TIESAS SPRIEDUMS (virspalāta)

2022. gada 20. septembrī*

[Teksts labots ar 2022. gada 27. oktobra rīkojumu]

Lūgums sniegt prejudiciālu nolēmumu – Personas datu apstrāde elektronisko komunikāciju nozarē – Komunikāciju konfidencialitāte – Elektronisko komunikāciju pakalpojumu sniedzēji – Informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta glabāšana – Direktīva 2002/58/EK – 15. panta 1. punkts – Eiropas Savienības Pamattiesību harta – 6., 7., 8. un 11. pants, kā arī 52. panta 1. punkts – LES 4. panta 2. punkts

Apvienotajās lietās C-793/19 un C-794/19

par lūgumiem sniegt prejudiciālu nolēmumu atbilstoši LESD 267. pantam, ko *Bundesverwaltungsgericht* (Federālā administratīvā tiesa, Vācija) iesniegusi ar 2019. gada 25. septembra lēmumiem un kas Tiesā reģistrēti 2019. gada 29. oktobrī, tiesvedībās

Bundesrepublik Deutschland, kuru pārstāv *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*,

pret

SpaceNet AG (C-793/19),

Telekom Deutschland GmbH (C-794/19),

TIESA (virspalāta)

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

ģenerāladvokāts: M. Kamposs Sančess-Bordona [*M. Campos Sánchez-Bordona*],

sekretārs: D. Diterts [*D. Dittert*], nodaļas vadītājs,

ņemot vērā rakstveida procesu un 2021. gada 13. septembra tiesas sēdi,

* Tiesvedības valoda – vācu.

ņemot vērā apsvērumus, ko snieguši:

– *Bundesrepublik Deutschland*, kuru pārstāv *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen*, vārdā – *C. Mögelin*, pārstāvis,

– [labots ar 2022. gada 27. oktobra rīkojumu] *SpaceNet AG* vārdā – *M. Bäcker, Universitätsprofessor*,

– *Telekom Deutschland GmbH* vārdā – *T. Mayen, Rechtsanwalt*,

– Vācijas valdības vārdā – *J. Möller, F. Halibi, M. Hellmann, D. Klebs* un *E. Lankenau*, pārstāvji,

– Dānijas valdības vārdā – *M. Jespersen, J. Nymann-Lindegren, V. Pasternak Jørgensen* un *M. Søndahl Wolff*, pārstāvji,

– Igaunijas valdības vārdā – *A. Kalbus* un *M. Kriisa*, pārstāves,

– Īrijas vārdā – *A. Joyce* un *J. Quaney*, pārstāvji, kam palīdz *D. Fennelly, BL*, un *P. Gallagher, SC*,

– Spānijas valdības vārdā – *L. Aguilera Ruiz*, pārstāvis,

– Francijas valdības vārdā – *A. Daniel, D. Dubois, J. Illouz, E. de Moustier* un *T. Stéhelin*, pārstāvji,

– Kipras valdības vārdā – *I. Neophytou*, pārstāve,

– Nīderlandes valdības vārdā – *M. K. Bulterman, A. Hanje* un *C. S. Schillemans*, pārstāves,

– Polijas valdības vārdā –*B. Majczyna, D. Lutostańska* un *J. Sawicka*, pārstāvji,

– Somijas valdības vārdā – *A. Laine* un *M. Pere*, pārstāves,

– Zviedrijas valdības vārdā – *H. Eklinder, A. Falk, J. Lundberg, C. Meyer-Seitz, R. Shahsavan Eriksson* un *H. Shev*, pārstāves,

– Eiropas Komisijas vārdā – *G. Braun, S. L. Kalėda, H. Kranenborg, M. Wasmeier* un *F. Wilman*, pārstāvji,

– Eiropas Datu aizsardzības uzraudzītāja vārdā – *A. Buchta, D. Nardi, N. Stolič* un *K. Ujazdowski*, pārstāvji,

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

pasludina šo spriedumu.

Spriedums

1 Lūgumi sniegt prejudiciālu nolēmumu ir par to, kā interpretēt Eiropas Parlamenta un Padomes Direktīvas 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko

komunikāciju) (OV 2002, L 201, 37. lpp.), redakcijā ar grozījumiem, kas izdarīti ar Eiropas Parlamenta un Padomes 2009. gada 25. novembra Direktīvu 2009/136/EK (OV 2009, L 337, 11. lpp.) (turpmāk tekstā – "Direktīva 2002/58"), 15. panta 1. punktu, lasot to Eiropas Savienības Pamattiesību hartas (turpmāk tekstā – "Harta") 6.–8. un 11. panta, kā arī 52. panta 1. punkta un LES 4. panta 2. punkta gaismā.

2 Šie lūgumi ir iesniegti saistībā ar tiesvedībām starp *Bundesrepublik Deutschland* (Vācijas Federatīvā Republika), kuru pārstāv *Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen* (Federālā elektroenerģijas, gāzes, telekomunikāciju, pasta un dzelzceļa tīklu aģentūra, Vācija), no vienas puses, un uzņēmumiem *SpaceNet AG* (lieta C-793/19) un *Telekom Deutschland GmbH* (lieta C-794/19), no otras puses, par šiem uzņēmumiem uzlikto pienākumu glabāt informāciju par savu klientu telekomunikāciju datu plūsmu un atrašanās vietas datus.

Atbilstošās tiesību normas

Savienības tiesības

Direktīva 95/46/EK

3 Eiropas Parlamenta un Padomes Direktīva 95/46/EK (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV 1995, L 281, 31. lpp.) kopš 2018. gada 25. maija ir atcelta ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (OV 2016, L 119, 1. lpp.).

4 Direktīvas 95/46 3. panta 2. punktā bija noteikts:

"Šī direktīva neattiecas uz personas datu apstrādi:

– tādu pasākumu gaitā, uz kuru neattiecas Kopienas tiesību akti, kā Līguma par Eiropas Savienību V un VI sadaļā paredzētie pasākumi un, jebkurā gadījumā, uz apstrādes operācijām attiecībā uz sabiedrisko drošību, aizsardzību, valsts drošību (ieskaitot valsts ekonomisko labklājību, ja apstrādes operācija attiecas uz valsts drošības jautājumiem) un uz valsts pasākumiem krimināltiesību jomā;

– ko veic fiziska persona tikai un vienīgi personiska vai mājsaimnieciska pasākuma gaitā."

Direktīva 2002/58

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

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

[..]

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

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

[..]

(11) Tāpat kā Direktīva [95/46], 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 [pārtveršanu] vai pieņemt citus pasākumus, ja tie nepieciešami jebkuram no šiem nolūkiem un ir saskaņā ar [Romā 1950. gada 4. novembrī parakstīto] Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvenciju, kā skaidrots Eiropas Cilvēktiesību tiesas nolēmumos. Šādiem pasākumiem jābūt atbilstošiem, stingri samērīgiem ar paredzēto nolūku un nepieciešamiem demokrātiskā sabiedrībā, un tiem jāatbilst attiecīgajiem drošības pasākumiem saskaņā ar Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvenciju."

6 Šīs direktīvas 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 aprite Kopienā.

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

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

7 Saskaņā ar minētās direktīvas 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:

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

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 līmenim, kad informāciju var attiecināt uz identificējamu abonentu vai lietotāju, kas saņem šo informāciju;

[..]."

8 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."

9 Saskaņā ar šīs direktīvas 5. pantu "Komunikāciju konfidencialitāte":

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

[..]

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."

10 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.

[..]"

11 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 tādam līmenim un tik ilgi, cik nepieciešams, lai sniegtu pievienotās vērtības pakalpojumus. Pakalpojuma sniedzējam ir jāinformē lietotāji vai abonenti 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. [..]"

12 Direktīvas 2002/58 15. panta "Direktīvas [95/46] dažu noteikumu piemērošana" 1. punktā ir noteikts:

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

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

Vācijas tiesības

TKG

13 2004. gada 22. jūnija *Telekommunikationsgesetz* (Telekomunikāciju likums; *BGBl*. 2004 I, 1190. lpp.), redakcijā, kas piemērojama pamatlietām (turpmāk tekstā – "*TKG*"), 113.a panta 1. punkta pirmais teikums ir formulēts šādi:

"Pienākumi attiecībā uz 113.b–113.g pantā noteiktās informācijas par datu plūsmu glabāšanu, izmantošanu un drošību attiecas uz operatoriem, kas sniedz publiski pieejamus telekomunikāciju pakalpojumus galalietotājiem."

14 Saskaņā ar *TKG* 113.b pantu:

"(1) Operatoriem, kas minēti 113.a panta 1. punktā, ir jāglabā dati valsts teritorijā šādā kārtībā:

1. šā panta 2. un 3. punktā minētie dati jāglabā desmit nedēļas,

2. šā panta 4. punktā minētie atrašanās vietas dati jāglabā četras nedēļas.

(2) Publiski pieejamu telefonijas pakalpojumu sniedzējiem ir jāglabā:

1. zvanītāja un adresāta, kā arī – pārslēgšanas un pāradresēšanas gadījumā katra nākamā iesaistītā – abonenta numurs vai cits identifikators,

2. savienojuma sākuma un beigu datums un laiks, norādot atbilstošo laika joslu,

3. dati par izmantoto pakalpojumu, ja tālruņa pakalpojuma ietvaros ir iespējams izmantot dažādus pakalpojumus,

4. mobilā tālruņa pakalpojumu gadījumā arī
   a) zvanītāja un adresāta pieslēguma mobilo abonentu starptautiskais identifikators,
   b) zvanītāja un adresāta galaierīces starptautiskais identifikators,
   c) priekšapmaksas pakalpojumu gadījumā – pakalpojuma pirmās aktivizēšanas datums un laiks, norādot atbilstošo laika joslu,

5. interneta tālruņa pakalpojumu gadījumā arī zvanītāja un adresāta IP (interneta protokola) adreses un piešķirtie lietotāja identifikatori.

