



Judikatūras krājums

TIESAS SPRIEDUMS (virspalāta)

2016. gada 21. decembrī*

[Teksts grozīts ar 2017. gada 16. marta rīkojumu]

Lūgums sniegt prejudiciālu nolēmumu — Elektroniskie sakari — Personas datu apstrāde — Elektronisko sakaru konfidencialitāte — Aizsardzība — Direktīva 2002/58/EK — 5., 6. un 9. pants, kā arī 15. panta 1. punkts — Eiropas Savienības Pamattiesību harta — 7., 8. un 11. pants, kā arī 52. panta 1. punkts — Valsts tiesību akti — Elektronisko sakaru pakalpojumu sniedzēji — Pienākums visaptveroši un nediferencēti saglabāt informāciju par datu plūsmu un atrašanās vietas datus — Valsts iestādes — Piekļuve datiem — Tiesas vai neatkarīgas administratīvas iestādes iepriekšējas kontroles neesamība — Saderība ar Savienības tiesībām

Apvienotās lietas C-203/15 un C-698/15

par lūgumiem sniegt prejudiciālu nolēmumu atbilstoši LESD 267. pantam, ko *Kammarrätten i Stockholm* (Administratīvā apelācijas tiesa Stokholmā, Zviedrija) un *Court of Appeal (England & Wales) (Civil Division)* (Apelācijas tiesa (Anglija un Velsa) (Civillietu palāta), Apvienotā Karaliste) iesniedza attiecīgi ar 2015. gada 29. aprīļa un 2015. gada 9. decembra lēmumiem, kas Tiesā reģistrēti 2015. gada 4. maijā un 2015. gada 28. decembrī tiesvedībās

Tele2 Sverige AB (C-203/15)

pret

Post- och telestyrelsen

un

Secretary of State for the Home Department (C-698/15)

pret

Tom Watson ,

Peter Brice ,

Geoffrey Lewis ,

piedaloties

Open Rights Group ,

* * Tiesvedības valodas – zviedru un angļu.

Privacy International ,

The Law Society of England and Wales .

TIESA (virspalāta)

šādā sastāvā: priekšsēdētājs K. Lēnartss [*K. Lenaerts*], priekšsēdētāja vietnieks A. Ticano [*A. Tizzano*], palātu priekšsēdētāji R. Silva de Lapuerta [*R. Silva de Lapuerta*], T. fon Danvics [*T. von Danwitz*] (referents), Ž. L. da Krušs Vilasa [*J. L. da Cruz Vilaça*], E. Juhāss [*E. Juhász*] un M. Vilars [*M. Vilaras*], tiesneši E. Borgs Bartets [*A. Borg Barthet*], J. Malenovskis [*J. Malenovský*], E. Levits, Ž. K. Bonišo [*J. C. Bonichot*], A. Arabadžijevs [*A. Arabadjiev*], S. Rodins [*S. Rodin*], F. Biltšens [*F. Biltgen*] un K. Likurgs [*C. Lycourgos*],

ģenerālvokāts H. Saugmandsgors Ēe [*H. Saugmandsgaard Øe*],

sekretāre S. Stremholma [*C. Strömholm*], administratore,

ņemot vērā Tiesas priekšsēdētāja 2016. gada 1. februāra lēmumu piemērot lietai C-698/15 paātrināto tiesvedību, kas paredzēta Tiesas Reglamenta 105. panta 1. punktā,

ņemot vērā rakstveida procesu un 2016. gada 12. aprīļa tiesas sēdi,

ņemot vērā apsvērumus, ko iesniedza

- *Tele2 Sverige AB* vārdā – *M. Johansson* un *N. Torgerzon*, advokater, kā arī *E. Lagerlöf* un *S. Backman*,
- *M. Watson* vārdā – *J. Welch* un *E. Norton*, solicitors, *I. Steele*, advocate, *B. Jaffey*, barrister, kā arī *D. Rose*, QC,
- *P. Brice* un *G. Lewis* vārdā – *A. Suterwalla* un *R. de Mello*, barristers, *R. Drabble*, QC, kā arī *S. Luke*, solicitor,
- *Open Rights Group* un *Privacy International* vārdā – *D. Carey*, solicitor, kā arī *R. Mehta* un *J. Simor*, barristers,
- *The Law Society of England and Wales* vārdā – *T. Hickman*, barrister, kā arī *N. Turner*,
- Zviedrijas valdības vārdā – *A. Falk*, *C. Meyer-Seitz*, *U. Persson* un *N. Otte Widgren*, kā arī *L. Swedenborg*, pārstāvji,
- Apvienotās Karalistes valdības vārdā – *S. Brandon* un *L. Christie*, kā arī *V. Kaye*, pārstāvji, kuriem palīdz *D. Beard*, *G. Facenna* un *J. Eadie*, QC, kā arī *S. Ford*, barrister,
- Beļģijas valdības vārdā – *J. C. Halleux* un *S. Vanrie*, kā arī *C. Pochet*, pārstāvji,
- Čehijas Republikas valdības vārdā – *M. Smolek* un *J. Vlácil*, pārstāvji,
- Dānijas valdības vārdā – *C. Thorning* un *M. Wolff*, pārstāvji,
- Vācijas valdības vārdā – *T. Henze* un *M. Hellmann*, kā arī *J. Kemper*, pārstāvji, kuriem palīdz *M. Kottmann* un *U. Karpenstein*, Rechtsanwälte,
- Igaunijas valdības vārdā – *K. Kraavi-Käerdi*, pārstāve,

- Īrijas vārdā – *E. Creedon* un *L. Williams*, kā arī *A. Joyce*, pārstāvji, kuriem palīdz *D. Fennelly*, *BL*,
- Spānijas valdības vārdā – *A. Rubio González*, pārstāvis,
- Francijas valdības vārdā – *G. de Bergues*, *D. Colas* un *F.-X. Bréchet*, kā arī *C. David*, pārstāvji,
- Kipras valdības vārdā – *K. Kleanthous*, pārstāve,
- Ungārijas valdības vārdā – *M. Fehér* un *G. Koós*, pārstāvji,
- Nīderlandes valdības vārdā – *K. Bulterman* un *M. Gijzen*, kā arī *J. Langer*, pārstāvji,
- Polijas valdības vārdā – *B. Majczyna*, pārstāvis,
- Somijas valdības vārdā – *J. Heliskoski*, pārstāvis,
- Eiropas Komisijas vārdā – *H. Krämer*, *K. Simonsson*, *H. Kranenborg* un *D. Nardi*, kā arī *P. Costa de Oliveira* un *J. Vondung*, pārstāvji,

noklausījusies ģenerālvokāta secinājumus 2016. gada 19. jūlija tiesas sēdē,
pasludina šo spriedumu.

Spriedums

- 1 Lūgumi sniegt prejudiciālu nolēmumu ir par to, kā interpretēt Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīvas 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privātās dzīves aizsardzību un elektroniskajām komunikācijām) (OV 2002, L 201, 37. lpp.), kurā grozījumi ir 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, lasot to Eiropas Savienības Pamattiesību hartas (turpmāk tekstā – “Harta”) 7. un 8. panta, kā arī 52. panta 1. punkta gaismā.
- 2 Šie lūgumi tika iesniegti divās tiesvedībās, pirmkārt, starp *Tele2 Sverige AB* un *Post- och telestyrelsen* (Zviedrijas Pasta un telekomunikāciju uzraudzības iestāde, turpmāk tekstā – “PTS”) par rīkojumu, kuru šī pēdējā minēta iestāde izdevusi attiecībā uz *Tele2 Sverige*, nosakot pienākumu attiecībā uz tās abonentiem un reģistrētajiem lietotājiem saglabāt informāciju par datu plūsmu un atrašanās vietas datus (lieta C-203/15), un, otrkārt, starp *Tom Watson*, *Peter Brice* un *Geoffrey Lewis*, no vienas puses, un *Secretary of State for the Home Department* (Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes iekšlietu ministrs), no otras puses, par *Data Retention and Investigatory Powers Act 2014* (2014. gada Likums par datu uzglabāšanu un izmeklēšanas pilnvarām, turpmāk tekstā – “DRIPA”) 1. panta saderību ar Savienības tiesībām (lieta C-698/15).

Atbilstošās tiesību normas

Savienības tiesības

Direktīva 2002/58

- 3 Direktīvas 2002/58 preambulas 2., 6., 7., 11., 21., 22., 26. un 30. apsvērumā ir noteikts:

“(2) Šī direktīva respektē pamattiesības un ievēro principus, kas jo īpaši ir atzīti [Hartā]. Šī direktīva jo īpaši nodrošina pilnība 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 1995. gada 24. oktobra] Direktīva 95/46/EK [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 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.

[..]

(21) Lai aizsargātu komunikāciju konfidencialitāti, tostarp gan komunikāciju saturu, gan informāciju attiecībā uz šādām komunikācijām, jāpieņem pasākumi, lai liegtu neatļautu piekļuvi komunikācijām, izmantojot publiskos komunikāciju tīklus un publiski pieejamus elektronisko komunikāciju pakalpojumus. Valsts tiesību akti dažās dalībvalstīs liedz tikai tišu neatļautu piekļuvi komunikācijām.

(22) Aizliegums personām, kas nav lietotāji, vai bez to piekrišanas glabāt informāciju par komunikācijām un ar tām saistītu informāciju par datu plūsmu, nav paredzēts, lai aizliegtu jebkādu automātisku, pagaidu vai islaicīgu šīs informācijas uzglabāšanu, ja to dara tikai tādēļ, lai

veiktu pārraidīšanu elektronisko komunikāciju tīklā, un ar noteikumu, ka informāciju neuzglabā ilgāk, kā nepieciešams, lai veiktu pārraidīšanu un datu plūsmas pārvaldi, un ka uzglabāšanas laikā ir garantēta konfidencialitāte. [..]

[..]

- (26) Tādi dati, kas attiecas uz abonentiem un ir apstrādāti elektronisko komunikāciju tīklos, lai izveidotu savienojumu un pārraidītu informāciju, iekļauj informāciju par fizisku personu privāto dzīvi un attiecas uz tiesībām ievērot juridisku personu likumīgās intereses. Šādus datus drīkst uzglabāt tikai tādā apmērā, cik vajadzīgs, lai sniegtu pakalpojumu ar nolūku sagatavot rēķinus un veikt norēķinus par starpsavienojumiem, un tos glabā ierobežotu laiku. Jebkuru tālāku šādu datu apstrādi [..] var atļaut tikai tad, ja abonents ir tam piekritis, pamatojoties uz publiski pieejamu komunikāciju pakalpojumu sniedzēja dotu precīzu un pilnīgu informāciju par tādas tālākas apstrādes veidiem, ko tas nodomājis veikt, un par abonenta tiesībām nesniegt vai atsaukt savu piekrišanu šādai apstrādei. [..]

[..]

- (30) Sistēmas elektronisko komunikāciju tīklu nodrošināšanai un pakalpojumu sniegšanai jāveido tā, lai ierobežotu nepieciešamo personas datu apjomu līdz stingri noteiktam minimumam. [..]”

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 Direktīv[u] [95/46] 1. punktā minētaj[ā] nolūk[ā]. Turklāt ar tiem paredz to abonentu likumīgo interešu aizsardzību, kuri ir juridiskas personas.

3. Šī direktīva neattiecas uz darbībām, uz kurām neattiecas Eiropas Kopienas dibināšanas līgums, tādām kā tās, kas iekļautas Līguma par Eiropas Savienību 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 Saskaņā ar Direktīvas 2002/58 2. pantu “Definīcijas”:

“Izņemot gadījumus, kad noteikts savādāk, piemēro definīcijas, kas minētas Direktīvā [95/46] un Eiropas Parlamenta un Padomes 2002. gada 7. marta Direktīvā 2002/21/EK par kopējo regulatīvo bāzi elektronisko komunikāciju tīkliem un pakalpojumiem (pamatdirektīva) [(OV 2002, L 108, 33. lpp.)].

Piemēro arī šādas definīcijas:

[..]

- b) “informācija par datu plūsmu” ir jebkuri dati, kas apstrādāti ar nolūku pārsūtīt komunikāciju elektronisko komunikāciju tīklā vai ar nolūku sagatavot rēķinu;
- c) “atrašanās vietas dati” ir jebkuri dati, kuri apstrādāti elektronisko komunikāciju tīklā vai kurus apstrādā elektronisko komunikāciju pakalpojuma sniedzējs, norādot publiski pieejamu elektronisko komunikāciju pakalpojuma lietotāja gala iekārtas ģeogrāfisko atrašanās vietu;

d) “komunikācija” ir jebkāda informācija, ar kuru apmainās vai kuru pārsūta starp noteiktu skaitu personu, izmantojot publiski pieejamu elektronisko komunikāciju pakalpojumu. Tajā neiekļauj informāciju, kas, izmantojot elektronisko komunikāciju tīklu, pārsūtīta [pārraidīta] sabiedrībai kā apraides pakalpojuma daļa, izņemot līdz limenim, kad informāciju var attiecināt uz identificējamu abonentu vai lietotāju, kas saņem šo informāciju;

[..]”

6 Direktīvas 2002/58 3. pantā “Attiecīgie pakalpojumi” ir paredzēts:

“Šī direktīva attiecas uz personas datu apstrādi saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu publiskos komunikāciju tīklos Kopienā, tostarp publiskos komunikāciju tīklos, kuros var izmantot datu vākšanas un identifikācijas ierīces.”

7 Šis direktīvas 4. pants “Apstrādes drošība” ir formulēts šādi:

“1. Publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzējam attiecīgā gadījumā kopā ar tīkla operatoru jāveic attiecīgi tehniski un organizatoriski pasākumi, lai nodrošinātu savu pakalpojumu drošību attiecībā uz tīkla drošību. Ņemot vērā jaunākos sasniegumus un to ieviešanas izmaksas, šiem pasākumiem nodrošina iespējamajam riskam atbilstīgu drošības līmeni.

1.a Neskarot Direktīvu [95/46], ar 1. punktā minētajiem pasākumiem nodrošina vismaz to, ka:

- personas datiem var piekļūt tikai pilnvarots personāls un tikai ar likumu atļautiem mērķiem,
- uzglabātos vai pārsūtītos personas datus aizsargā no nejaušas vai nelikumīgas iznīcināšanas, nejaušas nozaudēšanas vai izmaiņšanas un no neatļautas vai nelikumīgas uzglabāšanas, apstrādes, piekļuves vai izpaušanas, un
- nodrošina, ka tiek īstenota drošības politik[a] saistībā ar personas datu apstrādi.

