Lieta C-793/19

Lūguma sniegt prejudiciālu nolēmumu kopsavilkums saskaņā ar Tiesas Reglamenta 98. panta 1. punktu

Iesniegšanas datums:

2019. gada 29. oktobris

Iesniedzējtiesa:

Bundesverwaltungsgericht [Federālā administratīvā tiesa] (Vācija)

Datums, kurā pieņemts iesniedzējtiesas nolēmums:

2019. gada 25. septembris

Prasītāja un atbildētāja revīzijas tiesvedībā:

SpaceNet AG

Atbildētāja un revīzijas sūdzības iesniedzēja:

Bundesrepublik Deutschland

Pamatlietas priekšmets

Prasība atzīt, ka *SpaceNet* nav jāsaglabā *TKG* 113.b panta 3. punktā minētā informācija par telekomunikāciju datu plūsmu attiecībā uz saviem klientiem, kuriem šis uzņēmums sniedz interneta piekļuves pakalpojumus.

Lūguma sniegt prejudiciālu nolēmumu priekšmets un juridiskais pamats

Savienības tiesību, it īpaši Direktīvas 2002/58 15. panta 1. punkta, kā arī sprieduma *Tele2 Sverige* un *Watson* u.c. interpretācija; LESD 267. pants.

Prejudiciālais jautājums

Vai Direktīvas 2002/58/EK 15. pants, lasot to kopā ar Eiropas Savienības Pamattiesību hartas 7., 8. un 11. pantu, kā arī 52. panta 1. punktu, no vienas puses, un Eiropas Savienības Pamattiesību hartas 6. pantu, kā arī Līguma par Eiropas Savienību 4. pantu, no otras puses, ir jāinterpretē tādējādi, ka tas nepieļauj valsts tiesisko regulējumu, kurā publiski pieejamu elektronisko komunikāciju

pakalpojumu sniedzējiem tiek noteikts pienākums saglabāt šo pakalpojumu gala lietotāju datu plūsmas un atrašanās vietas datus, ja

– šis pienākums nav saistīts ar īpašu iemeslu vietas, laika vai telpas ziņā,

– saglabāšanas pienākums, sniedzot publiski pieejamus tālruņa pakalpojumus – ieskaitot īsziņu, multivides vai līdzīgu ziņu, kā arī neatbildētu vai neveiksmīgu zvanu pārsūtīšanu – attiecas uz šādiem datiem:

  – zvanītāja un adresāta pieslēguma, kā arī pārslēgšanas un pāradresēšanas gadījumā katra nākamā iesaistītā pieslēguma tālruņa numuru vai citu identifikatoru,

  – savienojuma sākuma un beigu datumu un laiku vai – īsziņas, multivides vai līdzīgas ziņas pārsūtīšanas gadījumā – ziņas nosūtīšanas un saņemšanas laiku, norādot piemērojamo laika joslu,

  – datiem par izmantoto pakalpojumu, ja tālruņa pakalpojuma ietvaros ir iespējams izmantot dažādus pakalpojumus,

  – mobilā tālruņa pakalpojumu gadījumā arī

    – zvanītāja un adresāta pieslēguma mobilo abonentu starptautisko identifikatoru,

    – zvanītāja un adresāta gala ierīces starptautisko identifikatoru,

    – pakalpojuma pirmās aktivizēšanas datumu un laiku, norādot piemērojamo laika joslu, ja par pakalpojumiem ir samaksāts avansā,

    – to šūnu nosaukumus, kas izmantotas zvanītāja un adresāta pieslēgumā, uzsākot savienojumu,

  – interneta tālruņa pakalpojumu gadījumā arī zvanītāja un adresāta pieslēguma interneta protokola adresēm un piešķirtajiem lietotāja identifikatoriem,

– saglabāšanas pienākums, sniedzot publiski pieejamus interneta piekļuves pakalpojumus, attiecas uz šādiem datiem:

  – interneta protokola adresi, kas abonentam piešķirta interneta lietošanai,

  – interneta lietošanai izmantotā pieslēguma nepārprotamu identifikatoru, kā arī piešķirto lietotāja identifikatoru,