Pirmā daļa ir piemērojama *mutatis mutandis*

1. īsziņas, multivides vai līdzīgas ziņas pārsūtīšanai; šajā gadījumā pirmās daļas 2. punktā minētās norādes ir aizvietojamas ar ziņas nosūtīšanas un saņemšanas laiku;

2. neatbildētiem vai nesekmīgiem zvaniem, ja notikusi tīkla pārvaldības iejaukšanās [..].

(3) Publiski pieejamu interneta pakalpojumu sniedzējiem ir jāglabā:

1. IP adrese, kas abonentam piešķirta interneta lietošanai,

2. interneta lietošanai izmantotā savienojuma nepārprotams identifikators, kā arī piešķirtais lietotāja identifikators,

3. ar piešķirto IP adresi veiktās interneta lietošanas sākuma un beigu datums un laiks, norādot atbilstošo laika joslu.

(4) Mobilo sakaru lietošanas gadījumā ir jāglabā to telefonijas šūnu nosaukums, kuras, uzsākot savienojumu, izmantotas zvanītājam un adresātam. Ja publiski pieejamu internetpiekļuves pakalpojumu kontekstā tiek lietoti mobilie sakari, ir jāglabā interneta savienojuma sākumā izmantoto telefonijas šūnu nosaukums. Jāglabā arī dati, kas ļauj noteikt attiecīgo telefonijas šūnu apkalpojošās antenas ģeogrāfisko atrašanās vietu un maksimālo apraides zonu.

(5) Saskaņā ar šo pantu netiek glabāts komunikācijas saturs, dati par aplūkotajām tīmekļvietnēm un dati par elektroniskā pasta pakalpojumiem.

(6) Datus par 99. panta 2. punktā paredzētajām komunikācijām saskaņā ar šo normu nevar glabāt. Tas ir *mutatis mutandis* piemērojams telefonijas komunikācijām, ko veic 99. panta 2. punktā minētie subjekti. Šā likuma 99. panta 2. punkta otrais un septītais teikums tiek piemērots *mutatis mutandis*.

[..]”

15 *TKG* 99. panta 2. punktā minētās komunikācijas, uz kurām ir norādīts *TKG* 113.b panta 6. punktā, ir komunikācijas ar sociāla vai reliģiska rakstura personām, iestādēm un organizācijām, kuras piedāvā personām – kuras pārsvarā paliek anonīmas – telefoniskas palīdzības pakalpojumus psiholoģiska vai sociāla rakstura ārkārtas situācijās un uz kurām pašām vai kuru darbiniekiem šajā ziņā attiecas īpaši konfidencialitātes pienākumi. *TKG* 99. panta 2. punkta otrajā un ceturtajā teikumā paredzētais izņēmums ir pakārtots prasībai par to, ka zvana saņēmējiem pēc viņu pieteikuma jābūt iekļautiem Federālās elektroenerģijas, gāzes, telekomunikāciju, pasta un dzelzceļa tīklu aģentūras pārvaldītajā sarakstā pēc tam, kad abonenta numuru īpašnieki ir pierādījuši savu uzdevumu, iesniedzot apliecinājumu no kādas iestādes vai subjekta, vai fonda, kas ir publisko tiesību subjekti.

16 Saskaņā ar *TKG* 113.c panta 1. un 2. punktu:

“(1) Saskaņā ar 113.b pantu glabātos datus var:

1. pārsūtīt tiesībaizsardzības iestādei, ja tā šādu pārsūtīšanu pieprasa, atsaucoties uz tiesību normu, kas sniedz tai tiesības vākt 113.b pantā paredzētos datus īpaši smagu noziedzīgu nodarījumu apkarošanai;

2. pārsūtīt federālo zemju drošības iestādēm, ja tās šādu pārsūtīšanu pieprasa, atsaucoties uz tiesību normu, kas sniedz tām tiesības vākt 113.b pantā paredzētos datus konkrētu draudu personas veselībai, dzīvībai vai brīvībai vai federatīvās valsts vai federālās zemes pastāvēšanas apdraudējuma novēršanai;

[..].

(2) Saskaņā ar 113.b pantu glabātos datus personas vai iestādes, uz kurām attiecas pienākumi, kas noteikti 113.a panta 1. punktā, var izmantot tikai [šā panta] 1. punktā noteiktajiem mērķiem."

17 *TKG* 113.d pantā ir noteikts:

"113.a panta 1. punktā paredzētā pienākuma subjektam ir jānodrošina, ka dati, kas glabāti atbilstoši 113.b panta 1. punktam saskaņā ar glabāšanas pienākumu, būtu ar jaunākajam tehnikas attīstības līmenim atbilstošiem tehniskajiem un organizatoriskajiem pasākumiem aizsargāti pret neatļautu kontroli un izmantošanu. Šie pasākumi ir konkrēti šādi:

1. īpaši drošas šifrēšanas procedūras izmantošana,

2. uzglabāšana atsevišķās uzglabāšanas infrastruktūrās, kas ir nodalītas no parastajām operatīvajām funkcijām paredzētajām,

3. uzglabāšana, nodrošinot augsta līmeņa aizsardzību pret kiberuzbrukumiem personas datu apstrādes informācijas sistēmām, kas ir atsaistītas no interneta,

4. piekļuves ierobežojumi telpām, kuras tiek izmantotas datu apstrādei, tikai personām, kam ir īpašs pilnvarojums, kuru piešķīris šā pienākuma adresāts, un

5. vismaz divu personu, kam ir pienākuma subjekta piešķirts īpašs pilnvarojums, obligāta piedalīšanās datu piekļuves procesā."

18 *TKG* 113.e pants ir formulēts šādi:

"(1) 113.a panta 1. punktā paredzētā pienākuma subjektam ir jānodrošina, lai datu aizsardzības kontroles nolūkos tiktu reģistrēta katra piekļuve un, konkrētāk, glabāto datu nolasīšana, kopēšana, grozīšana, dzēšana un izslēgšana atbilstoši 113.b panta 1. punktam saskaņā ar glabāšanas pienākumu. Ir jāprotokolē:

1. piekļuves laiks,

2. personas, kas piekļūst datiem,

3. piekļuves mērķis un veids.

(2) Protokolētos datus drīkst izmantot tikai datu aizsardzības kontroles mērķiem.

(3) 113.a panta 1. punktā paredzētā pienākuma subjektam ir jānodrošina, ka protokolētie dati tiek izdzēsti pēc viena gada."

19 Lai nodrošinātu īpaši augstu datu drošības un kvalitātes līmeni, Federālā elektroenerģijas, gāzes, telekomunikāciju, pasta un dzelzceļa tīklu aģentūra saskaņā ar *TKG* 113.f panta 1. punktu nosaka to prasību kopumu, kas saskaņā ar šā likuma 113.f panta 2. punktu ir regulāri jāizvērtē un pēc vajadzības jāpielāgo. *TKG* 113.g pants prasa, lai pienākuma subjekta iesniedzamajā drošības politikas izklāstā tiktu norādīti konkrēti drošības pasākumi.

StPO

20 *Strafprozessordnung* (Kriminālprocesa kodekss; turpmāk tekstā – "*StPO*") 100.g panta 2. punkta pirmais teikums ir formulēts šādi:

"Ja konkrēti fakti ir pamats aizdomām, ka persona ir izdarījusi kādu no otrajā teikumā paredzētajiem īpaši smagiem noziedzīgiem nodarījumiem vai piedalījusies tā izdarīšanā kā līdzdalībniece, vai – apstākļos, kad par attiecīgā noziedzīgā nodarījuma mēģinājumu ir paredzēta krimināltatbildība, – ir mēģinājusi izdarīt šādu noziedzīgu nodarījumu un šis nodarījums arī konkrētajā gadījumā ir kvalificējams kā īpaši smags, informāciju par datu plūsmu, kas ir glabāta saskaņā ar [*TKG*] 113.b pantu, var ievākt tad, ja noskaidrot faktus vai aizdomās turētās personas atrašanās vietu ar citiem līdzekļiem būtu pārāk sarežģīti vai neiespējami un ja datu vākšana ir samērīga ar lietas nozīmīgumu."

21 *StPO* 101.a panta 1. punktā ir noteikts, ka informācijas par datu plūsmu vākšanai saskaņā ar *StPO* 100.g pantu ir vajadzīga tiesas atļauja. Saskaņā ar *StPO* 101.a panta 2. punktu lēmuma motīvu daļā ir jāizklāsta būtiskie apsvērumi par pasākuma nepieciešamību un piemērotību konkrētajā gadījumā. *StPO* 101.a panta 6. punktā ir paredzēts pienākums par to informēt attiecīgo telekomunikāciju dalībniekus.

Pamatlietas un prejudiciālais jautājums

22 *SpaceNet* un *Telekom Deutschland* Vācijā sniedz publiski pieejamus internetpiekļuves pakalpojumus. Otrā no tām Vācijā sniedz arī publiski pieejamus tālruņa pakalpojumus.

23 Šie pakalpojumu sniedzēji cēla prasību *Verwaltungsgericht Köln* (Ķelnes Administratīvā tiesa, Vācija), lai apstrīdētu tiem saskaņā ar *TKG* 113.a panta 1. punktu apvienojumā ar 113.b pantu uzlikto pienākumu no 2017. gada 1. jūlija glabāt ar savu klientu telekomunikācijām saistīto informāciju par datu plūsmu un atrašanās vietas datus.

