Judikatūras krājums

TIESAS SPRIEDUMS (virspalāta)

2014. gada 8. aprīlī*

Elektroniskās komunikācijas — Direktīva 2006/24/EK — Publiski pieejami elektronisko komunikāciju pakalpojumi vai publiski pieejami komunikāciju tīkli — Tādu datu saglabāšana, kurus iegūst vai apstrādā saistībā ar šādu pakalpojumu sniegšanu — Spēkā esamība — Eiropas Savienības Pamattiesību hartas 7., 8. un 11. pants

Apvienotās lietas C-293/12 un C-594/12

par lūgumiem sniegt prejudiciālu nolēmumu atbilstoši LESD 267. pantam, ko *High Court* (Īrija) un *Verfassungsgerichtshof* (Austrija) iesniedza ar lēmumiem, kas pieņemti attiecīgi 2012. gada 27. janvārī un 2012. gada 28. novembrī un kas Tiesā reģistrēti 2012. gada 11. jūnijā un 2012. gada 19. decembrī, tiesvedībās

Digital Rights Ireland Ltd (C-293/12)

pret

Minister for Communications, Marine and Natural Resources,

Minister for Justice, Equality and Law Reform,

Commissioner of the Garda Síochána,

Īriju,

The Attorney General,

piedaloties

Irish Human Rights Commission,

un

Kärntner Landesregierung (C-594/12),

Michael Seitlinger,

Christof Tschohl u.c.

* Tiesvedības valodas – angļu un vācu.

TIESA (virspalāta)

šādā sastāvā: priekšsēdētājs V. Skouris [*V. Skouris*], priekšsēdētāja vietnieks K. Lēnartss [*K. Lenaerts*], palātu priekšsēdētāji A. Ticano [*A. Tizzano*], R. Silva de Lapuerta [*R. Silva de Lapuerta*], T. fon Danvics [*T. von Danwitz*] (referents), E. Juhāss [*E. Juhász*], E. Borgs Bartets [*A. Borg Barthet*], K. G. Fernlunds [*C. G. Fernlund*] un Ž. L. da Krušs Vilasa [*J. L. da Cruz Vilaça*], tiesneši A. Ross [*A. Rosas*], Dž. Arestis [*G. Arestis*], Ž. K. Bonišo [*J.-C. Bonichot*], A. Arabadžijevs [*A. Arabadjiev*], K. Toadere [*C. Toader*] un K. Vajda [*C. Vajda*],

ģenerāladvokāts P. Kruss Viljalons [*P. Cruz Villalón*],

sekretārs K. Malaceks [*K. Malacek*], administrators,

ņemot vērā rakstveida procesu un 2013. gada 9. jūlija tiesas sēdi,

ņemot vērā apsvērumus, ko sniedza:

— *Digital Rights Ireland Ltd* vārdā – *F. Callanan*, *SC*, un *F. Crehan*, *BL*, kurus pilnvarojis *S. McGarr*, *solicitor*,

— *M. Seitlinger* vārdā – *G. Otto*, *Rechtsanwalt*,

— *C. Tschohl* u.c. vārdā – *E. Scheucher*, *Rechtsanwalt*,

— *Irish Human Rights Commission* vārdā – *P. Dillon Malone*, *BL*, kuru pilnvarojusi *S. Lucey*, *solicitor*,

— Īrijas vārdā – *E. Creedon* un *D. McGuinness*, pārstāvji, kuriem palīdz *E. Regan*, *SC*, un *D. Fennelly*, *JC*,

— Austrijas valdības vārdā – *G. Hesse* un *G. Kunnert*, pārstāvji,

— Spānijas valdības vārdā – *N. Díaz Abad*, pārstāve,

— Francijas valdības vārdā – *G. de Bergues* un *D. Colas*, kā arī *B. Beaupère-Manokha*, pārstāvji,

— Itālijas valdības vārdā – *G. Palmieri*, pārstāve, kurai palīdz *A. De Stefano*, *avvocato dello Stato*,

— Polijas valdības vārdā – *B. Majczyna* un *M. Szpunar*, pārstāvji,

— Portugāles valdības vārdā – *L. Inez Fernandes* un *C. Vieira Guerra*, pārstāvji,

— Apvienotās Karalistes valdības vārdā – *L. Christie*, pārstāvis, kam palīdz *S. Lee*, *barrister*,

— Eiropas Parlamenta vārdā – *U. Rösslein* un *A. Caiola*, kā arī *K. Zejdová*, pārstāvji,

— Eiropas Savienības Padomes vārdā – *J. Monteiro* un *E. Sitbon*, kā arī I. Šulce, pārstāvji,

— Eiropas Komisijas vārdā – *D. Maidani*, kā arī *B. Martenczuk* un *M. Wilderspin*, pārstāvji,

noklausījusies ģenerāladvokāta secinājumus 2013. gada 12. decembra tiesas sēdē,

pasludina šo spriedumu.

Spriedums

1 Lūgumi sniegt prejudiciālu nolēmumu ir par 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 L 105, 54. lpp.) spēkā esamību.

2 *High Court* iesniegtais lūgums (lieta C-293/12) attiecas uz tiesvedību starp *Digital Rights Ireland Ltd.* (turpmāk tekstā – "*Digital Rights*") un *Minister for Communications, Marine and Natural Resources* [Komunikāciju, jūras un dabas resursu ministru], *Minister for Justice, Equality and Law Reform* [Tieslietu, līdztiesības un likumu reformu ministru], *Commissioner of the Garda Síochána* [Īrijas policijas priekšnieku], kā arī *Attorney General* [Īrijas valsts augstāko tieslietu ierēdni] par tiesību un administratīvo aktu par tādu datu saglabāšanu, kas saistīti ar elektroniskajām komunikācijām, tiesiskumu.

3 *Verfassungsgerichtshof* iesniegtais lūgums (lieta C-594/12) attiecas uz konstitucionālajām prasībām, kuras šajā tiesā cēla attiecīgi *Kärntner Landesregierung* (Karintijas Federālās zemes valdība), kā arī *M. Seitlinger*, *C. Tschohl* un 11 128 citi prasītāji par likuma, ar kuru Austrijas tiesībās transponēta Direktīva 2006/24, saderīgumu ar Federālo konstitūciju (*Bundes-Verfassungsgesetz*).

Atbilstošās tiesību normas

Direktīva 95/46/EK

4 Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvas 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV L 281, 31. lpp.) mērķis atbilstoši tās 1. panta 1. punktam ir aizsargāt fizisko personu pamattiesības un brīvības un jo īpaši viņu tiesības uz privātās dzīves neaizskaramību attiecībā uz personas datu apstrādi.

5 Attiecībā uz šādu datu apstrādes drošību šīs direktīvas 17. panta 1. punktā noteikts:

"Dalībvalstis paredz to, ka personas datu apstrādātājam jāīsteno atbilstoši tehniski un organizatoriski pasākumi, lai aizsargātu personas datus pret nejaušu vai nelikumīgu iznīcināšanu vai nejaušu pazaudēšanu, pārveidošanu, nesankcionētu atklāšanu vai piekļuvi, īpaši, ja apstrāde ietver datu pārraidi pa elektronisko sakaru tīklu, un pret visām citām nelikumīgām apstrādes formām.

Ņemot vērā tehnisko un organizatorisko pasākumu pašreizējo līmeni un to īstenošanas izmaksas, šādi pasākumi nodrošina apstrādes un aizsargājamo datu raksturīgajiem riskiem atbilstošu drošības pakāpi."

Direktīva 2002/58/EK

6 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 privāto dzīvi un elektronisko komunikāciju) (OV L 201, 37. lpp.), kas grozīta ar Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīvu 2009/136/EK (OV L 337, 11. lpp.; turpmāk tekstā – "Direktīva 2002/58"), mērķis atbilstoši tās 1. panta 1. punktam ir saskaņot dalībvalstu noteikumus, ar kuriem jānodrošina pamattiesību un pamatbrīvību līdzvērtīgs aizsardzības līmenis un it 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 aprite Eiropas Savienībā. Saskaņā ar šī paša panta 2. punktu šīs direktīvas noteikumi precizē un papildina Direktīvu 95/46 iepriekš 1. punktā minētajā nolūkā.

7 Attiecībā uz datu apstrādes drošību Direktīvas 2002/58 4. pantā paredzēts:

"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/EK, 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 izmainīšanas un no neatļautas vai nelikumīgas uzglabāšanas, apstrādes, piekļuves vai izpaušanas un

— nodrošina, ka tiek īstenota drošības politika saistībā ar personas datu apstrādi.

Attiecīgās valsts iestādes ir pilnvarotas veikt to pasākumu novērtējumu, ko veic publiski pieejamu elektronisko sakaru pakalpojumu sniedzēji, un publicēt ieteikumus par paraugpraksi attiecībā uz drošības līmeni, kāds jāsasniedz ar šiem pasākumiem.