[..]”

8 Saskaņā ar Direktīvas 2002/58 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.

[..]

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.”

9 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.”

10 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. [..]”

11 Minētās direktīvas 15. pantā “Direktīvas [95/46] dažu noteikumu piemērošana” ir paredzēts:

“1. 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 nepieciešamību, 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. Tālāb dalībvalstis, cita starpā, var pieņemt tiesību aktus, paredzot datu saglabāšanu [kuros paredzēts, ka datus saglabā] ierobežotā laikposmā, kas pamatots ar šajā punktā noteiktajiem iemesliem. Visi šajā punktā minētie pasākumi [tiesību akti] ir saskaņā ar Kopienas tiesību aktu vispārējiem principiem, tostarp tie[m], kas minēti Eiropas Savienības dibināšanas līguma 6. panta 1. un 2. punktā.

[..]

1.b Pakalpojumu sniedzēji izstrādā iekšējās procedūras, lai atbildētu uz pieprasījumiem piekļūt lietotāju personas datiem, pamatojoties uz valsts noteikumiem, kas pieņemti saskaņā ar 1. punktu. Pakalpojumu sniedzēji pēc kompetentās valsts iestādes pieprasījuma sniedz tai informāciju par minētajām procedūrām, saņemto pieprasījumu skaitu, attiecīgo juridisko pamatojumu un pakalpojumu sniedzēju atbildēm.

2. Direktīvas [95/46] III nodaļas noteikumus par tiesiskās aizsardzības līdzekļiem, atbildību un sankcijām piemēro, ņemot vērā valsts noteikumus, kas pieņemti saskaņā ar šo direktīvu, un ņemot vērā individuālās tiesības, kuras izriet no šīs direktīvas.

[..]”

Direktīva 95/46

- 12 Direktīvas 95/46 22. pants, kurš iekļauts tās III nodaļā, ir formulēts šādi:

“Neierobežojot nevienu administratīva rakstura līdzekli, kuru var paredzēt, *inter alia*, 28. pantā minētajai uzraudzības iestādei pirms vēšanās tiesas iestādē, dalībvalstis nodrošina katras personas tiesības uz tiesiskas aizsardzības līdzekli par jebkuru tiesību, ko šai personai garantē minētajai datu apstrādei piemērojamais attiecīgās valsts likums, pārkāpumu.”

Direktīva 2006/24/EK

- 13 Eiropas Parlamenta un Padomes 2006. gada 15. marta Direktīvas 2006/24/EK par tādu datu saglabāšanu, kurus iegūst vai apstrādā saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu vai publiski pieejamu komunikāciju tīklu nodrošināšanu, un par grozījumiem Direktīvā 2002/58/EK (OV 2006, L 105, 54. lpp.) 1. panta “Priekšmets un darbības joma” 2. punktā ir paredzēts:

“Šī direktīva attiecas uz noslodzes datiem [informāciju par datu plūsmu] un atrašanās vietas datiem par juridiskām personām un fiziskām personām un uz datiem, kas ar tiem saistīti, kuri ir nepieciešami abonenta vai reģistrēta lietotāja identificēšanai. To nepiemēro elektronisko komunikāciju saturam, tostarp informācijai, kura skatīta, izmantojot elektronisko komunikāciju tīklu.”

- 14 Atbilstoši šīs direktīvas 3. pantam “Pienākums saglabāt datus”:

“1. Atkāpjoties no Direktīvas [2002/58] 5., 6. un 9. panta, dalībvalstis pieņem pasākumus, lai nodrošinātu, ka šīs direktīvas 5. panta minētie dati tiek saglabāti saskaņā ar šīs direktīvas noteikumiem tiktāl, ciktāl tos ir ieguvuši vai apstrādājuši publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzēji vai publiski pieejamu komunikāciju tīklu operatori, sniedzot attiecīgos komunikāciju pakalpojumus šo valstu jurisdikcijā.

2. Šā panta 1. punktā paredzētais pienākums saglabāt datus ietver 5. pantā norādīto datu saglabāšanu saistībā ar neveiksmīgu izsaukuma mēģinājumu, kad šos datus ir ieguvuši vai apstrādājuši un uzglabājuši (attiecībā uz telefonijas datiem) vai reģistrējuši (attiecībā uz interneta datiem) publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzēji vai publiski pieejamu komunikāciju tīklu operatori, sniedzot attiecīgus pakalpojumus attiecīgās dalībvalsts jurisdikcijā. Šī direktīva neprasa saglabāt datus saistībā ar nesavienotiem izsaukumiem.”

Zviedrijas tiesību akti

- 15 No lūguma sniegt prejudiciālu nolēmumu lietā C-203/15 izriet, ka Zviedrijas likumdevējs, lai transponētu Direktīvu 2006/24 valsts tiesībās, izdarīja grozījumus *lagen (2003:389) om elektronisk kommunikation* (Likums (2003:389) par elektroniskajiem sakariem, turpmāk tekstā – “LEK”) un *förordningen (2003:396) om elektronisk kommunikation* (Noteikumi (2003:396) par elektroniskajiem sakariem). Abi šie tiesību akti to redakcijās, kas piemērojamas strīdos pamatlietās, ietver normas par datu saistībā ar elektronisko saziņu saglabāšanu, kā arī valsts iestāžu piekļuvi šiem datiem.
- 16 Piekļuvi minētajiem datiem turklāt reglamentē *lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet* (Likums (2012:278) par datu attiecībā uz elektronisko saziņu izpaušanu saistībā ar tiesībsargājošo iestāžu izmeklēšanas darbībām, turpmāk tekstā – “Likums 2012:278”), kā arī *rättegångsbalken* (Tiesu procesa kodekss, turpmāk tekstā – “RB”).

Par pienākumu saglabāt datus saistībā ar elektronisko saziņu

- 17 Saskaņā ar iesniedzējtiesas norādēm lietā C-203/15 LEK 6. nodaļas 16. panta normās, lasot kopsakarā ar šī likuma 2. nodaļas 1. pantu, elektronisko sakaru pakalpojumu sniedzējiem ir noteikts pienākums saglabāt datus, kuru saglabāšana ir paredzēta Direktīvā 2006/24. Runa ir par datiem attiecībā uz abonementiem un visu nepieciešamo elektronisko saziņu, lai atrastu un identificētu saziņas avotu un adresātu, lai noteiktu tās datumu, laiku, ilgumu un raksturu, lai identificētu izmantotu saziņas līdzekli, kā arī lai noteiktu izmantotās mobilās saziņas līdzekļa atrašanās vietu saziņas sākuma un beigu brīdī. Pienākums saglabāt datus attiecas uz tiem datiem, kuri iegūti un apstrādāti saistībā ar telefonijas pakalpojumu, ar mobilā pieslēguma telefonijas pakalpojumu, elektronisko īsziņu sistēmu, ar piekļuves internetam pakalpojumu, kā arī piekļuves internetam kapacitātes pakalpojuma sniegšanu (pieslēguma režīms). Šis pienākums attiecas arī uz datiem par saziņu, kad savienojums nav noticis. Tas tomēr neattiecas uz saziņu saturu.
- 18 Noteikumu (2003:396) par elektroniskajiem sakariem 38.–43. pantā ir precizētas datu, kuri ir jāsaglabā, kategorijas. Attiecībā uz telefonijas pakalpojumiem tostarp ir jāsaglabā dati attiecībā uz zvaniem un numuriem, uz kuriem ticis zvanīts, kā arī izsekojamiem datumiem un laikiem par saziņas sākumu un beigām. Attiecībā uz telefonijas pakalpojumiem ar mobilā pieslēguma punktu ir noteikti tādi papildu pienākumi kā, piemēram, datu par atrašanās vietu saziņas sākumā un beigās saglabāšanu. Attiecībā uz telefonijas pakalpojumiem, izmantojot IP paketi, papildus iepriekš minētajiem datiem tostarp ir jāsaglabā dati attiecībā uz izsaucēja un zvana adresāta IP adresēm. Attiecībā uz elektroniskā pasta sistēmām tostarp ir jāsaglabā dati par izsaucēju un zvanu adresātu numuriem, IP adresēm vai jebkuru citu elektroniskā pasta adresi. Attiecībā uz piekļuves internetam pakalpojumiem, piemēram, ir jāsaglabā dati attiecībā uz lietotāju IP adresēm, kā arī izsekojamie pieslēgšanās interneta piekļuves pakalpojumam un atslēgšanās no tā datumi un laiki.

Par datu saglabāšanas ilgumu

- 19 Saskaņā ar LEK 6. nodaļas 16.d pantu šīs nodaļas 16.a pantā norādītie dati elektroniskās saziņas pakalpojumu sniedzējiem ir jāsaglabā sešus mēnešus no saziņas pabeigšanas dienas. Pēc tam tie ir nekavējoties jāizdzēš, izņemot minētās nodaļas 16.d panta otrajā daļā paredzētās tiesību normas, kurās ir noteikts citādi.

Par piekļuvi saglabātajiem datiem

- 20 Valsts iestāžu piekļuvi saglabātajiem datiem reglamentē Likuma 2012:278, LEK un RB normas.

– Likums 2012:278

- 21 Saistībā ar izmeklēšanas darbībām Valsts policija, *Säkerhetspolisen* (Drošības policija, Zviedrija) un *Tullverket* (Muitas administrācija, Zviedrija), pamatojoties uz Likuma 2012:278 1. pantu, saskaņā ar šajā likumā noteiktajiem nosacījumiem, nezinot sakara elektroniskā tīkla nodrošinātājam vai, piemērojot *LEK*, atļautā elektroniskās saziņas pakalpojuma sniedzējam, var ievākt datus attiecībā uz elektroniskās saziņas tīklā nosūtītajām ziņām, elektroniskās saziņas aprīkojumu, kas izvietots noteiktā ģeogrāfiskā zonā, kā arī par vienu vai vairākām ģeogrāfiskajām zonām, kur atrodas vai atradās elektroniskās saziņas aprīkojums.
- 22 Atbilstīgi Likuma 2012:278 2. un 3. pantam datus principā var ievākt, ja pasākumam atbilstoši apstākļiem ir īpaša nozīme, lai novērstu, aizkavētu vai atklātu noziedzīgu darbību, kas aptver vienu vai vairākus noziegumus, par kuriem soda ar brīvības atņemšanu uz laiku, kas pārsniedz divus gadus, vai kādu no 3. pantā minētajiem noziegumiem, par kuriem soda ar brīvības atņemšanu līdz diviem gadiem. Pamatiem, kuru dēļ piemēro šo pasākumu, ir jāpiemīt lielākam svaram nekā apsvērumiem attiecībā uz kaitējumu vai apdraudējumu, ko šis pasākums izraisa tam, attiecībā uz ko to piemēro, vai tam pretējai interesei. Saskaņā ar minētā likuma 5. pantu pasākuma ilgums nevar pārsniegt vienu mēnesi.
- 23 Lēmumu piemērot šādu pasākumu izdod attiecīgās iestādes direktors vai cita šim nolūkam pilnvarota persona. Tas nav pakļauts iepriekšējai tiesas vai neatkarīgas administratīvas iestādes kontrolei.
- 24 Saskaņā ar Likuma 2012:278 6. pantu *Säkerhets och integritetsskyddsmynden* (Drošības un integritātes aizsardzības komisija, Zviedrija) ir jāinformē par ikvienu lēmumu atļaut ievākt datus. Saskaņā ar *lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet* (Likums (2007:980) par noteiktu kriminālvajāšanas darbību uzraudzību) 1. pantu šai iestādei ir jāuzrauga, kā kriminālvajāšanas iestādes piemēro likumu.

– *LEK*

- 25 Saskaņā ar *LEK* 6. nodaļas 22. panta pirmās daļas 2. punktu elektronisko sakaru pakalpojumu sniedzējam pēc prokuratūras, valsts policijas, drošības policijas vai jebkuras citas ar noziedzības apkarošanu saistītas iestādes pieprasījuma ir jāsniedz dati par abonementu, ja šie dati attiecas uz iespējamu noziegumu. Saskaņā ar iesniedzējtiesas norādēm lietā C-203/15 nav nepieciešams, lai runa būtu par smagu noziegumu.

– *RB*

- 26 *RB* reglamentē saglabāto datu izpaušanu valsts iestādēm saistībā ar pirmstiesas izmeklēšanu. Saskaņā ar *RB* 27. nodaļas 19. pantu “elektronisko sakaru uzraudzības piemērošana”, par to neinformējot trešās personas, principā ir atļauta saistībā ar pirmstiesas izmeklēšanu, kas tostarp vērsta uz noziegumiem, par kuriem paredzēts sodīt ar brīvības atņemšanu uz laiku līdz sešiem mēnešiem. Ar “elektronisko sakaru uzraudzības piemērošanu” saskaņā ar *RB* 27. nodaļas 19. pantu saprot datu iegūšanu, par to neinformējot trešās personas, attiecībā uz ziņu, kas nosūtīta, izmantojot elektronisko sakaru tīklu, attiecīgajiem elektronisko sakaru aprīkojumiem, kas atrodas vai atradās noteiktā ģeogrāfiskā zonā, kā arī vienu vai vairākām ģeogrāfiskām zonām, kur atrodas vai atradās noteikts elektronisko sakaru aprīkojums.
- 27 Saskaņā ar iesniedzējtiesas norādēm lietā C-203/15 informācija par ziņas saturu nevar tikt iegūta, pamatojoties uz *RB* 27. nodaļas 19. pantu. Principā elektronisko sakaru uzraudzības piemērošana saskaņā ar *RB* 27. nodaļas 20. pantu var tikt noteikta tikai, ja ir pārliecinošas norādes, kas ļauj personu turēt aizdomās par to, ka tā izdarījusi pārkāpumu un ka pasākums ir īpaši nepieciešams izmeklēšanas vajadzībām, turklāt šim pēdējam minētajam pasākumam ir jāattiecas uz noziegumu, par kuru soda ar

brīvības atņemšanu uz laiku, kas ilgāks par diviem gadiem, vai šāda nozieguma mēģinājumu, sagatavošanos tam vai organizētu grupu šāda nozieguma izdarīšanai. Saskaņā ar *RB* 27. nodaļas 21. pantu prokuroram, izņemot steidzamības gadījumus, ir jāprasa kompetentajai tiesai atļaut piemērot elektronisko sakaru uzraudzību.

