novēršanu: nodrošināt Kopienas finanšu tirgu integritāti un paaugstināt investoru uzticību minētajiem tirgiem. [..]

[..]

(37) Uzraudzības efektivitāte tiks garantēta, pateicoties vienotam iedarbīgu pilnvaru un darbības līdzekļu minimumam katras dalībvalsts kompetentās iestādes rīcībā. Arī tirgus dalībniekiem un visiem ekonomiskā procesa dalībniekiem savā līmenī jāveicina tirgus integritāte. [..]

[..]

(41) Dalībvalstis atsevišķi pilnā mērā nevar sasniegt iecerētās rīcības mērķi, proti, novērst tirgus ļaunprātīgu izmantošanu, ļaunprātīgi izmantojot iekšējo informāciju un īstenojot tirgus manipulācijas, un tādējādi minēto pasākumu mēroga un nozīmīguma dēļ šo mērķi var labāk sasniegt Kopienas līmenī; Kopiena var noteikt pasākumus saskaņā ar subsidiaritātes principu, kā noteikts [LES] 5. pantā. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šī direktīva nepārsniedz šā mērķa sasniegšanai vajadzīgo.

(44) Šajā direktīvā ir respektētas pamattiesības un ievēroti principi, kuri jo īpaši atzīti [Hartā], un konkrēti tās 11. pantā, un Eiropas Cilvēktiesību [un pamatbrīvību aizsardzības] konvencijas 10. pantā; [..].”

11 Šīs direktīvas 11. pantā ir noteikts:

“Neskarot tiesu iestāžu kompetenci, katra dalībvalst[s] norīko vienu administratīvu iestādi, lai nodrošinātu saskaņā ar šo direktīvu pieņemto noteikumu piemērošanu.

[..]”

12 Saskaņā ar minētās direktīvas 12. pantu:

“1. Kompetentajai iestādei piešķir visas uzraudzības un izmeklēšanas pilnvaras, kuras ir vajadzīgas tās uzdevumu izpildei. [..]

2. Neskarot 6. panta 7. punktu, šā panta 1. punktā minētās pilnvaras īsteno atbilstīgi valsts tiesību aktiem un tajās ietilpst vismaz tiesības[:]

a) piekļūt jebkuram dokumentam jebkādā formā un saņemt tā kopiju;

[..]

d) pieprasīt esošo[s] telefonsarunu ierakstus un esošos datu plūsmas ierakstus;

[..].”

Regula Nr. 596/2014

13 Ar Regulu Nr. 596/2014 kopš 2016. gada 3. jūlija ir atcelta un aizstāta Direktīva 2003/6.

14 Šīs regulas 1., 2., 7., 24., 44., 62., 65., 66., 77. un 86. apsvērumi ir formulēti šādi:

“(1) Patiess iekšējais finanšu pakalpojumu tirgus ir izšķiroši nozīmīgs ekonomikas izaugsmei un darbvietu izveidei Savienībā.

(2) Lai finanšu tirgus būtu vienots, efektīvs un pārredzams, ir vajadzīga tirgus integritāte. Ekonomiskā izaugsme un labklājība nebūs iespējama, ja vērtspapīru tirgu darbība nebūs vienmērīga un sabiedrība neuzticēsies šiem tirgiem. Tirgus ļaunprātīga izmantošana kaitē finanšu tirgu integritātei un vājina sabiedrības uzticību vērtspapīriem un atvasinātajiem instrumentiem.

[..]

(7) Tirgus ļaunprātīga izmantošana ir jēdziens, kas ietver nelikumīgu rīcību finanšu tirgos, un šīs regulas nozīmē tā būtu jāsaprot kā iekšējās informācijas izmantošana tirdzniecībā, šādas informācijas nelikumīga izpaušana un tirgus manipulācija. Šāda rīcība kavē pilnīgu un atbilstīgu tirgus pārredzamību, kas ir visu integrēto finanšu tirgu dalībnieku veikto tirdzniecības darījumu priekšnoteikums.

[..]

(24) Ja juridiska vai fiziska persona, kuras rīcībā ir iekšējā informācija, savā vārdā vai trešās puses vārdā tieši vai netieši iegādājas vai atsavina, vai mēģina iegādāties vai atsavināt finanšu instrumentus, uz kuriem attiecas minētā informācija, tam vajadzētu nozīmēt, ka minētā persona ir izmantojusi minēto informāciju. Minētais pieņēmums neskar tiesības uz aizstāvību. Jautājums par to, vai persona ir pārkāpusi iekšējās informācijas izmantošanas tirdzniecībā aizliegumu vai mēģinājusi darījumā izmantot iekšējo informāciju, būtu jāizskata, ņemot vērā šīs regulas mērķi, proti, aizsargāt finanšu tirgus integritāti un veicināt

ieguldītāju uzticēšanos, kas savukārt balstās uz pārliecību, ka pret ieguldītājiem būs vienlīdzīga attieksme un viņi tiks aizsargāti no iekšējās informācijas ļaunprātīgas izmantošanas.

[..]

(44) Daudziem finanšu instrumentiem cenas tiek noteiktas, atsaucoties uz etaloniem. Etalona, tostarp starpbanku piedāvājuma likmju, faktiskas manipulācijas vai manipulāciju mēģinājums var nopietni ietekmēt pašvību tirgum un radīt ievērojamus zaudējumus ieguldītājiem vai izkropļot reālo ekonomiku. [..]

(62) Uzraudzības efektivitāti nodrošina iedarbīgu instrumentu, pilnvaru un resursu kopums, kas ir katras dalībvalsts kompetentās iestādes rīcībā. Tādēļ šī regula jo īpaši nosaka minimālo uzraudzības un izmeklēšanas pilnvaru kopumu, kāds būtu jāpiešķir dalībvalstu kompetentajām iestādēm saskaņā ar valsts tiesību aktiem. Minētās pilnvaras būtu jāīsteno, vēršoties kompetentajās tiesu iestādēs, ja tā noteikts valsts tiesību aktos. [..]

[..]

(65) Esoši telefonsarunu un datu plūsmas ieraksti no ieguldījumu brokeru sabiedrībām, kredītiestādēm un finanšu iestādēm, kas veic un reģistrē darījumu izpildi, kā arī esoši telefonsarunu un datu plūsmas ieraksti, kurus glabā telesakaru operatori, ir svarīgi un dažreiz vienīgie pierādījumi, lai konstatētu un pierādītu iekšējās informācijas izmantošanu tirdzniecībā un tirgus manipulācijas. Telefonsarunu un datu plūsmas ieraksti var palīdzēt noteikt tās personas identitāti, kas ir atbildīga par nepatiesas vai maldinošas informācijas izplatīšanu, vai to, ka personas ir sazinājušās konkrētā brīdī un ka starp diviem vai vairāk cilvēkiem pastāv attiecības. Tādēļ būtu jānodrošina iespēja kompetentajām iestādēm pieprasīt telefonsarunu, elektroniskās saziņas un datu plūsmas ierakstus, kas ir kādas ieguldījumu brokeru sabiedrības, kredītiestādes vai finanšu iestādes rīcībā saskaņā ar [Eiropas Parlamenta un Padomes] Direktīvu 2014/65/ES [(2014. gada 15. maijs) par finanšu instrumentu tirgiem un ar ko groza Direktīvu 2002/92/ES un Direktīvu 2011/61/ES (OV 2014, L 173, 349. lpp.)]. Piekļuve datiem un telefonsarunu ierakstiem ir vajadzīga, lai nodrošinātu pierādījumus un izmeklēšanas virzienus attiecībā uz iespējamu iekšējās informācijas izmantošanu tirdzniecībā vai iespējamām tirgus manipulācijām un līdz ar to – lai konstatētu tirgus ļaunprātīgu izmantošanu un piemērotu sankcijas par to. Lai Savienībā izveidotu vienlīdzīgus konkurences nosacījumus attiecībā uz piekļuvi telefonsarunu un datu plūsmas ierakstiem, kas ir telesakaru operatora rīcībā, vai esošiem telefonsarunu un datu plūsmas ierakstiem, kas ir ieguldījumu brokeru sabiedrības, kredītiestādes vai finanšu iestādes rīcībā, kompetentajām iestādēm saskaņā ar valsts tiesību aktiem būtu jāspēj pieprasīt telefonsarunu un datu plūsmas ierakstus, kas ir telesakaru operatora rīcībā, ciktāl to atļauj valsts tiesību akti, un esošus telefonsarunu un datu plūsmas ierakstus, kas ir ieguldījumu brokeru sabiedrības rīcībā, tajos gadījumos, kad pastāv pamatotas aizdomas, ka šādi ieraksti, kas attiecas uz pārbaudes vai izmeklēšanas priekšmetu, var būt svarīgi, lai pierādītu iekšējās informācijas izmantošanu tirdzniecībā vai tirgus manipulācijas, ar ko pārkāpj šo regulu. Piekļuve telefonsarunu un datu plūsmas ierakstiem, kas ir telesakaru operatora rīcībā, neietver piekļuvi balss saziņas pa telefonu saturam.

(66) Lai gan šajā regulā ir precizētas minimālās pilnvaras, kādām vajadzētu būt kompetentajām iestādēm, minētās pilnvaras ir jāisteno atbilstīgi pilnīgai valsts tiesību sistēmai, kas garantē pamattiesību ievērošanu, tostarp tiesību uz privātumu ievērošanu. Lai īstenotu minētās pilnvaras, kas var būtiski pārkāpt tiesības uz privātās un ģimenes dzīves, mājokļa un saziņas neaizskaramību, dalībvalstīm būtu jāievieš pienācīgi un efektīvi aizsargpasākumi pret jebkādu ļaunprātīgu izmantošanu, piemēram, attiecīgā gadījumā prasīb[a] saņemt iepriekšēju atļauju no attiecīgās dalībvalsts tiesu iestādes. Dalībvalstīm būtu jāpieļauj iespēja, ka kompetentās iestādes varētu īstenot šādas iejaukšanās pilnvaras tiktāl, cik tas būtu nepieciešams pienācīgai nopietnu gadījumu izmeklēšanai, ja nepastāv līdzvērtīgi risinājumi tāda paša rezultāta sasniegšanai.

[..]

(77) Šajā regulā ir ievērotas pamattiesības un principi, kas atzīti [Hartā]. Tādēļ regula būtu jāinterpretē un jāpiemēro saskaņā ar minētajām tiesībām un principiem. [..]

[..]

(86) Ņemot vērā to, ka šīs regulas mērķi, proti, novērst tirgus ļaunprātīgu izmantošanu iekšējās informācijas izmantošanas tirdzniecībā, iekšējās informācijas nelikumīgas izplatīšanas un tirgus manipulāciju veidā, nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, bet mēroga un ietekmes dēļ minēto mērķi var labāk sasniegt Savienības līmenī, Savienība var pieņemt pasākumus saskaņā ar [LES] 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā regulā paredz vienīgi tos pasākumus, kas ir vajadzīgi minētā mērķa sasniegšanai.”

15 Saskaņā ar minētās regulas 1. pantu:

“Ar šo regulu izveido kopēju tiesisku regulējumu attiecībā uz iekšējās informācijas izmantošanu tirdzniecībā, iekšējās informācijas nelikumīgu izpaušanu un tirgus manipulācijām (tirgus ļaunprātīgu izmantošanu), kā arī pasākumus nolūkā novērst tirgus ļaunprātīgu izmantošanu, lai nodrošinātu Savienības finanšu tirgu integritāti un uzlabotu ieguldītāju aizsardzību un uzticēšanos minētajiem tirgiem.”

16 Šīs pašas regulas 3. panta “Definīcijas” 1. punkta 27. apakšpunktā ir noteikts:

“Šajā regulā piemēro šādas definīcijas:

[..]

27) “datu plūsmas ieraksti” ir “datu plūsmas” ieraksti, kā definēts Eiropas Parlamenta un Padomes Direktīvas [2002/58] 2. panta otrās daļas b) punktā.”