2. Tīkla drošības pārkāpuma īpaša riska dēļ publiski pieejamu elektronisko komunikāciju pakalpojuma sniedzējam attiecīgie abonenti jāinformē par šādu risku, un, ja šis risks ir ārpus pakalpojuma sniedzēja pieņemto pasākumu darbības jomas, par jebkuriem tiesiskās aizsardzības līdzekļiem, iekļaujot norādi par iespējamām ietvertajām izmaksām."

8 Attiecībā uz komunikāciju un informācijas par datu plūsmu konfidencialitāti šīs direktīvas 5. panta 1. un 3. punktā noteikts:

"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/EK [ir] nodrošināts ar skaidru un visaptverošu informāciju, tostarp par apstrādes nolūku. Tas neliedz jebkādu tehnisku uzglabāšanu vai piekļuvi, kas paredzēta vienīgi, lai veiktu vai atvieglotu saziņas pārraidīšanu elektronisko komunikāciju tīklā, vai kas noteikti nepieciešama, lai sniegtu informācijas sabiedrības pakalpojumu, ko skaidri pieprasījis abonents vai lietotājs."

9 Saskaņā ar Direktīvas 2002/58 6. panta 1. punktu:

"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. pantu un 15. panta 1. punktu."

10 Direktīvas 2002/58 15. panta 1. punktā ir noteikts:

"Dalībvalstis var pieņemt tiesību aktus, lai ierobežotu šīs direktīvas 5. un 6. pantā, 8. panta 1., 2., 3. un 4. punktā un 9. pantā minēto tiesību un pienākumu darbības jomu, ja šādi ierobežojumi ir vajadzīgi saskaņā ar nepieciešamiem, atbilstīgiem un samērīgiem pasākumiem demokrātiskā sabiedrībā, lai garantētu valsts drošību, aizsardzību, sabiedrības drošību un krimināl pārkāpumu vai elektroniskās komunikāciju sistēmas nevēlamas izmantošanas novēršanu, izmeklēšanu, noteikšanu un krimināl vajāšanu, kā noteikts Direktīvas 95/46/EK 13. panta 1. punktā. Tālab dalībvalstis, cita starpā, var pieņemt tiesību aktus, paredzot datu saglabāšanu ierobežotā laikposmā, kas pamatots ar šajā punktā noteiktajiem iemesliem. Visi šajā punktā minētie pasākumi ir saskaņā ar Kopienas tiesību aktu vispārējiem principiem, tostarp tiem, kas minēti Eiropas Savienības dibināšanas līguma [Līguma par Eiropas Savienību] 6. panta 1. un 2. punktā."

Direktīva 2006/24

11 Konsultējusies ar tiesībsargājošo iestāžu, elektronisko komunikāciju nozares un datu aizsardzības ekspertu pārstāvjiem, 2005. gada 21. septembrī Komisija publiskoja politikas attiecībā uz noteikumiem par informācijas par datu plūsmas saglabāšanu alternatīvu ietekmes analīzi (turpmāk tekstā – "ietekmes analīze"). Pamatojoties uz šo analīzi, tika izstrādāts priekšlikums Eiropas Parlamenta un Padomes direktīvai par datu saglabāšanu, kuri apstrādāti saistībā ar publisko elektronisko sakaru pakalpojumu sniegšanu, ar ko labo Direktīvu 2002/58/EK (COM(2005) 438, galīgā redakcija; turpmāk tekstā – "direktīvas priekšlikums"), kas tika publiskots tai pašā dienā un kā rezultātā, pamatojoties uz EKL 95. pantu, tika pieņemta Direktīva 2006/24.

12 Direktīvas 2006/24 preambulas 4. apsvērumā ir noteikts:

"Direktīvas 2002/58/EK 15. panta 1. punktā izklāstīti nosacījumi, saskaņā ar kuriem dalībvalstis var ierobežot minētās direktīvas 5. pantā, 6. pantā, 8. panta 1., 2., 3. un 4. punktā un 9. pantā paredzēto tiesību un pienākumu darbības jomu. Šādiem ierobežojumiem ir jābūt pasākumiem, kas ir nepieciešami, atbilstīgi un demokrātiskas sabiedrības kontekstā samērīgi ar sabiedriskās kārtības uzturēšanas mērķiem, t.i., lai garantētu nacionālo drošību (t.i., valsts drošību), aizsardzību, sabiedrības drošību vai lai novērstu, izmeklētu, atklātu vai sodītu noziedzīgus nodarījumus vai elektronisko komunikāciju sistēmu neatļautu lietošanu."

13 Saskaņā ar Direktīvas 2006/24 preambulas 5. apsvēruma pirmo teikumu "vairākas dalībvalstis ir pieņēmušas tiesību aktus, kuri paredz, ka pakalpojumu sniedzēji saglabā datus noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un krimināl vajāšanas mērķiem".

14 Direktīvas 2006/24 preambulas 7.–11. apsvērums ir formulēti šādi:

"(7) Tieslietu un iekšlietu padomes 2002. gada 19. decembra secinājumos uzsvērts, ka sakarā ar elektronisko komunikāciju iespēju ievērojamo pieaugumu īpaši svarīgi ir dati, kuri attiecas uz elektronisko komunikāciju izmantošanu, un tāpēc tie ir vērtīgs līdzeklis noziedzīgu nodarījumu, jo īpaši organizētās noziedzības, novēršanai, izmeklēšanai, atklāšanai un krimināl vajāšanai.

(8) Deklarācijā par terorisma apkarošanu, kuru Eiropadome pieņēma 2004. gada 25. martā, doti norādījumi Padomei pārbaudīt pasākumus noteikumu izveidei pakalpojumu sniedzējiem attiecībā uz informācijas saglabāšanu par noslodzes datiem.

(9) Saskaņā ar [1950. gada 4. novembrī Roma parakstītās] Eiropas Cilvēktiesību konvencijas [Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas] 8. pantu ikvienam ir tiesības uz to, ka tiek respektēta viņa privātā dzīve un sarakste. Valsts iestādes var iejaukties, pārkāpjot šīs tiesības, tikai saskaņā ar tiesību aktiem un tikai tad, ja demokrātiskā sabiedrībā tas ir vajadzīgs, *inter alia*, lai

nodrošinātu valsts aizsardzību vai sabiedrisko drošību, nepieļautu nekārtības vai noziedzību vai aizsargātu cilvēku tiesības un brīvības. Tā kā datu saglabāšana ir izrādījusies tik nepieciešams un efektīvs izmeklēšanas līdzeklis tiesībaizsardzībai vairākās dalībvalstīs un jo īpaši nopietnos gadījumos, piemēram, saistībā ar organizēto noziedzību un terorismu, ir nepieciešams uz noteiktu laiku un ievērojot šajā direktīvā paredzētos nosacījumus nodrošināt, ka saglabātos datus dara pieejamus tiesībsargājošajām iestādēm. [..]

(10) 2005. gada 13. jūlijā Padome savā Deklarācijā par nosodījumu terora aktiem Londonā vēlreiz uzsvēra nepieciešamību pēc iespējas ātrāk pieņemt kopējus pasākumus attiecībā uz telekomunikāciju datu saglabāšanu.

(11) Ņemot vērā nozīmi, kāda noslodzes datiem un atrašanās vietas datiem ir noziedzīgu nodarījumu izmeklēšanā, atklāšanā un kriminālvajāšanā, par ko liecina vairāku dalībvalstu veiktie pētījumi un praktiskā pieredze, ir nepieciešams Eiropas līmenī nodrošināt, lai dati, kurus iegūst vai apstrādā publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzēji vai publiski pieejamu komunikāciju tīklu operatori, tiktu saglabāti noteiktu laiku, ievērojot šajā direktīvā paredzētos nosacījumus."

15 Minētās direktīvas preambulas 16., 21. un 22. apsvērumā ir precizēts:

"(16) Pakalpojumu sniedzējiem uzliktie pienākumi attiecībā uz pasākumiem datu kvalitātes nodrošināšanai, kas izriet no Direktīvas 95/46/EK 6. panta, un to pienākumi attiecībā uz pasākumiem konfidencialitātes un datu apstrādes drošības nodrošināšanai, kas izriet no minētās direktīvas 16. un 17. panta, pilnībā attiecas uz datu saglabāšanu šīs direktīvas nozīmē.

(21) Ņemot vērā to, ka šis direktīvas mērķus – proti, saskaņot pakalpojumu sniedzēju pienākumus attiecībā uz konkrētu datu saglabāšanu un šo datu pieejamības nodrošināšanu smagu noziegumu, kā noteikts katras dalībvalsts tiesību aktos, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem – nevar pietiekami labi sasniegt atsevišķās dalībvalstīs, un to, ka šīs direktīvas mēroga un iedarbības dēļ šos mērķus var labāk sasniegt Kopienas līmenī, Kopiena var pieņemt pasākumus saskaņā ar Līguma 5. pantā noteikto subsidiaritātes principu. Saskaņā ar minētajā pantā noteikto proporcionalitātes principu šajā direktīvā paredz vienīgi tos pasākumus, kas vajadzīgi šo mērķu sasniegšanai.