Par saglabāto daru drošību un aizsardzību

- 28 Saskaņā ar *LEK* 6. nodaļas 3.a pantu elektronisko sakaru pakalpojumu sniedzējiem, kuriem ir pienākums saglabāt datus, ir jāveic atbilstoši tehniski un organizatoriski pasākumi, lai nodrošinātu datu aizsardzību to apstrādes laikā. Saskaņā ar iesniedzējtiesas norādēm lietā C-203/15 Zviedrijas tiesībās tomēr nav paredzētas tiesību normas par datu saglabāšanas vietu.

Apvienotās Karalistes tiesības

DRIPA

- 29 *DRIPA* 1. pantā “Pilnvaras datu par attiecīgajām komunikācijām saglabāšanas jomā, piemērojot garantijas” ir paredzēts:

“(1) [Iekšlietu ministrs], izdodot administratīvu aktu (“rikojumu par datu saglabāšanu”), var pieprasīt valsts telesakaru operatoram saglabāt atbilstošos datus par komunikācijām, ja iekšlietu ministrs uzskata, ka šī prasība ir nepieciešama un samērīga, lai sasniegtu vienu vai vairākus *Regulation of Investigatory Powers Act 2000* (2000. gada Izmeklēšanas pilnvaru regulēšanas likums) 22. panta 2. punkta a)–h) apakšpunktā paredzētos mērķus (mērķi, kuri pamato datu attiecībā uz komunikācijām iegūšanu).

(2) Rīkojumā, kurā noteikts pienākums saglabāt datus, var:

- (a) paredzēt, ka tas attiecas uz konkrētu operatoru vai jebkuru operatoru kategoriju;
- (b) pieprasīt saglabāt visus datus vai jebkuru datu kategoriju;
- (c) norādīt laikposmu vai laikposmus, kuru laikā dati ir jāsaglabā;
- (d) paredzēt citas prasības vai ierobežojumus saistībā ar datu saglabāšanu;
- (e) paredzēt citas prasības citiem nolūkiem;
- (f) paredzēt, ka tas attiecas uz datiem, kuri eksistē vai neeksistē dienā, kurā ir pieņemts vai stājies spēkā rīkojums par [datu] saglabāšanu.

(3) [Iekšlietu ministrs], izdodot noteikumus, var paredzēt papildu prasības par atbilstošo datu par komunikācijām saglabāšanu.

(4) Šajos noteikumos jo īpaši var paredzēt:

- (a) prasības pirms rīkojuma par datu saglabāšanu izdošanas;
- (b) maksimālo laikposmu, kura laikā dati jāsaglabā saskaņā ar rīkojumu par [datu] saglabāšanu;
- (c) rīkojuma par [datu] saglabāšanu saturu, izdošanu, stāšanos spēkā, pārskatīšanu, grozīšanu vai atcelšanu;

- (d) saskaņā ar šo pantu saglabāto datu integritāti, drošību vai aizsardzību, piekļuvi tiem, kā arī to izpaušanu vai to iznīcināšanu;
- (e) attiecīgo prasību vai ierobežojumu ieviešanu vai atbilstības šīs prasībām un ierobežojumiem ievērošanas pārbaudi;
- (f) labas prakses kodeksu attiecībā uz attiecīgajām prasībām, ierobežojumiem vai pilnvarām;
- (g) kārtību, kādā iekšlietu ministrs (ar vai bez nosacījumiem) atlīdzina izdevumus, kas rodas valsts telekomunikāciju operatoriem, izpildot attiecīgās prasības un ierobežojumus;
- (h) to, ka [*Data Retention (EC Directive) Regulations 2009* (2009. gada Noteikumi par datu saglabāšanu (EK direktīvas izpratnē)] zaudē spēku, un ka turpmāk dati jāsaglabā saskaņā ar šo pantu.

(5) Maksimālais laikposms, kas paredzēts saskaņā ar 4. punkta b) apakšpunktu, nedrīkst pārsniegt 12 mēnešus, sākot no dienas, kas minēta saistībā ar datiem, uz kuriem attiecas 3. punkta noteikumi.

[..]”

- 30 *DRIPA* 2. pantā izteiciens “atbilstošie dati attiecībā uz sakariem” ir definēts kā “atbilstošie dati par tāda veida sakariem, kas minēti 2009. gada Noteikumu par datu saglabāšanu (EK direktīvas izpratnē) pielikumā, ciktāl šos datus Apvienotajā Karalistē iegūst vai apstrādā valsts telesakaru operatori, sniedzot attiecīgus telesakaru pakalpojumus”.

RIPA

- 31 2000. gada Likuma, ar ko reglamentē izmeklēšanas pilnvaras (turpmāk tekstā – “*RIPA*”), 21. panta “Sakaru datu iegūšana un izpaušana”, kurš ietverts šī likuma II nodaļā, 4. punktā ir noteikts:

“Šajā nodaļā “sakaru dati” nozīmē jebkuru vienu no turpmāk minētajiem jēdzieniem:

- (a) jebkura informācija par datu plūsmu, kas iekļauta ziņojumā vai pievienota tam (ja to izdara sūtītājs vai kāds cits) jebkura pasta pakalpojuma vai telesakaru sistēmas mērķiem, ja ar to šie dati tiek vai var tikt nosūtīti;
- (b) jebkura informācija, kas neiekļauj ziņojuma saturu (izņemot jebkuru informāciju, kas minēta a) apakšpunktā) un attiecas uz jebkuras personas izmantoto lietošanas veidu:
 - (i) attiecībā uz jebkuru pasta pakalpojumu vai telesakaru pakalpojumu vai
 - (ii) saistībā ar jebkura telesakaru pakalpojuma sniegšanu jebkurai personai vai jebkuras telesakaru sistēmas daļas izmantošanu;
- (c) jebkura informācija, kas nav minēta a) vai b) apakšpunktā, kuru tur vai ir ieguvusi persona, kas sniedz pasta pakalpojumu vai telesakaru pakalpojumu, ja tā ir saistīta ar personām, kurām tā sniedz pakalpojumu.”

- 32 Saskaņā ar iesniedzējtiesas nolēmumā lietā C-698/15 ietvertajām norādēm šie dati ietver “datus par lietotāja atrašanās vietu”, bet neiekļauj datus saistībā ar komunikācijas saturu.

- 33 Attiecībā uz piekļuvi saglabātajiem datiem *RIPA* 22. pantā ir noteikts:

“(1) Šo pantu piemēro, kad šīs nodaļas mērķiem atbildīgā persona uzskata, ka šī panta 2. punktā minēto iemeslu dēļ ir jāiegūst jebkuri sakaru dati.

(2) Šajā punktā minēto iemeslu dēļ ir nepieciešams iegūt datus saistībā ar sakariem, ja tie ir nepieciešami:

- (a) valsts drošības interesēs;
- (b) noziegumu novēršanai vai atklāšanai un sabiedriskās kārtības traucējumu novēršanai;
- (c) Apvienotās Karalistes ekonomiskās labklājības interesēs;
- (d) sabiedrības drošības interesēs;
- (e) lai aizsargātu sabiedrības veselību;
- (f) lai aprēķinātu un iekasētu jebkurus nodokļus, nodevas, maksājumus vai citas summas, iemaksas vai maksas, kas maksājamas valsts iestādei;
- (g) lai ārkārtas situācijās novērstu personas nāvi vai ievainojumu, vai jebkādu kaitējumu tās fiziskajai vai garīgajai veselībai vai lai mīkstinātu jebkuru ievainojumu vai kaitējumu personas fiziskajai vai garīgajai veselībai;
- (h) jebkuram citam mērķim (kurš nav norādīts a)–g) punktā), kas minēts [iekšlietu ministra] izdotā rīkojumā.

(4) Ja vien 5. punktā nav noteikts citādi, atbildīgā persona – kad tā uzskata, ka telesakaru operatora vai pasta operatora rīcībā ir vai varētu būt šie dati vai ka tam būtu jāspēj tos iegūt, – var pieprasīt telesakaru operatoram vai pasta operatoram, lai šis operators

- (a) iegūst datus, ja tie vēl nav tā rīcībā, un
- (b) jebkurā gadījumā izpauž datus, kas ir tā rīcībā vai ko tas vēlāk ir ieguvis.

(5) Atbildīgā persona nedrīkst dot atļauju atbilstoši 3. punktam vai iesniegt pieprasījumu saskaņā ar 4. punktu, izņemot, ja tā uzskata, ka konkrēto datu iegūšana, ievērojot [datu iegūšanas prasības] vai ja tā prasīta saskaņā ar atļauju vai pieprasījumu, ir samērīga ar mērķi, kas sasniedzams ar datu iegūšanu.”

³⁴ Saskaņā ar RIPA 65. pantu sūdzības var *iesniegt Investigatory Powers Tribunal* (Izmeklēšanas pilnvaru tiesa, Apvienotā Karaliste), ja ir pamats uzskatīt, ka dati iegūti neatbilstošā veidā.

Data Retention Regulations 2014

³⁵ *Data Retention Regulations 2014* (2014. gada Datu saglabāšanas noteikumi), kas pieņemti, pamatojoties uz DRIPA, ir iedalīti trīs daļās, no kurām otrā daļa ietver šo noteikumu 2.–14. pantu. 4. pantā “Pieprasījumi [datu] saglabāšanas jomā” ir paredzēts:

“(1) pieprasījumos [datu] saglabāšanas jomā ir jānorāda:

- (a) sabiedriskais telesakaru operators (vai operatoru definīcija), kuriem tie ir saistoši,
- (b) dati attiecībā uz atbilstošajiem sakariem, kuri ir jāsaglabā,
- (c) laikposmu vai laikposmus, kuru laikā dati jāsaglabā,
- (d) jebkura cita prasība vai ierobežojums saistībā ar datu saglabāšanu.

(2) Pieprasījumā par datu saglabāšanu nevar prasīt, lai dati tiktu saglabāti ilgāk par 12 mēnešiem, sākot no:

- (a) saistībā ar informāciju par datu plūsmu vai datiem attiecībā uz pakalpojuma izmantošanu – attiecīgo sakaru dienas un
- (b) gadījumā, kad ir dati attiecībā uz abonentiem – dienas, kurā attiecīgā persona pārtrauc [izmantot] konkrēto sakaru pakalpojumu, vai dienas, kurā dati ir izmainīti (ja šis datums ir iestājies agrāk).

[..]”

36 Saskaņā ar šo noteikumu 7. pantu “Datu integritāte un drošība”:

“(1) Sabiedriskais telesakaru operators, kurš saglabā datus, piemērojot [DRIPA] 1. pantu:

- (a) nodrošina, lai datiem piemistu līdzvērtīga integritāte un lai tie būtu pakļauti vismaz tādām pašām drošības līmenim kā dati no sistēmām, no kurām tie iegūti,
- (b) nodrošina ar piemērotiem tehniskiem un organizatoriskiem pasākumiem, lai vienīgi personāls, kuram ir speciālas atļaujas, var piekļūt datiem un
- (c) aizsargāt ar piemērotiem tehniskiem un organizatoriskiem pasākumiem datus pret prettiesisku iznīcināšanu, nejaušiem zudumiem vai bojājumiem, vai pret neatļautu saglabāšanu, apstrādi, piekļuvi vai izpaušanu.

(2) Sabiedriskajam telesakaru operatoram, kurš saglabā datus attiecībā uz sakariem saskaņā ar [DRIPA] 1. pantu, ir jāiznīcina dati, ja datu saglabāšana vairs nav ar šo pantu atļauta un nav citādi atļauta ar likumu.

(3) 2. punktā paredzētā prasība iznīcināt datus ir prasība, kas nozīmē, ka dati ir jāizdzēš, lai padarītu neiespējamu piekļuvi šiem datiem.

(4) Ir pietiekami, ja operators veic pasākumus, lai dati tiktu izdzēsti katru mēnesi vai īsākos laikposmos atbilstoši operatora praktiskajām iespējām.”

37 Minēto noteikumu 8. pantā “Saglabāto datu izpaušana” ir paredzēts:

“(1) Sabiedriskajam telesakaru operatoram ir jāievieš piemērotas drošības sistēmas (ietverot tehniskos un organizatoriskos pasākumus), kas nosaka piekļuvi datiem saistībā ar komunikācijām, kuras saglabātas saskaņā ar [DRIPA] 1. pantu, lai novērstu jebkuru izpaušanu, kas neizriet no [DRIPA] 1. panta 6. punkta a) apakšpunkta.

(2) Sabiedriskajam telesakaru operatoram, kas saglabā datus saskaņā ar [DRIPA] 1. pantu, ir jāsaglabā dati tādējādi, lai tos, atbildot uz pieprasījumiem, varētu izpaust bez nepamatotas kavēšanās.”

38 Šo pašu noteikumu 9. pantā “Par informāciju atbildīgā komisāra veiktā kontrole” ir noteikts:

“Par informāciju atbildīgais komisārs kontrolē šajā nodaļā paredzēto prasību un ierobežojumu ieviešanu saskaņā ar [DRIPA] 1. pantā paredzētajām saglabāto datu integritātes, drošības un iznīcināšanas prasībām.”