  – interneta lietošanas piešķirtajā interneta protokola adresē sākuma un beigu datumu un laiku, norādot piemērojamo laika joslu,

  - mobilo sakaru lietošanas gadījumā tās šūnas nosaukumu, kas izmantota, uzsākot interneta savienojumu,

- nedrīkst saglabāt šādus datus:
  - komunikācijas saturu,
  - datus par atvērtajām tīmekļvietnēm,
  - datus par elektroniskā pasta pakalpojumiem,
  - datus, kuri ir tādu savienojumu pamatā, ko veic no/uz sociālās vai ar baznīcu saistītas jomas personu, iestāžu un organizāciju pieslēgumiem,
- atrašanās vietas datiem, proti, izmantotās šūnas nosaukuma, glabāšanas ilgums ir četras nedēļas un pārējiem datiem – desmit nedēļas,
- ir garantēta saglabāto datu efektīva aizsardzība pret ļaunprātīgas izmantošanas riskiem un jebkādu prettiesisku piekļuvi, un
- saglabātos datus drīkst izmantot tikai, lai izmeklētu īpaši smagus noziedzīgus nodarījumus un novērstu konkrētus draudus personas veselībai, dzīvībai vai brīvībai vai arī valstij vai federālajai zemei, izņemot abonentam interneta lietošanai piešķirtu interneta protokola adresi, ko ir atļauts izmantot abonentu informācijas iegūšanai, lai izmeklētu jebkādus noziedzīgus nodarījumus, novērstu sabiedriskās drošības un kārtības apdraudējumu, kā arī veiktu izlūkdienestu uzdevumus?

Atbilstošās Savienības tiesību normas

Eiropas Savienības Pamattiesību harta (turpmāk tekstā – "Harta"), tās 6., 7., 8., 11. un 52. pants

Līgums par Eiropas Savienību (LES), tā 4. un 6. pants

Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju), kas grozīta ar Eiropas Parlamenta un Padomes Direktīvu 2009/136/EK (2009. gada 25. novembris) (turpmāk tekstā – Direktīva 2002/58), tās 5., 6., 8. un 9. pants, it īpaši 15. pants; 11. apsvērums

Atbilstošās valsts tiesību normas

Telekommunikationsgesetz (*TKG*) [Telekomunikāciju likums], tā 113.a panta 1. punkta pirmais teikums ("Personas, kurām noteikti pienākumi"), 113.b pants ("Pienākumi saglabāt informāciju par datu plūsmu"), 113.c pants ("Datu

izmantošana"), 113.d pants ("Datu drošības garantēšana"), 113.e pants ("Reģistrēšana" [ko attiecībā uz piekļuvi saglabātajiem datiem veic persona, kurai noteikti pienākumi]), 113.f pants ("Prasības" [attiecībā uz tehniskajiem un citiem pasākumiem]), 99. panta 2. punkts ("Detalizēts savienojumu saraksts", attiecībā uz pozīcijām, kas detalizētajā savienojumu sarakstā netiek identificētas)

Strafprozessordnung (*StPO*) [Kriminālprocesa kodekss], tā 100.g panta 2. punkts ("Informācijas par datu plūsmu ievākšana" saskaņā ar *TKG* 113.b pantu)

Atbilstošā Tiesas judikatūra

Eiropas Savienības Tiesas spriedums, 2016. gada 21. decembris, *Tele2 Sverige* un *Watson* u.c., C-203/15 un C-698/15, EU:C:2016:970 (turpmāk tekstā – "spriedums *Tele2 Sverige* un *Watson* u.c.)

Spriedums, 2014. gada 8. aprīlis, *Digital Rights Ireland* un *Seitlinger* u.c., C-293/12 un C-594/12, EU:C:2014:238 (turpmāk tekstā – "spriedums *Digital Rights Ireland* u.c.")