(22) Šī direktīva respektē pamattiesības un ievēro principus, kas jo īpaši ir atzīti Eiropas Savienības Pamattiesību hartā. Jo īpaši šīs direktīvas un Direktīvas 2002/58/EK mērķis ir pilnībā ievērot pilsoņu pamattiesības – respektu pret privāto dzīvi un komunikācijām un viņu personas datu aizsardzību, kā nostiprināts Hartas 7. un 8. pantā."

16 Direktīvā 2006/24 paredzēts publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzēju vai publiski pieejamu komunikāciju tīklu operatoru pienākums saglabāt noteiktus datus, kurus tie iegūst vai apstrādā. Šajā ziņā šīs direktīvas 1.–9., 11. un 13. pantā ir noteikts:

"1. pants

Priekšmets un darbības joma

1. Šīs direktīvas mērķis ir saskaņot dalībvalstu noteikumus attiecībā uz publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzēju vai publiski pieejamu komunikāciju tīklu operatoru pienākumiem, kas attiecas uz noteiktu datu, kurus tie iegūst vai apstrādā, saglabāšanu, lai nodrošinātu, ka šie dati ir pieejami smagu noziegumu, kas katrā dalībvalstī noteikti tiesību aktos, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem.

2. Šī direktīva attiecas uz noslodzes datiem 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.

2. pants

Definīcijas

1. Šajā direktīvā piemēro definīcijas, kas lietotas Direktīvā 95/46/EK, Eiropas Parlamenta un Padomes Direktīvā 2002/21/EK (2002. gada 7. marts) par kopējiem reglamentējošiem noteikumiem attiecībā uz elektronisko komunikāciju tīkliem un pakalpojumiem (pamatdirektīva) [..] un Direktīvā 2002/58/EK.

2. Šajā direktīvā:

a) "dati" ir noslodzes dati un atrašanās vietas dati, un ar tiem saistīti dati, kas ir nepieciešami abonenta vai lietotāja identificēšanai;

b) "lietotājs" ir jebkura juridiska persona vai fiziska persona, kas izmanto publiski pieejamu elektronisko komunikāciju pakalpojumu personīgiem vai uzņēmējdarbības mērķiem, ne vienmēr būdama šā pakalpojuma abonents;

c) "telefonijas pakalpojumi" ir izsaukumi (tostarp balss izsaukumi, balss pasts un konferences izsaukumi, un datu sūtīšana), papildpakalpojumi (tostarp izsaukumu pāradresācija un izsaukumu pārsūtīšana) un ziņojumu sūtīšanas un multimediju pakalpojumi (tostarp īsziņu pakalpojumi, paplašināts īsziņu formāts vai multivides pakalpojumi);

d) "lietotāja identifikators" ir unikāls identifikācijas numurs, ko piešķir personai, abonējot vai reģistrējot interneta piekļuves pakalpojumu vai interneta komunikāciju pakalpojumu;

e) "šūnas ID" ir tās šūnas identifikators, kurā mobilās telefonijas izsaukums ir radies vai izbeidzies;

f) "neveiksmīgs izsaukuma mēģinājums" ir komunikācija, ja tālruņa izsaukuma rezultātā veiksmīgi ir noticis savienojums, bet tas nav atbildēts, vai notikusi tīkla pārvaldības iejaukšanās.

3. pants

Pienākums saglabāt datus

1. Atkāpjoties no Direktīvas 2002/58/EK 5., 6. un 9. panta, dalībvalstis pieņem pasākumus, lai nodrošinātu, ka šīs direktīvas 5. pantā 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.

4. pants

Piekļuve datiem

Dalībvalstis pieņem pasākumus, lai nodrošinātu, ka saskaņā ar šo direktīvu saglabātie dati īpašos gadījumos un atbilstoši attiecīgās valsts tiesību aktiem tiek paredzēti vienīgi kompetentām valsts iestādēm. Procedūras, kas jāievēro, un nosacījumus, kas jāizpilda, lai saņemtu piekļuvi saglabātajiem datiem atbilstīgi nepieciešamības un proporcionalitātes [samērīguma] prasībām, visas dalībvalstis nosaka savos tiesību aktos, ņemot vērā attiecīgus Eiropas Savienības tiesību aktus vai starptautisko publisko tiesību aktus un jo īpaši ECPAK, kā to ir interpretējusi Eiropas Cilvēktiesību tiesa.

5. pants

Saglabājamo datu kategorijas

1. Dalībvalstis nodrošina šādu datu kategoriju saglabāšanu atbilstoši šai direktīvai:

a) dati, kuri ir nepieciešami, lai izsekotu un identificētu komunikācijas avotu:

   1) attiecībā uz fiksētā tīkla telefoniju un mobilo telefoniju:

      i) izsaucēja tālruņa numurs;

      ii) abonenta vai reģistrētā lietotāja vārds vai nosaukums un adrese;

   2) attiecībā uz interneta piekļuvi, interneta e-pastu un interneta telefoniju:

      i) piešķirtais(-ie) lietotāja identifikators(-i);

      ii) lietotāja identifikators un tālruņa numurs, kuri piešķirti ikvienai komunikācijai, kas ienāk publiskajā telefonu tīklā;

      iii) abonenta vai reģistrētā lietotāja vārds vai nosaukums un adrese, kuram komunikācijas laikā piešķirta interneta protokola (IP) adrese, lietotāja identifikators vai telefona numurs;

b) dati, kuri ir nepieciešami, lai identificētu komunikācijas galamērķi:

   1) attiecībā uz fiksētā tīkla telefoniju un mobilo telefoniju:

      i) izsaucamais(-ie) numur[s(-i)] (izsauktais telefona numurs vai numuri), un gadījumos, kad ir iesaistīti papildu pakalpojumi, tādi kā izsaukuma pārvade vai izsaukuma pāradresācija, numurs vai numuri, uz ko pāradresēti izsaukumi;

      ii) abonenta(-u) vai reģistrētā(-o) lietotāja(-u) vārds(-i) vai nosaukums(-i) un adrese(-s);

   2) attiecībā uz interneta e-pastu un interneta telefoniju:

      i) paredzētā(-o) interneta telefonijas izsaukuma saņēmēja(-u) lietotāja identifikators vai telefona numurs;

      ii) tā(-o) abonenta(-u) vai reģistrētā(-o) lietotāja(-u) vārds(-i) vai nosaukums(-i) un adrese(-s) un lietotāja identifikators, kurš(-i) ir paredzētais(-ie) komunikācijas saņēmējs(-i);

c) dati, kuri ir nepieciešami, lai noteiktu komunikācijas datumu, laiku un ilgumu:

1) attiecībā uz fiksētā tīkla telefoniju un mobilo telefoniju – komunikācijas sākuma un beigu datums un laiks;

2) attiecībā uz interneta piekļuvi, interneta e-pastu un interneta telefoniju:

i) interneta piekļuves pakalpojuma pieteikuma un atteikuma datums un laiks, pamatojoties uz noteiktu laika zonu, kopā ar IP dinamisko vai statisko adresi, kuru komunikācijai piešķīris interneta piekļuves pakalpojumu sniedzējs, un reģistrētā lietotāja vai abonenta lietotāja identifikators;

ii) interneta e-pasta pakalpojuma vai interneta telefonijas pieteikuma un atteikuma datums un laiks, pamatojoties uz noteiktu laika zonu;

d) dati, kuri ir nepieciešami, lai noteiktu komunikācijas veidu:

1) attiecībā uz fiksētā tīkla telefoniju un mobilo telefoniju: izmantotais telefonijas pakalpojums;

2) attiecībā uz interneta e-pastu un interneta telefoniju: izmantotais interneta pakalpojums;

e) dati, kuri ir nepieciešami, lai identificētu lietotāja komunikāciju aprīkojumu vai aprīkojumu, kas veic tā funkcijas:

1) attiecībā uz fiksētā tīkla telefoniju – izsaucamo telefona numuru vai telefona numuru, no kura veic izsaukumu;

2) attiecībā uz mobilo telefoniju:

i) izsaucamo telefona numuru vai telefona numuru, no kura veic izsaukumu;

ii) izsaucēja starptautiskā mobilā abonenta identitāte (IMSI);

iii) izsaucēja starptautiskā mobilā aprīkojuma identitāte (IMEI);

iv) izsaucamā abonenta IMSI;

v) izsaucamā abonenta IMEI;

vi) anonīmu priekšapmaksas pakalpojumu gadījumos pakalpojuma sākotnējās aktivizēšanas datums un laiks un atrašanās vietas identifikators (šūnas ID), no kuras pakalpojums tika aktivizēts;

3) attiecībā uz interneta piekļuvi, interneta e-pastu un interneta telefoniju:

i) izsaucējs tālruņa numurs iezvanpieejas piekļuvei;

ii) komunikācijas ierosinātāja ciparu abonenta līnija (DSL) vai cits nobeiguma punkta numurs;

f) dati, kuri ir nepieciešami, lai noteiktu mobilo sakaru iekārtas atrašanās vietu:

1) atrašanās vietas identifikators (šūnas ID) komunikācijas sākumā;

2) dati, kas identificē šūnas ģeogrāfisko atrašanās vietu, norādot to atrašanās identifikatoru (šūnas ID) tā perioda laikā, par kuru saglabāti komunikāciju dati.