24 2018. gada 20. aprīļa spriedumos *Verwaltungsgericht Köln* (Ķelnes Administratīvā tiesa) nosprieda, ka *SpaceNet* un *Telekom Deutschland* nav pienākuma glabāt *TKG* 113.b panta 3. punktā minēto informāciju par datu plūsmu saistībā ar to klientu telekomunikācijām, kuriem tās sniedz piekļuvi internetam, un ka *Telekom Deutschland* nav arīdzan pienākuma glabāt *TKG* 113.b panta 2. punkta pirmajā un otrajā teikumā paredzēto informāciju par datu plūsmu saistībā ar to klientu telekomunikācijām, kuriem tā sniedz piekļuvi publiski pieejamiem tālruņa pakalpojumiem. Proti, ievērojot 2016. gada 21. decembra spriedumu *Tele2 Sverige* un *Watson* u.c. (C-203/15 un C-698/15, EU:C:2016:970), minētā tiesa uzskatīja, ka šis glabāšanas pienākums ir pretrunā Savienības tiesībām.

25 Vācijas Federatīvā Republika par šiem spriedumiem iesniedza revīzijas sūdzību *Bundesverwaltungsgericht* (Federālā administratīvā tiesa, Vācija), kas ir iesniedzējtiesa.

26 Iesniedzējtiesas ieskatā – tas, vai ar *TKG* 113.a panta 1. punktu apvienojumā ar 113.b pantu uzliktais glabāšanas pienākums ir pretrunā Savienības tiesībām, ir atkarīgs no Direktīvas 2002/58 interpretācijas.

27 Šajā ziņā iesniedzējtiesa norāda, ka 2016. gada 21. decembra spriedumā *Tele2 Sverige* un *Watson* u.c. (C-203/15 un C-698/15, EU:C:2016:970) Tiesa jau ir skaidri atzinusi, ka tiesiskie regulējumi, kuros tiek reglamentēta gan informācijas par datu plūsmu un atrašanās vietas datu glabāšana, gan valsts iestāžu piekļuve šiem datiem, principā ietilpst Direktīvas 2002/58 piemērošanas jomā.

28 Tā arī norāda – ņemot vērā, ka pamatlietās aplūkotais glabāšanas pienākums ierobežo no Direktīvas 2002/58 5. panta 1. punkta, 6. panta 1. punkta un 9. panta 1. punkta izrietošās tiesības, tas varētu būt attaisnojams, tikai pamatojoties uz šīs direktīvas 15. panta 1. punktu.

29 Šajā ziņā tā atgādina – no 2016. gada 21. decembra sprieduma *Tele2 Sverige* un *Watson* u.c. (C-203/15 un C-698/15, EU:C:2016:970) izriet, 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 glabāšana attiecībā uz visiem abonentiem un reģistrētiem lietotājiem un attiecībā uz visiem elektronisko komunikāciju līdzekļiem.

30 Iesniedzējtiesa uzskata, ka pamatlietās aplūkotais valsts tiesiskais regulējums – gluži tāpat kā tie valstu tiesiskie regulējumi, kas tika aplūkoti lietās, kurās tika taisīts minētais spriedums, – savukārt neprasa nedz iemeslu šo datu glabāšanai, nedz saikni starp glabātajiem datiem un noziedzīgu nodarījumu vai sabiedrības drošības apdraudējumu. Proti, šajā valsts tiesiskajā regulējumā esot noteikts pienākums bez iemesla un vispārēji glabāt lielāko daļu no visas būtiskās informācijas par telekomunikāciju datu plūsmu, nešķirojot pēc personas, laika vai ģeogrāfiski.

31 Tomēr, iesniedzējtiesas ieskatā, nav izslēdzams, ka pamatlietās aplūkotais glabāšanas pienākums varētu būt attaisnojams saskaņā ar Direktīvas 2002/58 15. panta 1. punktu.

32 Pirmām kārtām, tā norāda, ka – atšķirībā no tiesiskajiem regulējumiem, kas tika aplūkoti lietās, kurās taisīts 2016. gada 21. decembra spriedums *Tele2 Sverige* un *Watson* u.c. (C-203/15 un C-698/15, EU:C:2016:970), – pamatlietās aplūkotais valsts tiesiskais regulējums neprasa glabāt visu informāciju par datu plūsmu saistībā ar visu abonentu un reģistrēto lietotāju telekomunikācijām visos elektroniskās komunikācijas līdzekļos. Glabāšanas pienākums ne vien neattiecoties uz komunikāciju saturu, bet – kā izriet no *TKG* 113.b panta 5. un 6. punkta – nedrīkstot glabāt arī informāciju par apmeklētajām tīmekļvietnēm, elektroniskā pasta pakalpojumu datus un datus, kas tiek izmantoti sociāla vai reliģiska rakstura komunikācijās uz vai no noteiktām līnijām.

33 Otrām kārtām, minētā tiesa arī norāda: *TKG* 113.b panta 1. punktā ir paredzēts, ka atrašanās vietas dati jāglabā četras nedēļas un informācija par datu plūsmu – desmit nedēļas, lai gan Eiropas Parlamenta un Padomes Direktīvā 2006/24/EK (2006. gada 15. marts) 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.) – uz kuru bija balstīti valstu tiesiskie regulējumi,

kas tika aplūkoti lietās, kurās taisīts 2016. gada 21. decembra spriedums *Tele2 Sverige* un *Watson* u.c. (C-203/15 un C-698/15, EU:C:2016:970), – bija paredzēts, ka glabāšana jāveic uz laiku, kura ilgums ir no sešiem mēnešiem līdz diviem gadiem.

34 Iesniedzējtiesas ieskatā, lai arī ar noteiktu komunikācijas līdzekļu vai datu kategoriju izslēgšanu un glabāšanas ilguma samazināšanu nav pietiekami, lai pilnībā novērstu datu subjektu profilēšanas risku, pamatlietās aplūkotā valsts tiesiskā regulējuma īstenošanas kontekstā šis risks esot vismaz ievērojami samazināts.

35 Trešām kārtām, šajā tiesiskajā regulējumā esot noteikti stingri ierobežojumi attiecībā uz glabāto datu aizsardzību un piekļuvi tiem. Tādējādi, pirmkārt, tajā esot garantēta glabāto datu efektīva aizsardzība pret ļaunprātīgas izmantošanas riskiem un jebkādu prettiesisku piekļuvi tiem. Otrkārt, glabātos datus drīkstot izmantot tikai, lai apkarotu smagus noziedzīgus nodarījumus vai novērstu konkrētus draudus personas veselībai, dzīvībai vai brīvībai vai arī federatīvās valsts vai federālās zemes pastāvēšanai.

36 Ceturtām kārtām, Direktīvas 2002/58 15. panta 1. punktu interpretēt tādējādi, ka ar Savienības tiesībām ir vispārīgi nesaderīga ikviena bez iemesla veikta datu glabāšana, būtu pretrunā no Hartas 6. pantā nostiprinātajām tiesībām uz drošību izrietošajam dalībvalstu pienākumam rīkoties.

37 Piektām kārtām, iesniedzējtiesa uzskata, ka gadījumā, ja Direktīvas 2002/58 15. pantu interpretētu tādējādi, ka tam ir pretrunā visaptveroša datu glabāšana, ievērojami tiktu ierobežota valsts likumdevēja rīcības brīvība ar noziegumu apkarošanu un sabiedrības drošību saistītajā jomā, kura saskaņā ar LES 4. panta 2. punktu paliek vienīgi katras dalībvalsts atbildībā.

38 Sestām kārtām, iesniedzējtiesa uzskata, ka ir jāņem vērā Eiropas Cilvēktiesību tiesas judikatūra, un norāda, ka minētā tiesa ir nospriedusi, ka Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvencijas (turpmāk tekstā – "ECPAK") 8. pants neliedz pieņemt tādas valstu tiesību normas, kas paredz pārrobežu datu plūsmas masveida pārtveršanu, ņemot vērā draudus, ar ko pašlaik saskaras daudzas valstis, un tehniskos līdzekļus, ar kuriem teroristi un noziedznieki tagad var izdarīt sodāmas darbības.

39 Šādos apstākļos *Bundesverwaltungsgericht* (Federālā administratīvā tiesa) nolēma apturēt tiesvedību un uzdot Tiesai šādu prejudiciālu jautājumu:

"Vai Direktīvas [2002/58] 15. pants, lasot to kopā ar [Hartas] 7., 8. un 11. pantu, kā arī 52. panta 1. punktu, no vienas puses, un [minētās Hartas] 6. pantu, kā arī [LES] 4. pantu, no otras puses, ir jāinterpretē tādējādi, ka tas nepieļauj valsts tiesisko regulējumu, kurā publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzējiem tiek noteikts pienākums glabāt informāciju par šo pakalpojumu galalietotāju datu plūsmu un atrašanās vietas datus, ja:

1) šis pienākums nav pakārtots nevienam īpašam nosacījumam vietas, laika vai telpas ziņā;

2) publiski pieejamu tālruņa pakalpojumu – ieskaitot īsziņu, multivides vai līdzīgu ziņu, kā arī neatbildētu vai nesekmīgu zvanu pārsūtīšanas – gadījumā glabāšanas pienākums attiecas uz šādiem datiem:
   a) zvanītāja un adresāta, kā arī pārslēgšanas un pāradresēšanas gadījumā katra nākamā iesaistītā tālruņa numuru vai citu identifikatoru;

b) savienojuma sākuma un beigu datumu un laiku vai – multivides vai līdzīgas ziņas pārsūtīšanas gadījumā – ziņas nosūtīšanas un saņemšanas laiku, norādot atbilstošo laika joslu;
c) datiem par izmantoto pakalpojumu, ja tālruņa pakalpojuma ietvaros ir iespējams izmantot dažādus pakalpojumus;
d) mobilā tālruņa pakalpojumu gadījumā arī:
   i) zvanītāja un adresāta mobilo abonentu starptautisko identifikatoru;
   ii) zvanītāja un adresāta galaierīces starptautisko identifikatoru;
   iii) priekšapmaksas pakalpojumu gadījumā arī pakalpojuma pirmās aktivizēšanas datumu un laiku, norādot piemērojamo laika joslu;
   iv) to šūnu nosaukumiem, kuras izmantotas zvanītāja un adresāta savienojumā, uzsākot savienojumu;
e) interneta tālruņa pakalpojumu gadījumā arī zvanītāja un adresāta IP (interneta protokola) adresēm un piešķirtajiem lietotāja identifikatoriem;