17 Regulas Nr. 596/2014 14. pantā “Iekšējās informācijas izmantošanas tirdzniecībā un iekšējās informācijas nelikumīgas izpaušanas aizliegums” ir noteikts:

“Persona nevar:

a) iesaistīties iekšējās informācijas izmantošanā tirdzniecībā vai tās mēģinājumā;

- b) ieteikt citai personai iesaistīties iekšējās informācijas izmantošanā tirdzniecībā vai mudināt citu personu iesaistīties iekšējās informācijas izmantošanā tirdzniecībā; vai
- c) nelikumīgi izpaust iekšējo informāciju.”

18 Šīs regulas 22. pantā ir paredzēts:

“Neskarot tiesu iestāžu kompetenču jomas, katra dalībvalsts šīs regulas nolūkiem norīko vienu administratīvu kompetento iestādi. [..]”

19 Minētās regulas 23. panta “Kompetento iestāžu pilnvaras” 2. un 3. punktā ir noteikts:

“2. Lai veiktu savus pienākumus saskaņā ar šo regulu, kompetentajām iestādēm saskaņā ar valstu tiesību aktiem ir vismaz šādas uzraudzības un izmeklēšanas pilnvaras:

a) piekļūt jebkādiem dokumentiem un datiem jebkādā formātā un saņemt vai izgatavot to kopiju;

[..]

g) pieprasīt ieguldījumu brokeru sabiedrību, kredītiestāžu vai citu finanšu iestāžu rīcībā esošo[s] telefona sarunu, elektroniskās saziņas vai datu plūsmas ierakstus;

h) ciktāl to atļauj valsts tiesību akti, pieprasīt telekomunikāciju operatora rīcībā esošos datu plūsmas ierakstus, ja ir pamatotas aizdomas par pārkāpumu un šādi ieraksti var būt vajadzīgi 14. panta a) vai b) punkta vai 15. panta pārkāpuma izmeklēšanai;

[..].

3. Dalībvalstis nodrošina, ka ir ieviesti atbilstīgi pasākumi, lai kompetentajām iestādēm būtu visas uzraudzības un izmeklēšanas pilnvaras, kas vajadzīgas to pienākumu veikšanai.

[..]”

Francijas tiesības

CPCE

20 *Code des postes et des communications électroniques* (Pasta un elektronisko sakaru kodekss), redakcijā, kas piemērojama pamatlīetu faktiskajiem apstākļiem (turpmāk tekstā – “*CPCE*”), L. 34-1. pantā bija noteikts:

“I. – Šo pantu piemēro personas datu apstrādei, sniedzot sabiedrībai elektronisko komunikāciju pakalpojumus; konkrēti – to piemēro tīkliem, kuros ir datu vākšanas un identifikācijas iekārtas.

II. – Elektronisko komunikāciju operatori un it īpaši personas, kas piedāvā sabiedrībai piekļuvi komunikāciju pakalpojumiem tiešsaistē, dzēš vai anonimizē visu informāciju par datu plūsmu, ja vien III, IV, V un VI punktā nav noteikts citādi.

Personas, kas sniedz elektronisko komunikāciju pakalpojumus sabiedrībai, saskaņā ar iepriekšējā daļā noteikto paredz iekšējās procedūras, lai izpildītu kompetento iestāžu pieprasījumus.

Personām, kuras, veicot savu galveno vai papildu uzņēmējdarbību, piedāvā sabiedrībai savienojumu, kas ar piekļuvi tīklam nodrošina komunikāciju tiešsaistē, pat bez maksas, ir pienākums ievērot tiesību normas, kuras saskaņā ar šo pantu piemērojamas elektronisko komunikāciju operatoriem.

III. – Lai izmeklētu un atklātu noziedzīgus nodarījumus vai *code de la propriété intellectuelle* [Intelektuālā īpašuma kodeksa] L. 336-3. pantā noteiktā pienākuma neizpildes gadījumus un veiktu kriminālvajāšanu par tiem vai lai novērstu Kriminālkodeksa 323-1. līdz 323-3-1. pantā minētos sodāmos uzbrukumus datu automātiskās apstrādes sistēmām, konkrētu datu kategoriju dzēšanas vai anonimizēšanas operācijas var atlikt uz laiku, kas nepārsniedz vienu gadu, tikai tadē, lai vajadzības gadījumā sniegtu tos tiesu iestādei vai augstajai iestādei, kas minēta Intelektuālā īpašuma kodeksa L. 331-12. pantā, vai nacionālajai informācijas sistēmu drošības iestādei, kas minēta *code de la défense* [Aizsardzības kodeksa] L. 2321-1. pantā. *Conseil d'État* [Valsts padome] dekrētā, kas pieņemts pēc Nacionālās informātikas un brīvību komisijas atzinuma, VI punktā paredzētajās robežās tiek noteiktas šīs datu kategorijas un to glabāšanas ilgums atkarībā no operatoru darbības un komunikāciju rakstura, kā arī vajadzības gadījumā kārtība, kādā ir kompensējamas identificējamās un konkrētās papildizmaksas, kas rodas saistībā ar pakalpojumiem, kurus operatori tālab sniedz pēc valsts pieprasījuma.

[..]

VI. – Saskaņā ar III, IV un V punktā paredzētajiem nosacījumiem glabāti un apstrādāti tiek tikai tie dati, kas attiecas uz operatoru sniegto pakalpojumu lietotāju identificēšanu, šo operatoru nodrošināto komunikāciju tehniskajiem parametriem un galaiekārtu atrašanās vietu.

Tie nekādā gadījumā nedrīkst būt dati par komunikāciju saturu vai šo komunikāciju laikā izmantoto informāciju.

Šos datus glabā un apstrādā saskaņā ar noteikumiem, kas paredzēti 1978. gada 6. janvāra *loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés* [Likumā Nr. 78-17 par informātiku, datnēm un brīvībām].

Operatori veic visus vajadzīgos pasākumus, lai novērstu šo datu izmantošanu šajā pantā neparedzētiem mērķiem.”

- 21 Pasta un elektronisko sakaru kodeksa, redakcijā ar grozījumiem, kas izdarīti ar 2021. gada 30. jūlija *loi n° 2021-998 relative à la prévention d'actes de terrorisme et au renseignement* (Likums Nr. 2021-998 par teroraktu novēršanu un izlūkdienestiem; 2021. gada 31. jūlija *JORF*, teksts Nr. 1), L. 34-1. panta II *bis*–III *bis* punktā ir paredzēts:

“II *bis* – Elektronisko komunikāciju operatoriem ir pienākums glabāt:

1° kriminālprocesu, sabiedrības drošības apdraudējumu novēršanas un valsts drošības aizsardzības vajadzībām: informāciju par lietotāja identitāti – piecus gadus pēc viņa liguma beigām;

2° tiem pašiem mērķiem, kas minēti šā II *bis* punkta 1°. apakšpunktā: citu informāciju, ko sniedzis lietotājs līguma noslēgšanas vai konta izveides brīdī, kā arī maksājumu informāciju – vienu gadu pēc viņa līguma darbības beigām vai konta slēgšanas;

3° noziedzības un smagu noziedzīgu nodarījumu, nopietnu sabiedrības drošības apdraudējumu novēršanas un valsts drošības aizsardzības vajadzībām: tehniskos datus, kas ļauj identificēt savienojuma avotu, vai datus par izmantotajām galaiekārtām – līdz vienam gadam pēc savienojuma vai galaiekārtu lietošanas.

III. – Valsts drošības apsvērumu dēļ gadījumā, ja ir konstatēts faktiskais vai paredzams nopietns tās apdraudējums, premjerministrs drīkst ar dekrētu uzdot elektronisko komunikāciju operatoriem vienu gadu glabāt noteiktu kategoriju informāciju par datu plūsmu papildus datiem, kas minēti II *bis* punkta 3°. apakšpunktā, un *Conseil d'État* dekrētā noteiktos atrašanās vietas datus.

Premjerministra rīkojumu, kura piemērošanas ilgums nedrīkst pārsniegt vienu gadu, var pagarināt, ja joprojām pastāv apstākļi, kas pamatojuši tā izdošanu. Rīkojuma termiņa beigas neietekmē šā III punkta pirmajā daļā minēto datu glabāšanas ilgumu.

III *bis* – Iestādes – kurām saskaņā ar likumu ir piekļuve elektronisko komunikāciju datiem, lai novērstu un apkarotu noziedzību, smagus kriminālpārkāpumus un citus smagus to noteikumu pārkāpumus, kuru ievērošanu tās nodrošina, – var uzdot veikt operatoru saskaņā ar šo pantu glabāto datu operatīvo saglabāšanu, lai piekļūtu šiem datiem.”

22 *CPCE* R. 10-13. pants ir formulēts šādi:

“I. – Piemērojot L. 34-1. panta III punktu, elektronisko komunikāciju operatori noziedzīgu nodarījumu izmeklēšanas, atklāšanas un kriminālvajāšanas vajadzībām glabā:

- a) informāciju, kas ļauj identificēt lietotāju;
- b) datus par izmantotajām komunikāciju galaiekārtām;
- c) visu komunikāciju tehniskos datus, kā arī datumu, laiku un ilgumu;
- d) datus par pieprasītajiem vai izmantotajiem papildu pakalpojumiem un to sniedzējiem;
- e) datus, kas ļauj identificēt komunikācijas adresātu vai adresātus.

II. – Telefonijas darbību gadījumā operators glabā II punktā minētos datus un arī tos datus, kas ļauj identificēt komunikācijas avotu un atrašanās vietu.

III. – Šajā pantā minētie dati tiek glabāti vienu gadu, skaitot no to ieraksta datuma.

[..]”

LCEN

- 23 2004. gada 21. jūnija *loi n° 2004-575 pour la confiance dans l'économie numérique* (Likums Nr. 2004-575 par uzticēšanās veicināšanu digitālajai ekonomikai; 2004. gada 22. jūnija *JORF*, 11168. lpp.), redakcijā, kas piemērojama pamatlīetu faktiskajiem apstākļiem (turpmāk tekstā – “*LCEN*”), 6. pantā bija paredzēts:

“I. – 1. Personas, kuru darbība ir piekļuves nodrošināšana komunikāciju pakalpojumiem tiešsaistē, informē savus abonentus par tehniskajiem līdzekļiem, kas ļauj ierobežot piekļuvi noteiktiem pakalpojumiem vai tos atlasīt, un piedāvā tiem vismaz vienu no šiem līdzekļiem.

[..]

2. Fiziskās un juridiskās personas, kuras – pat bez maksas –, izmantojot publiskos komunikāciju pakalpojumus, nodrošina jebkāda veida signālu, teksta, attēlu, skaņu un ziņojumu, ko ir snieguši šo pakalpojumu adresāti, glabāšanu, lai darītu tos pieejamus sabiedrībai, nevar saukt pie civiltiesiskās atbildības par darbībām vai informāciju, kas uzglabāta pēc šo pakalpojumu saņēmēja pieprasījuma, ja tās faktiski nav zinājušas par to prettiesiskumu vai par faktiem un apstākļiem, kuri šķiet prettiesiski, vai arī – ja kopš brīža, kad tās par to ir uzzinājušas, tās ir veikušas atbilstošas darbības, lai šos datus izņemtu vai liegtu tiem pieeju.

[..]

II. – I punkta 1. un 2. apakšpunktā minētās personas tur un glabā datus, kas ļauj identificēt jebkuru personu, kura ir piedalījusies to sniegto pakalpojumu saturā vai tā daļas radīšanā.

Tās personām, kuras sniedz komunikācijas pakalpojumus sabiedrībai tiešsaistē, nodrošina tehniskos līdzekļus, kas ļauj tām izpildīt III punktā paredzētos identifikācijas nosacījumus.

Tiesu iestāde var pieprasīt I punkta 1. un 2. apakšpunktā minētajiem pakalpojumu sniedzējiem paziņot pirmajā daļā minētos datus.

Kriminālkodeksa 226-17., 226-21. un 226-22. panta noteikumi ir piemērojami šo datu apstrādei.