2. Saskaņā ar šo direktīvu nevar saglabāt datus, kas izpauž komunikācijas saturu.

6. pants

Saglabāšanas termiņi

Dalībvalstis nodrošina, ka 5. pantā norādītās datu kategorijas saglabā laiku, kas ir ne mazāk kā seši mēneši un ne ilgāk kā divi gadi no komunikācijas datuma.

7. pants

Datu aizsardzība un datu drošība

Neierobežojot noteikumus, kas pieņemti saskaņā ar Direktīvu 95/46/EK un Direktīvu 2002/58/EK, katra dalībvalsts nodrošina, ka publiski pieejamo elektronisko komunikāciju pakalpojumu sniedzēji un publiski pieejamo komunikāciju tīklu operatori attiecībā uz datiem, kas tiek saglabāti saskaņā ar šo direktīvu, ievēro vismaz šādus datu drošības principus:

a) saglabātajiem datiem ir tāda pati kvalitāte, un tiem piemēro tādus pašus drošības un aizsardzības noteikumus kā datiem tīklā;

b) attiecībā uz datiem īsteno atbilstīgus tehniskos un organizatoriskos pasākumus, lai aizsargātu tos pret nejaušu vai nelikumīgu iznīcināšanu, zudumu vai pārveidošanu, vai neatļautu vai nelikumīgu saglabāšanu, apstrādi, piekļuvi vai izpaušanu;

c) attiecībā uz datiem īsteno atbilstīgus tehniskos un organizatoriskos pasākumus, lai nodrošinātu, ka tie ir pieejami tikai īpaši pilnvarotiem darbiniekiem;

un

d) visus datus, izņemot tos, kuriem ir piekļūts un kuri ir rezervēti, saglabāšanas termiņa beigās iznīcina.

8. pants

Saglabāto datu uzglabāšanas prasības

Dalībvalstis nodrošina, lai visi 5. pantā norādītie dati tiktu saglabāti saskaņā ar šo direktīvu tā, ka saglabātos datus un jebkuru citu nepieciešamo informāciju, kas saistīta ar minētajiem datiem, būtu iespējams nekavējoties nodot kompetentajām iestādēm.

9. pants

Uzraudzības iestāde

1. Katra dalībvalsts norīko vienu vai vairākas valsts iestādes, kas ir atbildīgas par to noteikumu uzraudzību savā teritorijā, kurus dalībvalstis pieņēmušas saskaņā ar 7. pantu attiecībā uz uzglabāto datu drošību. Minētās iestādes var būt tās pašas, kas minētas Direktīvas 95/46/EK 28. pantā.

2. Šā panta 1. punktā minētās iestādes darbojas pilnīgi neatkarīgi, īstenojot minētajā punktā paredzēto uzraudzību.

[..]

11. pants

Direktīvas 2002/58/EK grozījums

Direktīvas 2002/58/EK 15. pantā iekļauj šādu punktu:

"1.a Šā panta 1. punkts neattiecas uz datiem, kurus [Direktīva 2006/24] konkrēti prasa saglabāt minētās direktīvas 1. panta 1. punktā paredzētajiem mērķiem."

[..]

13. pants

Aizsardzības līdzekļi, atbildība un sankcijas

1. Katra dalībvalsts veic nepieciešamos pasākumus, lai nodrošinātu, ka attiecībā uz datu apstrādi saskaņā ar šo direktīvu tiek pilnībā īstenoti attiecīgās valsts pasākumi, ar ko īsteno Direktīvas 95/46/EK III nodaļu, kurā paredzēti tiesiskas aizsardzības līdzekļi, atbildība un sankcijas.

2. Katra dalībvalsts jo īpaši veic nepieciešamos pasākumus, lai nodrošinātu, ka tāda tīša piekļuve saskaņā ar šo direktīvu saglabātajiem datiem vai tāda to nodošana, kas nav atļauta ar attiecīgās valsts tiesību aktiem, kuri pieņemti atbilstoši šai direktīvai, ir sodāma, tostarp ar administratīviem sodiem vai krimināsodiem, kas ir efektīvi, proporcionāli un preventīvi."

Pamatlietas un prejudiciālie jautājumi

Lieta C-293/12

17 *Digital Rights* 2006. gada 11. augustā cēla prasību *High Court* [Augstākajā tiesā], apgalvojot, ka tai pieder mobilais telefons, kas reģistrēts 2006. gada 3. jūnijā un ko tā kopš šī datuma ir lietojusi. *Digital Rights* apšauba valsts normatīvos un administratīvos aktus par datu par elektronisko komunikāciju saglabāšanu un tostarp lūdz, lai iesniedzējtiesa atzīst par spēkā neesošu Direktīvu 2006/24 un 2005. gada Krimināllikuma (ar terorismu saistīti nodarījumi) (*Criminal Justice (Terrorist Offences) Act 2005*) septīto daļu, kurā noteikts, ka telefona komunikāciju pakalpojumu sniedzējiem likumā noteiktu laikposmu jāsaglabā informācija par datu plūsmu un atrašanās vietu, lai novērstu, atklātu, izmeklētu un veiktu krimināvajāšanu par noziedzīgiem nodarījumiem, kā arī nodrošinātu valsts drošību.

18 *High Court*, uzskatot, ka tā nespēj izlemt tās izskatāmos jautājumus par valsts tiesībām, ja nav pārbaudīta Direktīvas 2006/24 spēkā esamība, nolēma apturēt tiesvedību un uzdot Tiesa šādus prejudiciālus jautājumus:

"1) Vai prasītājas tiesību ierobežojums attiecībā uz mobilās telefonijas izmantošanu, kas izriet no Direktīvas 2006/24 3., 4. un 6. pantā paredzētajām prasībām, ir nesaderīgs ar LES 5. panta 4. punktu tādēļ, ka tas ir nesamērīgs un nav nepieciešams vai ir nepiemērots, lai sasniegtu leģitīmos mērķus:

a) nodrošināt, ka atsevišķi dati ir pieejami smagu noziegumu izmeklēšanas, atklāšanas un krimināvajāšanas mērķiem,

un/vai

b) nodrošināt Eiropas Savienības iekšējā tirgus pareizu darbību?

2) Konkrēti,

a) vai Direktīva 2006/24 ir saderīga ar LESD 21. pantā paredzētajām pilsoņu tiesībām brīvi pārvietoties un dzīvot dalībvalstu teritorijā?

b) Vai Direktīva 2006/24 ir saderīga ar tiesībām uz privātās dzīves neaizskaramību, kas paredzētas Eiropas Savienības Pamattiesību hartas (turpmāk tekstā – "Harta") 7. pantā un [ECPAK] 8. pantā?

c) Vai Direktīva 2006/24 ir saderīga ar tiesībām uz personas datu aizsardzību, kas paredzētas Hartas 8. pantā?

d) Vai Direktīva 2006/24 ir saderīga ar tiesībām uz vārda brīvību, kas paredzētas Hartas 11. pantā un [ECPAK] 10. pantā?

e) Vai Direktīva 2006/24 ir saderīga ar tiesībām uz labu pārvaldību, kas paredzētas Hartas 41. pantā?

3) Cik lielā mērā saskaņā ar Līgumiem un it īpaši ar lojālas sadarbības principu, kas paredzēts LES 4. panta 3. punktā, valsts tiesai ir jāpārbauda un jāvērtē tas, vai valsts pasākumi, ar kuriem tiek transponēta Direktīva 2006/24, ir saderīgi ar [Hartā], tostarp tās 7. pantā, paredzētajām garantijām (kas ir iekļautas [ECPAK] 8. pantā)?"

Lieta C-594/12

19 Lūguma sniegt prejudiciālu nolēmumu lietā C-594/12 pamatā ir vairākas prasības, kuras *Verfassungsgerichtshof* [Konstitucionālajā tiesā] cēluši attiecīgi *Kärntner Landesregierung*, kā arī *M. Seitlinger*, *C. Tschohl* un 11 128 citi prasītāji, kuri lūdz atcelt 2003. gada Telekomunikāciju likuma (*Telekommunikationsgesetz 2003*) 102.a pantu, kurš šajā likumā tika iekļauts ar federālo likumu par grozījumu izdarīšanu šajā likumā (*Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird*, *BGBl* I, 27/2011), lai Austrijas tiesībās transponētu Direktīvu 2006/24. Šie lietas dalībnieki uzskata, ka ar šo 102.a pantu tiek pārkāptas privātpersonu pamattiesības uz datu aizsardzību.