Atzinums 1/15, 2017. gada 26. jūlijs, EU:C:2017:592

Papildus: spriedumi, 2019. gada 29. jūlijs, *Funke Medien* (C-469/17, EU:C:2019:623), 1978. gada 9. marts, *Simmenthal* (106/77, EU:C:1978:49), 2005. gada 3. maijs, *Berlusconi* u.c. (C-387/02, C-391/02 un C-403/02, EU:C:2005:270), 2010. gada 22. jūnijs, *Melki* un *Abdeli* (C-188/10 un C-189/10, EU:C:2010:363), 2014. gada 18. septembris, *Vueling Airlines* (C-487/12, EU:C:2014:2232).

Īss pamatlietas faktisko apstākļu un tiesvedības izklāsts

1 Prasītāja *SpaceNet AG* (turpmāk tekstā – "prasītāja" vai "*SpaceNet*") sniedz publiski pieejamus interneta piekļuves pakalpojumus. Tā apstrīd pienākumu, kurš tai noteikts ar *Telekommunikationsgesetz* (*TKG*) 2015. gada 10. decembrī publicētajā redakcijā 113.a panta 1. punktu apvienojumā ar šā likuma 113.b pantu un saskaņā ar kuru tai no 2017. gada 1. jūlija ir jāsaglabā informācija par tās klientu telekomunikāciju datu plūsmu.

2 Pirmajā instancē *Verwaltungsgericht* [Administratīvā tiesa] konstatēja, ka *SpaceNet* nav pienākuma saglabāt *TKG* 113.b panta 3. punktā minēto informāciju par telekomunikāciju datu plūsmu attiecībā uz saviem klientiem, kuriem tā nodrošina interneta piekļuvi. Atbildētāja, *Bundesrepublik Deutschland* [Vācijas Federatīvā Republika] (turpmāk tekstā – "atbildētāja"), izlaižot starpinstanci, iesniedza revīzijas sūdzību [*Sprungrevision*] par *Verwaltungsgericht* spriedumu.

3 Revīzijas sūdzība būtu jāapmierina tikai tad, ja minētajās *TKG* normās noteiktais publiski pieejamu telekomunikāciju pakalpojumu sniedzēju (turpmāk tekstā –

"telekomunikāciju pakalpojumu sniedzēji") pienākums saglabāt informāciju par telekomunikāciju datu plūsmu nav pretrunā Savienības tiesībām.

4 Šis telekomunikāciju pakalpojumu sniedzēju pienākums ierobežotu laiku glabāt konkrētu informāciju par datu plūsmu tika no jauna regulēts ar 2015. gada 10. decembra *Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten* (Likums, ar ko ievieš saglabāšanas pienākumu un maksimālo termiņu informācijas par datu plūsmu glabāšanai, turpmāk tekstā – "2015. gada 10. decembra likums").

5 Jauns tiesiskais regulējums bija nepieciešams pēc tam, kad *Bundesverfassungsgericht* [Federālā konstitucionālā tiesa] ar 2010. gada spriedumu pamattiesību pārkāpuma dēļ atzina par spēkā neesošām iepriekšējās tiesību normas, kurās bija reglamentēta datu saglabāšana, un kad pēc tam ar spriedumu *Digital Rights Ireland* u.c. tika atcelta arī Direktīva 2006/24, kuras transponēšanai bija pieņemtas šīs iepriekšējās tiesību normas. 2015. gada 10. decembra likuma uzdevums ir novērst nepilnības kriminālvajāšanas un apdraudējuma novēršanas jomā, vienlaikus ņemot vērā konstitucionālās un Savienības tiesību prasības, kas izriet no minētajiem spriedumiem.

6 Lai atbildētu uz jautājumu, vai *TKG* 113.a panta 1. punktā apvienojumā ar šā likuma 113.b pantu noteiktais saglabāšanas pienākums ir pretrunā Savienības tiesībām, ir vajadzīga Tiesas sniegta Direktīvas 2002/58 interpretācija un it īpaši precizējums, kā ir jāsaprot spriedums *Tele2 Sverige* un *Watson* u.c.

Īss lūguma sniegt prejudiciālu nolēmumu motīvu izklāsts

7 *TKG* 113.a panta 1. punkta pirmajā teikumā apvienojumā ar šā likuma 113.b pantu noteiktais pienākums saglabāt informāciju par telekomunikāciju datu plūsmu ierobežo tiesības, kas paredzētas Direktīvas 2002/58 5. panta 1. punktā, 6. panta 1. punktā un 9. panta 1. punktā.