3) publiski pieejamu internetpiekļuves pakalpojumu gadījumā glabāšanas pienākums attiecas uz šādiem datiem:
   a) IP adresi, kas abonentam piešķirta interneta lietošanai,
   b) interneta lietošanai izmantotā pieslēguma nepārprotamu identifikatoru, kā arī piešķirto lietotāja identifikatoru;
   c) interneta lietošanas ar piešķirto IP adresi sākuma un beigu datumu un laiku, norādot piemērojamo laika joslu;
   d) mobilo sakaru lietošanas gadījumā tās šūnas nosaukumu, kura izmantota, uzsākot interneta savienojumu;

4) nedrīkst glabāt šādus datus:
   a) komunikācijas saturu;
   b) datus par apmeklētajām tīmekļvietnēm;
   c) datus par elektroniskā pasta pakalpojumiem;
   d) datus, kuri izriet no komunikācijām uz/no sociālās vai reliģiskās jomas organizācijām, iestādēm vai personām piešķirtiem pieslēgumiem;

5) atrašanās vietas datu, proti, izmantotās šūnas nosaukuma, glabāšanas ilgums ir četras nedēļas un pārējiem datiem – desmit nedēļas;

6) ir garantēta glabāto datu efektīva aizsardzība pret ļaunprātīgas izmantošanas riskiem un jebkādu prettiesisku piekļuvi tiem; un

7) glabātos datus drīkst izmantot tikai, lai apkarotu smagus noziedzīgus nodarījumus un novērstu konkrētus draudus personas veselībai, dzīvībai vai brīvībai vai arī federatīvās valsts vai federālās zemes pastāvēšanai, izņemot abonentam interneta lietošanai piešķirtu IP adresi, ko ir atļauts izmantot abonentu informācijas iegūšanai, lai apkarotu jebkādus noziedzīgus nodarījumus, novērstu sabiedriskās drošības un kārtības apdraudējumu, kā arī veiktu izlūkdienestu uzdevumus?"

Tiesvedība Tiesā

40 Ar Tiesas priekšsēdētāja 2019. gada 3. decembra lēmumu lietas C-793/19 un C-794/19 tika apvienotas rakstveida un mutvārdu procesam, kā arī sprieduma taisīšanai.

41 Ar Tiesas priekšsēdētāja 2020. gada 14. jūlija lēmumu tiesvedība apvienotajās lietās C-793/19 un C-794/19 saskaņā ar Tiesas Reglamenta 55. panta 1. punkta b) apakšpunktu tika apturēta līdz sprieduma pasludināšanai lietā *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18).

42 Tā kā 2020. gada 6. oktobrī Tiesa pasludināja spriedumu lietā *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791), Tiesas priekšsēdētājs 2020. gada 8. oktobrī izdeva rīkojumu par tiesvedības atsākšanu apvienotajās lietās C-793/19 un C-794/19.

43 Iesniedzējtiesa, kurai sekretārs ir paziņojis šo spriedumu, norādīja, ka tā savu lūgumu sniegt prejudiciālu nolēmumu uztur.

44 Šajā ziņā iesniedzējtiesa vispirms norāda, ka pamatlietās aplūkotajā tiesiskajā regulējumā noteiktais glabāšanas pienākums attiecas uz mazāku datu daudzumu un īsāku glabāšanas ilgumu salīdzinājumā ar to, kas bija paredzēts valstu tiesiskajos regulējumos, kas bija aplūkoti lietās, kurās taisīts 2020. gada 6. oktobra spriedums *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791). Šo īpatnību dēļ esot mazāk iespējams, ka glabātie dati ļautu izdarīt ļoti precīzus secinājumus par to personu privāto dzīvi, kuru dati tikuši glabāti.

45 Pēc tam tā norāda, ka pamatlietās aplūkotais valsts tiesiskais regulējums nodrošinot efektīvu aizsardzību pret glabāto datu ļaunprātīgas izmantošanas un prettiesiskas piekļuves riskiem.

46 Visbeidzot tā norāda, ka jautājumā par pamatlietās aplūkotajā valsts tiesiskajā regulējumā paredzētās IP adrešu glabāšanas saderību ar Savienības tiesībām valda neskaidrība, jo starp 2020. gada 6. oktobra sprieduma *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791) 155. un 168. punktu esot vērojama zināma disonanse. Tādējādi, iesniedzējtiesas ieskatā, neskaidrība no minētā sprieduma izrietot jautājumā par to, vai Tiesa prasa, lai IP adrešu glabāšana būtu kāds ar valsts drošības aizsardzības, smagas noziedzības apkarošanas vai nopietna sabiedrības drošības apdraudējuma novēršanas mērķi saistīts iemesls, kā tas izriet no minētā sprieduma 168. punkta, vai turpretim IP adrešu glabāšana ir atļauta pat bez kāda konkrēta iemesla, jo no minētā sprieduma 155. punkta savukārt izrietot, ka nosacījumam par šādu mērķu esamību ir pakārtota tikai glabāto datu izmantošana.

Par prejudiciālo jautājumu

47 Ar prejudiciālo jautājumu iesniedzējtiesa būtībā vēlas noskaidrot, vai Direktīvas 2002/58 15. panta 1. punkts, lasot to Hartas 6.–8. un 11. panta, kā arī 52. panta 1. punkta un LES 4. panta 2. punkta gaismā, ir jāinterpretē tādējādi, ka tas nepieļauj valsts leģislatīvo pasākumu, kurā, atskaitot dažus izņēmumus, publiski pieejamu elektronisko komunikāciju pakalpojumu sniedzējiem šīs direktīvas 15. panta 1. punktā noteiktajos nolūkos, tostarp smagu noziedzīgu nodarījumu apkarošanai vai valsts drošības konkrēta apdraudējuma novēršanai, tiek noteikts pienākums visaptveroši un nediferencēti glabāt lielāko daļu informācijas par šo pakalpojumu galalietotāju datu plūsmu un atrašanās vietas datu, paredzot, ka tie ir jāglabā vairākas nedēļas, kā arī noteikumus, ar kuriem ir jānodrošina glabāto datu efektīva aizsardzība pret ļaunprātīgu izmantošanu un jebkādu nelikumīgu piekļuvi šiem datiem.

Par Direktīvas 2002/58 piemērojamību

48 Attiecībā uz Īrijas, kā arī Francijas, Nīderlandes, Polijas un Zviedrijas valdību argumentāciju, ka, tā kā pamatlietās aplūkotais valsts tiesiskais regulējums ir pieņemts konkrēti valsts drošības aizsardzības nolūkos, tas neietilpst Direktīvas 2002/58 piemērošanas jomā, pietiek vien atgādināt, ka tāds valsts tiesiskais regulējums kā pamatlietās aplūkotais, kurā elektronisko komunikāciju pakalpojumu sniedzējiem ir noteikts pienākums glabāt informāciju par datu plūsmu un atrašanās vietas datus konkrēti tālab, lai aizsargātu valsts drošību un apkarotu noziedzību, ietilpst Direktīvas 2002/58 piemērošanas jomā (spriedums, 2020. gada 6. oktobris, *La Quadrature du Net* u.c., C-511/18, C-512/18 un C-520/18, EU:C:2020:791, 104. punkts).

Par Direktīvas 2002/58 15. panta 1. punkta interpretāciju

No Tiesas judikatūras izrietošo principu atgādinājums

49 Tiesas pastāvīgās judikatūras atziņa ir tāda, ka, interpretējot Savienības tiesību normu, ir jāņem vērā ne tikai tās teksts, bet arī tās konteksts un šo normu ietverošā tiesiskā regulējuma mērķi, un tostarp šā tiesiskā regulējuma izstrādes vēsture (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 32. punkts, kā arī tajā minētā judikatūra).

50 No paša Direktīvas 2002/58 15. panta 1. punkta formulējuma izriet, ka tiesību akti, kurus ar tajā paredzētajiem nosacījumiem dalībvalstīm ir atļauts pieņemt, drīkst būt vērsti tikai uz to, lai "ierobežotu" tostarp Direktīvas 2002/58 5., 6. un 9. pantā minēto tiesību un pienākumu "darbības jomu" (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 33. punkts).

51 Par šīs direktīvas izveidoto sistēmu, kurā ietilpst tās 15. panta 1. punkts, jāatgādina, ka saskaņā ar minētās direktīvas 5. panta 1. punkta pirmo un otro teikumu dalībvalstīm ir ar valsts tiesību aktiem jānodrošina gan ar publisko komunikāciju tīkla un publiski pieejamu elektronisko komunikāciju pakalpojumu starpniecību veiktās saziņas konfidencialitāte, gan ar to saistītās informācijas par datu plūsmu konfidencialitāte. Konkrēti – tām ir jāaizliedz komunikāciju un saistītās informācijas par datu plūsmu noklausīšanās, ierakstīšana, uzglabāšana vai cita veida pārtveršana vai pārraudzība personām, kas nav lietotāji, bez attiecīgo lietotāju piekrišanas, izņemot gadījumus, kad to darīt ir ar likumu atļauts saskaņā ar šīs pašas direktīvas 15. panta 1. punktu (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 34. punkts).