20 *Verfassungsgerichtshof* šaubās tostarp par to, vai Direktīva 2006/24 ir saderīga ar Hartu, ciktāl ar to tiek atļauts ilgstoši uzglabāt virkni dažādu datu attiecībā uz neierobežotu skaitu personu. Datu saglabāšana attiecas gandrīz tikai uz tādām personām, kuru rīcība nekādā veidā nepamato datu par viņām saglabāšanu. Šīs personas tiek pakļautas paaugstinātam riskam, ka iestādes iegūst viņu datus, iepazīstas ar to saturu, uzzina par šo personu privāto dzīvi un šos datus izmanto dažādiem mērķiem, ņemot vērā it īpaši neierobežoto tādu personu skaitu, kurām vismaz sešus mēnešus būs piekļuve datiem. Pēc iesniedzējtiesas domām, pastāv šaubas, pirmkārt, par to, vai šī direktīva ir piemērota, lai sasniegtu tās izvirzītos mērķus, un, otrkārt, par iejaukšanās attiecīgajās pamattiesībās samērīgumu.

21 Šādos apstākļos *Verfassungsgerichtshof* nolēma apturēt tiesvedību un uzdot Tiesai šādus prejudiciālus jautājumus:

"1) Par Savienības iestāžu rīcības spēkā esamību:

Vai Direktīvas 2006/24 3.–9. pants ir saderīgi ar [Hartas] 7., 8. un 11. pantu?

2) Par Līgumu interpretāciju:

a) Vai, ņemot vērā paskaidrojumus par Hartas 8. pantu, kuri ir izstrādāti saskaņā ar Hartas 52. panta 7. punktu, lai sniegtu norādes Hartas interpretācijai, un kuri *Verfassungsgerichtshof* pienācīgi ir jāievēro, Direktīva 95/46 un Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regula (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un organizācijās un par šādu datu brīvu apriti [(OV 2001, L 8, 1. lpp.)], izvērtējot tiesību aizskāruma pieļaujamību, ir jāņem vērā tikpat lielā mērā, cik Hartas 8. panta 2. punktā un 52. panta 1. punktā minētie nosacījumi?

b) Kāda saistība pastāv starp Hartas 52. panta 3. punkta pēdējā teikumā norādītajām "Savienības tiesībām" un direktīvām tiesību uz datu aizsardzību jomā?

c) Vai Hartas 8. panta interpretācijā, ņemot vērā, ka Direktīvā 95/46 un Regulā [..] Nr. 45/2001 ir ietverti Hartā paredzēto pamattiesību uz datu aizsardzību īstenošanas nosacījumi un ierobežojumi, ir jāņem vērā grozījumi, kas izriet no vēlāk pieņemtiem sekundāro tiesību aktiem?

d) Vai, ņemot vērā Hartas 52. panta 4. punktu, Hartas 53. pantā paredzētais augstāka aizsardzības līmeņa nodrošināšanas princips nozīmē, ka Hartā noteiktās robežas attiecībā uz pieļaujamiem ierobežojumiem sekundāro tiesību aktos ir jāapraksta vēl šaurāk?

e) Vai, ņemot vērā Hartas 52. panta 3. punktu, preambulas piekto daļu un paskaidrojumu par [tās] 7. pantu, kuros norādīts, ka 7. pantā garantētās tiesības atbilst ECPAK 8. pantā garantētajām tiesībām, no Eiropas Cilvēktiesību tiesas judikatūras par ECPAK 8. pantu var secināt norādes par Hartas 8. panta interpretāciju, kas ietekmē šī pēdējā minētā panta interpretāciju?"

22 Ar Tiesas priekšsēdētāja 2013. gada 11. jūnija rīkojumu lietas C-293/12 un C-594/12 tika apvienotas mutvārdu procesam un sprieduma taisīšanai.

Par prejudiciālajiem jautājumiem

Par otrā jautājuma b)–d) punktu lietā C-293/12 un pirmo jautājumu lietā C-594/12

23 Ar otrā jautājuma b)–d) punktu lietā C-293/12 un pirmo jautājumu lietā C-594/12, kuri jāizskata kopā, iesniedzējtiesas būtībā lūdz Tiesu pārbaudīt Direktīvas 2006/24 spēkā esamību no Hartas 7., 8. un 11. panta viedokļa.

Par Hartas 7., 8. un 11. panta atbilstību attiecībā uz jautājumu par Direktīvas 2006/24 spēkā esamību

24 No Direktīvas 2006/24 1. panta un tās preambulas 4., 5., 7.–11, 21. un 22. apsvēruma izriet, ka tās galvenais mērķis ir saskaņot dalībvalstu noteikumus attiecībā uz publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzēju vai publiski pieejamu komunikāciju tīklu operatoru pienākumiem, kas attiecas uz noteiktu datu, kurus tie iegūst vai apstrādā, saglabāšanu, lai nodrošinātu, ka šie dati ir pieejami smagu noziegumu, tādu kā ar organizēto noziedzību un terorismu saistītie, novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem, ievērojot Hartas 7. un 8. pantā nostiprinātās tiesības.

25 Direktīvas 2006/24 3. pantā paredzētais publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzēju vai publiski pieejamu komunikāciju tīklu operatoru pienākums saglabāt tās 5. pantā minētos datus, lai attiecīgā gadījumā tos darītu pieejamus kompetentajām valsts iestādēm, rada jautājumus gan par Hartas 7. pantā nostiprināto privātās dzīves un saziņas neaizskaramību, gan tās 8. pantā paredzēto personas datu aizsardzību, kā arī par Hartas 11. pantā garantēto vārda brīvību.

26 Šajā ziņā jānorāda, ka dati, kas jāsaglabā publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzējiem vai publiski pieejamu komunikāciju tīklu operatoriem atbilstoši Direktīvas 2006/24 3. un 5. pantam, ir it īpaši dati, kas nepieciešami, lai izsekotu un identificētu komunikācijas avotu un tās galamērķi, lai noteiktu komunikācijas datumu, laiku, ilgumu un veidu, lietotāja komunikāciju aprīkojumu, kā arī lai noteiktu mobilo sakaru iekārtas atrašanās vietu, un šie dati ietver tostarp abonenta vai reģistrētā lietotāja vārdu vai nosaukumu, izsaucēja un izsaucamo telefona numuru, kā arī attiecībā uz interneta pakalpojumiem – IP adresi. Šie dati ļauj it īpaši noteikt, kas ir persona, ar kuru abonents vai reģistrētais lietotājs ir sazinājies, un kādā veidā, kā arī noteikt komunikācijas laiku un vietu, no kurienes tā notikusi. Turklāt tie ļauj uzzināt, cik bieži abonents vai reģistrētais lietotājs noteiktā laikposmā ir sazinājies ar konkrētām personām.

27 Šie dati, skatīti kopumā, var ļaut izdarīt ļoti precīzus secinājumus par personu, kuru dati tikuši saglabāti, privāto dzīvi, tostarp ikdienas paradumiem, pastāvīgajām vai pagaidu dzīvesvietām, ikdienas vai citām gaitām, veiktajām darbībām, šo personu sociālajām attiecībām un aprindām, kurās tās mēdz uzturēties.

28 Šādos apstākļos, pat ja – kā izriet no Direktīvas 2006/24 1. panta 2. punkta un 5. panta 2. punkta – šī direktīva neļauj saglabāt datus, kas attiecas uz komunikācijas saturu, un informāciju, kura skatīta, izmantojot elektronisko komunikāciju tīklu, nevar izslēgt, ka attiecīgo datu saglabāšana var ietekmēt to, kā abonenti vai reģistrētie lietotāji izmanto saziņas līdzekļus, uz kuriem attiecas šī direktīva, un tādējādi to, kā viņi izmanto savu Hartas 11. pantā garantēto vārda brīvību.

29 Datu saglabāšana, lai tiem, iespējams, varētu piekļūt kompetentas valsts iestādes, kā to paredz Direktīva 2006/24, tieši un konkrēti ietekmē privāto dzīvi un tādējādi Hartas 7. pantā garantētās tiesības. Turklāt uz šādu datu saglabāšanu attiecas Hartas 8. pants tādēļ, ka tā ir personas datu apstrāde šīs tiesību normas izpratnē un tādējādi tai katrā ziņā jāatbilst no šī panta izrietošajām datu aizsardzības prasībām (spriedums *Volker und Markus Schecke* un *Eifert*, C-92/09 un C-93/09, EU:C:2010:662, 47. punkts).

30 Lai gan lūgumi sniegt prejudiciālu nolēmumu šajās lietās izvirza it īpaši principa jautājumu par to, vai abonentu un reģistrēto lietotāju dati var vai nevar tikt saglabāti, ņemot vērā Hartas 7. pantu, tie attiecas arī uz jautājumu, vai Direktīva 2006/24 atbilst no Hartas 8. panta izrietošajām personas datu aizsardzības prasībām.