8 Tas iejaucas elektroniskās komunikācijas konfidencialitātē, kas ir aizsargāta šīs direktīvas 5. panta 1. punkta pirmajā teikumā, un ir pretrunā principam, saskaņā ar kuru ikvienai personai, kura nav lietotājs, principā ir aizliegts bez tās piekrišanas saglabāt informāciju par datu plūsmu, kas saistīta ar elektronisko komunikāciju.

9 Turklāt šis pienākums nav atbilstīgs direktīvas 6. pantā noteiktajai prasībai, ka informāciju par datu plūsmu drīkst apstrādāt un saglabāt tikai, lai sagatavotu rēķinus par pakalpojumiem, to tirdzniecības nolūkā un lai sniegtu pievienotās vērtības pakalpojumus līdz tādam līmenim un tik ilgi, cik nepieciešams.

10 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, Direktīvas 2002/58 9. panta 1. punkta pirmajā teikumā ir noteikts, ka šādus datus var apstrādāt tikai tad, kad tie ir padarīti anonīmi, vai ar lietotāju vai abonentu piekrišanu, līdz tādam

līmenim un tik ilgi, cik nepieciešams, lai sniegtu pievienotās vērtības pakalpojumus. Tiesiskajā regulējumā netiek ievērota arī šī prasība, jo saskaņā ar *TKG* 113.b panta 1. punkta 2. apakšpunktu apvienojumā ar šā likuma 4. punktu ir jāsaglabā arī tajos minētie atrašanās vietas dati.

11 Direktīvas 2002/58/EK 5. panta 1. punktā, 6. panta 1. punktā un 9. panta 1. punktā noteikto tiesību ierobežojums ir attaisnots tikai tad, ja tiesisko regulējumu *TKG* 113.a panta 1. punkta pirmajā teikumā apvienojumā ar šā likuma 113.b pantu var pamatot ar Direktīvas 2002/58 15. panta 1. punktu.

12 Saskaņā ar to dalībvalstis var pieņemt tiesību aktus, lai ierobežotu šīs direktīvas 5. un 6. pantā, 8. panta 1., 2., 3. un 4. punktā un 9. pantā minētās tiesības un pienākumus, ja šāds ierobežojums ir vajadzīgs saskaņā ar nepieciešamiem, atbilstīgiem un samērīgiem pasākumiem demokrātiskā sabiedrībā, lai garantētu valsts drošību, aizsardzību, sabiedrības drošību un noziedzīgu nodarījumu vai elektroniskās komunikāciju sistēmas nevēlamas izmantošanas novēršanu, izmeklēšanu, noteikšanu un kriminālvajāšanu, kā noteikts Direktīvas 95/46 13. panta 1. punktā. Tālab dalībvalstis tostarp var pieņemt tiesību aktus, paredzot datu saglabāšanu ierobežotā laikposmā, kas pamatots ar šajā punktā noteiktajiem iemesliem. Visiem šajā punktā minētajiem pasākumiem ir jābūt saskaņā ar Kopienas tiesību aktu vispārējiem principiem, tostarp tiem, kas minēti Līguma par Eiropas Savienību (LES) 6. panta 1. un 2. punktā.

13 Atbilstoši Tiesas apsvērumiem spriedumā *Tele2 Sverige* un *Watson* u.c., it īpaši šā sprieduma 82. un nākamajos punktos, kā arī 108. un nākamajos punktos, tas, vai ir pieļaujams valsts tiesiskais regulējums par datu saglabāšanu saskaņā ar Direktīvas 2002/58 15. panta 1. punktu, ir atkarīgs no tā, vai pastāv pietiekams iemesls. Tas nozīmē, ka dati tiek ievākti tikai par personām, kas norāda uz saikni ar smagiem noziedzīgiem nodarījumiem, ka tiek piemērots ierobežojums attiecībā uz reģionu, laikposmu un saziņas līdzekļiem, kuri attiecas uz šo iemeslu, un ka tiek ievākti tikai dati, kas ir būtiski norādīto noziedzīgo nodarījumu atklāšanai.