Labas prakses kodekss

- 39 *Acquisition and Disclosure of Communications Data Code of Practice* (Labas prakses par datu attiecībā uz sakariem iegūšanu un izpaušanu kodekss, turpmāk tekstā – “Labas prakses kodekss”) 2.5.–2.9. un 2.36.–2.45. punktā ir ietvertas norādes par datu attiecībā uz sakariem iegūšanas nepieciešamību un samērīgumu. Saskaņā ar iesniedzējtiesas paskaidrojumiem lietā C-698/15 un atbilstoši šī kodeksa 3.72.–3.77. punktam īpaša uzmanība ir jāvelta nepieciešamībai un samērīgumam, kad pieprasītie dati attiecībā uz sakariem attiecas uz personu, kas ir tādas profesijas pārstāvis, kuras ietvaros tā iegūst ar dienesta noslēpumu aizsargātu vai citādi konfidenciālu informāciju.
- 40 Saskaņā ar minētā kodeksa 3.78.–3.84. punktu tiesas rīkojums tiek prasīts īpašā gadījumā, kad pieprasījums attiecas uz datiem par komunikācijām, kas veiktas, lai identificētu žurnālistu avotu. Saskaņā ar šī paša kodeksa 3.85.–3.87. punktu tiesas apstiprinājums tiek prasīts gadījumā, ja piekļuves pieteikumu ir formulējušas pašvaldību iestādes. Tiesas vai neatkarīgas [valsts] iestādes atļauja savukārt nav nepieciešama, lai piekļūtu tādiem datiem par sakariem, kurus aizsargā likumā noteikts dienesta noslēpums, vai datiem par sakariem, ko veikuši ārsti, parlamenta deputāti vai reliģisko konfesiju amatpersonas.
- 41 Labas prakses kodeksa 7.1. punktā ir paredzēts, ka dati par sakariem, kas iegūti vai saņemti saskaņā ar *RIPA* noteikumiem, kā arī visi izvilkumi, apkopojumi un kopijas ir jāapstrādā un jāuzglabā droši. Turklāt ir jāievēro *Data Protection Act* (Likums par datu aizsardzību) ietvertās prasības.
- 42 Saskaņā ar Labas prakses kodeksa 7.18. punktu, kad Apvienotās Karalistes valsts iestāde plāno iespējamu datu attiecībā uz sakariem izpaušanu ārvalstu iestādēm, tai tostarp ir jāpārbauda, vai šie dati tiks piemērotā veidā aizsargāti. Tomēr no šī kodeksa 7.22. punkta izriet, ka datu nodošana uz trešajām valstīm var notikt, kad šī nodošana ir nepieciešama primāru vispārējo interešu apsvērumu dēļ, pat ja trešā valsts nenodrošina piemērotu aizsardzības līmeni. Saskaņā ar iesniedzējtiesas apsvērumiem lietā C-698/15 iekšlietu ministrs var izdot valsts drošības apliecinājumu, atbrīvojot no pienākumu attiecībā uz konkrētajiem datiem ievērot tiesību aktos paredzētos noteikumus.
- 43 Minētā kodeksa 8.1. punktā ir atgādināts, ka *RIPA* iecel *Interception of Communications Commissioner* (sakaru pārtveršanas komisārs, Apvienotā Karaliste), kura uzdevums ir veikt neatkarīgu *RIPA* I daļas II nodaļā norādīto pilnvaru un pienākumu izpildes un īstenošanas pārraudzību. Tādējādi, kā izriet no šī paša kodeksa 8.3. punkta, šim komisāram ir atļauts vienīgi informēt fizisku personu par aizdomām, ka pilnvaras iespējams ir tikušas izmantotas nelikumīgi, ja komisārs var “pierādīt, ka fiziskai personai kaitējumu ir radījusi kāda tīša rīcība vai piesardzības trūkums”.

Pamatlietas un prejudiciālie jautājumi

Lietā C-203/15

- 44 2014. gada 9. aprīlī *Tele2 Sverige*, Zviedrijā reģistrēts elektronisko sakaru pakalpojumu sniedzējs, paziņoja *PTS*, ka pēc Direktīvas 2006/24 atzišanas par spēkā neesošu ar 2014. gada 8. aprīļa spriedumu *Digital Rights Ireland* u.c. (C-293/12 un C-594/12, turpmāk tekstā – “spriedums *Digital Rights*”, EU:C:2014:238) tā no 2014. gada 14. aprīļa pārtraukšot saglabāt datus attiecībā uz elektroniskajiem sakariem, kuri ietilpst *LEK* piemērošanas jomā, un ka tā izdzēsīs līdz šim datumam saglabātos datus.
- 45 2014. gada 15. aprīlī *Rikspolisstyrelsen* (Galvenā valsts policijas pārvalde, Zviedrija) iesniedza *PTS* sūdzību, jo *Tele2 Sverige* tai vairs nepaziņoja konkrētos datus.

- 46 2014. gada 29. aprīlī *justitieminister* (tieslietu ministrs, Zviedrija) iecēla īpašo referentu, kuram tika uzdots analizēt konkrēto Zviedrijas tiesisko regulējumu saistībā ar spriedumu *Digital Rights*. 2014. gada 13. jūnija ziņojumā “Datalagring, EU-rätten och svensk rätt, Nr. Ds 2014:23” (Datu saglabāšana, Savienības tiesības un Zviedrijas tiesības, turpmāk tekstā – “2014. gada ziņojums”) īpašais referents secināja, ka valsts tiesiskais regulējums attiecībā uz datu saglabāšanu, kāds tas paredzēts LEK 16.a–16.f. pantā, nav pretrunā ne Savienības tiesībām, ne Romā 1950. gada 4. novembrī parakstītajai Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijai (turpmāk tekstā – “ECPAK”). Īpašais referents uzsvēra, ka spriedums *Digital Rights* nevarēja tikt interpretēts tādējādi, ka tas izslēdz pašu principu par datu vispārēju un nediferencētu saglabāšanu. Viņa ieskatā, spriedums *Digital Rights* arī nav jāsaprot tādā nozīmē, ka Tiesa tajā būtu paredzējusi virkni kritēriju, kuri visi ir jāizpilda, lai tiesiskais regulējums varētu tikt uzskatīts par samērīgu. Lai noteiktu Zviedrijas tiesiskā regulējuma saderību ar Savienības tiesībām, esot jāizvērtē visi apstākļi, proti, datu saglabāšanas apjoms, ņemot vērā tiesību normas par piekļuvi datiem, par to saglabāšanas ilgumu, par to aizsardzību, kā arī par to drošību.
- 47 Pamatojoties uz minēto, 2014. gada 19. jūnijā *PTS* informēja *Tele2 Sverige*, ka tā neizpilda valsts tiesiskajā regulējumā paredzētos pienākumus, nesaglabājot LEK paredzētos datus sešus mēnešus noziedzības apkarošanas nolūkā. *PTS* ar 2014. gada 27. jūnija rīkojumu tai pēc tam noteica pienākumu vēlākais 2014. gada 25. jūlijā saglabāt šos datus.
- 48 Uzskatot, ka 2014. gada rīkojums balstījās uz sprieduma *Digital Rights* kļūdainu interpretāciju un ka datu saglabāšanas pienākums ir pretrunā ar Hartu garantētajām pamattiesībām, *Tele2 Sverige* cēla prasību *Förvaltningsrätten i Stockholm* (Administratīvā tiesa Stokholmā, Zviedrija) par 2014. gada 27. jūnija rīkojumu. Tā kā ar 2014. gada 13. oktobra spriedumu šī tiesa prasību noraidīja, *Tele2 Sverige* iesniedzējtiesā iesniedza apelācijas sūdzību par šo spriedumu.
- 49 Iesniedzējtiesas ieskatā, Zviedrijas tiesiskā regulējuma saderība ar Savienības tiesībām ir jāizvērtē Direktīvas 2002/58 15. panta 1. punkta gaismā. Proti, lai gan šajā direktīvā esot noteikts princips, saskaņā ar kuru dati attiecībā uz informāciju par datu plūsmu un atrašanās vietas dati ir jāizdzēš vai jāpadara par anonīmiem, kad tie vairs nav nepieciešami saziņas tālāk nodošanai, minētās direktīvas 15. panta 1. punktā esot ieviesta atkāpe no šī principa, jo ar to dalībvalstīm esot atļauts sašaurināt šo pienākumu par izdzēšanu vai padarīšanu par anonīmu vai arī paredzēt datu saglabāšanu, kad to pamato viens no šajā pantā paredzētajiem pamatiem. Tādējādi Savienības tiesības atsevišķās situācijās ļaujot saglabāt datus attiecībā uz elektroniskajiem sakariem.
- 50 Iesniedzējtiesa tomēr vēlas noskaidrot, vai tāds visaptverošs un nediferencēts pienākums saglabāt datus attiecībā uz elektroniskajiem sakariem kā pamatlietā aplūkotais, ņemot vērā spriedumu *Digital Rights*, ir saderīgs ar Direktīvas 2002/58 15. panta 1. punktu, lasot to Hartas 7. un 8. panta, kā arī 52. panta 1. punkta gaismā. Ņemot vērā šajā ziņā atšķirīgos pušu viedokļus, Tiesai būtu jāspriež viennozīmīgi attiecībā uz to, vai, kā uzskata *Tele2 Sverige*, datu attiecībā uz elektroniskajiem sakariem visaptveroša un nediferencēta saglabāšana pati par sevi ir nesaderīga ar Hartas 7. un 8. pantu, kā arī ar 52. panta 1. punktu vai, kā izrietot no 2014. gada ziņojuma, šādas datu saglabāšanas saderība ir jāizvērtē, ņemot vērā tiesību normas par piekļuvi datiem, to aizsardzību un drošību, kā arī saglabāšanas ilgumu.
- 51 Šajos apstākļos iesniedzējtiesa nolēma apturēt tiesvedību un uzdot Tiesai šādus prejudiciālus jautājumus:
- “1) Vai vispārējs pienākums saglabāt datus, kas attiecas uz visām personām un visiem elektroniskās saziņas līdzekļiem, kā arī visu informāciju par datu plūsmu, neparedzot nekādu diferencēšanu, ierobežojumus vai izņēmumus, ņemot vērā mērķi apkarot noziedzību [...], ir saderīgs ar Direktīvas 2002/58 15. panta 1. punktu, ņemot vērā Hartas 7. un 8. pantu, kā arī 52. panta 1. punktu?

- 2) Ja atbilde uz pirmo jautājumu ir noliedzīga – vai šāds pienākums par [datu] saglabāšanu tomēr ir pieļaujams, ja
- a) ir precīzi noregulēta valstu iestāžu piekļuve saglabājamiem datiem, kā precizēts [lūguma sniegt prejudiciālu nolēmumu] 19.–36. punktā, un
 - b) ir precīzi reglamentētas datu aizsardzības un drošības prasības, kā precizēts [lūguma sniegt prejudiciālu nolēmumu] 38.–43. punktā, kā arī
 - c) visi attiecīgie dati ir jāsaglabā sešus mēnešus, sākot no dienas, kad saziņa ir tikusi pabeigta, un pēc tam tie ir jāizdzēš, kā izklāstīts [lūguma sniegt prejudiciālu nolēmumu] 37. punktā?”

Lietā C-698/15

- 52 *T. Watson, P. Brice un G. Lewis* katrs atsevišķi cēla prasību *High Court of Justice (England & Wales), Queens’ Bench Division (Divisional Court)* (Augstā tiesa (Anglija un Velsa), *Queen’s Bench* nodaļa (Kolēģija), Apvienotā Karaliste), lūdzot pārbaudīt *DRIPA* 1. panta tiesiskumu, atsaucoties tostarp uz šī panta nesaderību ar Hartas 7. un 8. pantu, kā arī ar ECPAK 8. pantu.
- 53 Ar 2015. gada 17. jūlija spriedumu *High Court of Justice (England & Wales), Queens’ Bench Division (Divisional Court)* (Augstā tiesa (Anglija un Velsa), *Queen’s Bench* nodaļa (Kolēģija)) konstatēja, ka spriedumā *Digital Rights* “ES tiesībās” ir noteiktas “obligātas prasības”, kas piemērojamas attiecībā uz dalībvalstu tiesiskajiem regulējumiem datu attiecībā uz sakariem saglabāšanas jomā, kā arī attiecībā uz piekļuvi šādiem datiem. Šīs tiesas ieskatā, tā kā Tiesa šajā spriedumā uzskatīja, ka Direktīva 2006/24 ir nesaderīga ar samērīguma principu, šai direktīvai identiska satura valsts tiesiskais regulējums arī nevar būt saderīgs ar šo principu. No sprieduma *Digital Rights* pamatā esošās sistēmas izrietot, ka ar tiesisko regulējumu, kas nosaka vispārējo kārtību datu attiecībā uz sakariem saglabāšanai, ir pārkāptas Hartas 7. un 8. pantā garantētās tiesības, ja vien šis tiesiskais regulējums nav papildināts ar kārtību par piekļuvi datiem, kas noteikta valsts tiesībās un kurā paredzētas pietiekamas garantijas šo tiesību saglabāšanai. Tādējādi *DRIPA* 1. pants neesot saderīgs ar Hartas 7. un 8. pantu, jo tajā nav noteikti skaidri un precīzi noteikumi attiecībā uz piekļuvi saglabājamiem datiem un to izmantošanu un piekļuve šiem datiem nav pakļauta iepriekšējai kontrolei, ko veic tiesa vai neatkarīga administratīva iestāde.
- 54 Iekšlietu ministrs par šo spriedumu iesniedza apelācijas sūdzību *Court of Appeal (England & Wales) (Civil Division)* (Apelācijas tiesa (Anglija un Velsa) (Civillietu palāta), Apvienotā Karaliste).
- 55 Šī tiesa norāda, ka ar *DRIPA* 1. panta 1. punktu iekšlietu ministrs ir pilnvarots bez iepriekšējas tiesas vai neatkarīgas administratīvas iestādes atļaujas pieņemt vispārēju kārtību, kurā valsts telesakaru operatoriem noteikts pienākums saglabāt visus datus attiecībā uz jebkuru pasta pakalpojumu vai jebkuru telesakaru pakalpojumu laikposmā līdz 12 mēnešiem, ja tas uzskata, ka šāda prasība ir nepieciešama un samērīga, lai sasniegtu Apvienotās Karalistes tiesiskajā regulējumā paredzētos mērķus. Pat ja šie dati neietver saziņas saturu, tie varētu būt tādi, ar kuriem tiek īstenota īpaši izteikta iejaukšanās sakaru pakalpojumu lietotāju privātajā dzīvē.
- 56 Iesniedzējtiesas nolēmumā un tās 2015. gada 20. novembra spriedumā, kas pieņemts apelācijas tiesvedības ietveros un ar ko iesniedzējtiesa nolēma Tiesai iesniegt šo lūgumu sniegt prejudiciālu nolēmumu, iesniedzējtiesa uzskata, ka valsts tiesību normas attiecībā uz datu saglabāšanu noteikti reglamentē Direktīvas 2002/58 15. panta 1. punkts un tajās ir jāievēro no Hartas izrietošās prasības. Tomēr saskaņā ar šīs direktīvas 1. panta 3. punktu Savienības likumdevējs neesot saskaņojis normas attiecībā uz piekļuvi saglabājamiem datiem.
- 57 Attiecībā uz sprieduma *Digital Rights* ietekmi uz pamatlietā izvirzītajiem jautājumiem iesniedzējtiesa norāda, ka lietā, kurā pasludināts šis spriedums, Tiesā tika iesniegts lūgums sniegt prejudiciālu nolēmumu par Direktīvas 2006/24, nevis valsts tiesiskā regulējuma spēkā esamību. It īpaši ņemot vērā ciešo saikni starp datu saglabāšanu un piekļuvi šiem datiem, būtu bijis nepieciešams, ka papildus šai direktīvai tiek noteikta virkne garantiju un ka spriedumā *Digital Rights*, vērtējot ar minēto direktīvu

paredzētās datu saglabāšanas kārtības tiesiskumu, būtu analizēti noteikumi attiecībā uz piekļuvi šiem datiem. Tiesa tādā šajā spriedumā neesot plānojusi paredzēt obligātas prasības, kas piemērojamas valstu tiesiskajiem regulējumiem attiecībā uz piekļuvi datiem, ar kuriem netiek ieviestas Savienības tiesības. Turklāt Tiesas argumentācija esot bijusi cieši saistīta ar mērķi, kas sasniedzams ar šo pašu direktīvu. Tomēr valsts tiesiskais regulējums esot jāvērtē, ņemot vērā ar to sasniedzamos mērķus un tā kontekstu.