31 Ņemot vērā iepriekš minētos apsvērumus, lai atbildēto uz otrā jautājuma b)–d) punktu lietā C-293/12 un uz pirmo jautājumu lietā C-594/12, jāpārbauda Direktīvas 2006/24 spēkā esamība no Hartas 7. un 8. panta viedokļa.

Par iejaukšanās Hartas 7. un 8. pantā nostiprinātajās tiesībās pastāvēšanu

32 Paredzot Direktīvas 2006/24 5. panta 1. punktā minēto datu saglabāšanu un ļaujot kompetentajām valsts iestādēm tiem piekļūt, šī direktīva, kā to norādījis ģenerāladvokāts it īpaši savu secinājumu 39. un 40. punktā, veido atkāpi no Direktīvā 95/46 un Direktīvā 2002/58 noteiktās tiesību uz privātās dzīves neaizskaramības aizsardzības sistēmas attiecībā uz personas datu apstrādi elektronisko komunikāciju nozarē; šajās pēdējās direktīvās ir paredzēta komunikācijas un informācijas par datu

plūsmu konfidencialitāte, kā arī pienākums izdzēst vai padarīt anonīmu šo informāciju, kad tā vairs nav nepieciešama saziņas pārraidīšanai, izņemot, ja tā ir nepieciešama rēķina izrakstīšanai, un vienīgi tik ilgi, kamēr šī vajadzība pastāv.

33 Lai pierādītu, ka pastāv iejaukšanās pamattiesībās uz privātās dzīves neaizskaramību, nav nozīmes tam, vai attiecīgajai informācijai par privāto dzīvi ir vai nav delikāts raksturs, vai tam, vai attiecīgajām personām ir vai nav radītas iespējamas neērtības šīs iejaukšanās dēļ (šajā ziņā skat. spriedumu *Österreichischer Rundfunk* u.c., C-465/00, C-138/01 un C-139/01, EU:C:2003:294, 75. punkts).

34 No tā izriet, ka Direktīvas 2006/24 3. un 6. pantā paredzētais komunikāciju pakalpojumu sniedzēju vai publiski pieejamu komunikāciju tīklu operatoru pienākums noteiktu laiku saglabāt datus par personas privāto dzīvi un saziņu, kādi tie paredzēti šīs direktīvas 5. pantā, pats par sevi veido iejaukšanos Hartas 7. pantā garantētajās tiesībās.

35 Turklāt kompetento valsts iestāžu piekļuve datiem ir papildu iejaukšanās šajās pamattiesībās (attiecībā uz ECPAK 8. pantu skat. ECT 1987. gada 26. marta spriedumu lietā *Leander* pret Zviedriju, A sērija, Nr. 116, 48. punkts; *Rotaru* pret Rumāniju, Nr. 28341/95, 46. punkts; *CEDH* 2000-V, kā arī *Weber* un *Saravia* pret Vāciju (lēmums), Nr. 54934/00, 79. punkts, *CEDH* 2006-XI). Tādējādi arī Direktīvas 2006/24 4. un 8. pants, kuros paredzēti noteikumi par kompetento valsts iestāžu piekļuvi datiem, veido iejaukšanos Hartas 7. pantā garantētajās tiesībās.

36 Tāpat Direktīva 2006/24 veido iejaukšanos Hartas 8. pantā garantētajās pamattiesībās uz personas datu aizsardzību, jo tajā paredzēta personas datu apstrāde.

37 Jāatzīst, ka Direktīvas 2006/24 veidotā iejaukšanās Hartas 7. un 8. pantā nostiprinātajās pamattiesībās, kā norādījis arī ģenerāladvokāts tostarp savu secinājumu 77. un 80. punktā, ir plaša un tādējādi uzskatāma par īpaši būtisku. Turklāt apstāklis, ka datu saglabāšana un to vēlāka izmantošana notiek, abonentu vai reģistrēto lietotāju par to neinformējot, var, kā to norādījis ģenerāladvokāts savu secinājumu 52. un 72. punktā, attiecīgajām personām radīt sajūtu, ka viņu privātā dzīve tiek pastāvīgi uzraudzīta.

Par iejaukšanās Hartas 7. un 8. pantā nostiprinātajās tiesībās attaisnojumu

38 Atbilstoši Hartas 52. panta 1. punktam visiem tajā atzīto tiesību un brīvību izmantošanas ierobežojumiem ir jābūt noteiktiem tiesību aktos, tajos jārespektē šo tiesību un brīvību būtība un, ievērojot samērīguma principu, ierobežojumus šīm tiesībām un brīvībām drīkst uzlikt tikai tad, ja tie ir nepieciešami un patiešām atbilst vispārējas nozīmes mērķiem, ko atzinusi Savienība, vai vajadzībai aizsargāt citu personu tiesības un brīvības.

39 Attiecībā uz pamattiesību uz privātās dzīves neaizskaramību un citu Hartas 7. pantā nostiprināto tiesību būtību jāatzīst, ka, kaut arī ar Direktīvu 2006/24 prasītā datu saglabāšana ir īpaši būtiska iejaukšanās šajās tiesībās, tā nav tāda, kas aizskartu minēto būtību, jo, kā izriet no tās 1. panta 2. punkta, šī direktīva neļauj uzzināt pašu elektronisko komunikāciju saturu.

40 Šī datu saglabāšana arī nav tāda, kas aizskartu Hartas 8. pantā nostiprināto pamattiesību uz personas datu aizsardzību būtību, tādēļ, ka Direktīvas 2006/24 7. pantā paredzēts noteikums par datu aizsardzību un drošību, saskaņā ar kuru, neierobežojot noteikumus, kas pieņemti saskaņā ar Direktīvu 95/46 un Direktīvu 2002/58, publiski pieejamo elektronisko komunikāciju pakalpojumu sniedzējiem un publiski pieejamo komunikāciju tīklu operatoriem jāievēro noteikti datu aizsardzības un drošības principi, atbilstoši kuriem dalībvalstis nodrošina, ka tiek īstenoti atbilstīgi tehniskie un organizatoriskie pasākumi, lai datus aizsargātu pret nejaušu vai nelikumīgu iznīcināšanu, zudumu vai pārveidošanu.

41 Attiecībā uz jautājumu, vai šī iejaukšanās atbilst vispārējo interešu mērķim, jānorāda, ka, lai gan Direktīva 2006/24 ir domāta, lai saskaņotu dalībvalstu noteikumus attiecībā uz minēto pakalpojumu sniedzēju vai tīklu operatoru pienākumiem, kas attiecas uz noteiktu datu, kurus tie iegūst vai apstrādā, saglabāšanu, tās materiālais mērķis, kā izriet no tās 1. panta 1. punkta, ir nodrošināt, lai šie dati būtu pieejami smagu noziegumu, kas katrā dalībvalstī noteikti tiesību aktos, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķiem. Tādējādi šīs direktīvas materiālais mērķis ir sekmēt cīņu pret smagiem noziegumiem un galu galā – sabiedrības drošību.

42 No Tiesas judikatūras izriet, ka cīņa pret starptautisko terorismu, lai nodrošinātu starptautisko mieru un drošību, ir Savienības vispārējo interešu mērķis (šajā ziņā skat. spriedumu *Kadi* un *Al Barakaat International Foundation*/Padome un Komisija, C-402/05 P un C-415/05 P, EU:C:2008:461, 363. punkts, kā arī spriedumu *Al-Aqsa*/Padome, C-539/10 P un C-550/10 P, EU:C:2012:711, 130. punkts). Tas pats attiecas uz cīņu pret smagiem noziegumiem, lai nodrošinātu sabiedrības drošību (šajā ziņā skat. spriedumu *Tsakouridis*, C-145/09, EU:C:2010:708, 46. un 47. punkts). Turklāt šajā ziņā jānorāda, ka Hartas 6. pantā atzītas ikvienas personas tiesības ne vien uz brīvību, bet arī uz drošību.

43 Šajā ziņā no Direktīvas 2006/24 preambulas 7. apsvēruma izriet, ka sakarā ar elektronisko komunikāciju piedāvāto iespēju ievērojamo pieaugumu 2002. gada 19. decembra [secinājumos] Tieslietu un iekšlietu padome uzskatīja, ka īpaši svarīgi ir dati, kuri attiecas uz elektronisko komunikāciju izmantošanu, un tāpēc tie ir vērtīgs līdzeklis noziedzīgu nodarījumu, it īpaši organizētās noziedzības, novēršanai un apkarošanai.

44 Tādējādi jāatzīst, ka datu saglabāšana, lai kompetentajām valsts iestādēm ļautu tiem iespējami piekļūt, kāda tā paredzēta Direktīvā 2006/24, patiešām atbilst vispārējo interešu mērķim.

45 Šādos apstākļos jāpārbauda konstatētās iejaukšanās samērīgums.