52 Šajā ziņā Tiesa jau ir nospriedusi, ka Direktīvas 2002/58 5. panta 1. punktā ir nostiprināts gan elektronisko komunikāciju, gan ar tām saistītās informācijas par datu plūsmu konfidencialitātes princips, un tajā tostarp ir paredzēts aizliegums principā visām personām, kas nav lietotāji, bez viņu piekrišanas uzglabāt šīs komunikācijas un minēto informāciju (spriedumi, 2020. gada 6. oktobris, *La Quadrature du Net* u.c., C-511/18, C-512/18 un C-520/18, EU:C:2020:791, 107. punkts, kā arī 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 35. punkts).

53 Šajā tiesību normā ir atspoguļots mērķis, ar kādu Savienības likumdevējs pieņēma Direktīvu 2002/58. Proti, no Direktīvas 2002/58 pamatā esošā Priekšlikuma Eiropas Parlamenta un Padomes direktīvai par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (COM(2000) 385, galīgā redakcija) paskaidrojuma raksta izriet, ka

Savienības likumdevējs ir vēlējies "rīkoties tādējādi, ka personas datu augsts aizsardzības līmenis un privātā dzīve turpina būt garantēta attiecībā uz visiem elektronisko sakaru pakalpojumiem neatkarīgi no izmantotās tehnoloģijas". Tādējādi minētās direktīvas mērķis, kā izriet tostarp no tās 6. un 7. apsvēruma, ir aizsargāt elektronisko komunikāciju pakalpojumu lietotājus pret riskiem viņu personas datiem un privātajai dzīvei, kurus izraisa jaunās tehnoloģijas un arvien lielāka jauda datu automatizētai glabāšanai un apstrādei. Konkrēti, kā norādīts tās pašas direktīvas 2. apsvērumā, Savienības likumdevēja vēlme ir nodrošināt, lai pilnībā tiktu ievērotas Hartas 7. un 8. pantā nostiprinātās tiesības uz privātās dzīves aizsardzību un personas datu aizsardzību (šajā nozīmē skat. spriedumu, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 36. punkts, kā arī tajā minētā judikatūra).

54 Pieņemot Direktīvu 2002/58, Savienības likumdevējs ir konkretizējis šīs tiesības tādējādi, ka elektronisko komunikāciju līdzekļu lietotājiem principā ir tiesības sagaidīt, ka viņu komunikācijas un ar tām saistītie dati paliek anonīmi un nevar tikt reģistrēti, ja vien viņi nav tam piekrituši (spriedumi, 2020. gada 6. oktobris, *La Quadrature du Net* u.c., C-511/18, C-512/18 un C-520/18, EU:C:2020:791, 109. punkts, kā arī 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 37. punkts).

55 Attiecībā uz informācijas par abonentu un lietotāju datu plūsmu apstrādi un uzglabāšanu, ko veic elektronisko komunikāciju pakalpojumu sniedzēji, Direktīvas 2002/58 6. panta 1. punktā ir paredzēts, ka šī informācija ir jādzēš vai jāpadara anonīma, kad tā vairs nav nepieciešama komunikāciju pārraidīšanai, un 2. punktā ir precizēts, ka informāciju par datu plūsmu, kas nepieciešama, lai abonentam sagatavotu rēķinu un veiktu norēķinus par starpsavienojumiem, var apstrādāt tikai tik ilgi, kamēr nav beidzies termiņš, kura laikā var likumīgi apstrīdēt rēķinu vai piedzīt tā samaksu. Attiecībā uz atrašanās vietas datiem, kas nav informācija par datu plūsmu, minētās direktīvas 9. panta 1. punktā ir noteikts, ka šos datus var apstrādāt tikai pakārtoti zināmiem nosacījumiem un tikai pēc tam, kad vai nu tie ir padarīti anonīmi, vai arī ir saņemta lietotāju vai abonentu piekrišana.

56 Tāpēc Direktīvā 2002/58 piekļuve šiem datiem ne tikai tiek pakārtota garantijām, kuru mērķis ir novērst ļaunprātīgu izmantošanu, bet tajā ir arī nostiprināts it īpaši princips, ka trešām personām tos uzglabāt ir aizliegts (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 39. punkts).

57 Tā kā Direktīvas 2002/58 15. panta 1. punktā dalībvalstīm ir ļauts pieņemt tādus leģislatīvus pasākumus tostarp šīs direktīvas 5., 6. un 9. pantā minēto tiesību un pienākumu "darbības jomas" ierobežošanai, kuri izriet no šā sprieduma 52. punktā atgādinātajiem komunikāciju konfidencialitātes un ar tiem saistīto datu uzglabāšanas aizlieguma principiem, šī tiesību norma paredz izņēmumu no vispārīgā principa, kas noteikts tostarp šīs direktīvas 5., 6. un 9. pantā, un tāpēc atbilstoši pastāvīgajai judikatūrai tā ir jāinterpretē šauri. Tātad šāda tiesību norma nav pamats tam, lai atkāpe no principiālā pienākuma nodrošināt elektronisko komunikāciju un ar tām saistīto datu konfidencialitāti un konkrēti no minētās direktīvas 5. pantā paredzētā aizlieguma uzglabāt šos datus pati kļūtu par principu, jo pretējā gadījumā tiktu būtiski sašaurināta šā panta piemērošanas joma (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 40. punkts, kā arī tajā minētā judikatūra).

58 Savukārt par mērķiem, kas var pamatot Direktīvas 2002/58 5., 6. un 9. pantā paredzēto tiesību un pienākumu ierobežojumu, Tiesa jau ir nospriedusi, ka šīs direktīvas 15. panta 1. punkta pirmajā teikumā ietvertais šo mērķu uzskaitījums ir izsmeļošs un tādēļ atbilstoši šai normai pieņemtajam

leģislatīvajam pasākumam ir patiešām un stingri jāatbilst kādam no šiem mērķiem (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 41. punkts, kā arī tajā minētā judikatūra).

59 Turklāt no Direktīvas 2002/58 15. panta 1. punkta trešā teikuma izriet, ka dalībvalstu saskaņā ar šo tiesību normu pieņemtajiem pasākumiem ir jāatbilst Savienības tiesību vispārējiem principiem, tostarp samērīguma principam, un jānodrošina Hartā garantēto pamattiesību ievērošana. Šajā ziņā Tiesa jau ir nospriedusi, ka dalībvalsts tiesiskajā regulējumā noteiktais pienākums elektronisko komunikāciju pakalpojumu sniedzējiem glabāt informāciju par datu plūsmu, lai vajadzības gadījumā to padarītu pieejamu kompetentajām valsts iestādēm, izraisa jautājumus par atbilstību ne tikai Hartas 7. un 8. pantam, bet arī Hartas 11. pantam par vārda brīvību, kas ir gan viens no būtiskajiem demokrātiskas un plurālistiskas sabiedrības pamatiem, gan viena no vērtībām, uz kuras saskaņā ar LES 2. pantu ir balstīta Eiropas Savienība (šajā nozīmē skat. spriedumu, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 42. un 43. punkts, kā arī tajos minētā judikatūra).

60 Šajā ziņā jāprecizē, ka pati informācijas par datu plūsmu un atrašanās vietas datu glabāšana, pirmkārt, ir atkāpe no Direktīvas 2002/58 5. panta 1. punktā paredzētā aizlieguma jebkurai personai, kas nav lietotājs, uzglabāt šos datus un, otrkārt, iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās uz privātās dzīves neaizskaramību un personas datu aizsardzību, un nav nozīmes tam, vai attiecīgajai informācijai par privāto dzīvi ir vai nav sensitīvs raksturs, vai ieinteresētajām personām ir vai nav radītas neērtības šīs iejaukšanās dēļ un vai glabātie dati vēlāk tiek vai netiek izmantoti (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 44. punkts, kā arī tajā minētā judikatūra).

61 Šis secinājums vēl jo vairāk šķiet pamatots tāpēc, ka informācija par datu plūsmu un atrašanās vietas dati var atklāt informāciju par daudziem datu subjektu privātās dzīves aspektiem, ieskaitot sensitīvu informāciju, piemēram, seksuālo orientāciju, politiskos uzskatus, reliģisko, filozofisko, sabiedrisko vai citu pārliecību, kā arī veselības stāvokli, lai gan šādi dati turklāt ir īpaši aizsargāti Savienības tiesībās. Minētie dati kopumā var ļaut izdarīt ļoti precīzus secinājumus par to personu privāto dzīvi, kuru dati tikuši glabāti, proti, ikdienas paradumiem, pastāvīgās vai pagaidu uzturēšanās vietām, ikdienas vai citām gaitām, veiktajām darbībām, šo personu sociālajiem kontaktiem un aprindām, kurās tās mēdz uzturēties. Konkrēti, šie dati sniedz iespējas noteikt attiecīgo personu profilu, kas tiesību uz privātās dzīves neaizskaramību kontekstā savukārt ir tikpat sensitīva informācija kā pats šīs komunikācijas saturs (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 45. punkts, kā arī tajā minētā judikatūra).

62 Tāpēc, pirmkārt, informācijas par datu plūsmu un atrašanās vietas datu glabāšana tiesībaizsardzības mērķiem var apdraudēt Hartas 7. pantā nostiprinātās tiesības uz saziņas neaizskaramību, un tas elektroniskās komunikācijas līdzekļu lietotājus var atturēt izmantot vārda brīvību, kas ir garantēta tās 11. pantā; un šī ietekme ir vēl jo būtiskāka, jo lielāks ir glabāto datu apjoms un jo lielāka ir to daudzveidība. Otrkārt, ņemot vērā visaptverošas un nediferencētas glabāšanas pasākuma ceļā pastāvīgi glabājamās informācijas par datu plūsmu un atrašanās vietas datu ievērojamo apjomu, kā arī no šiem datiem iegūstamās informācijas sensitīvo raksturu, ļaunprātīgas izmantošanas un prettiesiskas piekļuves risku rada jau pati elektronisko komunikāciju pakalpojumu sniedzēju veiktā minēto datu glabāšana (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 46. punkts, kā arī tajā minētā judikatūra).