14 Šim apstāklim acīmredzami neatbilst atbildētājas viedoklis, ka jau pats fakts, ka tiek izmantoti interneta piekļuves vai tālruņa pakalpojumi, ir uzskatāms par pietiekamu iemeslu datu saglabāšanai. Spriedumā *Tele2 Sverige* un *Watson* u.c. minēto pieņēmumu par jebkādas datu beziemesla saglabāšanas vispārēju nesaderību ar Savienības tiesībām neatspēko arī atbildētājas norāde uz Tiesas 2017. gada 26. jūlija atzinumu par Kanādas un Eiropas Savienības nolīgumu par pasažieru datu reģistra datu pārsūtīšanu. Saistībā ar nepieciešamību iejaukties pamattiesībās uz privātās dzīves neaizskaramību un uz personas datu aizsardzību Tiesa gan ir uzsvērusi, ka PDR datu pārsūtīšana uz Kanādu notiek neatkarīgi no jebkādām objektīvām pazīmēm, kas liecinātu, ka pasažieri varētu apdraudēt sabiedrisko drošību Kanādā. Tomēr šajā gadījumā tā nav datu saglabāšana bez iemesla, jo saglabāšana un pārsūtīšana ir saistītas ar robežkontrolēm, kas saskaņā ar piemērojamām Kanādas tiesību normām attiecas uz visiem pasažieriem, kuri vēlas ieceļot Kanādā vai izceļot no tās. Līdz ar pasažieru izceļošanu šis saglabāšanas iemesls zūd. Tāpēc turpmāka saglabāšana pēc šā brīža – kā jauns

iemesls – ir atkarīga no tā, vai pastāv objektīvas pazīmes, kas liecina, ka attiecīgie pasažieri var radīt apdraudējumu saistībā ar cīņu pret terorismu un smagiem starptautiskiem noziegumiem.

15 Ja Tiesas judikatūra ir jāsaprot tādējādi, ka datu beziemesla saglabāšana nekādos apstākļos nav saderīga ar Savienības tiesībām, nav iespējams apmierināt atbildētājas revīzijas sūdzību par pārsūdzēto *Verwaltungsgericht* spriedumu. Tas tādēļ, ka tāpat kā Zviedrijas un Apvienotās Karalistes tiesību aktos par datu saglabāšanu, kas bija sprieduma *Tele2 Sverige* un *Watson* u.c. priekšmets, *TKG* 113.a panta 1. punkta pirmajā teikumā apvienojumā ar šā likuma 113.b pantu netiek prasīts nedz saglabāšanas iemesls, kas ir plašāks par interneta piekļuves vai tālruņa pakalpojumu vienkāršu izmantošanu, nedz saikne starp saglabātajiem datiem un noziedzīgu nodarījumu vai sabiedriskās drošības apdraudējumu. Drīzāk runa ir par tiesisko regulējumu, kurā ir noteikta beziemesla, vispārēja saglabāšana, nešķirojot pēc personas, laika vai ģeogrāfiski, attiecībā uz lielu daļu no visas būtiskās informācijas par telekomunikāciju datu plūsmu.

16 Tomēr, neraugoties uz apsvērumiem spriedumā *Tele2 Sverige* un *Watson* u.c., iesniedzējtiesa pieļauj iespēju, ka *TKG* 113.a panta 1. punkta pirmajā teikumā apvienojumā ar šā likuma 113.b pantu noteikto pienākumu bez iemesla saglabāt informāciju par telekomunikāciju datu plūsmu var pamatot ar Direktīvas 2002/58 15. panta 1. punktu, proti, ņemot vērā turpmāk minētos apsvērumus:

17 Pirmkārt, strīdīgajās *TKG* normās netiek prasīts saglabāt visu abonentu un reģistrēto lietotāju informāciju par telekomunikāciju datu plūsmu attiecībā uz visiem elektronisko sakaru līdzekļiem. Saglabāšanas pienākums neattiecas ne tikai uz saziņas saturu, bet drīkst nesaglabāt arī datus par atvērtajām tīmekļvietnēm, elektroniskā pasta pakalpojumu datus, kā arī datus, kuri ir tādu savienojumu pamatā, ko veic no/uz sociālās vai ar baznīcu saistītas jomas pieslēgumiem (skat. *TKG* 113.b panta 5. un 6. punktu). Ja konkrēti sakaru līdzekļi vai datu kategorijas ir atbrīvoti no saglabāšanas pienākuma, tas, protams, neļauj novērst attiecīgo personu profilēšanas risku, bet tā vismaz var būtiski samazināt šo risku.