46 Šajā ziņā jāatgādina, ka saskaņā ar Tiesas pastāvīgo judikatūru atbilstoši samērīguma principam Savienības iestāžu tiesību aktiem ir jābūt piemērotiem attiecīgajā tiesiskajā regulējumā noteikto leģitīmo mērķu sasniegšanai un tie nedrīkst pārsniegt to, kas ir to sasniegšanai atbilstošs un nepieciešams (šajā ziņā skat. spriedumu *Afton Chemical*, C-343/09, EU:C:2010:419, 45. punkts; spriedumu *Volker und Markus Schecke* un *Eifert*, EU:C:2010:662, 74. punkts; spriedumu *Nelson* u.c., C-581/10 un C-629/10, EU:C:2012:657, 71. punkts; spriedumu *Sky Österreich*, C-283/11, EU:C:2013:28, 50. punkts, kā arī spriedumu *Schaible*, C-101/12, EU:C:2013:661, 29. punkts).

47 Attiecībā uz pārbaudi tiesā par šo nosacījumu ievērošanu, ja runa ir par iejaukšanos pamattiesībās, Savienības likumdevēja novērtējuma brīvība var būt ierobežota atkarībā no virknes faktoru, tostarp skartās jomas, attiecīgo Hartā garantēto tiesību rakstura, iejaukšanās rakstura un būtiskuma, kā arī tās mērķa (pēc analoģijas attiecībā uz ECPAK 8. pantu skat. ECT spriedumu lietā *S* un *Marper* pret Apvienoto Karalisti [*GC*], Nr. 30562/04 un 30566/04, 102. punkts, *CEDH 2008-V*).

48 Šajā lietā, ņemot vērā, pirmkārt, nozīmīgo lomu, kas personas datu aizsardzībai ir attiecībā uz pamattiesībām uz privātās dzīves neaizskaramību, un, otrkārt, ar Direktīvu 2006/24 radītās iejaukšanās šajās tiesībās apjomu un būtiskumu, Savienības likumdevēja novērtējuma brīvība ir ierobežota un tādējādi jāveic stingra pārbaude.

49 Attiecībā uz jautājumu, vai datu saglabāšana ir piemērota Direktīvas 2006/24 izvirzītā mērķa sasniegšanai, jāatzīst, ka, ņemot vērā elektronisko komunikāciju pieaugošo nozīmīgumu, dati, kas atbilstoši šai direktīvai jāsaglabā, sniedz par kriminālvajāšanu atbildīgajām kompetentajām valsts iestādēm papildu iespējas atklāt smagus noziegumus un tādējādi šajā ziņā tie ir noderīgs krimināllizmeklēšanas instruments. Līdz ar to šādu datu saglabāšana var tikt uzskatīta par piemērotu šīs direktīvas izvirzītā mērķa sasniegšanai.

50 Šo vērtējumu nevar likt apšaubīt apstāklis, uz kuru savos Tiesai iesniegtajos rakstveida apsvērumos atsaukušies it īpaši *M. Tschohl* un *C. Seitlinger*, kā arī Portugāles valdība, – ka pastāv vairāki elektronisko komunikāciju veidi, kas neietilpst Direktīvas 2006/24 piemērošanas jomā vai kas atļauj anonīmu komunikāciju. Lai gan ir tiesa, ka šis apstāklis var ierobežot datu saglabāšanas pasākuma piemērotību izvirzītā mērķa sasniegšanai, tas, kā to norāda ģenerāladvokāts savu secinājumu 137. punktā, tomēr nav tāds, kas šo pasākumu padarītu par nederīgu.

51 Attiecībā uz Direktīvā 2006/24 noteiktās datu saglabāšanas nepieciešamo raksturu jāatzīst, ka patiešām cīņa pret smagiem noziegumiem, tostarp pret organizēto noziedzību un terorismu, ir sabiedrības drošības garantēšanai noteicoša un tās efektivitāte var lielā mērā būt atkarīga no moderno izmeklēšanas tehniku izmantošanas. Tomēr šāds vispārējo interešu mērķis, lai cik būtisks tas būtu, pats par sevi nevar attaisnot to, ka tāds [datu] saglabāšanas pasākums kā ar Direktīvu 2006/24 noteiktais tiek uzskatīts par nepieciešamu šīs cīņas īstenošanai.

52 Attiecībā uz tiesībām uz privātās dzīves neaizskaramību ir jānorāda, ka atbilstoši Tiesas pastāvīgajai judikatūrai to aizsardzība katrā ziņā prasa, lai atkāpes no personas datu aizsardzības un tās ierobežojumi tiktu īstenoti absolūti nepieciešamā ietvaros (spriedums *IPI*, C-473/12, EU:C:2013:715, 39. punkts un tajā minētā judikatūra).

53 Šajā ziņā jāatgādina, ka personas datu aizsardzība, kas izriet no Hartas 8. panta 1. punktā skaidri izteiktā pienākuma, ir īpaši nozīmīga tās 7. pantā nostiprinātajām tiesībām uz privātās dzīves neaizskaramību.

54 Tādējādi attiecīgajā Savienības tiesiskajā regulējumā jāparedz skaidri un precīzi noteikumi, kas reglamentētu attiecīgā pasākuma apjomu un piemērošanu un noteiktu minimālas prasības tādējādi, lai personām, kuru dati tikuši saglabāti, būtu pietiekamas garantijas, kas ļautu to personas datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku, kā arī pret jebkādu nelikumīgu piekļuvi šiem datiem un to nelikumīgu izmantošanu (pēc analoģijas attiecībā uz ECPAK 8. pantu skat. ECT 2008. gada 1. jūlija spriedumu lietā *Liberty* u.c. pret Apvienoto Karalisti, Nr. 58243/00, 62. un 63. punkts, iepriekš minēto spriedumu lietā *Rotaru* pret Rumāniju, 57.–59. punkts, kā arī iepriekš minēto spriedumu lietā *S* un *Marper* pret Apvienoto Karalisti, 99. punkts).

55 Šādu garantiju nepieciešamība ir vēl jo svarīgāka tādēļ, ka – kā paredzēts Direktīvā 2006/24 – personas dati tiek apstrādāti automātiski un pastāv ievērojams nelikumīgas piekļuves šiem datiem risks (pēc analoģijas attiecībā uz ECPAK 8. pantu skat. iepriekš minēto ECT spriedumu lietā *S* un *Marper* pret Apvienoto Karalisti, 103. punkts, kā arī 2013. gada 18. aprīļa spriedumu lietā *M. K.* pret Franciju, Nr. 19522/09, 35. punkts).

56 Attiecībā uz jautājumu, vai Direktīvas 2006/24 radītā iejaukšanās ir ierobežota ar absolūti nepieciešamo, jānorāda, ka atbilstoši šīs direktīvas 3. pantam, to skatot kopsakarā ar tās 5. panta 1. punktu, ar šo direktīvu ir uzlikts pienākums saglabāt visu informāciju par datu plūsmu attiecībā uz fiksētā tīkla telefoniju, mobilo telefoniju, interneta piekļuvi, interneta e-pastu, kā arī interneta telefoniju. Tādējādi tā attiecas uz visu veidu elektronisko komunikāciju, kuras izmantošana ir ļoti izplatīta un kuras nozīme ikviena ikdienas dzīvē pieaug. Turklāt saskaņā ar šīs direktīvas 3. pantu tā attiecas uz visiem abonentiem un reģistrētajiem lietotājiem. Tādējādi tā rada iejaukšanos gandrīz visu Eiropas iedzīvotāju pamattiesībās.

57 Šajā ziņā jāatzīst, pirmkārt, ka Direktīva 2006/24 vispārīgā veidā aptver visas personas un visus elektroniskās komunikācijas līdzekļus, kā arī visu informāciju par datu plūsmu bez kādām atšķirībām, ierobežojumiem vai izņēmumiem saistībā ar mērķi cīnīties pret smagiem noziegumiem.

58 Proti, pirmām kārtām, Direktīva 2006/24 vispārīgi attiecas uz visām personām, kuras izmanto elektronisko komunikāciju pakalpojumus, tomēr šīs personas, kuru dati tiek saglabāti, pat netieši neatrodas situācijā, kas varētu būt pamats kriminālvajāšanai. Tādējādi tā attiecas pat uz personām,

attiecībā uz kurām nepastāv nekādas norādes, kas ļautu domāt, ka viņu rīcībai varētu būt sakars – kaut vai netiešs vai attāls – ar smagiem noziegumiem. Turklāt tajā nav paredzēti nekādi izņēmumi, un tādējādi tā attiecas pat uz personām, uz kuru saziņu atbilstoši valsts tiesību normām attiecas profesionālais noslēpums.