63 Tomēr, ciktāl ar Direktīvas 2002/58 15. panta 1. punktu dalībvalstīm ir atļauts ierobežot šā sprieduma 51.–54. punktā minētās tiesības un pienākumus, šī tiesību norma atspoguļo faktu, ka Hartas 7., 8. un 11. pantā ietvertās tiesības nav uztveramas kā absolūtas prerogatīvas, bet gan jāaplūko saistībā ar to funkciju sabiedrībā. Proti, Harta – kā redzams no tās 52. panta 1. punkta – pieļauj, ka šādām tiesībām var noteikt izmantošanas ierobežojumus, ciktāl šie ierobežojumi ir paredzēti tiesību aktos, ar tiem tiek respektēta šo tiesību būtība un, ievērojot samērīguma principu, šie ierobežojumi ir nepieciešami un patiešām atbilst Savienības atzītiem vispārējo interešu mērķiem vai vajadzībai aizsargāt citu personu tiesības un brīvības. Tādējādi, interpretējot Direktīvas 2002/58 15. panta 1. punktu Hartas gaismā, ir vienlīdz jāņem vērā gan tas, cik nozīmīgas ir Hartas 3., 4., 6. un 7. pantā garantētās tiesības, gan tas, cik nozīmīgi citu personu tiesību un brīvību aizsardzībai ir valsts drošības un smagas noziedzības apkarošanas mērķi (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 48. punkts, kā arī tajā minētā judikatūra).

64 Tādējādi konkrēti attiecībā uz efektīvu cīņu pret noziedzīgiem nodarījumiem, kuros cietušie ir nepilngadīgas personas un citas neaizsargātas personas, ir jāņem vērā, ka no Hartas 7. panta valsts iestādēm var izrietēt pozitīvi pienākumi, lai veiktu tiesiskus pasākumus privātās un ģimenes dzīves aizsardzībai. Šādi pienākumi var izrietēt arī no minētā 7. panta attiecībā uz mājokļa un saziņas aizsardzību, kā arī no 3. un 4. panta attiecībā uz personu fiziskās un garīgās neaizskaramības aizsardzību un attiecībā uz spīdzināšanas un necilvēcīgas vai pazemojošas izturēšanās aizliegumu (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 49. punkts, kā arī tajā minētā judikatūra).

65 Tātad, ņemot vērā šos dažādos pozitīvos pienākumus, ir jāsalāgo dažādās aplūkotās leģitīmās intereses un tiesības un jāievieš tiesiskais regulējums, kas paver iespēju veikt šādu salāgošanu (šajā nozīmē skat. spriedumu, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 50. punkts, kā arī tajā minētā judikatūra).

66 Šajā kontekstā no paša Direktīvas 2002/58 15. panta 1. punkta pirmā teikuma formulējuma izriet, ka dalībvalstis var pieņemt tiesību aktus, kas paredz atkāpi no šā sprieduma 52. punktā minētā konfidencialitātes principa, ja tas ir "nepieciešam[i], atbilstīg[i] un samērīg[i] [..] demokrātiskā sabiedrībā"; šīs direktīvas 11. apsvērumā šajā ziņā ir precizēts, ka šādam tiesību aktam ir jābūt "stingri" samērīgam ar paredzēto nolūku.

67 Šajā ziņā jāatgādina, ka pamattiesību uz privātās dzīves neaizskaramību aizsardzība atbilstoši Tiesas pastāvīgajai judikatūrai nozīmē, ka atkāpes no personas datu aizsardzības un tās ierobežojumi ir jāīsteno absolūti nepieciešamā ietvaros. Turklāt vispārējo interešu mērķa sasniegšanā nevar neņemt vērā to, ka šis mērķis ir jāsalāgo ar šā pasākuma skartajām pamattiesībām, līdzsvarojot šo vispārējo interešu mērķi ar attiecīgajām tiesībām (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 52. punkts, kā arī tajā minētā judikatūra).

68 Konkrētāk, no Tiesas judikatūras izriet, ka iespēja dalībvalstīm pamatot tostarp Direktīvas 2002/58 5., 6. un 9. pantā paredzēto tiesību un pienākumu ierobežojumus ir jāizvērtē, izsverot šāda ierobežojuma radītās iejaukšanās smagumu un pārbaudot, vai vispārējo interešu mērķa nozīmīgums ir samērīgs ar iejaukšanās smagumu (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 53. punkts, kā arī tajā minētā judikatūra).

69 Lai izpildītu samērīguma prasību, valsts tiesiskajā regulējumā ir jāparedz skaidri un precīzi noteikumi, kas reglamentē attiecīgā pasākuma tvērumu un piemērošanu un paredz minimālās prasības, lai tā rezultātā personām, kuru personas dati tikuši pārsūtīti, būtu pietiekamas garantijas, kas ļautu šos datus efektīvi aizsargāt pret ļaunprātīgas izmantošanas risku. Šiem tiesību aktiem ir jābūt juridiski saistošiem valsts tiesībās, un tajos it īpaši jānorāda, kādos apstākļos un saskaņā ar kādiem nosacījumiem var īstenot pasākumu, kas ietver šādu datu apstrādi, tādējādi garantējot, ka šāda iejaukšanās notiek tikai absolūti nepieciešamajā apmērā. Šādu garantiju sniegšanas nepieciešamība ir vēl jo svarīgāka tad, ja personas dati tiek apstrādāti automātiski un pastāv ievērojams risks, ka šiem datiem var nelikumīgi piekļūt. Šie apsvērumi ir it īpaši svarīgi, ja runa ir par tādas kategorijas personas datu aizsardzību kā sensitīvi dati (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 54. punkts, kā arī tajā minētā judikatūra).

70 Tādējādi valsts tiesību aktiem, kuros paredzēta personas datu glabāšana, vienmēr ir jāatbilst objektīviem kritērijiem, kas veido saikni starp glabājamiem datiem un sasniedzamo mērķi (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 55. punkts, kā arī tajā minētā judikatūra).

71 Runājot par vispārējo interešu mērķiem, kuri var attaisnot pasākumu, kas pieņemts saskaņā ar Direktīvas 2002/58 15. panta 1. punktu, no Tiesas judikatūras, konkrēti, no 2020. gada 6. oktobra sprieduma *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791), izriet, ka saskaņā ar samērīguma principu šo mērķu starpā pastāv hierarhija atkarībā no to konkrētā nozīmīguma un ka šāda pasākuma mērķa nozīmīgumam ir jābūt samērīgam ar tā radītās iejaukšanās smagumu (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 56. punkts).

72 Tāpēc attiecībā uz valsts drošības aizsardzību, kura ir svarīgāka par pārējiem Direktīvas 2002/58 15. panta 1. punktā minētajiem mērķiem, Tiesa ir konstatējusi, ka šai tiesību normai, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, nav pretrunā leģislatīvi pasākumi, ar kuriem – gadījumā, ja elektronisko komunikāciju pakalpojumu sniedzējiem ir izdots rīkojums veikt visaptverošu un nediferencētu informācijas par datu plūsmu un atrašanās vietas datu glabāšanu situācijās, kad attiecīgā dalībvalsts sastopas ar nopietniem draudiem valsts drošībai, kuri izrādās patiesi un faktiski vai paredzami, – valsts drošības aizsardzības nolūkā ir atļauts pieņemt lēmumu, kurā paredzēts, ka šo rīkojumu var pakļaut efektīvai pārbaudei tiesā vai arī neatkarīgā administratīvā iestādē, kuras nolēmumam ir saistoša iedarbība, lai pārbaudītu šādas situācijas esamību, kā arī paredzēto nosacījumu un garantiju ievērošanu, un minēto rīkojumu var izdot vienīgi uz absolūti nepieciešamo laiku, tomēr šo termiņu var pagarināt, ja šāds apdraudējums joprojām pastāv (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 58. punkts, kā arī tajā minētā judikatūra).

73 Attiecībā uz noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķi Tiesa ir norādījusi, ka saskaņā ar samērīguma principu vienīgi smagas noziedzības apkarošana un nopietna valsts drošības apdraudējuma novēršana var pamatot tādu smagu iejaukšanos Hartas 7. un 8. pantā noteiktajās pamattiesībās, par kādu ir uzskatāma informācijas par datu plūsmu un atrašanās vietas datu glabāšana. Tādējādi ar vispārīgu noziedzīgu nodarījumu novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas mērķi var attaisnot vienīgi tādu iejaukšanos minētajās pamattiesībās, kas nav smaga (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 59. punkts, kā arī tajā minētā judikatūra).

74 Jautājumā par smagas noziedzības apkarošanas mērķi Tiesa ir nospriedusi, ka valsts tiesību akti, kas paredz tālab visaptveroši un nediferencēti glabāt informāciju par datu plūsmu un atrašanās vietas datus, pārsniedz absolūti nepieciešamā robežas un nav uzskatāmi par demokrātiskā sabiedrībā pamatotiem. Proti, ievērojot no informācijas par datu plūsmu un atrašanās vietas datiem iegūstamās informācijas sensitīvo raksturu, šīs informācijas konfidencialitāte ir būtiska, lai nodrošinātu tiesības uz privātās dzīves neaizskaramību. Tādējādi, ņemot vērā, pirmkārt, šā sprieduma 62. punktā minēto atturošo iedarbību uz Hartas 7. un 11. pantā paredzēto pamattiesību īstenošanu, ko var izraisīt šo datu glabāšana, un, otrkārt, šādas glabāšanas radītās iejaukšanās smagumu, demokrātiskā sabiedrībā ir svarīgi, lai tā – kā paredzēts ar Direktīvu 2002/58 izveidotajā sistēmā – būtu izņēmums, nevis princips un lai šos datus nevarētu glabāt sistemātiski un nepārtraukti. Tas tā ir, pat ņemot vērā gan mērķus apkarot smagu noziedzību un novērst nopietnus draudus sabiedriskajai drošībai, gan šiem mērķiem piešķiramo nozīmīgumu (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 65. punkts, kā arī tajā minētā judikatūra).