18 Vēl svarīgāku atšķirību starp šajā lietā strīdīgajām *TKG* tiesību normām un Direktīvas 2006/24 iepriekšējo tiesisko regulējumu respektīvi uz to balstītajiem Zviedrijas un Apvienotās Karalistes tiesību aktiem, par kuriem bija runa spriedumā *Tele2 Sverige* un *Watson* u.c., iesniedzējtiesa, otrkārt, saskata apstāklī, ka glabāšanas termiņš no sešiem mēnešiem līdz diviem gadiem (skat. Direktīvas 2006/24 6. pantu) saskaņā ar *TKG* 113.b panta 1. punktu ir ievērojami saīsināts līdz četrām un attiecīgi desmit nedēļām.

19 Attiecīgo personu profilēšanas risks ir uzskatāms par jo mazāku, jo vairāk ir saīsināti laikposmi, kuros tiek glabāta informācija par datu plūsmu. Proti, jo īsāks ir glabāšanas laikposms, jo neizbēgami nepilnīgāks kļūst personības profils un jo mazāk intensīvi tiek ierobežotas pamattiesības.

20 Treškārt, uz šajā lietā strīdīgajām *TKG* normām attiecas stingri ierobežojumi attiecībā uz saglabāto datu aizsardzību un piekļuvi šiem datiem. Pirmām kārtām ar *TKG* 113.d un nākamo pantu prasībām tiek garantēta saglabāto datu efektīva aizsardzība pret ļaunprātīgas izmantošanas riskiem un jebkādu prettiesisku piekļuvi. Otrām kārtām saskaņā ar *TKG* 113.c panta 1. punktu saglabātos datus drīkst izmantot tikai, lai apkarotu smagus noziedzīgus nodarījumus vai novērstu konkrētus draudus personas veselībai, dzīvībai vai brīvībai vai arī valstij vai federālajai zemei.

21 Saskaņā ar *StPO* 100.g panta 2. punktu informācijas par datu plūsmu ievākšana kriminālprocesa vajadzībām ir atkarīga no tā, vai pastāv aizdomas par kādu īpaši smagu noziedzīgu nodarījumu, kuri izsmeļoši ir norādīti likumā, nodarījums ir īpaši smags arī individuālā gadījumā, būtu ļoti sarežģīti vai bezcerīgi citādi noskaidrot faktiskos apstākļus vai personas, pret kuru tiek veikts kriminālprocess, atrašanās vietu un datu ievākšana ir samērīga ar lietas nozīmīgumu. Saskaņā ar *StPO* 100.g panta 4. pantu ir aizliegts ievākt vai izmantot informāciju par datu plūsmu attiecībā uz *StPO* 53. panta 1. punkta pirmā teikuma 1.–5. punktā minētajiem dienesta noslēpuma glabātājiem, piemēram, advokātiem, ārstiem vai žurnālistiem. Turklāt *StPO* 101.a panta 1. punktā attiecībā uz informācijas par datu plūsmu ievākšanu saskaņā ar *StPO* 100.g pantu ir paredzēta tiesnešu prerogatīva.

22 Ir tiesa, ka šie ierobežojošie piekļuves noteikumi nav piemērojami attiecībā uz interneta protokola adresi, kas abonentam piešķirta interneta lietošanai. Tas tādēļ, ka saskaņā ar *TKG* 113.c panta 1. punkta 3. apakšpunktu to var izmantot arī, iegūstot abonentu informāciju, lai izmeklētu jebkādus noziedzīgus nodarījumus un novērstu sabiedriskās drošības un kārtības apdraudējumus, kā arī kopumā veiktu izlūkdienestu uzdevumus. Tomēr ir jāpieņem, ka informācijas sniegšana par to, kurš pieslēguma īpašnieks bija pieslēdzies jau zināmā interneta protokola adresē, neļauj izveidot personības un pārvietošanās profilu.