Conseil d'État dekrētā, kas pieņemts pēc Nacionālās informātikas un brīvību komisijas atzinuma, ir definēti pirmajā daļā minētie dati un noteikts to glabāšanas ilgums un noteikumi.

[..]”

CMF

- 24 *Code monétaire et financier* (Monetārais un finanšu kodekss), redakcijā, kas piemērojama pamatlīetu faktiskajiem apstākļiem (turpmāk tekstā – “*CMF*”), L. 621-10. panta pirmajā daļā bija noteikts:

“Izmeklētāji un kontrolieri izmeklēšanas vai kontroles vajadzībām var pieprasīt jebkādus dokumentus neatkarīgi no to datu nesēja veida. Izmeklētāji turklāt var pieprasīt datus, kurus ir glabājuši un apstrādājuši elektronisko komunikāciju operatori saistībā ar [*CPCE*] L. 34-1. pantu un pakalpojumu sniedzēji, kas minēti [*LCEN*] 6. panta I punkta 1. un 2. apakšpunktā, un iegūt šo datu kopiju.

[..]”

- 25 Nemot vērā, ka *Conseil constitutionnel* (Konstitucionālā padome, Francija) 2017. gada 21. jūlija lēmumā atzina *CMF* L.621-10. panta pirmās daļas otro teikumu par neatbilstošu konstitūcijai, likumdevējs ar 2018. gada 23. oktobra *loi n° 2018-898 relative à la lutte contre la fraude* (Likums Nr. 2018-898 par krāpšanas apkarošanu; 2018. gada 24. oktobra *JORF*, teksts Nr. 1) šo Monetāro un finanšu kodeksu papildināja ar jaunu L. 621-10-2. pantu, kurā ir paredzēts:

“Regulā [Nr. 596/2014] definētās tirgus ļaunprātīgas izmantošanas izmeklēšanai izmeklētāji var pieprasīt datus, ko saskaņā ar [*CPCE*] L. 34-1. pantā noteiktajiem nosacījumiem un ierobežojumiem glabā un apstrādā telekomunikāciju operatori, kā arī datus, ko glabā un apstrādā [*LCEN*] 6. panta I punkta 1. un 2. apakšpunktā minētie pakalpojumu sniedzēji.

Lai saņemtu šā panta pirmajā daļā minētos datus, ir nepieciešama savienojuma datu pieprasījumu uzrauga iepriekšēja atļauja.

Savienojuma datu pieprasījumu uzrauga funkcijas pilda pārmaiņus *Conseil d’État* pilnsapulces ievēlēts *Conseil d’État* kārtējais vai goda loceklis un pēc tam *Cour de cassation* pilnsapulces ievēlēts minētās tiesas kārtējais vai goda tiesnesis. Viņa aizstājēju no otras tiesu iestādes ieceļ tādā pašā kārtībā. Savienojuma datu pieprasījumu uzraugu un viņa aizstājēju ievēlē amatā uz četrus gadu termiņu, kas nav pagarināms.

[..]

Amata pienākumu izpildē savienojuma datu pieprasījumu uzraugs nedrīkst ne saņemt, ne lūgt nekādas norādes nedz no *Autorité des marchés financiers*, nedz no kādas citas varas iestādes. Viņam ir jāievēro dienesta noslēpums saskaņā ar nosacījumiem, kas paredzēti šā kodeksa L. 621-4. pantā.

[Atļaujas pieprasījums] tiek izskatīts, pamatojoties uz *Autorité des marchés financiers* ģenerālsekretāra vai tā vietnieka motivētu pieteikumu. Šajā pieteikumā ir jāizklāsta tā pamatojums.

Atļauju pievieno izmeklēšanas lietai.

Telekomunikāciju operatoru un šā panta pirmajā daļā minēto pakalpojumu sniedzēju sniegtos datus izmeklētāji izmanto tikai un vienīgi tās izmeklēšanas vajadzībām, saistībā ar kuru tie ir saņēmuši atļauju.

Savienojuma dati saistībā ar faktiem, attiecībā uz kuriem *Autorité des marchés financiers* kolēģija ir paudusi iebildumus, tiek iznīcināti pēc sešiem mēnešiem kopš Sankciju komisijas vai pārsūdzības izskatošo tiesu galīga nolēmuma. Administratīvā izlīguma gadījumā sešu mēnešu termiņš sākas no izlīguma izpildes.

Savienojuma dati saistībā ar faktiem, attiecībā uz kuriem *Autorité des marchés financiers* kolēģija nav paudusi iebildumus, tiek iznīcināti vienu mēnesi pēc kolēģijas lēmuma.

Gadījumā, ja izmeklēšanas ziņojums tiek nosūtīts finanšu prokuroram vai arī finanšu prokurors virza publisko apsūdzību [..], *Autorité des marchés financiers* nodod savienojuma datus finanšu prokuroram un tos neglabā.

Šā panta piemērošanas kārtība tiek noteikta *Conseil d'État* izdotā dekrētā.”

Pamatlietas, prejudiciālie jautājumi un tiesvedība Tiesā

- 26 Ar 2014. gada 22. maija lēmumu par kriminālprocesa sākšanu pret VD un SR tika uzsākta izmeklētājtiesneša vadīta pirmstiesas izmeklēšana par darbībām, kas kvalificējas kā iekšējās informācijas ļaunprātīga izmantošana un šīs izmantošanas slēpšana. Pēc tam ar 2014. gada 14. novembrī pieņemto pirmo papildlēmumu par kriminālprocesa sākšanu šī izmeklēšana tika paplašināta, aptverot arī darbības, kas kvalificējas kā līdzdalība.
- 27 2015. gada 23. un 25. septembrī *Autorité des marchés financiers* (Finanšu tirgus uzraudzības iestāde (*AMF*), Francija) iesniedza izmeklētājtiesnesim informāciju, kas bija tās rīcībā saistībā ar kādu izmeklēšanu, kuru tā bija veikusi saskaņā ar *CMF* L. 621-10. pantu, konkrēti – no VD un SR veiktajiem tālruņa zvaniem izsecināmus personas datus, ko *AMF*, pamatojoties uz *CPCE* L. 34-1. pantu, bija savākusi no elektronisko komunikāciju pakalpojumu operatoriem.
- 28 Pamatojoties uz šo *AMF* ziņojumu, ar 2015. gada 29. septembrī, 2015. gada 22. decembrī un 2016. gada 23. novembrī pieņemtiem trim papildlēmumiem par kriminālprocesa sākšanu izmeklēšana tika paplašināta, aptverot arī darbības, kas kvalificējas kā korupcija un nelikumīgi iegūtu līdzekļu legalizēšana.
- 29 VD un SR tika atzīti par aizdomās turētajiem, 2017. gada 10. martā inkriminējot VD iekšējās informācijas izmantošanu un nelikumīgi iegūtu līdzekļu legalizēšanu un 2017. gada 29. maijā inkriminējot SR iekšējās informācijas izmantošanu.
- 30 Tā kā par aizdomās turētajiem viņi tika atzīti, pamatojoties uz *AMF* sniegto informāciju par datu plūsmu, VD un SR katrs vērsās *cour d'appel de Paris* (Parīzes apelācijas tiesa, Francija) ar prasību, izvirzot tostarp pamatu būtībā par to, ka esot pārkāpts Direktīvas 2002/58 15. panta 1. punkts, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā. Konkrēti, atsaucoties uz judikatūru, kas izriet no 2016. gada 21. decembra sprieduma *Tele2 Sverige* un *Watson* u.c. (C-203/15 un C-698/15, EU:C:2016:970), VD un SR apstrīdēja, ka šī iestāde ir tiesīga vākt minētos datus, pamatojoties uz *CMF* L. 621-10. pantu un *CPCE* L. 34-1. pantu, tāpēc, ka šīs normas, pirmkārt, nav saderīgas ar Savienības tiesībām, jo paredz savienojuma datu visaptverošu un nediferencētu glabāšanu, un, otrkārt, tajās nav nekādi ierobežotas *AMF* izmeklētāju pilnvaras pieprasīt tiem nosūtīt glabātos datus.
- 31 Ar diviem 2018. gada 20. decembra un 2019. gada 7. marta spriedumiem *cour d'appel de Paris* (Parīzes apelācijas tiesa) noraidīja VD un SR prasības. No lūgumos sniegt prejudiciālu nolēmumu norādītā izriet, ka pamatu par Direktīvas 2002/58 15. panta 1. punkta, lasot Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, pārkāpumu pirmās instances tiesas ir noraidījušas, pamatojoties konkrēti uz apstākli, ka Regulas Nr. 596/2014 par tirgus ļaunprātīgu izmantošanu 23. panta 2. punkta h) apakšpunkts ļauj kompetentajām iestādēm – ciktāl tas atbilst valsts tiesību aktiem – pieprasīt telekomunikāciju operatora rīcībā esošos datu plūsmas ierakstus, ja ir pamatotas aizdomas par šīs regulas 14. panta a) vai b) punktā noteiktā iekšējās informācijas izmantošanas tirdzniecībā aizlieguma pārkāpumu un šādi ieraksti var būt vajadzīgi šā pārkāpuma izmeklēšanai.
- 32 Par šiem spriedumiem VD un SR iesniedza kasācijas sūdzību iesniedzējtiesā, izvirzot pamatu par to, ka citastarp esot pārkāptas iepriekšējā punktā minētās Hartas un Direktīvas 2002/58 normas.