58 Attiecībā uz nepieciešamību Tiesā iesniegt lūgumu sniegt prejudiciālu nolēmumu iesniedzējtiesa uzsver, ka iesniedzējtiesas nolēmuma pieņemšanas dienā sešas citas dalībvalstu tiesas, no kurām piecas ir pēdējās instances tiesas, bija atcēlušas valsts tiesību aktus, pamatojoties uz spriedumu *Digital Rights*. Atbilde uz izvirzītajiem jautājumiem tādā neesot acīmredzama, tomēr tā ir nepieciešama, lai izspriestu lietas, par kurām šajā tiesā celtas prasības.

59 Šajos apstākļos *Court of Appeal (England & Wales) (Civil Division)* (Apelācijas tiesa (Anglija un Velsa) (Civillietu palāta)) nolēma apturēt tiesvedību un uzdot Tiesai šādus prejudiciālus jautājumus:

“1) Vai spriedums *Digital Rights* (tostarp it īpaši šā sprieduma 60.–62. punkts) nosaka obligātas prasības Savienības tiesībās, kuras piemērojamas dalībvalsts tiesiskajam regulējumam, kas reglamentē piekļuvi saskaņā ar valsts tiesību aktiem saglabājamiem datiem, lai nodrošinātu atbilstību Hartas 7. un 8. pantam?

2) Vai ar spriedumu *Digital Rights* Hartas 7. un/vai 8. panta piemērošanas joma tiek noteikta plašāka par ECPAK 8. panta piemērošanas jomu, kāda tā noteikta Eiropas Cilvēktiesību tiesas judikatūrā?”

Par tiesvedību Tiesā

60 Ar 2016. gada 1. februāra rīkojumu *Davis* u.c. (C-698/15, nav publicēts, EU:C:2016:70) Tiesas priekšsēdētājs apmierināja *Court of Appeal (England & Wales) (Civil Division)* (Apelācijas tiesa (Anglija un Velsa) (Civillietu palāta)) lūgumu lietai C-698/15 piemērot paātrināto tiesvedību, kas paredzēta Tiesas Reglamenta 105. panta 1. punktā.

61 Ar Tiesas priekšsēdētāja 2016. gada 10. marta lēmumu lietas C-203/15 un C-698/15 tika apvienotas mutvārdu procesā un sprieduma taisīšanai.

Par prejudiciālajiem jautājumiem

Par pirmo jautājumu lietā C-203/15

62 Ar pirmo jautājumu lietā C-203/15 *Kammarrätten i Stockholm* (Administratīvā apelācijas tiesa Stokholmā) būtībā vēlas noskaidrot, vai Direktīvas 2002/58 15. panta 1. punkts, lasot Hartas 7. un 8. panta, kā arī 52. panta 1. punkta gaismā, ir jāinterpretē tādējādi, ka tam pretrunā ir tāds valsts tiesiskais regulējums kā pamatlietā aplūkotois, kurā noziedzības apkarošanas nolūkā ir paredzēts visaptverošs un nediferencēts [pienākums] saglabāt visu informāciju par datu plūsmu un atrašanās vietas datus attiecībā uz visiem abonentiem un reģistrētiem lietotājiem un attiecībā uz visiem elektronisko sakaru veidiem.

63 Šo jautājumu tostarp izraisa tas, ka Direktīva 2006/24, kura transponēta ar pamatlietā aplūkoto valsts tiesisko regulējumu, ar spriedumu *Digital Rights* tika atzīta par spēkā neesošu, bet pusēm ir dažādi viedokļi par šī sprieduma tvērumu un tā ietekmi uz šo tiesisko regulējumu, kas reglamentē informācijas par datu plūsmu un atrašanās vietas datu saglabāšanu, kā arī valsts iestāžu piekļuvi šiem datiem.

- 64 Vispirms ir jāizvērtē, vai tāds valsts tiesiskais regulējums kā pamatlietā aplūkotais ietilpst Savienības tiesību piemērošanas jomā.

Par Direktīvas 2002/58 piemērošanas jomu

- 65 Dalībvalstis, kuras Tiesā ir iesniegušas rakstveida apsvērumus, izteica atšķirīgus viedokļus attiecībā uz to, vai un kādā mērā valstu tiesiskie regulējumi par informācijas par datu plūsmu un atrašanās vietas datu saglabāšanu, kā arī valsts iestāžu piekļuvi šiem datiem noziedzības apkarošanas nolūkā ietilpst Direktīvas 2002/58 piemērošanas jomā. Proti, lai gan tostarp Beļģijas, Dānijas, Vācijas, Igaunijas un Īrijas, kā arī Nīderlandes valdības ir izteikušas viedokli, ka uz šo jautājumu ir jāatbild apstiprinoši, Čehijas Republikas valdība uz šo jautājumu ierosināja atbildēt noliedzoši, norādot, ka šo tiesisko regulējumu vienīgais mērķis ir noziedzības apkarošana. Savukārt Apvienotās Karalistes valdība norādīja, ka šīs direktīvas piemērošanas jomā ietilpst vienīgi tiesiskie regulējumi par datu saglabāšanu, nevis par valsts iestāžu, kurām ir kompetence kriminālvajāšanas jomā, piekļuvi šiem datiem.
- 66 Visbeidzot, lai gan Komisija Tiesai lietā C-203/15 iesniegtajos rakstveida apsvērumos uzskatīja, ka pamatlietā aplūkotais valsts tiesiskais regulējums ietilpst Direktīvas 2002/58 piemērošanas jomā, tā savos rakstveida apsvērumos lietā C-698/15 norādīja, ka šīs direktīvas piemērošanas jomā ietilpst vienīgi valsts tiesību normas attiecībā uz datu saglabāšanu, nevis tiesību normas attiecībā uz valsts iestāžu piekļuvi šiem datiem. Tomēr, tās ieskatā, šīs pēdējās minētās tiesību normas ir jāņem vērā, lai novērtētu, vai valsts tiesiskais regulējums, kas reglamentē datu saglabāšanu, ko veic elektronisko sakaru pakalpojumu sniedzēji, ir uzskatāms par nesamērīgu iejaukšanos ar Hartas 7. un 8. pantu garantētajās pamattiesībās.
- 67 Šajā ziņā ir jānorāda, ka Direktīvas 2002/58 piemērošanas joma ir jāizvērtē, it īpaši ņemot vērā tās vispārējo struktūru.
- 68 Direktīvas 2002/58 1. panta 1. punktā ir paredzēta to dalībvalstu tiesību normu saskaņošana, kas nepieciešamas, lai nodrošinātu pamattiesību un pamatbrīvību līdzvērtīgu aizsardzības līmeni, jo īpaši tiesības uz privāto dzīvi un konfidencialitāti saistībā ar personas datu apstrādi elektronisko sakaru nozarē.
- 69 Ar šīs direktīvas 1. panta 3. punktu no tās piemērošanas jomas izslēgtas “valsts darbības” tajā paredzētajās jomās, proti, it īpaši valsts darbības krimināltiesību jomā un valsts darbības, kas attiecas uz sabiedrības drošību, aizsardzību, valsts drošību, tostarp valsts ekonomisko labklājību, ja darbības attiecas uz valsts drošības jautājumiem (pēc analogijas attiecībā uz Direktīvas 95/46 3. panta 2. punkta pirmo ievilkumu skat. spriedumus, 2003. gada 6. novembris, *Lindqvist*, C-101/01, EU:C:2003:596, 43. punkts, kā arī 2008. gada 16. decembris, *Satakunnan Markkinapörssi* un *Satamedia*, C-73/07, EU:C:2008:727, 41. punkts).
- 70 Direktīvas 2002/58 3. pantā ir paredzēts, ka šī direktīva attiecas uz personas datu apstrādi saistībā ar publiski pieejamu elektronisko sakaru pakalpojumu sniegšanu publiskos sakaru pakalpojumu tīklos Savienībā, tostarp publiskos sakaru tīklos, kuros var izmantot datu iegūšanas un identifikācijas ierīces (turpmāk tekstā – “elektronisko sakaru ierīces”). Līdz ar to minētā direktīva ir jāuzskata par tādu, kas reglamentē šādu pakalpojumu sniedzēju darbības.
- 71 Direktīvas 2002/58 15. panta 1. punktā dalībvalstīm ir atļauts, ievērojot tajā paredzētos nosacījumus, 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”. Minētās direktīvas 15. panta 1. punkta otrajā teikumā kā piemēri ir norādīti tiesību akti, kurus tādad var pieņemt dalībvalstis, “paredzot datu saglabāšanu”.

- 72 Protams, Direktīvas 2002/58 15. panta 1. punktā paredzētie tiesību akti ir valsts vai valsts iestāžu atbilstošās darbības, kas nepieder pie fizisko personu darbības jomām (šajā ziņā skat. spriedumu, 2008. gada 29. janvāris, *Promusicae*, C-275/06, EU:C:2008:54, 51. punkts). Turklāt mērķi, kuri saskaņā ar šo tiesību normu ir jāsasniedz ar šādiem tiesību aktiem, konkrētajai gadījumā – valsts drošības, aizsardzības un sabiedrības drošības nodrošināšana, kā arī noziedzīgu nodarījumu vai neatļautas elektronisko sakaru sistēmas izmantošanas novēršana, izmeklēšana, atklāšana un kriminālvajāšana, būtiski sakrīt ar mērķiem, kas sasniedzami ar šīs direktīvas 1. panta 3. punktā paredzētajām darbībām.
- 73 Tomēr, ņemot vērā Direktīvas 2002/58 vispārējo struktūru, šī sprieduma iepriekšējā punktā izvirzītie elementi neļauj secināt, ka Direktīvas 2002/58 15. panta 1. punktā paredzētie tiesību akti ir izslēgti no šīs direktīvas piemērošanas jomas, pretējā gadījumā šī tiesību norma pavisam zaudētu lietderību. Proti, minētā tiesību norma obligāti nozīmē, ka tajā noteiktie valsts pasākumi – kā, piemēram, pasākumi saistībā ar datu saglabāšanu noziedzības apkarošanas mērķiem – ietilpst šīs direktīvas piemērošanas jomā, jo šajā pēdējā minētajā direktīvā dalībvalstīm ir tieši atļauts šos tiesību aktus pieņemt vienīgi, ievērojot tajā paredzētos nosacījumus.
- 74 Turklāt tiesību akti, kas paredzēti Direktīvas 2002/58 15. panta 1. punktā, saskaņā ar šajā tiesību normā paredzētajiem mērķiem reglamentē elektronisko sakaru pakalpojumu sniedzēju darbību. Tātad šis 15. panta 1. punkts, lasot kopsakarā ar minētās direktīvas 3. pantu, ir jāinterpretē tādējādi, ka šādi tiesību akti ietilpst šīs pašas direktīvas piemērošanas jomā.
- 75 It īpaši šajā piemērošanas jomā ietilpst tāds tiesību akts kā pamatlietā aplūkotais, kurš šiem pakalpojumu sniedzējiem nosaka pienākumu saglabāt informāciju par datu plūsmu un atrašanās vietas datus, jo šāda darbība noteikti nozīmē, ka šie pakalpojumu sniedzēji apstrādās personas datus.
- 76 Minētajā piemērošanas jomā ietilpst arī tiesību akts, kurš tāpat kā pamatlietā aplūkotais attiecas uz valsts iestāžu piekļuvi elektronisko sakaru pakalpojumu sniedzēju saglabātajiem datiem.
- 77 Proti, elektronisko sakaru konfidencialitātes un attiecīgās informācijas par datu plūsmu aizsardzība, kas garantēta Direktīvas 2002/58 5. panta 1. punktā, attiecas uz pasākumiem, kurus veic jebkura cita persona, kas nav lietotājs, neraugoties uz to, vai runa ir par personām vai par privāto vai publisko tiesību subjektiem. Kā apstiprināts šīs direktīvas preambulas 21. apsvērumā, lai aizsargātu elektronisko sakaru konfidencialitāti, tās mērķis ir liegt [“jebkuru”] neatļautu “piekļuvi” komunikācijām, tostarp [“jebkurai”] informācij[ai] attiecībā uz šādām komunikācijām”.
- 78 Šajos apstākļos tiesību akts – ar kuru dalībvalsts, pamatojoties uz Direktīvas 2002/58 15. panta 1. punktu, elektronisko sakaru pakalpojumu sniedzējiem šajā tiesību normā minēto mērķu dēļ nosaka pienākumu saskaņā ar attiecīgajā tiesību aktā paredzētajiem nosacījumiem piešķirt valsts iestādēm piekļuvi minēto pakalpojumu sniedzēju saglabātajiem datiem – attiecas uz šo pakalpojumu sniedzēju veikto personas datu apstrādi, proti, apstrādi, kas ietilpst šīs direktīvas piemērošanas jomā.
- 79 Turklāt, tā kā datu saglabāšana tiek veikta tikai, lai attiecīgajā gadījumā datus padarītu pieejamus kompetentajām valsts iestādēm, valsts tiesiskais regulējums, kurā paredzēta datu saglabāšana, principā noteikti nozīmē tiesību normu par kompetento valsts iestāžu piekļuvi elektronisko sakaru pakalpojumu sniedzēju saglabātajiem datiem pastāvēšanu.
- 80 Šo interpretāciju apstiprina Direktīvas 2002/58 15. panta 1.b punkts, saskaņā ar kuru pakalpojumu sniedzēji, pamatojoties uz saskaņā ar šīs direktīvas 15. panta 1. punktu pieņemtajām valsts tiesību normām, nosaka iekšējo procedūru, kurā paredz kārtību, kādā atbild uz pieteikumiem par piekļuvi personas datiem attiecībā uz lietotājiem.
- 81 No iepriekš minētā izriet, ka tāds valsts tiesiskais regulējums kā pamatlietās C-203/15 un C-698/15 aplūkotais ietilpst Direktīvas 2002/58 piemērošanas jomā.