23 Pat ievērojot *SpaceNet* argumentāciju un pieņemot, ka aizvien vairāk tiek izmantotas tehniskas metodes, kad interneta protokola adresi vairs nevar viennozīmīgi attiecināt uz konkrētu telekomunikāciju pieslēgumu, bet gan tikai uz vairāku pieslēgumu grupu, un tāpēc abonentu informācijas iegūšana ir kļuvusi par ievērojama vēriena pasākumu, šādas abonentu informācijas iegūšanas iejaukšanās intensitāte joprojām ir daudz zemāka par to, kāda ir informācijas par telekomunikāciju datu plūsmu pieprasīšanai un izmantošanai.

24 Ceturtkārt, par labu pieņēmumam, ka *TKG* 113.a panta 1. punkta pirmajā teikumā apvienojumā ar šā likuma 113.b pantu noteiktais pienākums bez iemesla saglabāt informāciju par telekomunikāciju datu plūsmu var tikt pamatots ar Direktīvas 2002/58 15. panta 1. punktu, liecina arī fakts, ka tādējādi valsts likumdevējs ir izpildījis pienākumus rīkoties, kuri dalībvalstīm izriet no Hartas 6. pantā garantētajām tiesībām uz drošību. Spriedumā *Digital Rights Ireland* u.c. Tiesa skaidri ir minējusi Hartas 6. pantu un šajā saistībā ir norādījusi, ka cīņa pret starptautisko terorismu, lai saglabātu mieru pasaulē un starptautisko drošību, ir

Savienības vispārējo interešu mērķis un ka tas pats attiecas uz smagu noziedzīgu nodarījumu apkarošanu, lai nodrošinātu sabiedrisko drošību.

25 Šādā kontekstā iesniedzējtiesa šaubās, vai Tiesas līdzšinējā judikatūra ir jāsaprot tādējādi, ka datu beziemesla saglabāšanu nevar pamatot ar Direktīvas 2002/58 15. panta 1. punktu ne tikai tās konkrētajā formulējumā, kas ir atrasts Direktīvā 2002/58 un uz to balstītajos Zviedrijas un Apvienotās Karalistes tiesību aktos, bet arī principā. Tas tādēļ, ka informācijas par datu plūsmu saglabāšanas pamatjēdzienu nav iespējams saskaņot ar bez jebkādiem ierobežojumiem formulēto Tiesas prasību, lai saglabājamie dati tiktu nošķirti pēc personām, laikposmiem un ģeogrāfiskām teritorijām.

26 Pret pieņēmumu, ka informācijas par datu plūsmu beziemesla saglabāšana *per se* ir nesaderīga ar Hartu, iesniedzējtiesas skatījumā liecina arī prasība izveidot līdzsvaru starp dalībvalstu pienākumu garantēt tās teritorijā esošo personu drošību, no vienas puses, un Hartas 7. un 8. pantā nostiprināto pamattiesību ievērošanu, no otras puses.

27 Tādējādi no Tiesas judikatūras iesniedzējtiesa nevar nepārprotami secināt, ka valsts likumdevējiem vairs nav jābūt iespējai, pamatojoties uz visaptverošu izvērtējumu, ieviest datu saglabāšanu bez iemesla – attiecīgā gadījumā papildinot to ar stingriem piekļuves noteikumiem –, lai ņemtu vērā specifisko apdraudējuma potenciālu, kas ir saistīts ar jaunajiem telekomunikāciju līdzekļiem.

28 Piektkārt, iesniedzējtiesa norāda, ka gadījumā, ja datu beziemesla saglabāšanu principā nevar pamatot ar Direktīvas 2002/58 15. panta 1. punktu un līdz ar to nav nozīmes konkrētajiem noteikumiem par attiecīgajiem sakaru līdzekļiem, par saglabājamo datu kategorijām, par glabāšanas ilgumu, par nosacījumiem attiecībā uz piekļuvi saglabātajiem datiem un par aizsardzību pret ļaunprātīgas izmantošanas riskiem, būtu būtiski ierobežota valstu likumdevēju rīcības brīvība kriminālprocesa un sabiedriskās drošības jomā, kas saskaņā ar LES 4. panta 2. punkta trešo teikumu katrā ziņā principā paliek katras dalībvalsts ekskluzīvas atbildības jomā.