59 Otrām kārtām, lai gan tā ir domāta cīņas pret smagiem noziegumiem sekmēšanai, minētajā direktīvā nav prasīta nekāda saikne starp datiem, kuru saglabāšana tiek paredzēta, un sabiedriskās drošības apdraudējumu, un it īpaši tā nav ierobežota ar vai nu tādu datu saglabāšanu, kas attiecas uz noteiktu laika posmu un/vai ģeogrāfisko zonu, un/vai noteiktu personu loku, kuras varētu būt vienā vai citā veidā iesaistītas smagā noziegumā, vai ar datu saglabāšanu par tādām personām, kuras citu iemeslu dēļ ar to datu saglabāšanu varētu sekmēt smagu noziegumu atklāšanu vai kriminālvajāšanu.

60 Otrkārt, papildus šai jebkādu robežu neesamībai Direktīvā 2006/24 nav paredzēti nekādi objektīvi kritēriji, kas ļautu ierobežot kompetento valsts iestāžu piekļuvi datiem un to vēlāku izmantošanu tādu noziegumu novēršanas, izmeklēšanas, atklāšanas vai kriminālvajāšanas mērķiem, kuri, ņemot vērā iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās apjomu un būtiskumu, varētu tikt uzskatīti par pietiekami smagiem, lai attaisnotu šādu iejaukšanos. Gluži pretēji – Direktīvas 2006/24 1. panta 1. punktā vienīgi ietverta atsauce uz smagiem noziegumiem, kas katrā dalībvalstī noteikti valsts tiesību aktos.

61 Turklāt attiecībā uz kompetento valsts iestāžu piekļuvi datiem un to vēlāku izmantošanu Direktīvā 2006/24 nav ietverti atbilstošie materiālie un procesuālie nosacījumi. Šīs direktīvas 4. pantā, kurā reglamentēta šo iestāžu piekļuve saglabātajiem datiem, nav skaidri noteikts, ka šai piekļuvei attiecīgajiem datiem un to vēlākai izmantošanai ir jābūt strikti ierobežotai ar mērķi novērst un atklāt precīzi noteiktus smagus noziegumus, kā arī nodrošināt kriminālvajāšanu par tiem, bet tajā vienīgi paredzēts, ka dalībvalstis nosaka procedūras, kas jāievēro, un nosacījumus, kas jāizpilda, lai saņemtu piekļuvi saglabātajiem datiem, ievērojot nepieciešamības un samērīguma prasības.

62 Konkrēti, Direktīvā 2006/24 nav paredzēti nekādi objektīvi kritēriji, kas ļautu ierobežot to personu skaitu, kurām ir atļauts piekļūt datiem un vēlāk tos izmantot, līdz absolūti nepieciešamajam izvirzītā mērķa sasniegšanai. It īpaši šo kompetento valsts iestāžu piekļuve saglabātajiem datiem nav pakļauta iepriekšējai kontrolei, ko veiktu vai nu tiesa, vai alternatīva neatkarīga administratīva vienība, kuras lēmums paredzētu ierobežot piekļuvi datiem un to izmantošanu ar to, kas ir absolūti nepieciešams izvirzītā mērķa sasniegšanai, un kas tiktu pieņemts pēc šo iestāžu pamatota lūguma, kas iesniegts ar [noziedzīgu nodarījumu] novēršanu, atklāšanu vai kriminālvajāšanu saistītu procedūru ietvaros. Nav arī paredzēts precīzs dalībvalstu pienākums noteikt šādus ierobežojumus.

63 Treškārt, attiecībā uz datu saglabāšanas ilgumu Direktīvas 2006/24 6. pantā paredzēts pienākums tos saglabāt vismaz sešus mēnešus, nenosakot nekādas atšķirības starp šīs direktīvas 5. pantā paredzētajām datu kategorijām atkarībā no to iespējamā noderīguma izvirzītā mērķa sasniegšanai vai personām, uz kurām tie attiecas.

64 Šis ilgums turklāt ir no sešiem mēnešiem līdz, augstākais, divdesmit četriem mēnešiem, un nav precizēts, ka saglabāšanas ilguma noteikšanai jābūt pamatotai ar objektīviem kritērijiem, lai nodrošinātu, ka tā ir ierobežota ar absolūti nepieciešamo.

65 No iepriekš minētā izriet, ka Direktīvā 2006/24 nav paredzēti skaidri un precīzi noteikumi, kas reglamentētu iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās apjomu. Tādējādi jāatzīst, ka šī direktīva Savienības tiesību sistēmā rada plaša apjoma un īpaši būtisku iejaukšanos šajās pamattiesībās un šī iejaukšanās nav precīzi reglamentēta ar tiesību normām, kas ļautu nodrošināt, lai tā patiešām būtu ierobežota ar absolūti nepieciešamo.

66 Turklāt attiecībā uz noteikumiem par publiski pieejamo elektronisko komunikāciju pakalpojumu sniedzēju un publiski pieejamo komunikāciju tīklu operatoru saglabāto datu drošību un aizsardzību jāatzīst, ka Direktīvā 2006/24 nav paredzētas pietiekamas garantijas, tādas kā Hartas 8. pantā prasītās, kas ļautu nodrošināt saglabāto datu efektīvu aizsardzību pret ļaunprātīgas izmantošanas risku, kā arī pret jebkādu nelikumīgu piekļuvi šiem datiem un to nelikumīgu izmantošanu. Proti, pirmkārt, Direktīvas 2006/24 7. pantā nav paredzēti konkrēti un milzīgajam datu apjomam, kuru saglabāšana prasīta ar šo direktīvu, pielāgoti noteikumi par datu delikāto raksturu, kā arī par nelikumīgas piekļuves tiem risku, kas it īpaši būtu domāti skaidrai un striktai attiecīgo datu aizsardzības un drošības reglamentēšanai, lai nodrošinātu pilnīgu to neaizskaramību un konfidencialitāti. Turklāt nav paredzēts arī skaidrs dalībvalstu pienākums šādus noteikumus pieņemt.

67 Ar Direktīvas 2006/24 7. pantu, to lasot kopā ar Direktīvas 2002/58 4. panta 1. punktu un Direktīvas 95/46 17. panta 1. punkta otro daļu, nav nodrošināts, ka šie pakalpojumu sniedzēji ar tehnisku un organizatorisku pasākumu palīdzību piemēros īpaši augstu aizsardzības līmeni, bet šiem sniedzējiem tostarp atļauts, nosakot to piemērojamo drošības līmeni, ņemt vērā ekonomiska rakstura apsvērumus attiecībā uz drošības pasākumu izmaksām. It īpaši Direktīvā 2006/24 nav garantēta datu neatgriezeniska iznīcināšana pēc to saglabāšanas termiņa beigām.

68 Otrkārt, jāpiebilst, ka ar šo direktīvu nav prasīts, lai attiecīgie dati tiktu saglabāti Savienības teritorijā, un tādējādi nevar uzskatīt, ka būtu pilnībā nodrošināta Hartas 8. panta 3. punktā skaidri prasītā neatkarīgas iestādes kontrole pār iepriekšējos divos punktos minēto aizsardzības un drošības prasību ievērošanu. Tomēr šāda kontrole, kas veikta, pamatojoties uz Savienības tiesībām, ir būtiska sastāvdaļa personu aizsardzībā attiecībā uz personas datu apstrādi (šajā ziņā skat. spriedumu Komisija/Austrija, C-614/10, EU:C:2012:631, 37. punkts).

69 Ņemot vērā visus iepriekš minētos apsvērumus, jāuzskata, ka, pieņemot Direktīvu 2006/24, Savienības likumdevējs ir pārsniedzis samērīguma principa ievērošanas noteiktās robežas, ņemot vērā Hartas 7. un 8. pantu un 52. panta 1. punktu.

70 Šādos apstākļos Direktīvas 2006/24 spēkā esamība no Hartas 11. panta viedokļa nav jāpārbauda.

71 Tādējādi uz otrā jautājuma b)–d) punktu lietā C-293/12 un pirmo jautājumu lietā C-594/12 jāatbild, ka Direktīva 2006/24 nav spēkā.

Par pirmo jautājumu un otrā jautājuma a) un e) punktu, kā arī trešo jautājumu lietā C-293/12 un otro jautājumu lietā C-594/12

72 No iepriekšējā punktā nospriestā izriet, ka uz pirmo jautājumu, otrā jautājuma a) un e) punktu un trešo jautājumu lietā C-293/12, kā arī otro jautājumu lietā C-594/12 nav jāatbild.

Par tiesāšanās izdevumiem

73 Attiecībā uz pamatlietas dalībniekiem šī tiesvedība ir stadija procesā, kuru izskata iesniedzējtiesa, un tā lemj par tiesāšanās izdevumiem. Izdevumi, kas radušies, iesniedzot apsvērumus Tiesai, un kas nav minēto lietas dalībnieku izdevumi, nav atlīdzināmi.

Ar šādu pamatojumu Tiesa (virspalāta) nospriež:

Eiropas Parlamenta un Padomes 2006. gada 15. marta Direktīva 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 nav spēkā.

[Paraksti]