Par Direktīvas 2002/58 15. panta 1. punkta interpretāciju saskaņā ar Hartas 7., 8. un 11. punktu, kā arī 52. panta 1. punktu

- 82 Ir jānorāda, ka saskaņā ar Direktīvas 2002/58 1. panta 2. punktu šīs direktīvas noteikumi “precizē un papildina” Direktīvu 95/46. Direktīvas 2002/58 mērķis, kā paredzēts tās preambulas 2. apsvērumā, ir nodrošināt it īpaši, ka tiek pilnībā ievērotas Hartas 7. un 8. pantā paredzētās tiesības. Šajā ziņā no priekšlikuma Eiropas Parlamenta un Padomes Direktīvai [2002/58/EK] par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (COM(2000) 385, galīgā redakcija), kas ir Direktīvas 2002/58 pamatā, paskaidrojuma raksta izriet, ka Savienības likumdevējs ir vēlējis “rīkoties tādējādi, ka personas datu augsts aizsardzības līmenis un privātā dzīve turpina būt garantēta attiecībā uz visiem elektronisko sakaru pakalpojumiem neatkarīgi no izmantotās tehnoloģijas”.
- 83 Šajā nolūkā Direktīva 2002/58 ietver specifiskas tiesību normas, kuras, kā izriet tostarp no tās preambulas 6. un 7. apsvēruma, ir vērstas uz to, lai aizsargātu elektronisko sakaru pakalpojumu lietotājus pret riskiem personas datiem un privātajai dzīvei, kas izriet no jaunajām tehnoloģijām un arvien lielākas jaudas datu automatizētai glabāšanai un apstrādei.
- 84 It īpaši šīs direktīvas 5. panta 1. punktā ir paredzēts, ka dalībvalstīm ar saviem valsts tiesību aktiem ir jāgarantē ar sakaru valsts tīkla un sabiedrībai pieejamo elektronisko sakaru pakalpojumiem elektronisko sakaru pakalpojumu palīdzību veikto sakaru konfidencialitāte, kā arī ar tiem saistītās informācijas par datu plūsmu konfidencialitāte.
- 85 Ar Direktīvu 2002/58 ieviestais sakaru konfidencialitātes princips tostarp nozīmē, kā izriet no tās 5. panta 1. punkta otrā teikuma, ka principā ir noteikts aizliegums attiecībā uz jebkuru citu personu, kas nav lietotājs, bez tās iepriekšējas atļaujas uzglabāt informāciju par datu plūsmu attiecībā uz elektroniskajiem sakariem. Izņēmumi attiecas vienīgi uz personām, kam to darīt ir atļauts ar likumu saskaņā ar šīs direktīvas 15. panta 1. punktu, un tehnisko uzglabāšanu, kas nepieciešama komunikācijas pārsūtīšanai (šajā ziņā skat. spriedumu, 2008. gada 29. janvāris, *Promusicae*, C-275/06, EU:C:2008:54, 47. punkts).
- 86 Tādējādi un kā to apstiprina Direktīvas 2002/58 preambulas 22. un 26. preambula, informācijas par datu plūsmu apstrāde un uzglabāšana saskaņā ar šīs direktīvas 6. pantu ir atļauta tikai tādā mērā un tik ilgi, kas nepieciešams rēķinu izrakstīšanai par pakalpojumiem, to laišanai tirgū un pakalpojumu ar pievienoto vērtību sniegšanai (šajā ziņā skat. spriedumu, 2008. gada 29. janvāris, *Promusicae*, C-275/06, EU:C:2008:54, 47. un 48. punkts). It īpaši attiecībā uz rēķinu izrakstīšanu par pakalpojumiem šāda apstrāde ir atļauta līdz laikposma beigām, kurā rēķins var tikt likumīgi apstrādāts vai var tikt piemērota piespiedu izpilde, lai saņemtu tā samaksu. Pēc šī laikposma beigām apstrādātie un uzglabātie dati ir jāizdzēš vai jāpadara par anonīmiem. Attiecībā uz atrašanās vietas datiem, kas nav informācija par datu plūsmu, minētās direktīvas 9. panta 1. punktā ir paredzēts, ka šos datus var apstrādāt tikai, ja izpildīti noteikti nosacījumi, kad tie ir padarīti par anonīmiem, vai arī ar lietotāju vai abonentu piekrišanu.
- 87 Direktīvas 2002/58 5. un 6. panta, kā arī 9. panta 1. punkta, kuru mērķis ir garantēt sakaru un ar tiem saistīto datu konfidencialitāti, kā arī mazināt ļaunprātības riskus, piemērošanas joma turklāt ir jāizvērtē šīs direktīvas preambulas 30. apsvēruma gaismā, saskaņā ar kuru “sistēmas elektronisko komunikāciju tīklu nodrošināšanai un pakalpojumu sniegšanai jāveido tā, lai ierobežotu nepieciešamo personas datu apjomu līdz stingri noteiktam minimumam”.
- 88 Protams, Direktīvas 2002/58 15. panta 1. punkts ļauj dalībvalstīm ieviest izņēmumus no šīs direktīvas 5. panta 1. punktā paredzētā vispārējā pienākuma nodrošināt personas datu konfidencialitāti, kā arī no attiecīgajiem pienākumiem, kas tostarp norādīti minētās direktīvas 6.–9. pantā (šajā ziņā skat. spriedumu, 2008. gada 29. janvāris, *Promusicae*, C-275/06, EU:C:2008:54, 50. punkts).

- 89 Tomēr Direktīvas 2002/58 15. panta 1. punkts, ciktāl ar to dalībvalstīm ir atļauts ierobežot vispārējā principa nodrošināt sakaru un ar tiem saistītās informācijas par datu plūsmu konfidencialitāti piemērošanas jomu, saskaņā ar Tiesas pastāvīgo judikatūru ir jāinterpretē šauri (skat. pēc analogijas spriedumu, 2012. gada 22. novembris, *Probst*, C-119/12, EU:C:2012:748, 23. punkts). Šāda tiesību norma tātad nevar pamatot, ka atkāpe no šī vispārējā principa, it īpaši no aizlieguma uzglabāt šos datus, kas paredzēts šīs direktīvas 5. pantā, kļūst par normu, pretējā gadījumā tiktu būtiski sašaurināta šīs tiesību normas piemērošanas joma.
- 90 Šajā ziņā ir jānorāda, ka Direktīvas 2002/58 15. panta 1. punkta pirmajā teikumā ir paredzēts, ka tiesību aktu, uz kuriem tas attiecas un kuros ir paredzēta atkāpe no sakaru un ar tiem saistītās informācijas par datu plūsmu konfidencialitātes principa, mērķis ir “[garantēt] valsts drošību, aizsardzību, sabiedrības drošību un kriminālpārskatību [noziedzīgu nodarījumu] vai elektroniskās komunikāciju sistēmas nevēlamas izmantošanas novēršanu, izmeklēšanu, noteikšanu [atklāšanu] un kriminālvajāšanu” vai sasniegt kādu no pārējiem mērķiem, kas paredzēti Direktīvas 95/46 13. panta 1. punktā, uz kuru norāda Direktīvas 2002/58 15. panta 1. punkta pirmais teikums (šajā ziņā skat. spriedumu, 2008. gada 29. janvāris, *Promusicae*, C-275/06, EU:C:2008:54, 53. punkts). Šāds mērķu uzskaitījums ir uzskatāms par izsmeltošu, kā arī izriet no šīs pēdējās minētās direktīvas 15. panta 1. punkta otrā teikuma, saskaņā ar kuru tiesību akti ir jāpamato ar kādu no minētās direktīvas 15. panta 1. punkta pirmajā teikumā “noteiktajiem iemesliem [mērķiem]”. Tātad dalībvalstis nevar pieņemt šādus pasākumus citu mērķu dēļ, kuri nav uzskaitīti Direktīvas 2002/58 15. panta 1. punkta pirmajā teikumā.
- 91 Turklāt Direktīvas 2002/58 15. panta 1. punkta trešajā teikumā ir paredzēts, ka “vis[us] [šīs direktīvas 15. panta 1. punktā] minēt[os] pasākum[us] [tiesību aktus] [pieņem] saskaņā ar [Savienības] tiesību aktu vispārējiem principiem, tostarp tie[m], kas minēti Eiropas Savienības dibināšanas līguma 6. panta 1. un 2. punktā”, kuri ietver arī vispārējus principus un pamattiesības, kuras kopš attiecīgā laika ir garantētas ar Hartu. Direktīvas 2002/58 15. panta 1. punkts tātad ir jāinterpretē ar Hartu garantēto pamattiesību gaismā (pēc analogijas attiecībā uz Direktīvu 95/46 skat. spriedumus, 2003. gada 20. maijs, *Österreichischer Rundfunk* u.c., C-465/00, C-138/01 un C-139/01, EU:C:2003:294, 68. punkts; 2014. gada 13. maijs, *Google Spain* un *Google*, C-131/12, EU:C:2014:317, 68. punkts, kā arī 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 38. punkts).
- 92 Šajā ziņā ir jāuzsver, ka ar tādu valsts tiesisko regulējumu kā pamatlietā aplūkotsais elektronisko sakaru pakalpojumu sniedzējiem noteiktais pienākums saglabāt informāciju par [datu] plūsmu, lai to vajadzības gadījumā padarītu pieejamu kompetentajām valsts iestādēm, izraisa jautājumus ne tikai par Hartas 7. un 8. panta ievērošanu, kuri ir tieši norādīti prejudiciālajos jautājumos, bet arī par Hartas 11. pantā garantēto vārda brīvību (pēc analogijas attiecībā uz Direktīvu 2006/24 skat. spriedumu *Digital Rights*, 25. un 70. punkts).
- 93 Tātad gan Hartas 7. pantā garantēto tiesību uz privātās dzīves neaizskaramību, gan arī tās 8. pantā garantēto tiesību uz personas datu aizsardzību nozīmīgums, kāds tas izriet no Tiesas judikatūras (šajā ziņā skat. spriedumu, 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 39. punkts un tajā minētā judikatūra), ir jāņem vērā, interpretējot Direktīvas 2002/58 15. panta 1. punktu. Tā tas ir arī attiecībā uz vārda brīvību, ņemot vērā īpašo nozīmi, kas piemīt šai brīvībai jebkurā demokrātiskā sabiedrībā. Šīs pamattiesības, kas garantētas Hartas 11. pantā, veido vienu no demokrātiskas un plurālistiskas sabiedrības būtiskajiem pamatiem, kas ir to vērtību starpā, uz kurām pamatojoties saskaņā ar LES 2. pantu ir dibināta Savienība (šajā ziņā skat. spriedumus, 2003. gada 12. jūnijs, *Schmidberger*, C-112/00, EU:C:2003:333, 79. punkts, un 2011. gada 6. septembris, *Patriciello*, C-163/10, EU:C:2011:543, 31. punkts).
- 94 Šajā ziņā ir jāatgādina, ka saskaņā ar Hartas 52. panta 1. punktu visiem tajā atzīto tiesību un brīvību izmantošanas ierobežojumiem ir jābūt noteiktiem tiesību aktos un tajos ir jārespektē šo tiesību un brīvību būtība. Ievērojot samērīguma principu, šo tiesību un brīvību izmantošanas ierobežojumus

drīkst noteikt tikai tad, ja tie ir nepieciešami un patiešām atbilst vispārējo interešu mērķiem, ko atzinusi Savienība, vai vajadzībai aizsargāt citu personu tiesības un brīvības (spriedums, 2016. gada 15. februāris, N., C-601/15 PPU, EU:C:2016:84, 50. punkts).