29 Visbeidzot, seškārt, tas, vai Tiesas apsvērumi spriedumā *Tele2 Sverige* un *Watson* u.c. ir jāsaprot kā dalībvalstīm adresēts aizliegums ar Direktīvas 2002/58 15. panta 1. punktu pamatot pienākuma bez iemesla saglabāt informāciju par telekomunikāciju datu plūsmu ieviešanu, iesniedzējtiesai nešķiet skaidrs arī, ņemot vērā Eiropas Cilvēktiesību tiesas (turpmāk tekstā – "ECT") jaunāko judikatūru.

30 Nesen 2018. gada 19. jūnija spriedumā ECT nosprieda, ka Zviedrijas tiesību akti par pārrobežu datu plūsmas masveida novērošanu ir saderīgi ar Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas (turpmāk tekstā – "ECPAK") 8. pantu. Ņemot vērā draudus, ar ko pašlaik saskaras valstis, tostarp postu, ko rada globālais terorisms un citi smagi noziedzīgi nodarījumi, piemēram, narkotisko vielu tirdzniecība, cilvēku tirdzniecība, bērnu seksuāla izmantošana un

kibernoziedzība, kā arī tehnisko attīstību, kas teroristiem un noziedzniekiem ļauj vieglāk izvairīties no viņu atklāšanas internetā, un elektronisko datu pārsūtīšanas veidu neparedzamību, lēmums izveidot masu novērošanas sistēmu, lai identificētu līdz šim nezināmus draudus valsts drošībai, joprojām ietilpst valsts novērtējuma brīvībā (ECT spriedums, 2018. gada 19. jūnijs, Nr. 35252/08 [ECLI:CE:ECHR:2018:0619JUD003525208], *Centrum för Rättvisa* pret Zviedriju, 112. punkts). Ciktāl ECT atsaucas uz elektronisko datu pārsūtīšanas veidu neparedzamību, kā arī uz tehnisko attīstību, kas teroristiem un noziedzniekiem ļauj vieglāk izvairīties no viņu atklāšanas internetā, tā vairāk nekā Eiropas Savienības Tiesa uzsver specifisko apdraudējuma potenciālu, kurš ir saistīts ar jaunajiem telekomunikāciju līdzekļiem.

31 Iesniedzējtiesa atsaucas uz Direktīvas 2002/58 11. apsvērumu un Hartas 52. panta 3. punktu, no kuriem izriet, ka ir jārada vajadzīgā saskaņotība starp Hartā nostiprinātajām tiesībām un attiecīgajām ECPAK garantētajām tiesībām, neietekmējot Savienības tiesību un Eiropas Savienības Tiesas autonomiju.

32 Nobeigumā iesniedzējtiesa min citas uzsāktas prejudiciālā nolēmuma tiesvedības, kurās runa ir par sprieduma *Tele2 Sverige* un *Watson* u.c. interpretāciju, proti, vai no tā ir jāsecina vispārējs datu beziemesla saglabāšanas aizliegums, no kura nevar atkāpties, nedz atsaucoties uz sabiedriskās drošības apdraudējuma novēršanas nozīmīgumu, nedz saistībā ar "kompensēšanu" ar ierobežojošiem piekļuves noteikumiem un augstām drošības prasībām.

33 Tiek minēti *Investigatory Powers Tribunal – London* [Londonas Izmeklēšanas pilnvaru tribunāla] (Apvienotā Karaliste) lūgumi sniegt prejudiciālu nolēmumu (C-623/17), *Conseil d'État* [Valsts padomes] (Francija) lūgumi sniegt prejudiciālu nolēmumu (C-511/18 un C-512/18) un Beļģijas Konstitucionālās tiesas (C-520/18) lūgums sniegt prejudiciālu nolēmumu.