75 Tiesa savukārt ir precizējusi, ka Direktīvas 2002/58 15. panta 1. punktam, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, nav pretrunā tādi leģislatīvi pasākumi, kas smagas noziedzības apkarošanas un nopietna sabiedrības drošības apdraudējuma novēršanas nolūkos paredz:

– mērķorientētu informācijas par datu plūsmu un atrašanās vietas datu glabāšanu, kura, pamatojoties uz objektīviem un nediskriminējošiem elementiem, tiek ierobežota atkarībā no attiecīgo personu kategorijām vai pamatojoties uz ģeogrāfisku kritēriju, uz laiku, kas nepārsniedz absolūti nepieciešamo, bet ko var pagarināt;

– savienojuma avotam piešķirto IP adrešu visaptverošu un nediferencētu glabāšanu uz laiku, kas nepārsniedz absolūti nepieciešamo;

– elektronisko komunikāciju līdzekļu lietotāju personas identitātes datu visaptverošu un nediferencētu glabāšanu; un

– ar kompetentās iestādes lēmumu, kas ir pakļauts efektīvai pārbaudei tiesā, noformēta rīkojuma izdošanu elektronisko komunikāciju pakalpojumu sniedzējiem uz noteiktu laiku operatīvi saglabāt (*quick freeze*) pakalpojumu sniedzēju rīcībā esošo informāciju par datu plūsmu un atrašanās vietas datus,

ja ar šiem pasākumiem, paredzot skaidrus un konkrētus noteikumus, tiek nodrošināts, ka attiecīgo datu glabāšana notiek atbilstoši tai paredzētajiem materiāltiesiskajiem un procesuālajiem nosacījumiem un ka datu subjektiem ir efektīvas garantijas pret ļaunprātīgas izmantošanas risku (spriedumi, 2020. gada 6. oktobris, *La Quadrature du Net* u.c., C-511/18, C-512/18 un C-520/18, EU:C:2020:791, 168. punkts, kā arī 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 67. punkts).

Par pasākumu, kas paredz vairākas nedēļas visaptveroši un nediferencēti glabāt lielāko daļu informācijas par datu plūsmu un atrašanās vietas datus

76 Iesniedzējtiesas izklāstītās pamatlietās aplūkotā valsts tiesiskā regulējuma raksturiezīmes ir jāizvērtē tieši šo principiālo apsvērumu gaismā.

77 Pirmām kārtām, runājot par glabāto datu apjomu, no iesniedzējtiesas lēmuma izriet, ka šajā tiesiskajā regulējumā noteiktais pienākums glabāt datus tālruņa pakalpojumu sniegšanas ietvaros attiecas tostarp uz datiem, kas ir nepieciešami, lai identificētu komunikācijas avotu un adresātu, komunikācijas sākuma un beigu datumu un laiku vai – īsziņu, multivides vai līdzīgu ziņu sūtīšanas gadījumā – ziņas nosūtīšanas un saņemšanas laiku, kā arī mobilā tālruņa izmantošanas gadījumā – to šūnu nosaukumus, kuras zvanītājs un adresāts izmantojuši, sākot komunikāciju. Internetpiekļuves pakalpojumu sniegšanas ietvaros glabāšanas pienākums attiecas tostarp uz abonentam piešķirto IP adresi, interneta lietošanas – kas veikta, izmantojot piešķirto IP adresi, – sākuma un beigu datumu un laiku, kā arī – mobilo sakaru lietošanas gadījumā – tās šūnas nosaukumu, kas izmantota, sākot interneta savienojumu. Tiek glabāti arī dati, kas ļauj noteikt attiecīgo telefonijas šūnu apkalpojošās antenas ģeogrāfisko atrašanās vietu un maksimālo apraides zonu.

78 Pamatlietās aplūkotais valsts tiesiskais regulējums patiešām no glabāšanas pienākuma izslēdz komunikāciju saturu un datus par apmeklētajām tīmekļvietnēm, savukārt šūnu identifikatoru liek glabāt tikai komunikācijas sākumā, tomēr jānorāda, ka tāpat būtībā bija arī ar Direktīvu 2006/24 transponējošajiem valstu tiesiskajiem regulējumiem, kas tika aplūkoti lietās, kurās taisīts 2020. gada 6. oktobra spriedums *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791). Taču, neraugoties uz šiem ierobežojumiem, Tiesa minētajā spriedumā ir nospriedusi, ka to datu kategorijas, kuri tika glabāti, pamatojoties uz šo direktīvu un minētajiem valstu tiesiskajiem regulējumiem, ļāva izdarīt ļoti precīzus secinājumus par attiecīgo datu subjektu privāto dzīvi, proti, to ikdienas paradumiem, pastāvīgās vai pagaidu uzturēšanās vietām, ikdienas vai citām gaitām, veiktajām darbībām, šo subjektu sociālajiem kontaktiem un aprindām, kurās tie mēdz uzturēties, un konkrēti – padarīt iespējamu šo personu profilēšanu.

79 Jākonstatē arī – lai gan pamatlietās aplūkotais tiesiskais regulējums neaptver datus par apmeklētajām tīmekļvietnēm, tas tomēr paredz IP adrešu glabāšanu. Tā kā IP adreses var tikt izmantotas, lai tostarp veiktu izsmeļošu interneta lietotāja tīklklejošanas un līdz ar to tā tiešsaistē veikto darbību izsekošanu, šie dati ļauj noteikt šā lietotāja detalizētu profilu. Tādējādi minēto IP adrešu glabāšana un analīze, kas prasa šādu izsekošanu, ir nopietna iejaukšanās Hartas 7. un 8. pantā garantētajās interneta lietotāja pamattiesībās (šajā nozīmē skat. spriedumu, 2020. gada 6. oktobris, *La Quadrature du Net* u.c., C-511/18, C-512/18 un C-520/18, EU:C:2020:791, 153. punkts).

80 Turklāt – kā rakstveida apsvērumos norādījusi *SpaceNet* –, lai gan uz datiem saistībā ar elektroniskā pasta pakalpojumiem neattiecas pamatlietās aplūkotajā tiesiskajā regulējumā paredzētais glabāšanas pienākums, attiecīgo datu kopumā šā veida datu īpatsvars ir niecīgs.

81 Kā secinājumu 60. punktā būtībā norāda ģenerāladvokāts, pamatlietās aplūkotajā valsts tiesiskajā regulējumā paredzētais glabāšanas pienākums attiecas uz ļoti plašu informācijas par datu plūsmu un atrašanās vietas datu kopumu, kas būtībā ir tāds pats kā to datu kopums, par kuru ir šā sprieduma 78. punktā atgādinātā pastāvīgā judikatūra.

82 Turklāt, atbildot uz tiesas sēdē uzdotu jautājumu, Vācijas valdība precizēja, ka to sociāla vai reliģiska rakstura personu, iestāžu un organizāciju sarakstā, kuru elektronisko komunikāciju dati netiek glabāti saskaņā ar *TKG* 99. panta 2. punktu un 113.b panta 6. punktu, ir reģistrētas tikai 1300 organizācijas, un tā acīmredzami ir visai niecīga daļa no visu to Vācijā esošo elektronisko komunikāciju pakalpojumu lietotāju kopskaita, uz kuru datiem attiecas pamatlietās aplūkotajā valsts tiesiskajā regulējumā paredzētais glabāšanas pienākums. Šādi tiek glabāti arī dienesta noslēpumu ievērojošo profesionāļu, piemēram, advokātu, ārstu vai žurnālistu, dati.

83 Tātad no iesniedzējtiesas lēmuma izriet, ka šajā valsts tiesiskajā regulējumā paredzētā informācijas par datu plūsmu un atrašanās vietas datu glabāšana attiecas uz gandrīz visu iedzīvotāju kopumu, pat ja tie – kaut vai netieši – nav tādā situācijā, kad attiecībā uz tiem būtu jāveic kriminālvajāšana. Turklāt tajā ir noteikts pienākums bez iemesla, visaptveroši un nešķirojot pēc personas, laika vai ģeogrāfiski, glabāt lielāko daļu informācijas par datu plūsmu un atrašanās vietas datu, kuru apjoms būtībā ir tāds pats kā to datu apjoms, kas tika glabāti lietās, par kurām ir šā sprieduma 78. punktā minētā judikatūra.

84 Tāpēc, ievērojot šā sprieduma 75. punktā atreferēto judikatūru, tāds datu glabāšanas pienākums kā pamatlietās aplūkotais – pretēji tam, ko apgalvo Vācijas valdība, – nav uzskatāms par datu mērķorientētu glabāšanu.

85 Otrām kārtām, runājot par datu glabāšanas ilgumu, jāteic, ka no Direktīvas 2002/58 15. panta 1. punkta otrā teikuma izriet, ka glabāšanas ilgums, kas paredzēts valsts tiesiskajā regulējumā, kurā noteikts visaptverošas un nediferencētas glabāšanas pienākums, noteikti ir viens no nozīmīgajiem faktoriem, kas ļauj konstatēt, vai šāds pasākums ir pretrunā Savienības tiesībām, jo šajā teikumā ir prasīts, lai šis ilgums būtu "ierobežots".