- 33 Attiecībā uz piekļuvi savienojuma datiem iesniedzējtiesa atsauca uz kādu *Conseil constitutionnel* (Konstitucionālā padome) 2017. gada 21. jūlija nolēmumu, no kura izrietot, ka Francijas tiesībās paredzētā kārtība, saskaņā ar kuru *AMF* izmeklētāji piekļūst glabātajiem personas datiem, neesot atbilstoša tiesībām uz privātās dzīves neaizskaramību, kas ir aizsargātas 1789. gada Cilvēka un pilsoņa tiesību deklarācijas 2. pantā, un uzsver, ka valsts likumdevējs – kaut arī tas amatpersonas, kurām ir pienācīgās pilnvaras un jāievēro dienesta noslēpums, ir apveltījis ar tiesībām pieprasīt šos datus izmeklēšanas ietvaros, taču nav piešķīris tām piespiedu izpildes pilnvaras – tomēr šajā kārtībā nav paredzējis nevienu citu garantiju, ar kuru varētu nodrošināt taisnīgu salāgošanu, no vienas puses, starp tiesībām uz privātās dzīves neaizskaramību un, no otras puses, sabiedriskās kārtības apdraudējumu novēršanu un noziedzīgo nodarījumu izdarītāju meklēšanu, un tāpēc *CMF* L. 621-10. panta pirmās daļas otrais teikums bija jāatzīst par neatbilstošu Francijas Konstitūcijai.
- 34 Turklāt iesniedzējtiesa norāda, pirmkārt, ka *Conseil constitutionnel* (Konstitucionālā padome) ir atzinusi, ka, ņemot vērā “acimredzami pārmērīgās” sekas, kādas šīs normas tūlītējai atcelšanai varētu būt uz jau iesāktajiem procesiem, atcelšanas diena jāatliek līdz 2018. gada 31. decembrim, un, otrkārt, tā kā *CMF* L. 621-10. panta pirmā daļa tika atzīta par neatbilstošu konstitūcijai, valsts likumdevējs šo kodeksu papildināja ar L. 621-10-2. pantu.
- 35 Iesniedzējtiesa, atgādinādama no 2016. gada 21. decembra sprieduma *Tele2 Sverige* un *Watson* u.c. (C-203/15 un C-698/15, EU:C:2016:970) 125. punkta izrietošos apsvērumus, uzskata, ka no šīs atzīšanas par neatbilstošu konstitūcijai neizriet, ka spēkā nebūtu *CMF* L. 621-10. panta pirmās daļas otrais teikums, kas bija piemērojams pamatlietu faktu norises laikā, ievērojot šīs normas atcelšanas seku atlikšanu. Tomēr tā uzskata, ka *AMF* izmeklētājiem saskaņā ar šo normu esošās tiesības iegūt savienojuma datus bez iepriekšējas tiesas vai neatkarīgas administratīvas iestādes kontroles neatbilst prasībām, kas izriet no Hartas 7., 8. un 11. panta, – atbilstoši tam, kā šos pantus interpretējusi Tiesa.
- 36 Šajos apstākļos šajā ziņā vienīgais jautājums esot par iespēju uz laiku atlikt *CMF* L. 621-10. panta atcelšanas sekas, lai gan šis pants nav saderīgs ar Hartu.
- 37 Par savienojuma datu glabāšanu iesniedzējtiesa vispirms norāda, ka – lai gan *CPCE* L. 34-1. panta II punktā ir noteikts principiāls pienākums, ka elektronisko komunikāciju pakalpojumu operatori ir jādzēš vai jāanonimizē visi plūsmas dati, – no šā pienākuma ir paredzēti vairāki izņēmumi, tostarp šīs normas III punktā paredzētais izņēmums saistībā ar “noziedzīgu nodarījumu izmeklēšanas, atklāšanas un kriminālvajāšanas vajadzībām”. Šo īpašo vajadzību dēļ noteiktu veidu dati ir dzēšami vai anonimizējami gadu vēlāk.
- 38 Šajā ziņā tā precizē, ka piecas datu kategorijas, uz kurām attiecas tostarp *CPCE* L. 34-1. panta III punkta nosacījumi, ir *CPCE* R. 10-13. pantā uzskaitītās kategorijas. Šie savienojuma dati tiek radīti vai apstrādāti komunikācijas rezultātā un sniedzot informāciju par šīs komunikācijas apstākļiem un pakalpojuma lietotājiem, taču nesniedzot nekādu informāciju par attiecīgo komunikāciju saturu.
- 39 Pēc tam – atgādinājusi 2016. gada 21. decembra sprieduma *Tele2 Sverige* un *Watson* u.c. (C-203/15 un C-698/15, EU:C:2016:970) 112. punktu, saskaņā ar kuru Direktīvas 2002/58 15. panta 1. punkts, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, ir jāinterpretē tādējādi, ka tam pretrunā ir tāds valsts tiesiskais regulējums, kurā noziedzības apkarošanas nolūkā ir paredzēta visaptveroša un nediferencēta visas informācijas par datu plūsmu un atrašanās vietas datu glabāšana attiecībā uz visiem abonentiem un reģistrētiem lietotājiem un visiem elektronisko sakaru līdzekļiem, – iesniedzējtiesa norāda, ka

pamatlietās *AMF* bija piekļuve elektronisko komunikāciju pakalpojumu operatoru glabātajiem datiem, pamatojoties uz aizdomām par iekšējās informācijas ļaunprātīgu izmantošanu un tirgus ļaunprātīgu izmantošanu, kas kvalificējas kā vairāki smagi noziegumi. Šī piekļuve esot attaisnota ar šīs iestādes vajadzību tās izmeklēšanas efektivitātes nodrošināšanas interesēs salīdzināt vairākus glabātos datus par noteiktu laikposmu, lai identificētu iekšējo informāciju, ar kuru ir apmainījušies attiecīgie subjekti un kura liecina par nelikumīgām darbībām šajā jomā.

- 40 Iesniedzējtiesa norāda, ka ar *AMF* veiktajām izmeklēšanām tika pildīti pienākumi, kas dalībvalstīm ir noteikti Direktīvas 2003/6 12. panta 2. punkta d) apakšpunktā un Regulas Nr. 596/2014 23. panta 2. punkta g) un h) apakšpunktā, lasot to kopsakarā ar šīs regulas 1. pantu; konkrēti – pienākums pieprasīt elektronisko komunikāciju pakalpojumu operatoru rīcībā esošos datu plūsmas ierakstus.
- 41 Iesniedzējtiesa arī uzsver, pirmkārt – atsaucoties uz minētās regulas 65. apsvērumu –, ka šie datu plūsmas ieraksti ir svarīgi un dažreiz vienīgie pierādījumi, lai konstatētu un pierādītu iekšējās informācijas izmantošanu tirdzniecībā un tirgus manipulācijas, jo var palīdzēt noteikt tās personas identitāti, kas ir atbildīga par nepatiesas vai maldinošas informācijas izplatīšanu, vai to, ka personas ir sazinājušās konkrētā brīdī.
- 42 Otrkārt, iesniedzējtiesa citē šīs pašas regulas 66. apsvērumu, no kura izriet, ka kompetentajām iestādēm finanšu jomā piešķirto pilnvaru īstenošana var nonākt konfliktā ar tiesībām uz privātās un ģimenes dzīves, mājokļa un saziņas neaizskaramību un ka tāpēc dalībvalstīm būtu jāievieš pienācīgi un efektīvi aizsargpasākumi pret jebkādu ļaunprātīgu izmantošanu, ierobežojot minētās pilnvaras tiktāl, cik tās būtu nepieciešamas pienācīgai nopietnu gadījumu izmeklēšanai, ja šajās valstīs nepastāv līdzvērtīgi risinājumi tāda paša rezultāta efektīvai sasniegšanai. Tās ieskatā no šā apsvēruma izrietot, ka noteikti tirgus ļaunprātīgas izmantošanas gadījumi ir uzskatāmi par smagiem noziegumiem.
- 43 Iesniedzējtiesa arī uzsver, ka pamatlietās iekšējā informācija, kas iespējami veido nelikumīgo darbību tirgū objektīvo pusi, būtībā bija mutiska un slepena.
- 44 Ievērojot iepriekš izklāstīto, iesniedzējtiesa vaicā, kā Direktīvas 2002/58 15. panta 1. punkts – lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā – būtu salāgojams ar prasībām, kas izriet no Direktīvas 2003/6 12. panta 2. punkta d) apakšpunkta un Regulas Nr. 596/2014 23. panta 2. punkta g) un h) apakšpunkta.
- 45 Visbeidzot, gadījumā, ja Tiesa atzītu, ka lietā aplūkotie tiesību akti par savienojuma datu glabāšanu neatbilst Savienības tiesībām, rastos jautājums par šo tiesību aktu seku provizorisku atstāšanu spēkā, lai novērstu tiesisko nedrošību un ļautu līdz šim savāktos un glabātos datus izmantot iekšējās informācijas ļaunprātīgas izmantošanas konstatēšanai un kriminālvajāšanai par to.
- 46 Šādos apstākļos *Cour de cassation* (Kasācijas tiesa) nolēma apturēt tiesvedību un uzdot Tiesai šādus prejudiciālus jautājumus, kas lietās C-339/20 un C-397/20 ir formulēti identiski:
"1) Vai [Direktīvas 2003/6] 12. panta 2. punkta a) un d) apakšpunkts, kā arī tos kopš 2016. gada 3. jūlija aizstājošais [Regulas Nr. 596/2014] 23. panta 2. punkta g) un h) apakšpunkts kopsakarā ar šīs regulas 65. apsvērumu nozīmē to, ka, ņemot vērā izmantotās informācijas slepenību un to, ka sabiedrība var tikt skarta kopumā, valsts likumdevējs elektronisko sakaru operatoriem var uzdot uz noteiktu laiku, taču visaptveroši glabāt savienojuma datus, lai [Direktīvas 2003/6] 11. pantā un [Regulas Nr. 596/2014] 22. pantā minētajai administratīvajai

iestādei ļautu – ja par konkrētām personām rodas iemesls šaubīties, vai tās nav iesaistītas iekšējās informācijas izmantošanā un tirgus manipulācijās, – pieprasīt no operatora esošos datu plūsmas ierakstus gadījumos, kad ir iemesli aizdomām, ka šiem ar izmeklēšanas priekšmetu saistītajiem ierakstiem var būt nozīme, lai pierādītu pārkāpumu, tostarp ļaujot izsekot kontaktiem, ko konkrētās personas ir nodibinājušas pirms šaubu rašanās?

- 2) Gadījumā, ja [...] Tiesas atbilde [uz pirmo jautājumu būtu tāda, kas] *Cour de cassation* [Kasācijas tiesai] liktu atzīt, ka Francijas tiesību akti par savienojuma datu glabāšanu neatbilst Savienības tiesībām, – vai šo tiesību aktu iedarbību varētu saglabāt uz noteiktu laiku, lai izvairītos no tiesiskās nedrošības un ļautu iepriekš iegūtos un glabātos datus izmantot atbilstoši kādam no šajos tiesību aktos noteiktajiem mērķiem?
- 3) Vai valsts tiesa drīkst uz noteiktu laiku saglabāt tiesiskā regulējuma iedarbību, kas ļauj tādas neatkarīgas administratīvas iestādes, kuras uzdevums ir veikt izmeklēšanu tirgus ļaunprātīgas izmantošanas jomā, amatpersonām iegūt savienojuma datus bez tiesas vai citas neatkarīgas administratīvas iestādes iepriekšējas kontroles?”

- 47 Ar Tiesas priekšsēdētāja 2020. gada 17. septembra lēmumu lietas C-339/20 un C-397/20 tika apvienotas rakstveida un mutvārdu procesam, kā arī sprieduma taisīšanai.
- 48 2021. gada 21. aprīlī *Conseil d'État* (Valsts padome, Francija) pasludināja spriedumu *French Data Network* u.c. (Nr. 393099, 394922, 397844, 397851, 424717, 424718), kurā tā tostarp izsprieda to, vai Savienības tiesībām atbilst vairākas valsts tiesību normas, kas ir nozīmīgas pamatlietās, proti, CPCE L. 34-1. pants un CPCE R. 10-13. pants.
- 49 Pēc Tiesas aicinājuma šajās lietās rīkotās tiesas sēdes dalībniekiem bija iespēja izklāstīt savu viedokli par to, vai šim *Conseil d'État* (Valsts padome) spriedumam ir nozīme šo lūgumu sniegt prejudiciālu nolēmumu izskatīšanas kontekstā.
- 50 Šajā tiesas sēdē Francijas valdības pārstāvis norādīja, ka ar minēto spriedumu *Conseil d'État* (Valsts padome) būtībā ir atzinusi par prettiesiskām normas, kas ļauj noziedzības apkarošanas nolūkos visaptveroši un nediferencēti glabāt savienojuma datus, izņemot IP adresu un elektronisko komunikāciju līdzekļu lietotāju identitātes datus, un tādējādi izpildījusi 2020. gada 6. oktobra spriedumā *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791) noteikto. Viņš tomēr precizēja, ka tiesvedības debašu gaitā *Conseil d'État* (Valsts padome) bija arī jāatbild uz Francijas valdības iebildi par to, ka šāda Savienības tiesību interpretācija esot pretrunā konstitucionāla ranga normām, proti, normām par sabiedriskās kārtības apdraudējumu novēršanu, konkrēti – par personu un mantas drošību, kā arī noziedzīgu nodarījumu izdarītāju noskaidrošanu.
- 51 Francijas valdības pārstāvis šajā ziņā paskaidroja, ka *Conseil d'État* (Valsts padome) šo iebildi esot noraidījusi divos posmos. Pirmkārt, tā atzina, ka savienojuma datu visaptveroša un nediferencēta glabāšana ir izšķirīgs faktors kriminālizmeklēšanas sekmīgam iznākumam un ka tā nav aizstājama ne ar vienu citu metodi. Otrkārt, *Conseil d'État* (Valsts padome) – pamatodamās konkrēti uz 2020. gada 6. oktobra sprieduma *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791) 164. punktu – atzina, ka datu operatīvā saglabāšana Savienības tiesībās ir atļauta, tostarp arī tad, kad šādi tiek saglabāti dati, kuri sākotnēji ir tikuši glabāti valsts drošības aizsardzības nolūkos.