- 95 Attiecībā uz šo pēdējo minēto aspektu Direktīvas 2002/58 15. panta 1. punkta pirmajā teikumā ir paredzēts, ka dalībvalstis var pieņemt tiesību aktu, atkāpjoties no sakaru un ar tiem saistītās informācijas par datu plūsmu konfidencialitātes principa, ja šis tiesību akts ir “nepieciešam[s], atbilstīg[s] un samērīg[s] [...] demokrātiskā sabiedrībā”, ņemot vērā šajā tiesību normā paredzētos mērķus. Šis direktīvas preambulas 11. apsvērumā ir precizēts, ka šādam tiesību aktam ir jābūt “stingri” samērīgam ar paredzēto nolūku. It īpaši attiecībā uz datu saglabāšanu minētās direktīvas 15. panta 1. punkta otrajā teikumā ir prasīts, lai tā notiktu “ierobežotā laikposmā”, “kas pamatots ar” kādu no šīs pašas direktīvas 15. panta 1. punkta pirmajā teikumā noteiktajiem pamatiem.
- 96 Samērīguma principa ievērošana izriet arī no Tiesas pastāvīgās judikatūras, saskaņā ar kuru pamattiesību uz privātās dzīves neaizskaramību aizsardzības Savienības limenī pamatā ir prasība, lai atkāpes no personas datu aizsardzības un tās ierobežojumi tiktu īstenoti absolūti nepieciešamā ietvaros (spriedumi, 2008. gada 16. decembris, *Satakunnan Markkinapörssi un Satamedia*, C-73/07, EU:C:2008:727, 56. punkts; 2010. gada 9. novembris, *Volker und Markus Schecke un Eifert*, C-92/09 un C-93/09, EU:C:2010:662, 77. punkts; *Digital Rights*, 52. punkts, kā arī 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 92. punkts).
- 97 Attiecībā uz to, vai tāds valsts tiesiskais regulējums kā lietā C-203/15 aplūkots, atbilst šiem nosacījumiem, ir jānorāda, ka tajā ir paredzēta visaptveroša un nediferencēta visas informācijas attiecībā uz datu plūsmu un atrašanās vietas datiem attiecībā uz visiem abonentiem un reģistrētiem lietotājiem saistībā ar visiem elektronisko sakaru līdzekļiem saglabāšana un ka tajā ir paredzēts pienākums elektronisko saziņu pakalpojumu sniedzējiem saglabāt šos datus sistemātiski un nepārtraukti, neizdarot nevienu izņēmumu. Tādējādi, kā izriet no iesniedzējtiesas nolēmuma, šajā tiesību aktā paredzētās datu kategorijas būtībā atbilst tām, kuru saglabāšana bija paredzēta Direktīvā 2006/24.
- 98 Dati, kuri tādējādi ir jāsaglabā elektronisko pakalpojumu sniedzējiem, ļauj atrast un identificēt saziņas avotu un tās adresātu, noteikt saziņas datumu, laiku, ilgumu un veidu, lietotāju izmantoto saziņas aparātu, kā arī noteikt mobilās saziņas aparāta atrašanās vietu. Šie dati ietver tostarp abonenta vai reģistrētā lietotāja vārdu un adresi, izsaucēja telefona numuru un zvana adresāta telefona numuru, kā arī IP adresi interneta pakalpojumiem. Šie dati it īpaši ļauj uzzināt, ar kuru personu abonents vai reģistrētais lietotājs ir sazinājies un kādu sakaru līdzekli viņš ir izmantojis, kā arī ļauj noteikt saziņas laiku un vietu, no kuras šī saziņa notikusi. Turklāt šie dati ļauj noskaidrot abonenta un reģistrēta lietotāja saziņas ar noteiktām personām biežumu noteiktā laikposmā (pēc analogijas attiecībā uz Direktīvu 2006/24 skat. spriedumu *Digital Rights*, 26. punkts).
- 99 Šie dati kopumā var ļaut izdarīt ļoti precīzus secinājumus par personu, kuru dati tikuši saglabāti, privāto dzīvi, proti, ikdienas paradumiem, pastāvīgajām vai pagaidu uzturēšanās vietām, ikdienas vai citām gaitām, veiktajām darbībām, šo personu sociālajiem kontaktiem un aprindām, kurās tās mēdz uzturēties (pēc analogijas attiecībā uz Direktīvu 2006/24 skat. spriedumu *Digital Rights*, 27. punkts). It īpaši, kā norādījis ģenerāladvokāts savu secinājumu 253., 254. un 257.–259. punktā, šie dati sniedz iespējas noteikt attiecīgo personu profilu, kas kontekstā ar tiesībām uz privātās dzīves neaizskaramību ir tikpat sensitīva informācija kā pats šis saziņas saturs.
- 100 Šādā tiesiskajā regulējumā ietvertā iejaukšanās ar Hartas 7. un 8. pantu paredzētajās pamattiesībās ir atzīstama par ļoti plašu un tā ir jāuzskata par īpaši nopietnu. Apstāklis, ka datu saglabāšanu veic, par to neinformējot elektronisko sakaru pakalpojumu lietotājus, attiecīgo personu apziņā var radīt sajūtu, ka to privātā dzīve tiek pastāvīgi uzraudzīta (pēc analogijas attiecībā uz Direktīvu 2006/24 skat. spriedumu *Digital Rights*, 37. punkts).

- 101 Pat ja ar šādu tiesisko regulējumu nav atļauta saziņas satura saglabāšana un tādējādi netiek apdraudēts minēto tiesību būtisks saturs (pēc analogijas attiecībā uz Direktīvu 2006/24 skat. spriedumu *Digital Rights*, 39. punkts), informācijas par datu plūsmu un atrašanās vietas datu saglabāšanai tomēr var būt ietekme uz elektronisko sakaru līdzekļu izmantošanu un līdz ar to uz to, kā šo līdzekļu lietotāji īsteno viņiem Hartas 11. pantā garantēto vārda brīvību (pēc analogijas attiecībā uz Direktīvu 2006/24 skat. spriedumu *Digital Rights*, 28. punkts).
- 102 Ņemot vērā iejaukšanās konkrētajās pamattiesībās smagumu valsts tiesiskajā regulējumā, kurā noziedzības apkarošanas nolūkā ir paredzēta informācijas par datu plūsmu un atrašanās vietas datu saglabāšana, vienīgi smago noziegumu apkarošana var pamatot šādu tiesību aktu (pēc analogijas attiecībā uz Direktīvu 2006/24 skat. spriedumu *Digital Rights*, 60. punkts).
- 103 Turklāt, ja smago noziegumu apkarošanas, kas it īpaši vērsta pret organizēto noziedzību un terorismu, efektivitāte var lielā mērā būt atkarīga no moderno izmeklēšanas tehniku izmantošanas, šāds vispārējo interešu mērķis, lai cik būtisks tas nebūtu, pats par sevi nevar pamatot, ka valsts tiesiskais regulējums, kurā paredzēta visas informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta saglabāšana, tiek uzskatīts par nepieciešamu minētās apkarošanas mērķiem (pēc analogijas attiecībā uz Direktīvu 2006/24 skat. spriedumu *Digital Rights*, 51. punkts).
- 104 Šajā ziņā ir jānorāda, pirmkārt, ka šāda tiesiskā regulējuma sekas, ņemot vērā šī sprieduma 97. punktā raksturotās pazīmes, ir tādas, ka informācijas par datu plūsmu un atrašanās vietas datu saglabāšana kļūst par normu, lai gan ar Direktīvu 2002/58 ieviestā kārtība prasa, lai šādu datu saglabāšana būtu izņēmums.
- 105 Otrkārt, tādā valsts tiesiskajā regulējumā kā pamatlietā aplūkotajā – kurš vispārīgi attiecas uz visiem abonentiem un reģistrētajiem lietotājiem un attiecas uz visiem elektronisko sakaru līdzekļiem, kā arī visu informāciju par datu plūsmu – nav paredzēta nekāda diferencēšana, ierobežojumi vai izņēmumi atkarībā no sasniedzamā mērķa. Tas vispārīgi attiecas uz visām personām, kuras izmanto elektronisko sakaru pakalpojumus, lai gan šīs personas pat netieši neatrodas situācijā, kurā var tikt piemērota kriminālvajāšana. Tas ir piemērojams pat attiecībā uz personām, par kurām nepastāv nekādas norādes, kas var ļaut uzskatīt, ka to rīcībai varētu būtu kaut netieša vai attālināta saikne ar smagiem noziegumiem. Turklāt tajā nav paredzēts neviens izņēmums, kā rezultātā to piemēro pat personām, uz kuru sakariem saskaņā ar valsts tiesību normām attiecas dienesta noslēpums (pēc analogijas attiecībā uz Direktīvu 2006/24 skat. spriedumu *Digital Rights*, 57. un 58. punkts).
- 106 Šāds tiesiskais regulējums neprasa nekādu saikni starp datiem, kurus ir paredzēts saglabāt, un draudiem sabiedrības drošībai. Tostarp tajā nav paredzēta vienīgi ierobežota saglabāšana, kas attiecas vai nu uz datiem saistībā ar kādu laikposmu un/vai ģeogrāfisku teritoriju un/vai personu loku, kuras var vienā vai otrā veidā būt iesaistītas smagā noziegumā, vai arī uz personām, kuru datu saglabāšana citu iemeslu dēļ varētu dot ieguldījumu noziegumu apkarošanā (pēc analogijas attiecībā uz Direktīvu 2006/24 skat. spriedumu *Digital Rights*, 59. punkts).
- 107 Tāds valsts tiesiskais regulējums kā pamatlietā aplūkotais tātad pārsniedz to, kas ir absolūti nepieciešams un nevar tikt uzskatīts par pamatotu demokrātiskā sabiedrībā, kā arī to prasa Direktīvas 2002/58 15. panta 1. punkts, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā.
- 108 Savukārt Direktīvas 2002/58 15. panta 1. punkts, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, nav pretrunā tam, ka dalībvalsts pieņem tiesisku regulējumu, ar ko preventīvi atļauts saglabāt iepriekš definētu informāciju par datu plūsmu un atrašanās vietas datus smagu noziegumu apkarošanas nolūkā ar nosacījumu, ka datu saglabāšana attiecībā uz saglabājamo datu kategorijām, iepriekš identificētiem saziņas līdzekļiem, attiecīgajām personām, kā arī noteikto saglabāšanas ilgumu aptver tikai absolūti nepieciešamo.

- 109 Lai nodrošinātu atbilstību šī sprieduma iepriekšējā punktā minētajām prasībām, šajā valsts tiesiskajā regulējumā, pirmkārt, ir jāparedz skaidri un precīzi noteikumi, kas reglamentē šāda datu saglabāšanas pasākuma apjomu un piemērošanu un nosaka minimālās prasības, lai personām, kuru dati tikuši saglabāti, būtu pietiekamas garantijas, kas ļauj efektīvi aizsargāt to personas datus pret ļaunprātīgu izmantošanu. Tajā it īpaši ir jānorāda, kādos apstākļos un saskaņā ar kādiem nosacījumiem datu saglabāšanas pasākums var preventīvi tikt veikts, tādējādi nodrošinot, ka šāds pasākums tiek ierobežots ar absolūti nepieciešamo (pēc analogijas attiecībā uz Direktīvu 2006/24 skat. spriedumu *Digital Rights*, 54. un tajā minētā judikatūra).
- 110 Otrkārt, attiecībā uz materiālajiem nosacījumiem, kuriem ir jāatbilst valsts tiesiskajam regulējumam, kas noziedzības apkarošanas ietvaros ļauj preventīvi saglabāt informāciju par datu plūsmu un atrašanās vietas datus, lai nodrošinātu, ka datu saglabāšana ir ierobežota ar absolūti nepieciešamo, ir jānorāda, ka, lai gan šie nosacījumi var atšķirties atkarībā no veiktajiem pasākumiem smagu noziegumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas nolūkā, datu saglabāšanai ir vienmēr jāatbilst objektīviem kritērijiem, ar kuriem konstatē saikni starp saglabājamajiem datiem un sasniedzamo mērķi. It īpaši šādiem nosacījumiem praktiski ir jābūt tādiem, kas faktiski ierobežo pasākuma apmēru un secīgi arī attiecīgo personu loku.
- 111 [Ar labojumiem, kas izdarīti ar 2017. gada 16. marta rīkojumu] Attiecībā uz šāda pasākuma ierobežošanu attiecībā uz potenciāli iesaistītu personu loku un situācijām valsts tiesiskajam regulējumam ir jābūt balstītam uz objektīviem apstākļiem, kas ļauj definēt personu loku, kuru datiem var būt kaut vai netieša saikne ar smagiem noziegumiem, vienā vai otrā veidā dot ieguldījumu smagu noziegumu apkarošanā vai novērst būtisku sabiedrības drošības risku. Šādu ierobežošanu var nodrošināt, piemērojot ģeogrāfisku kritēriju, kad kompetentās valsts iestādes, pamatojoties uz objektīviem elementiem, uzskata, ka vienā vai vairākās ģeogrāfiskajās zonās pastāv augsts risks saistībā ar sagatavošanos šādiem noziegumiem vai to izdarīšanu.
- 112 Ņemot vērā visus iepriekš izklāstītos apsvērumus, uz pirmo jautājumu lietā C-203/15 ir jāatbild, ka 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 saglabāšana attiecībā uz visiem abonentiem un reģistrētiem lietotājiem un attiecībā uz visiem elektronisko sakaru līdzekļiem.

Par otro jautājumu lietā C-203/15 un pirmo jautājumu lietā C-698/15

- 113 Vispirms ir jānorāda, ka *Kammarrätten i Stockholm* (Administratīvā apelācijas tiesa Stokholmā) otro jautājumu lietā C-203/15 ir uzdevusi tikai gadījumam, ja minētajā lietā atbilde uz pirmo jautājumu būtu noliedzīga. Tomēr šis otrais jautājums ir neatkarīgs no datu saglabāšanas vispārējā vai iepriekš selektīvi noteiktā rakstura šī sprieduma 108.–111. punkta izpratnē. Līdz ar to atbilde uz otro jautājumu lietā C-203/15 ir jāsniedz kopā ar atbildi uz pirmo jautājumu lietā C-698/15, kurš ir uzdots neatkarīgi no datu saglabāšanas pienākuma apjoma, kāds tiktu noteikts elektronisko sakaru pakalpojumu sniedzējiem.
- 114 Ar otro jautājumu lietā C-203/15 un pirmo jautājumu lietā C-698/15 iesniedzējtiesas būtībā vēlas noskaidrot, vai Direktīvas 2002/58 15. panta 1. punkts, lasot to Hartas 7. un 8. panta, kā arī 52. panta 1. punkta gaismā, ir jāinterpretē tādējādi, ka tam pretrunā ir valsts tiesiskais regulējums, kas reglamentē informācijas par datu plūsmu un atrašanās vietas datu aizsardzību un drošību, it īpaši valsts kompetento iestāžu piekļuvi saglabātajiem datiem, nenosakot, ka šo piekļuvi piešķir vienīgi saistībā ar smagu noziegumu apkarošanu; nepakļaujot šo piekļuvi iepriekšējai tiesas vai neatkarīgas administratīvas iestādes veiktai kontrolei un neprasot, lai konkrētie dati tiktu paturēti Savienības teritorijā.