- 52 Francijas valdības pārstāvis arī precizēja, ka *Conseil d'État* (Valsts padome) 2021. gada 21. aprīļa sprieduma *French Data Network* u.c. (Nr. 393099, 394922, 397844, 397851, 424717, 424718) rezultātā valsts likumdevējs ir papildinājis Pasta un elektronisko sakaru kodeksa L. 34-1. pantu ar III *bis* punktu, kā norādīts šā sprieduma 21. punktā.

Par prejudiciālajiem jautājumiem

Ievada apsvērumi

- 53 Pirmām kārtām, jāatgādina, ka pēc šo lūgumu sniegt prejudiciālu nolēmumu iesniegšanas *Conseil d'État* (Valsts padome) pasludināja 2021. gada 21. aprīļa spriedumu *French Data Network* u.c. (Nr. 393099, 394922, 397844, 397851, 424717, 424718), kurā konkrēti tika spriests par *CPCE* L. 34-1. panta un *CPCE* R. 10-13. panta atbilstību Savienības tiesībām.
- 54 Taču, kā secinājumu 42. punktā norāda ģenerāladvokāts un kā arīdzan izriet no iesniedzējtiesas sniegtajiem paskaidrojumiem, kas izklāstīti šā sprieduma 27., 37. un 38. punktā, šie panti ir “būtiski” pamatlietās aplūkotā *CMF* L. 621-10. panta piemērošanas kontekstā.
- 55 Tiesā rīkotajā tiesas sēdē Francijas pārstāvis – uzsvēris šā sprieduma 21. punktā minēto leģislatīvo evolūciju, kas attiecībā uz *CPCE* L. 34-1. pantu ir notikusi Tiesas 2020. gada 6. oktobra spriedumā *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791) veikto precizējumu rezultātā, – norādīja būtībā, ka pamatlietu izspriešanā iesniedzējtiesai atbilstoši 1789. gada Cilvēka un pilsoņa tiesību deklarācijas 7. un 8. pantā nostiprinātajam likuma piemērojamības laikā principam nāksies ņemt vērā valsts tiesību normas redakcijā, kas piemērojama pamatlietu faktiskajiem apstākļiem, kuri savukārt bija norisinājušies 2014. un 2015. gadā, un tāpēc *Conseil d'État* (Valsts padome) 2021. gada 21. aprīļa spriedums *French Data Network* u.c. (Nr. 393099, 394922, 397844, 397851, 424717, 424718) katrā ziņā nav ņemams vērā, izvērtējot šos lūgumus sniegt prejudiciālu nolēmumu.
- 56 Pastāvīgās judikatūras atziņa ir tāda, ka saistībā ar *LESD* 267. pantā noteikto procedūru tikai valsts tiesa, kura iztiesā lietu un kurai ir jāuzņemas atbildība par pieņemamo tiesas nolēmumu, ir tā, kas, ņemot vērā lietas īpatnības, var noteikt, cik lielā mērā prejudiciālais nolēmums ir vajadzīgs, lai šī tiesa varētu pieņemt nolēmumu, un cik atbilstīgi ir Tiesai uzdotie jautājumi. Tātad gadījumā, ja uzdotie jautājumi skar Savienības tiesību interpretāciju, Tiesai principā ir pienākums pieņemt nolēmumu (šajā nozīmē skat. spriedumu, 2010. gada 8. septembris, *Winner Wetten*, C-409/06, EU:C:2010:503, 36. punkts un tajā minētā judikatūra).
- 57 Atteikums lemt par valsts tiesas uzdotu prejudiciālo jautājumu ir iespējams tikai tad, ja ir acīmredzams, ka Savienības tiesību interpretācijai nav nekāda sakara ar pamatlietas apstākļiem vai tās priekšmetu, ja problēma ir hipotētiska vai arī ja Tiesai nav zināmi faktiskie un tiesību apstākļi, kas vajadzīgi, lai sniegtu lietderīgu atbildi uz tai uzdotajiem jautājumiem (šajā nozīmē skat. spriedumu, 2009. gada 19. novembris, *Filipiak*, C-314/08, EU:C:2009:719, 42. punkts un tajā minētā judikatūra).
- 58 Šajā lietā no lūgumiem sniegt prejudiciālu nolēmumu izriet, ka pirmais un trešais jautājums ir tieši par *CPCE* L. 34-1. pantu un *CPCE* R. 10-13. pantu, nevis par *CMF* L. 621-10. pantu, uz kuru pamatojoties *AMF* pieprasīja elektronisko komunikāciju pakalpojumu operatori sniegt

informāciju par datu plūsmu saistībā ar VD un SR tālruņa zvaniem, uz kuras pamata šīs personas tika atzītas par aizdomās turētajiem un kuras kā pierādījuma pieļaujamība tiek apstrīdēta pamatlietās.

- 59 Turklāt jānorāda, ka ar otro un trešo šajās lietās uzdoto jautājumu, kuros tiek izvērsti pirmais jautājums, iesniedzējtiesa būtībā jautā, vai gadījumā, ja aplūkotais valsts tiesiskais regulējums par savienojuma datu glabāšanu un piekļuvi izrādītos nesaderīgs ar Savienības tiesībām, šā regulējuma sekas tomēr nevarētu provizoriski palikt spēkā tālab, lai novērstu tiesisko nedrošību un ļautu datus, kas glabāti saskaņā ar šo tiesisko regulējumu, izmantot iekšējās informācijas ļaunprātīgas izmantošanas atklāšanai un kriminālvajāšanai par to.
- 60 Ievērojot iepriekš izklāstīto, kā arī to, ko secinājumu 44.–47. punktā norāda ģenerālvokāts, ir jāuzskata, ka – neatkarīgi no *Conseil d'État* (Valsts padome) 2021. gada 21. aprīļa sprieduma *French Data Network* u.c. (Nr. 393099, 394922, 397844, 397851, 424717, 424718), kā arī *Conseil constitutionnel* (Konstitucionālā padome) 2022. gada 25. februāra nolēmuma (Nr. 2021-976/977), ar kuru *CPCE* L. 34-1. pants šā sprieduma 20. punktā citētajā redakcijā ir atzīts par daļēji neatbilstošu konstitūcijai, – Tiesas atbilde uz uzdotajiem jautājumiem joprojām ir nepieciešama pamatlietu izpriešanai.
- 61 Otrām kārtām, jānorāda, ka Tiesā notikušajā tiesas sēdē VD pārstāvis apstrīdēja Regulas Nr. 596/2014 piemērojamību *ratione temporis*, būtībā apgalvojot, ka pamatlietas faktiskie apstākļi bija iestājušies pirms šīs regulas stāšanās spēkā. Tāpēc iesniedzējtiesas uzdoto jautājumu izvērtēšanā nozīme esot tikai Direktīvas 2003/6 normām.
- 62 Šajā ziņā jāatgādina, ka saskaņā ar pastāvīgo judikatūru jauna tiesību norma ir piemērojama, sākot no tā tiesību akta stāšanās spēkā, ar ko tā ir ieviesta, un ka, lai gan tā nav piemērojama tiesiskajām situācijām, kuras ir radušās un galīgi nostabilizējušās agrāka likuma spēkā esamības laikā, tā ir piemērojama to sekām nākotnē, kā arī jaunām tiesiskām situācijām. Ievērojot tiesību aktu atpakaļejoša spēka aizlieguma principu, citādi var būt tikai tad, ja jaunajai tiesību normai ir pievienoti īpaši noteikumi, kas īpaši paredz nosacījumus par tās piemērošanu laikā (šajā nozīmē skat. spriedumus, 2019. gada 15. janvāris, E.B., C-258/17, EU:C:2019:17, 50. punkts un tajā minētā judikatūra, kā arī 2020. gada 14. maijs, *Azienda Municipale Ambiente*, C-15/19, EU:C:2020:371, 57. punkts).
- 63 Savukārt, kā norādīts šā sprieduma 26.–29. punktā, lai gan pamatlietās aplūkotās tiesiskās situācijas patiešām ir radušās, kamēr nebija stājušies spēkā Regula Nr. 596/2014, ar kuru no 2016. gada 3. jūlija tika atcelta un aizstāta Direktīva 2003/6, pamatlietu virzība turpinājās arī pēc minētā datuma, tāpēc kopš minētā datuma šo situāciju sekām nākotnē saskaņā ar iepriekšējā punktā atgādināto principu ir piemērojama Regula Nr. 596/2014.
- 64 No tā izriet, ka Regulas Nr. 596/2014 normas šajā lietā ir piemērojamas. Turklāt iesniedzējtiesas minētās Direktīvas 2003/6 normas nav jānošķir no Regulas Nr. 596/2014 normām, jo šajās lietās Tiesas veicamās interpretācijas vajadzībām šīs normas saturiski ir būtībā līdzīgas.

Par pirmo jautājumu

- 65 Ar pirmo jautājumu šajās lietās iesniedzējtiesa būtībā vaicā, vai Direktīvas 2003/6 12. panta 2. punkta a) un d) apakšpunkts un Regulas Nr. 596/2014 23. panta 2. punkta g) un h) apakšpunkts, lasot tos kopsakarā ar Direktīvas 2002/58 15. panta 1. punktu un Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, ir jāinterpretē tādējādi, ka tiem ir pretrunā tādi

lēģislatīvi pasākumi kā pamatlietās aplūkoti, kuros tirgus ļaunprātīgas izmantošanas noziegumu – kuru starpā ir arī iekšējās informācijas ļaunprātīga izmantošana – apkarošanas nolūkos preventīvi tiek paredzēta informācijas par datu plūsmu visaptveroša un nediferencēta glabāšana gadu pēc tās ierakstīšanas.

- 66 Tiesai rakstveida apsvērumus iesniegušās pamatlietu puses un ieinteresētās personas šajā ziņā pauda atšķirīgus viedokļus. Igaunijas valdība un Īrija, kā arī Spānijas un Francijas valdības uzskata, ka Direktīvas 2003/6 12. panta 2. punkta a) un d) apakšpunkts, kā arī Regulas Nr. 596/2014 23. panta 2. punkta g) un h) apakšpunkts – lai arī implicīti – taču noteikti pilnvaro valsts likumdevēju uzlikt elektronisko komunikāciju pakalpojumu operatoriem pienākumu visaptveroši un nediferencēti glabāt datus, lai ļautu finanšu jomā kompetentajai iestādei atklāt iekšējās informācijas izmantošanu tirdzniecībā un sodīt par to. Tā kā no Regulas Nr. 596/2014 65. apsvēruma izriet, ka minētie datu plūsmas ieraksti ir svarīgi un dažreiz vienīgie pierādījumi, lai konstatētu un pierādītu iekšējās informācijas izmantošanu tirdzniecībā, šāds glabāšanas pienākums esot nepieciešams gan tālab, lai nodrošinātu minētās iestādes veiktās izmeklēšanas un kriminālvajāšanas efektivitāti un līdz ar to arī Direktīvas 2003/6 12. panta 2. punkta a) un d) apakšpunkta, kā arī Regulas Nr. 596/2014 23. panta 2. punkta h) apakšpunkta lietderīgo iedarbību, gan tālab, lai sasniegtu šajos instrumentos izvirzītos mērķus nodrošināt Savienības finanšu tirgu integritāti un vairogt ieguldītāju uzticēšanos šiem tirgiem.
- 67 Savukārt VD, SR, Polijas valdība un Eiropas Komisija apgalvo – tā kā šajās normās ir vienīgi noteikts ietvars pilnvarām prasīt elektronisko komunikāciju pakalpojumu operatoriem iesniegt viņu rīcībā “esošo” informāciju par datu plūsmu, tās reglamentē tikai jautājumu par piekļuvi šiem datiem.
- 68 Šajā ziņā jāatgādina, pirmām kārtām, ka saskaņā ar Tiesas pastāvīgo judikatūru, interpretējot Savienības tiesību normu, ir jāņem vērā ne tikai tās teksts, bet arī tās konteksts un šo normu ietverošā tiesiskā regulējuma mērķi, un tostarp šī tiesiskā regulējuma izstrādes vēsture (šajā nozīmē skat. spriedumu, 2018. gada 17. aprīlis, *Egenberger*, C-414/16, EU:C:2018:257, 44. punkts).
- 69 Attiecībā uz pirmajā jautājumā minēto tiesību normu formulējumu jākonstatē, ka Direktīvas 2003/6 12. panta 2. punkta d) apakšpunktā ir norādīts uz finanšu jomā kompetentās iestādes pilnvarām “pieprasīt esošo[s] telefonsarunu ierakstus un esošos datu plūsmas ierakstus” un Regulas Nr. 596/2014 23. panta 2. punkta g) un h) apakšpunktā ir norādīts uz šīs iestādes pilnvarām pieprasīt, pirmkārt, “ieguldījumu brokeru sabiedrību, kredītiestāžu vai citu finanšu iestāžu rīcībā esošo[s] [...] datu plūsmas ierakstus” un, otrkārt, “ciktāl to atļauj valsts tiesību akti, pieprasīt telekomunikāciju operatora rīcībā esošos datu plūsmas ierakstus”.
- 70 No šo tiesību normu formulējuma nepārprotami izriet, ka tajās ir vienīgi noteikti ietvari minētās iestādes pilnvarām “pieprasīt” šo operatoru rīcībā esošos datus, un tas nozīmē piekļuvi šiem datiem. Turklāt norāde uz minēto operatoru “rīcībā” “esošajiem” ierakstiem ļauj noprast, ka Savienības likumdevējs nav vēlējies reglamentēt valsts likumdevēja iespēju noteikt pienākumu šādus ierakstus glabāt.
- 71 Šajā ziņā jāatgādina, ka saskaņā ar pastāvīgo judikatūru Savienības tiesību normas interpretācijas rezultātā nedrīkst tikt pilnībā atņemta šīs tiesību normas skaidrā un precīzā formulējuma lietderīgā iedarbība. Tādējādi, tā kā Savienības tiesību normas jēga nepārprotami izriet no tās formulējuma, Tiesa nevar atkāpties no šīs interpretācijas (spriedums, 2022. gada 25. janvāris, *VYSOČINA WIND*, C-181/20, EU:C:2022:51, 39. punkts un tajā minētā judikatūra).

- 72 Pamatojums šā sprieduma 70. punktā ieskicētajai interpretācijai rodams gan Direktīvas 2003/6 12. panta 2. punkta a) un d) apakšpunkta un Regulas Nr. 596/2014 23. panta 2. punkta g) un h) apakšpunkta kontekstā, gan šo normu veidotā tiesiskā regulējuma mērķos.
- 73 Par šo normu kontekstu jānorāda – lai gan Direktīvas 2003/6 12. panta 1. punktā un Regulas Nr. 596/2014 23. panta 3. punktā, lasot to šīs regulas 62. apsvēruma gaismā, Savienības likumdevējs ir vēlējis likt dalībvalstīm veikt pasākumus, kas vajadzīgi tālab, lai finanšu jomā kompetento iestāžu rīcībā būtu iedarbīgu instrumentu, pilnvaru un resursu kopums, kā arī uzraudzības un izmeklēšanas pilnvaru kopums, lai nodrošinātu efektivitāti to uzdevumu veikšanā, šajās normās nav nekas teikts nedz par dalībvalstu varbūtējo iespēju tālab noteikt elektronisko komunikāciju pakalpojumu operatoriem pienākumu visaptveroši un nediferencēti glabāt informāciju par datu plūsmu, nedz par nosacījumiem, ar kādiem šiem operatoriem būtu jāglabā šie dati, lai tos vajadzības gadījumā iesniegtu kompetentajām iestādēm.
- 74 Ar Direktīvas 2003/6 12. panta 2. punktu un Regulas Nr. 596/2014 23. panta 2. punktu Savienības likumdevējs ir vienīgi vēlējis apveltīt finanšu jomā kompetento iestādi – nolūkā nodrošināt tās izmeklēšanas un uzraudzības uzdevumu veikšanas efektivitāti – ar tādām ierastām izmeklēšanas pilnvarām kā tās, kas ļauj šai iestādei piekļūt dokumentiem, veikt pārbaudes un kratīšanu vai izdot rīkojumus vai aizliegumus personām, kas tiek turētas aizdomās par tirgus ļaunprātīgas izmantošanas nodarījumiem, kuru starpā ir arī iekšējās informācijas ļaunprātīga izmantošana.
- 75 Turklāt jākonstatē, ka Regulas Nr. 596/2014 normās, kurās ir regulēts konkrēti jautājums par datu glabāšanu, proti, šīs regulas 11. panta 5. punkta pēdējā daļā, 6. punkta otrajā daļā, 8. punktā un 11. punkta c) apakšpunktā, 17. panta 1. punkta pirmajā daļā, 18. panta 5. punktā, kā arī 28. pantā, šāds glabāšanas pienākums ir noteikts tikai finanšu pakalpojumu sniedzējiem, kas uzskaitīti minētās regulas 23. panta 2. punkta g) apakšpunktā, un tāpēc tas attiecas tikai uz datiem saistībā ar finanšu darījumiem un saistībā ar šo konkrēto pakalpojumu sniedzēju sniegtajiem pakalpojumiem.
- 76 Par attiecīgā tiesiskā regulējuma mērķiem jānorāda, ka gan no Direktīvas 2003/6 2. un 12. apsvēruma, gan no Regulas Nr. 596/2014 1. panta, lasot to šīs regulas 2. un 24. apsvēruma gaismā, izriet, ka šo instrumentu mērķis ir nodrošināt Savienības finanšu tirgu integritāti un vairost ieguldītāju uzticēšanos šiem tirgiem un šī uzticēšanās balstās tostarp uz pārliecību, ka pret viņiem būs vienlīdzīga attieksme un viņi tiks aizsargāti no iekšējās informācijas ļaunprātīgas izmantošanas. Direktīvas 2003/6 2. panta 1. punktā un Regulas Nr. 596/2014 8. panta 1. punktā noteiktā iekšējās informācijas ļaunprātīgas izmantošanas aizlieguma mērķis tāpat ir nodrošināt līgumslēdzēju vienlīdzību biržas darījumos, izvairoties no tā, ka kāds no tiem, kura rīcībā ir iekšējā informācija un kurš tādēļ ir labvēlīgākā situācijā attiecībā pret citiem ieguldītājiem, gūst labumu uz to personu rēķina, kas to nezina (šajā nozīmē skat. spriedumu, 2022. gada 15. marts, *Autorité des marchés financiers*, C-302/20, EU:C:2022:190, 43., 65. un 77. punkts, kā arī tajos minētā judikatūra).
- 77 Regulas Nr. 596/2014 65. apsvērumā patiešām ir teikts, ka savienojuma datu ieraksti ir svarīgi un dažreiz vienīgie pierādījumi, lai konstatētu un pierādītu iekšējās informācijas izmantošanu tirdzniecībā un tirgus manipulācijas, tomēr šajā apsvērumā ir runa tikai par elektronisko komunikāciju pakalpojumu operatoru “rīcībā” esošajiem ierakstiem, kā arī par finanšu jomā kompetentās iestādes pilnvarām “pieprasīt” no šiem operatoriem “esošos” datus. Tādējādi no šā apsvēruma nekādi neizriet, ka Savienības likumdevējs ar šo regulu būtu vēlējis atzīt dalībvalstīm pilnvaras uzlikt elektronisko komunikāciju pakalpojumu operatoriem vispārīgu pienākumu glabāt datus.

- 78 Ievērojot iepriekš izklāstīto, jāuzskata, ka nedz Direktīva 2003/6, nedz Regula Nr. 596/2014 nav interpretējama tādējādi, ka tās varētu būt juridiskais pamats vispārīgam pienākumam glabāt elektronisko komunikāciju pakalpojumu operatoru rīcībā esošos datu plūsmas ierakstus tālab, lai varētu īstenot pilnvaras, kas finanšu jomā kompetentajai iestādei ir piešķirtas saskaņā ar Direktīvu 2003/6 un Regulu Nr. 596/2014.
- 79 Otrām kārtām, jāatgādina – kā secinājumu 53. un 61. punktā būtībā norāda ģenerālvokāts –, ka, tā kā jautājumā par datu saglabāšanu un – plašāk – par personas datu apstrādi elektronisko komunikāciju jomā atsaucies regulējums rodams Direktīvā 2002/58, tas, kā Tiesa interpretē šo direktīvu, ir attiecināms arī uz elektronisko komunikāciju pakalpojumu operatoru rīcībā esošajiem plūsmas datu ierakstiem, kurus finanšu jomā kompetentās iestādes Direktīvas 2003/6 11. panta un Regulas Nr. 596/2014 22. panta izpratnē var tiem pieprasīt.
- 80 Proti, Direktīvā 2002/58 – kā noteikts tās 1. panta 1. punktā – ir paredzēta dalībvalstu to noteikumu saskaņošana, ar kuriem jānodrošina pamattiesību un pamatbrīvību līdzvērtīgs aizsardzības līmenis, un jo īpaši tiesības uz privāto dzīvi un konfidencialitāti saistībā ar personas datu apstrādi elektronisko komunikāciju nozarē, kura aptver arī telekomunikāciju nozari.
- 81 Turklāt – kā izriet no šīs direktīvas 3. panta – minētā direktīva attiecas uz personas datu apstrādi saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu publiskos komunikāciju tīklos Savienībā, tostarp publiskos komunikāciju tīklos, kuros var izmantot datu vākšanas un identifikācijas ierīces. Tātad minētā direktīva ir jāuzskata par tādu, kas reglamentē šādu pakalpojumu sniedzēju, kuru vidū ir konkrēti arī telekomunikāciju operatori, darbības (šajā nozīmē skat. spriedumu, 2020. gada 6. oktobris, *La Quadrature du Net* u.c., C-511/18, C-512/18 un C-520/18, EU:C:2020:791, 93. punkts, kā arī tajā minētā judikatūra).
- 82 Ievērojot iepriekš izklāstīto, jāuzskata – kā secinājumu 62. un 63. punktā būtībā norāda ģenerālvokāts –, ka elektronisko komunikāciju pakalpojumu operatoru rīcībā esošo ierakstu apstrādes, kas veikta saskaņā ar Direktīvas 2003/6 12. panta 2. punkta d) apakšpunktu un Regulas Nr. 596/2014 23. panta 2. punkta g) un h) apakšpunktu, likumīguma vērtējums ir jāveic Direktīvā 2002/58 noteikto nosacījumu gaismā, kā arī ievērojot to, kā šī direktīva ir interpretēta Tiesas judikatūrā.
- 83 Apstiprinājums šai interpretācijai rodams arī Regulas Nr. 596/2014 3. panta 1. punkta 27. apakšpunktā, kurā ir noteikts, ka datu plūsmas ieraksti šīs regulas izpratnē ir definēti Direktīvas 2002/58 2. panta otrās daļas b) punktā [kā “informācija par datu plūsmu”].
- 84 Turklāt Direktīvas 2003/6 44. apsvērumā, kā arī Regulas Nr. 596/2014 66. un 77. apsvērumā ir teikts, ka šo tiesību aktu mērķis ir nodrošināt Hartā nostiprināto pamattiesību un principu, tostarp tiesību uz privātās dzīves neaizskaramību, ievērošanu. Šajā ziņā Savienības likumdevējs Regulas Nr. 596/2014 66. apsvērumā ir norādījis – lai īstenotu finanšu jomā kompetentajai iestādei saskaņā ar šo regulu piešķirtās pilnvaras, kas var būtiski pārkāpt tiesības uz privātās un ģimenes dzīves, mājokļa un saziņas neaizskaramību, dalībvalstīm būtu jāievieš pienācīgi un efektīvi aizsargpasākumi pret jebkādu ļaunprātīgu izmantošanu, piemēram, attiecīgā gadījumā prasība saņemt iepriekšēju atļauju no attiecīgās dalībvalsts tiesu iestādes. Dalībvalstīm būtu jāpieļauj iespēja, ka kompetentās iestādes varētu īstenot šādas iejaukšanās pilnvaras tiktāl, cik tas būtu nepieciešams pienācīgai nopietnu gadījumu izmeklēšanai, ja nepastāv līdzvērtīgi risinājumi tāda paša rezultāta sasniegšanai. No tā izriet, ka Direktīvā 2003/6 un Regulā Nr. 596/2014 paredzēto pasākumu piemērošana nekādā gadījumā nedrīkst kaitēt Direktīvā 2002/58

nodrošinātajai personas datu aizsardzībai (pēc analogijas skat. spriedumus, 2008. gada 29. janvāris, *Promusicae*, C-275/06, EU:C:2008:54, 57. punkts, un 2021. gada 17. jūnijs, *M.I.C.M.*, C-597/19, EU:C:2021:492, 124. punkts, kā arī tajā minētā judikatūra).