- 115 Attiecībā uz mērķiem, kas var pamatot valsts tiesisko regulējumu, kurā ir paredzēta atkāpe no elektronisko sakaru konfidencialitātes principa, ir jāatgādina, ka, ciktāl, kā konstatēts šī sprieduma 90.–102. punktā, Direktīvas 2002/58 15. panta 1. punkta pirmajā teikumā paredzēto mērķu uzskaitījums ir izsmēlošs, piekļuvei saglabājamiem datiem patiešām stingri ir jāatbilst vienam no šiem mērķiem. Turklāt, tā kā ar šo tiesisko regulējumu sasniedzamajam mērķim ir jābūt saskaņotam ar iejaukšanās pamattiesībās nopietnības pakāpi, ko izraisa šī piekļuve, no tā izriet, ka noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas jomā vienīgi smagu noziegumu apkarošana var pamatot šādu piekļuvei saglabājamiem datiem.
- 116 Attiecībā uz samērīguma principa ievērošanu valsts tiesiskajam regulējumam, kas reglamentē nosacījumus, saskaņā ar kuriem elektronisko sakaru pakalpojumu sniedzēji kompetentajām valsts iestādēm piešķir piekļuvei saglabājamiem datiem, saskaņā ar šī sprieduma 95. un 96. punktā konstatēto ir jānodrošina, ka šāda piekļuve tiek ierobežota ar absolūti nepieciešamo.
- 117 Turklāt, tā kā Direktīvas 2002/58 15. panta 1. punktā paredzētajiem tiesību aktiem saskaņā ar šīs direktīvas preambulas 11. apsvērumu ir “jāatbilst attiecīgajiem drošības pasākumiem”, tādā tiesību aktā, kā izriet no šī sprieduma 109. punktā minētās judikatūras, ir jāparedz skaidri un precīzi noteikumi, kuros norāda, kādos apstākļos un saskaņā ar kādiem nosacījumiem elektronisko sakaru pakalpojumu sniedzēji kompetentajām valsts iestādēm sniedz piekļuvei datiem. Tāpat šādam tiesību aktam ir jābūt valsts tiesībās juridiski saistošam.
- 118 Lai nodrošinātu to, ka kompetento valsts iestāžu piekļuve saglabājamiem datiem aprobežojas ar absolūti nepieciešamo, protams, valsts tiesībās ir jānosaka nosacījumi, kādos elektronisko sakaru pakalpojumu sniedzējiem piešķir šādu piekļuvei. Tomēr attiecīgajā valsts tiesiskajā regulējumā nevar vienīgi ietvert prasību, lai piekļuve atbilstu kādam no Direktīva 2002/58 15. panta 1. punktā paredzētajiem mērķiem, pat ja to pamato ar smagu noziegumu apkarošanu. Proti, šādā valsts tiesiskajā regulējumā ir arī jāparedz materiālie un procesuālie nosacījumi, kas reglamentē kompetento valsts iestāžu piekļuvei saglabājamiem datiem (pēc analogijas attiecībā uz Direktīvu 2006/24 skat. spriedumu *Digital Rights*, 61. punkts).
- 119 Tātad, tā kā vispārēja piekļuve visiem saglabājamiem datiem, kas nav atkarīga no jebkādas kaut arī netiešas saiknes ar sasniedzamo mērķi, nevar tikt uzskatīta par tādu, kas aprobežojas ar absolūti nepieciešamo, attiecīgajam valsts tiesiskajam regulējumam ir jābalstās uz objektīviem kritērijiem, lai definētu apstākļus un nosacījumus, saskaņā ar kuriem kompetentajām valsts iestādēm piešķir piekļuvei abonentu vai reģistrēto lietotāju datiem. Šajā ziņā piekļuvei principā saistībā ar mērķi apkarot noziedzību var piešķirt vienīgi to personu datiem, kuras tiek turētas aizdomās par smaga nozieguma plānošanu, sagatavošanu tam vai tā izdarīšanu vai arī kuras vienā vai otrā veidā ir saistītas ar šādu noziegumu (skat. pēc analogijas, ECT, 2015. gada 4. decembris, *Zakharov* pret Krieviju, CE:ECHR:2015:1204JUD004714306, 260. punkts). Tomēr īpašos gadījumos, proti, kad vitāli svarīgas valsts drošības, aizsardzības vai sabiedrības drošības intereses apraud teroristiskas darbības, piekļuvei var piešķirt arī citu personu datiem, ja pastāv objektīvi apstākļi, kas ļauj uzskatīt, ka šie dati konkrētajā gadījumā varētu sniegt efektīvu ieguldījumu šādu darbību apkarošanā.
- 120 Lai praksē nodrošinātu šo nosacījumu ievērošanu pilnībā, ir būtiski, ka kompetento valsts iestāžu piekļuve saglabājamiem datiem, izņemot atbilstoši pamatotus steidzamības gadījumus, principā ir pakļauta kontrolei, ko veic tiesa vai neatkarīga administratīva iestāde, un ka šīs tiesas vai šīs iestādes lēmums tiek pieņemts pēc tam, kad šīs iestādes iesniegušas pamatotu pieteikumu tostarp saistībā ar noziedzīga nodarījuma novēršanu, atklāšanu vai kriminālvajāšanas procedūrām (pēc analogijas attiecībā uz Direktīvu 2006/24 skat. spriedumu *Digital Rights*, 62. punkts; skat. arī pēc analogijas attiecībā uz ECPAK 8. pantu ECT, 2016. gada 12. janvāris, *Szabó* un *Vissy* pret Ungāriju, CE:ECHR:2016:0112JUD003713814, 77. un 80. punkts).

- 121 Tāpat ir būtiski, ka kompetentās valsts iestādes, kurām ir piešķirta piekļuve saglabātajiem datiem, par to informē attiecīgās personas atbilstoši piemērojamajām valsts procesuālajām normām no brīža, kad šī saziņa vairs nevar traucēt šo iestāžu veiktajai izmeklēšanai. Proti, šī informēšana faktiski ir nepieciešama, lai ļautu šīm personām to tiesību pārkāpuma gadījumā tostarp īstenot tiesības uz tiesisko aizsardzību, kas tieši paredzētas Direktīvas 2002/58 15. panta 2. punktā, lasot kopsakarā ar Direktīvas 95/46 22. pantu (skat. pēc analogijas spriedumus, 2009. gada 7. maijs, *Rijkeboer*, C-553/07, EU:C:2009:293, 52. punkts, kā arī 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 95. punkts).
- 122 Attiecībā uz noteikumiem par elektronisko sakaru pakalpojumu sniedzēju saglabātajiem datiem ir jākonstatē, ka ar Direktīvas 2002/58 15. panta 1. punktu dalībvalstīm nav atļauts atkāpties no tās 4. panta 1. punkta, kā arī 4. panta 1.a punkta. Šajās pēdējās minētajās tiesību normās ir paredzēts, ka šie pakalpojumu sniedzēji veic piemērotus tehniskus un organizatoriskus pasākumus, kas ļauj nodrošināt efektīvu saglabāto datu aizsardzību pret ļaunprātīgu izmantošanu, kā arī pret jebkāda cita veida prettiesisku piekļuvi šiem datiem. Ņemot vērā saglabāto datu apjomu, šo datu sensitīvo raksturu, kā arī prettiesiskas piekļuves šiem datiem risku, elektronisko sakaru pakalpojumu sniedzējiem minēto datu integritātes un konfidencialitātes nodrošināšanai pilnībā ir jāgarantē īpaši augsts aizsardzības līmenis ar piemērotiem tehniskiem un organizatoriskiem pasākumiem. It īpaši valsts tiesiskajā regulējumā ir jāparedz, ka [dati] netiek izpausti ārpus Savienības teritorijas, kā arī tas, ka dati pēc to saglabāšanas termiņa beigām tiek neatgriezeniski iznīcināti (pēc analogijas attiecībā uz Direktīvu 2006/24 skat. spriedumu *Digital Rights*, 66.–68. punkts).
- 123 Katrā ziņā dalībvalstīm ir jānodrošina, ka neatkarīga iestāde kontrolē ar Savienības tiesībām fizisku personu aizsardzības attiecībā uz personas datu apstrādi jomā garantētā aizsardzības līmeņa ievērošanu, kas ir kontrole, kāda ir tieši prasīta Hartas 8. panta 3. punktā un kura saskaņā ar Tiesas pastāvīgo judikatūru veido būtisku fizisku personu aizsardzības elementu saistībā ar personas datu apstrādi. Pretējā gadījumā personām, kuru personas dati ir tikuši saglabāti, tiktu liegtas Hartas 8. panta 1. un 3. punktā garantētās tiesības vērsties valsts uzraudzības iestādēs ar pieteikumu par viņu datu aizsardzību (šajā ziņā skat. spriedumus, *Digital Rights*, 68. punkts, kā arī 2015. gada 6. oktobris, *Schrems*, C-362/14, EU:C:2015:650, 41. un 58. punkts).
- 124 Iesniedzējtiesām ir jāpārbauda, vai un kādā mērā pamatlietā aplūkotajos tiesiskajos regulējumos ir ievērotas prasības, kas izriet no Direktīvas 2002/58 15. panta 1. punkta, lasot Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, kādas tās izklāstītas šī sprieduma 115.–123. punktā gan attiecībā uz kompetento valsts iestāžu piekļuvi saglabātajiem datiem, gan attiecībā uz šo datu aizsardzību un drošības līmeni.
- 125 Ņemot vērā visus iepriekš izklāstītos apsvērumus, uz otro jautājumu lietā C-203/15 un uz pirmo jautājumu lietā C-698/15 ir jāatbild, ka Direktīvas 2002/58 15. panta 1. punktu, lasot Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, ir jāinterpretē tādējādi, ka tam pretrunā ir tāds valsts tiesiskais regulējums, ar ko reglamentē informācijas par datu plūsmu un atrašanās vietas datu aizsardzību un drošību, it īpaši kompetento valsts iestāžu piekļuvi saglabātajiem datiem, saistībā ar noziedzības apkarošanu neierobežojot šo piekļuvi vienīgi ar smagās noziedzības apkarošanas mērķiem, nepakļaujot šo piekļuvi iepriekšējai tiesas vai neatkarīgas valsts iestādes kontrolei un neprasot, lai konkrētie dati netiktu izpausti ārpus Savienības teritorijas.

Par otro jautājumu lietā C-698/15

- 126 Ar otro jautājumu lietā C-698/15 *Court of Appeal (England & Wales) (Civil Division)* (Apelācijas tiesa (Anglija un Velsa) (Civillietu palāta)) būtībā vēlas noskaidrot, vai spriedumā *Digital Rights* Tiesa Hartas 7. un/vai 8. pantu ir interpretējusi nozīmē, kas pārsniedz to, kuru Eiropas Cilvēktiesību tiesa ir piešķirusi ECPAK 8. pantam.

- 127 Vispirms ir jāatgādina, ka, lai gan, kā apstiprināts LES 6. panta 3. punktā, ar ECPAK atzītās pamattiesības ietilpst Savienības tiesībās kā vispārējie principi, minētā konvencija, kamēr Savienība nav tai pievienojusies, nav Savienības tiesību sistēmā formāli integrēts juridisks instruments (skat. šajā ziņā spriedumu, 2016. gada 15. februāris, *N.*, C-601/15 PPU, EU:C:2016:84, 45. punkts un tajā minētā judikatūra).
- 128 Tādējādi Direktīvas 2002/58 interpretācija, par kuru ir runa šajā gadījumā, ir jāveic, ņemot vērā vienīgi Hartā garantētās pamattiesības (skat. šajā ziņā spriedumu, 2016. gada 15. februāris, *N.*, C-601/15 PPU, EU:C:2016:84, 46. punkts un tajā minētā judikatūra).
- 129 Turklāt ir jāatgādina, ka uz Hartas 52. pantu attiecināmie paskaidrojumi norāda, ka tās 52. panta 3. punkts ir vērsts uz to, lai nodrošinātu nepieciešamo saskaņotību ar Hartu un ECPAK, "tomēr negatīvi neietekmējot Savienības tiesību aktu un Eiropas Savienības Tiesas autonomiju" (spriedums, 2016. gada 15. februāris, *N.*, C-601/15 PPU, EU:C:2016:84, 47. punkts). It īpaši, kā tieši paredzēts Hartas 52. panta 3. punkta otrajā teikumā, tās 52. panta 3. punkta pirmais teikums neliedz Savienības tiesībās paredzēt plašāku aizsardzību par to, kāda paredzēta ECPAK. Papildus tam Hartas 8. pants attiecas uz pamattiesībām, kas ir nošķirtas no tām, kuras paredzētas tās 7. pantā un kurām nav identiskas pamattiesības ECPAK.
- 130 Saskaņā ar Tiesas pastāvīgo judikatūru pamats prejudiciāla jautājuma uzdošanai ir nevis konsultatīva viedokļa izteikšana par vispārīgiem vai hipotētiskiem jautājumiem, bet gan vajadzība faktiski iztiesāt lietu, kas saistīta ar Savienības tiesībām (šajā ziņā skat. spriedumus, 2012. gada 24. aprīlis, *Kamberaj*, C-571/10, EU:C:2012:233, 41. punkts; 2013. gada 26. februāris, *Åkerberg Fransson*, C-617/10, EU:C:2013:105, 42. punkts, kā arī 2014. gada 27. februāris, *Pohotovost*, C-470/12, EU:C:2014:101, 29. punkts).
- 131 Konkrētajā gadījumā, ņemot vērā šī sprieduma 128. un 129. punktā norādītos apsvērumus, jautājums par to, vai ar Hartas 7. un 8. punktu piešķirtā aizsardzība pārsniedz ar ECPAK 8. pantu garantēto aizsardzību, neskar Direktīvas 2002/58 interpretāciju, lasot Hartas gaismā, kas ir pamatlietā, proti, lietā C-698/15, aplūkots jautājums.
- 132 Tādējādi nešķiet, ka atbilde uz otro jautājumu lietā C-698/15 varētu sniegt norādes Savienības tiesību interpretācijai, kas, ņemot vērā šīs tiesības, ir nepieciešamas minētā strīda risinājumam.
- 133 Līdz ar to otrais jautājums lietā C-698/15 ir nepieņemams.

Par tiesāšanās izdevumiem

- 134 Attiecībā uz pamatlietu pusēm šī tiesvedība ir stadija procesā, kuru izskata iesniedzējtiesas, un tās 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 2002. gada 12. jūlija Direktīvas 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privātās dzīves aizsardzību un elektroniskajām komunikācijām), kurā grozījumi ir izdarīti ar Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīvu 2009/136/EK, 15. panta 1. punkts, lasot to Eiropas Savienības Pamattiesību 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 saglabāšana attiecībā uz visiem abonentiem un reģistrētiem lietotājiem un attiecībā uz visiem elektronisko sakaru līdzekļiem;

- 2) Direktīvas 2002/58, kurā grozījumi ir izdarīti ar Direktīvu 2009/136, 15. panta 1. punkts, lasot Eiropas Savienības Pamattiesību hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, ir jāinterpretē tādējādi, ka tam pretrunā ir tāds valsts tiesiskais regulējums, ar ko reglamentē informācijas par datu plūsmu un atrašanās vietas datu aizsardzību un drošību, it īpaši kompetento valsts iestāžu piekļuvi saglabātajiem datiem, saistībā ar noziedzības apkarošanu neierobežojot šo piekļuvi vienīgi ar smagās noziedzības apkarošanas mērķiem, nepakļaujot šo piekļuvi iepriekšējai tiesas vai neatkarīgas valsts iestādes kontrolei un neprasot, lai konkrētie dati netiktu izpausti ārpus Savienības teritorijas;
- 3) otrais *Court of Appeal (England & Wales) (Civil Division)* (Apelācijas tiesa (Anglija un Velsa) (Civillietu palāta)) uzdotais jautājums ir nepieņemams.

[Paraksti]