- 85 Tāpēc Direktīvas 2003/6 12. panta 2. punkta a) un d) apakšpunkts un Regulas Nr. 596/2014 23. panta 2. punkta g) un h) apakšpunkts ir jāinterpretē tādējādi, ka tie nepieļauj visaptveroši un nediferencēti glabāt informāciju par datu plūsmu un atrašanās vietas datus nolūkā apkarot tirgus ļaunprātīgas izmantošanas nodarījumus, konkrēti, iekšējās informācijas ļaunprātīgu izmantošanu, jo pienākumu veikt šādu glabāšanu ietverošā valsts tiesiskā regulējuma saderīgums ar Savienības tiesībām ir jāizvērtē, ņemot vērā Direktīvas 2002/58 15. panta 1. punktu, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā atbilstoši to interpretācijai Tiesas judikatūrā.
- 86 Jautājumā par šāda tiesiskā regulējuma saderīgumu ar nupat minētajām normām jāatgādina, ka, savstarpēji saistīti aplūkojot šā sprieduma 53., 54. un 58. punktu, ir skaidrs, ka, lai gan šie lūgumi sniegt prejudiciālu nolēmumu būtībā patiešām ir par *CMF* L. 621-10. pantu, uz kura pamata *AMF* lūdza elektronisko komunikāciju pakalpojumu operatorus iesniegt informāciju par datu plūsmu saistībā ar VD un SR veiktajiem tālruņa zvaniem, kuru dēļ šīs personas tika atzītas par aizdomās turētajiem, tomēr – kā secinājumu 42. punktā norāda ģenerālvokāts – *CPCE* L. 34-1. pants un *CPCE* R. 10-13. pants ir “būtiski” šā *CMF* L. 621-10. panta piemērošanai.
- 87 Proti, no iesniedzējtiesas paskaidrojumiem, kas atreferēti šā sprieduma 27., 37. un 38. punktā, izriet, ka, pirmkārt, aplūkojamo informāciju par datu plūsmu *AMF* izmeklētāji ir ieguvuši, pamatojoties uz *CPCE* L.34-1. pantu, redakcijā, kas piemērojama pamatlietu faktiskajiem apstākļiem, kura II punktā paredzētajam elektronisko komunikāciju pakalpojumu operatoru principiālajam pienākumam – dzēst vai anonimizēt visu informāciju par datu plūsmu – III punktā ir noteikti vairāki izņēmumi, tostarp izņēmums tālab, “lai izmeklētu un atklātu noziedzīgus nodarījumus [...]un veiktu kriminālvajāšanu par tiem”. Šo īpašo vajadzību dēļ noteiktu veidu datu dzēšana vai anonimizēšana bija veicama gadu vēlāk.
- 88 Otrkārt, iesniedzējtiesa precizē, ka piecas datu kategorijas, uz kurām attiecās *CPCE* L. 34-1. panta III punkts – redakcijā, kas piemērojama pamatlietu faktiskajiem apstākļiem –, bija *CPCE* R. 10-13. pantā uzskaitītās datu kategorijas, proti, informācija, kas ļauj identificēt lietotāju; dati par izmantotajām komunikāciju galaiekārtām; visu komunikāciju tehniskie dati, kā arī datums, laiks un ilgums; dati par pieprasītajiem vai izmantotajiem papildu pakalpojumiem un to sniedzējiem; un visbeidzot – dati, kas ļauj identificēt komunikācijas adresātu vai adresātus. No *CPCE* R. 10-13. panta II punkta – redakcijā, kas piemērojama pamatlietu faktiskajiem apstākļiem, – arī izriet, ka telefonijas darbību gadījumā attiecīgie operatori varēja glabāt arī datus, kas ļauj identificēt komunikācijas avotu un atrašanās vietu.
- 89 No tā izriet, ka pamatlietās aplūkotais tiesiskais regulējums aptver visus telefonsakaru līdzekļus un ietver visus šo līdzekļu lietotājus, šajā ziņā nekādi tos nešķirojot un tiem neparedzot nekādus izņēmumus. Turklāt dati, kurus saskaņā ar šo tiesisko regulējumu ir pienākums glabāt elektronisko komunikāciju pakalpojumu operatoriem, ir tieši tie, kas nepieciešami, lai atrastu komunikācijas avotu un adresātu, noteiktu komunikācijas datumu, laiku, ilgumu un veidu, identificētu izmantotos komunikācijas līdzekļus, kā arī noteiktu galaiekārtu un komunikāciju atrašanās vietu, un šo datu starpā ir arī lietotāja vārds un adrese, kā arī izsauceņa un izsaukamā lietotāja tālruņa numuri.

- 90 Tādējādi dati, kas saskaņā ar aplūkoto valsts tiesisko regulējumu ir jāglabā vienu gadu – lai gan tajos nav attiecīgo komunikāciju satura –, tomēr ļauj tostarp uzzināt, ar kuru personu tālruna sakaru lietotājs ir sazinājies un ar kādu komunikāciju līdzekli šī saziņa ir notikusi, noteikt komunikāciju datumu, laiku un ilgumu, kā arī vietu, no kuras tās ir notikušas, un uzzināt galaiekārtu atrašanās vietu, un tālab pat nav vajadzīgs, lai komunikācija būtu bijusi pārraidīta. Tie paver arī iespēju noteikt, cik bieži lietotājs ir sazinājies ar konkrētām personām kādā noteiktā laikposmā. Tāpēc ir uzskatāms, ka šie dati kopumā var ļaut izdarīt ļoti precīzus secinājumus par to personu privāto dzīvi, kuru dati tikuši glabāti, proti, par šo personu ikdienas paradumiem, pastāvīgajām vai pagaidu uzturēšanās vietām, ikdienas vai citām gaitām, veiktajām darbībām, sociālajiem kontaktiem un aprindām, kurās tās mēdz uzturēties. It īpaši šie dati ļauj profilēt attiecīgās personas un tāpēc tiesību uz privātās dzīves neaizskaramību kontekstā ir tikpat sensitīva informācija kā pats šo komunikāciju saturs (šajā nozīmē skat. spriedumu, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 45. punkts, kā arī tajā minētā judikatūra).
- 91 Jautājumā par aplūkotā tiesiskā regulējuma mērķiem jānorāda, ka šis regulējums ir vērstš tostarp uz to, lai izmeklētu un atklātu noziedzīgus nodarījumus – tostarp tirgus ļaunprātīgu izmantošanu, kuras paveids ir arī iekšējās informācijas ļaunprātīga izmantošana, – un veiktu kriminālvajāšanu par tiem.
- 92 Ievērojot šā sprieduma 86.–91. punktā izklāstīto, jākonstatē, ka ar aplūkoto tiesisko regulējumu valsts likumdevējs – tostarp noziedzīgu nodarījumu izmeklēšanas, atklāšanas un kriminālvajāšanas, kā arī noziedzības apkarošanas nolūkos – ir noteicis pienākumu visaptveroši un nediferencēti glabāt informāciju par datu plūsmu vienu gadu pēc tās ierakstīšanas.
- 93 Savukārt konkrēti no 2020. gada 6. oktobra sprieduma *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791) 140.–168. punkta, kā arī no 2022. gada 5. aprīļa sprieduma *Commissioner of An Garda Síochána* u.c. (C-140/20, EU:C:2022:258) 59.–101. punkta izriet, ka saskaņā ar Direktīvas 2002/58 15. panta 1. punktu šāda glabāšana ar šādiem mērķiem nav attaisnojama.
- 94 No tā izriet, ka tāds valsts tiesiskais regulējums kā pamatlietās aplūkotais, kurā elektronisko komunikāciju pakalpojumu sniedzējiem tiek uzlikts pienākums tirgus ļaunprātīgas izmantošanas nodarījumu – kuru starpā ir arī iekšējās informācijas ļaunprātīga izmantošana – apkarošanas nolūkos preventīvā kārtā visaptveroši un nediferencēti glabāt informāciju par datu plūsmu attiecībā uz visiem elektronisko komunikāciju līdzekļu lietotājiem, šo informāciju nekādi nediferencējot un neparedzot nekādus izņēmumus – un apstākļos, kad nav konstatēta saskaņā ar iepriekšējā punktā minēto judikatūru prasītā saikne starp glabājamiem datiem un izvirzīto mērķi –, pārsniedz absolūti nepieciešamā robežas un to nevar uzskatīt par attaisnotu demokrātiskā sabiedrībā, kā tas prasīts Direktīvas 2002/58 15. panta 1. punktā, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā (šajā nozīmē pēc analogijas skat. spriedumu, 2020. gada 6. oktobris, *Privacy International*, C-623/17, EU:C:2020:790, 81. punkts).
- 95 Ievērojot iepriekš izklāstīto, uz pirmo jautājumu lietās C-339/20 un C-397/20 ir atbildams, ka Direktīvas 2003/6 12. panta 2. punkta a) un d) apakšpunkts un Regulas Nr. 596/2014 23. panta 2. punkta g) un h) apakšpunkts, lasot tos kopsakarā ar Direktīvas 2002/58 15. panta 1. punktu un Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, ir jāinterpretē tādējādi, ka tiem ir pretrunā legīslatīvi pasākumi, kuros tirgus ļaunprātīgas izmantošanas nodarījumu – kuru starpā

ir arī iekšējās informācijas ļaunprātīga izmantošana – apkarošanas nolūkos preventīvi tiek paredzēta informācijas par datu plūsmu visaptveroša un nediferencēta glabāšana gadu pēc tās ierakstīšanas.

Par otro un trešo jautājumu

- 96 Ar šajās lietās uzdoto otro un trešo jautājumu, kuri jāizskata kopā, iesniedzējtiesa būtībā vēlas noskaidrot, vai Savienības tiesības ir jāinterpretē tādējādi, ka dalībvalsts tiesa drīkst ierobežot laikā sekas, kas izriet no apstākļa, ka tā saskaņā ar valsts tiesībām par spēkā neesošām ir atzinusi valsts tiesību normas – kurās, pirmkārt, elektronisko komunikāciju pakalpojumu operatori ir uzlikts pienākums visaptveroši un nediferencēti glabāt informāciju par datu plūsmu un, otrkārt, pieļauts, ka šī informācija tiek sniegta finanšu jomā kompetentajai iestādei, iepriekš nesaņemot tiesas vai neatkarīgas administratīvas iestādes atļauju –, jo šie tiesību akti ir nesaderīgi ar Direktīvas 2002/58 15. panta 1. punktu, lasot to Hartas gaismā.
- 97 Vispirms jāatgādina, ka ar Savienības tiesību pārākuma principu tiek nostiprināta Savienības tiesību prioritāte pār dalībvalstu tiesībām. Tātad šis princips uzliek par pienākumu visām dalībvalstu iestādēm nodrošināt dažādo Savienības tiesību normu pilnīgu iedarbību, jo dalībvalstu tiesības nevar ietekmēt iedarbību, kura šīm normām ir atzīta minēto valstu teritorijā. Saskaņā ar šo principu gadījumā, ja valsts tiesību aktus nav iespējams interpretēt atbilstīgi Savienības tiesību prasībām, valsts tiesai, kurai ir pienākums atbilstoši savai kompetencei piemērot Savienības tiesību normas, ir pienākums nodrošināt šo normu pilnīgu iedarbību, pēc savas ierosmes vajadzības gadījumā atstājot bez piemērošanas jebkuru tām pretrunā esošu valsts tiesību aktu normu, pat vēlāk pieņemtu, un nav nepieciešams lūgt vai gaidīt, lai tā vispirms tiktu atcelta likumdošanas kārtībā vai ar kādu citu konstitūcijā paredzētu metodi (šajā nozīmē skat. spriedumu, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 118. punkts, kā arī tajā minētā judikatūra).
- 98 Vienīgi Tiesa izņēmuma kārtā un primāro tiesiskās drošības apsvērumu dēļ var noteikt, ka īslaicīgi tiek apturētas sekas, kas izriet no Savienības tiesību normai pretrunā esošas valsts tiesību normas aizstāšanas ar šo Savienības normu. Šādas Tiesas interpretācijas iedarbības laikā ierobežojums ir pieļaujams tikai pašā spriedumā, kurā ir lemts par pieprasīto interpretāciju. Savienības tiesību pārākums un vienveidīga piemērošana tiktu apdraudēta, ja valsts tiesām būtu pilnvaras piešķirt valsts tiesību normām pārākumu pār Savienības tiesībām, kurām šis tiesību normas ir pretrunā, pat ja tas būtu tikai uz laiku (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 119. punkts, kā arī tajā minētā judikatūra).
- 99 Kādā lietā par to, vai ir likumīgi tādi pasākumi, kas veikti, neizpildot Savienības tiesībās noteikto pienākumu veikt iepriekšēju projekta ietekmes uz vidi un uz ietekmes uz aizsargātu teritoriju novērtējumu, Tiesa patiešām ir atzinusi, ka valsts tiesa, ja tas ir atļauts valsts tiesībās, izņēmuma kārtā var paturēt spēkā no šādiem pasākumiem izrietošās sekas, ja šo paturēšanu spēkā pamato primāri apsvērumi, kas saistīti ar nepieciešamību novērst reālus un nopietnus attiecīgās dalībvalsts elektroapgādes traucējumu draudus, kurus nevar novērst ar citiem līdzekļiem un alternatīvām, it īpaši iekšējā tirgū, taču šī paturēšana spēkā var attiekties tikai uz laiku, kas absolūti nepieciešams šā prettiesiskuma novēršanai (šajā nozīmē skat. spriedumu, 2019. gada 29. jūlijs, *Inter-Environnement Wallonie* un *Bond Beter Leefmilieu Vlaanderen*, C-411/17, EU:C:2019:622, 175., 176., 179. un 181. punkts).

- 100 Tomēr – atšķirībā no gadījuma, kad nav izpildīts tāds uz specifisko vides aizsardzības jomu attiecināms procesuālais pienākums kā projekta ietekmes iepriekšējs novērtējums, – Direktīvas 2002/58 15. panta 1. punkta, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, neievērošanu nevar novērst, izmantojot procedūru, kas ir pielīdzināma iepriekšējā punktā minētajai (šajā nozīmē skat. spriedumu, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána u.c.*, C-140/20, EU:C:2022:258, 121. punkts, kā arī tajā minētā judikatūra).
- 101 Proti, tādu valsts tiesību aktu kā pamatlietās aplūkoti seku saglabāšana nozīmētu, ka ar šiem tiesību aktiem elektronisko komunikāciju pakalpojumu operatoriem joprojām tiks noteikti pienākumi, kas ir pretrunā Savienības tiesībām un kas ietver nopietnu iejaukšanos to personu pamattiesībās, kuru dati ir tikuši glabāti (pēc analogijas skat. spriedumu, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána u.c.*, C-140/20, EU:C:2022:258, 122. punkts, kā arī tajā minētā judikatūra).
- 102 Tāpēc iesniedzējtiesa nevar ierobežot laikā tāda spēkā neesamības konstatējuma sekas, kurš tai saskaņā ar valsts tiesībām jāveic attiecībā uz pamatlietās aplūkotajiem valsts tiesību aktiem (pēc analogijas skat. spriedumu, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána u.c.*, C-140/20, EU:C:2022:258, 123. punkts, kā arī tajā minētā judikatūra).
- 103 Šajā ziņā arīdzan jāprecizē, ka īstenotās interpretācijas seku ierobežošana laikā 2016. gada 21. decembra spriedumā *Tele2 Sverige un Watson u.c.* (C-203/15 un C-698/15, EU:C:2016:970), kā arī 2020. gada 6. oktobra spriedumā *La Quadrature du Net u.c.* (C-511/18, C-512/18 un C-520/18, EU:C:2020:791) netika paredzēta, tāpēc saskaņā ar šā sprieduma 98. punktā atgādināto judikatūru šāda ierobežošana nav veicama Tiesas spriedumā, kas pasludināts pēc minētajiem spriedumiem.
- 104 Visbeidzot, ņemot vērā, ka iesniedzējtiesā tiek izskatītas prasības atzīt par nepieļaujamiem pierādījumus, kas iegūti no informācijas par datu plūsmu, tāpēc ka aplūkojamās valsts tiesību normas ir pretrunā Savienības tiesībām gan jautājumā par šo datu glabāšanu, gan jautājumā par piekļuvi tiem, ir jānoskaidro, kā pamatlietās pret VD un SR izmantoto pierādījumu pieļaujamību ietekmētu konstatējums par *CMF L. 621-10.* panta, redakcijā, kas piemērojama pamatlietu faktiskajiem apstākļiem, iespējamo nesaderīgumu ar Direktīvas 2002/58 15. panta 1. punktu, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā.
- 105 Šajā ziņā pietiek vien atsaukties uz Tiesas judikatūru par šo tēmu, konkrēti, uz principiem, kas atgādināti 2021. gada 2. marta sprieduma *Prokuratuur* (Piekļuves elektronisko komunikāciju datiem nosacījumi) (C-746/18, EU:C:2021:152) 41.–44. punktā; no šīs judikatūras izriet, ka atbilstoši dalībvalstu procesuālās autonomijas principam šī pieļaujamība ir vērtējama saskaņā ar valsts tiesībām ar nosacījumu, ka tiek ievēroti tostarp līdzvērtības un efektivitātes principi.
- 106 Par šo nupat minēto efektivitātes principu jāatgādina, ka tas valsts krimināllietu tiesai nosaka pienākumu neņemt vērā informāciju un pierādījumus, kas vai nu – pretrunā Savienības tiesībām – ir iegūti, visaptveroši un nediferencēti glabājot informāciju par datu plūsmu un atrašanās vietas datus, vai arī kompetentajai iestādei – tāpat pretrunā minētajām tiesībām – piekļūstot šiem datiem, kriminālprocesā, kas sākts pret personām, kuras tiek turētas aizdomās par noziedzīgu nodarījumu izdarīšanu, ja šīs personas nespēj efektīvi paust nostāju par šo informāciju un šiem pierādījumiem, kuri ir saistīti ar jomu, ko tiesa nepārzina, un kuri var būtiski ietekmēt faktu vērtējumu (šajā nozīmē skat. spriedumu, 2021. gada 2. marts, *Prokuratuur* (Piekļuves elektronisko komunikāciju datiem nosacījumi), C-746/18, EU:C:2021:152, 44. punkts un tajā minētā judikatūra).

- 107 Ņemot vērā iepriekš minētos apsvērumus, uz otro un trešo jautājumu šajās lietās ir atbildams, ka Savienības tiesības ir jāinterpretē tādējādi, ka tām ir pretrunā, ka dalībvalsts tiesa ierobežo laikā sekas, kas izriet no apstākļa, ka tā, pildot savu valsts tiesībās paredzēto uzdevumu, par spēkā neesošām ir atzinusi valsts tiesību normas – kurās, pirmkārt, elektronisko komunikāciju pakalpojumu operatoriem ir uzlikts pienākums visaptveroši un nediferencēti glabāt informāciju par datu plūsmu un, otrkārt, pieļauts, ka šī informācija tiek sniegta finanšu jomā kompetentajai iestādei, iepriekš nesaņemot tiesas vai neatkarīgas administratīvas iestādes atļauju –, jo šīs tiesību normas ir nesaderīgas ar Direktīvas 2002/58 15. panta 1. punktu, lasot to Hartas gaismā. Saskaņā ar dalībvalstu procesuālās autonomijas principu par tādu pierādījumu pieļaujamību, kuri iegūti, piemērojot ar Savienības tiesībām nesaderīgas valsts tiesību normas, ir jālemj atbilstoši valsts tiesībām ar nosacījumu, ka tiek ievēroti tostarp līdzvērtības un efektivitātes principi.

Par tiesāšanās izdevumiem

- 108 Attiecībā uz pamatlietas pusēm šī tiesvedība izriet no tiesvedības, kas notiek iesniedzējtiesā, tāpēc tā lemj par tiesāšanās izdevumiem. Izdevumi, kas radušies, iesniedzot apsvērumus Tiesai, un kas nav minēto pušu izdevumi, nav atlīdzināmi.

Ar šādu pamatojumu Tiesa (virspalāta) nospriež:

- 1) Eiropas Parlamenta un Padomes Direktīvas 2003/6/EK (2003. gada 28. janvāris) par iekšējās informācijas ļaunprātīgu izmantošanu un tirgus manipulācijām (tirgus ļaunprātīgu izmantošanu) 12. panta 2. punkta a) un d) apakšpunkts un Eiropas Parlamenta un Padomes Regulas (ES) Nr. 596/2014 (2014. gada 16. aprīlis) par tirgus ļaunprātīgu izmantošanu (tirgus ļaunprātīgas izmantošanas regula) un ar ko atceļ Eiropas Parlamenta un Padomes Direktīvu 2003/6/EK un Komisijas Direktīvas 2003/124/EK, 2003/125/EK un 2004/72/EK, 23. panta 2. punkta g) un h) apakšpunkts, lasot tos kopsakarā ar Eiropas Parlamenta un Padomes Direktīvas 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju), redakcijā ar grozījumiem, kas izdarīti ar Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīvu 2009/136/EK, 15. panta 1. punktu un Eiropas Savienības Pamattiesību hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā,**

ir jāinterpretē tādējādi, ka:

tiem ir pretrunā leģislatīvi pasākumi, kuros tirgus ļaunprātīgas izmantošanas nodarījumu – kuru starpā ir arī iekšējās informācijas ļaunprātīga izmantošana – apkarošanas nolūkos preventīvi tiek paredzēta informācijas par datu plūsmu visaptveroša un nediferencēta glabāšana gadu pēc tās ierakstīšanas.

- 2) Savienības tiesības ir jāinterpretē tādējādi, ka tām ir pretrunā, ka dalībvalsts tiesa ierobežo laikā sekas, kas izriet no apstākļa, ka tā, pildot savu valsts tiesībās paredzēto uzdevumu, par spēkā neesošām ir atzinusi valsts tiesību normas – kurās, pirmkārt, elektronisko komunikāciju pakalpojumu operatoriem ir uzlikts pienākums visaptveroši un nediferencēti glabāt informāciju par datu plūsmu un, otrkārt, pieļauts, ka šī informācija tiek sniegta finanšu jomā kompetentajai iestādei, iepriekš nesaņemot tiesas vai neatkarīgas administratīvas iestādes atļauju –, jo šīs tiesību normas ir nesaderīgas ar**

Direktīvas 2002/58, redakcijā ar grozījumiem, kas izdarīti ar Direktīvu 2009/136, 15. panta 1. punktu, lasot to Eiropas Savienības Pamattiesību hartas gaismā. Saskaņā ar dalībvalstu procesuālās autonomijas principu par tādu pierādījumu pieļaujamību, kuri iegūti, piemērojot ar Savienības tiesībām nesaderīgas valsts tiesību normas, ir jālemj atbilstoši valsts tiesībām ar nosacījumu, ka tiek ievēroti tostarp līdzvērtības un efektivitātes principi.

[Paraksti]