86 Šajā gadījumā šis ilgums, kas saskaņā ar *TKG* 113.b panta 1. punktu atrašanās vietas datiem ir četras nedēļas un pārējiem datiem – desmit nedēļas, patiešām ir manāmi īsāks par tiem, kas bija paredzēti visaptverošas un nediferencētas glabāšanas pienākumu noteicošajos valstu tiesiskajos regulējumos, kurus Tiesa izvērtēja 2016. gada 21. decembra spriedumā *Tele2 Sverige* un *Watson* u.c. (C-203/15 un C-698/15, EU:C:2016:970), 2020. gada 6. oktobra spriedumā *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791), kā arī 2022. gada 5. aprīļa spriedumā *Commissioner of An Garda Síochána* u.c. (C-140/20, EU:C:2022:258).

87 Tomēr – kā izriet no šā sprieduma 61. punktā atreferētās judikatūras – iejaukšanās smagums izriet no riska, ka, ņemot vērā glabāto datu apjomu un dažādību, šo datu kopums ļautu izdarīt visnotaļ precīzus secinājumus par tās personas vai personu privāto dzīvi, kuras vai kuru dati ir tikuši glabāti, un it īpaši nodrošinātu līdzekļus attiecīgā datu subjekta vai subjektu profilēšanai, kas tiesību uz privātās dzīves neaizskaramību kontekstā ir tikpat sensitīva informācija kā pats šīs komunikācijas saturs.

88 Tāpēc tādas informācijas par datu plūsmu vai tādu atrašanās vietas datu – kuri var sniegt ziņas par lietotāja ar elektronisko komunikāciju līdzekli veikto komunikāciju vai viņa izmantoto galaiekārtu atrašanās vietu – glabāšana katrā ziņā ir smaga iejaukšanās neatkarīgi gan no tā, cik ilgs ir šīs glabāšanas laikposms, gan no glabāto datu apjoma un iedabas, ja minētais šo datu kopums sniedz iespēju izdarīt ļoti precīzus secinājumus par kāda vai vairāku datu subjektu privāto dzīvi (par piekļuvi šādiem datiem skat. spriedumu, 2021. gada 2. marts, *Prokuratuur* (Piekļuves elektronisko komunikāciju datiem nosacījumi), C-746/18, EU:C:2021:152, 39. punkts).

89 Šajā ziņā pat ierobežota apjoma informācijas par datu plūsmu vai atrašanās vietas datu glabāšana vai šo datu glabāšana uz neilgu laiku var sniegt ļoti precīzu informāciju par elektronisko komunikāciju līdzekļa lietotāja privāto dzīvi. Turklāt pieejamo datu apjoms un no tiem izrietošā ļoti precīzā informācija par attiecīgās personas privāto dzīvi ir apstākļi, kurus var novērtēt tikai pēc iepazīšanās ar minētajiem datiem. Savukārt no minēto datu glabāšanas izrietošā iejaukšanās neizbēgami notiek, pirms var iepazīties ar datiem un informāciju, kas no tiem izriet. Tādējādi glabāšanas radītās iejaukšanās smaguma vērtējums noteikti tiek veikts, ņemot vērā risku, ko glabāto datu kategorija parasti rada datu subjektu privātajai dzīvei, turklāt nav nozīmes tam, vai

no tiem izrietošā informācija par privāto dzīvi konkrēti ir vai nav sensitīva (šajā nozīmē skat. spriedumu, 2021. gada 2. marts, *Prokuratuur* (Piekļuves elektronisko komunikāciju datiem nosacījumi), C-746/18, EU:C:2021:152, 40. punkts).

90 Šajā gadījumā, kā izriet no šā sprieduma 77. punkta un kā ir apstiprināts tiesas sēdē, informācijas par datu plūsmu un atrašanās vietas datu kopums, kas glabāts attiecīgi desmit nedēļas un četras nedēļas, var ļaut izdarīt ļoti precīzus secinājumus par personu, kuru dati tikuši glabāti, privāto dzīvi, proti, ikdienas paradumiem, pastāvīgās vai pagaidu uzturēšanās vietām, ikdienas vai citām gaitām, veiktajām darbībām, šo personu sociālajiem kontaktiem un aprindām, kurās tās mēdz uzturēties, un it īpaši ļauj profilēt attiecīgās personas.

91 Trešām kārtām, runājot par pamatlietās aplūkotajā valsts tiesiskajā regulējumā paredzētajām garantijām glabāto datu aizsardzībai pret ļaunprātīgas izmantošanas un nelikumīgas piekļuves riskiem, jānorāda, ka šo datu glabāšana un piekļuve tiem – kā izriet no šā sprieduma 60. punktā atgādinātās judikatūras – rada atšķirīgu veidu iejaukšanos Hartas 7. un 11. pantā garantētajās pamattiesībās, no kuriem katram ir vajadzīgs atšķirīgs attaisnojums saskaņā ar tās 52. panta 1. punktu. No tā secināms, ka valsts tiesību akti, ar kuriem tiek nodrošināts, ka pilnībā tiek ievēroti nosacījumi, kas izriet no judikatūras par Direktīvas 2002/58 interpretāciju jautājumā par piekļuvi glabātajiem datiem, gluži dabiski nespēj nedz ierobežot, nedz pat novērst to smago iejaukšanos gan šīs direktīvas 5. un 6. pantā, gan šajos pantos konkretizēto pamattiesību garantētajās tiesībās, kura izriet no šajos valsts tiesību aktos paredzētās šo datu visaptverošās glabāšanas (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 47. punkts).

92 Visbeidzot, ceturtām kārtām, par Eiropas Komisijas argumentu, ka īpaši smaga noziedzība būtu pielīdzināma draudiem valsts drošībai, Tiesa ir jau nospriedusi, ka valsts drošības aizsardzības mērķis atbilst primārajām interesēm aizsargāt valsts pamatfunkcijas un sabiedrības pamatintereses, novēršot un apkarojot tādas darbības, kas var nopietni destabilizēt valsts konstitucionālās, politiskās, ekonomiskās vai sociālās pamatstruktūras un it īpaši tieši apdraudēt pašu sabiedrību, iedzīvotājus vai valsti, kā, piemēram, terorisma darbības (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 61. punkts, kā arī tajā minētā judikatūra).

93 Atšķirībā no noziedzības – pat tad, ja tā ir īpaši smaga – valsts drošības apdraudējumam ir jābūt reālam un faktiskam vai vismaz paredzamam, un tas nozīmē, ka ir jābūt pietiekami konkrētiem apstākļiem, lai varētu attaisnot pasākumu informācijas par datu plūsmu un atrašanās vietas datu visaptverošai un nediferencētai glabāšanai uz ierobežotu laiku. Tātad šādi draudi pēc sava rakstura, smaguma un to veidojošo apstākļu specifiskuma dēļ atšķiras no vispārīgā un pastāvīgā riska, ka varētu rasties spriedze vai tikt traucēta, pat nopietni traucēta, sabiedrības drošība, vai izdarīti smagi noziegumi (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 62. punkts, kā arī tajā minētā judikatūra).

94 Tādējādi noziedzība – pat tad, ja tā ir īpaši smaga – nav pielīdzināma valsts drošības apdraudējumam. Proti, šādas pielīdzināšanas rezultātā iespējami tiktu radīta starpkategorija starp valsts drošību un sabiedrības drošību, lai uz otro no tām attiecinātu prasības, kādas ir attiecināmas uz pirmo (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 63. punkts).

Par pasākumiem, kas paredz mērķorientētu glabāšanu, operatīvo saglabāšanu vai IP adrešu glabāšanu

95 Vairāku dalībvalstu valdības, tostarp Francijas valdība, uzsver, ka tikai visaptveroša un nediferencēta glabāšana ļauj efektīvi sasniegt glabāšanas pasākumu mērķus, savukārt Vācijas valdība būtībā piebilst, ka šādu secinājumu neliek apšaubīt apstāklis, ka dalībvalstis var izmantot mērķorientētas glabāšanas un operatīvās saglabāšanas pasākumus, kas minēti šā sprieduma 75. punktā.

96 Šajā ziņā jānorāda, pirmām kārtām, ka krimināltvajāšanas efektivitāte parasti ir atkarīga nevis no kāda viena izmeklēšanas līdzekļa, bet gan no visiem valsts kompetento iestāžu rīcībā tālab esošajiem izmeklēšanas līdzekļiem (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 69. punkts).

97 Otrām kārtām, Direktīvas 2002/58 15. panta 1. punktā – lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā un atbilstoši tam, kā tas interpretēts šā sprieduma 75. punktā atgādinātajā judikatūrā, – ir ļauts dalībvalstīm smagas noziedzības apkarošanas un nopietnu sabiedrības drošības apdraudējumu novēršanas nolūkā pieņemt ne tikai pasākumus, kas paredz mērķorientētu glabāšanu un operatīvo saglabāšanu, bet arī pasākumus, kas paredz iespēju visaptveroši un nediferencēti glabāt gan elektronisko komunikāciju līdzekļu lietotāju personas identitātes datus, gan savienojuma avotam piešķirtās IP adreses (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 70. punkts).

98 Šai ziņā netiek apstrīdēts, ka elektronisko komunikāciju līdzekļu lietotāju personas identitātes datu glabāšana var palīdzēt apkarot smagus noziegumus, ciktāl šie dati palīdz identificēt personas, kuras ir izmantojušas šo līdzekļus, gatavojoties izdarīt vai izdarot tādu nodarījumu, kas kvalificējams kā smags noziegums (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 71. punkts).

99 Direktīvai 2002/58 nav pretrunā visaptveroši glabāt personas identitātes datus, lai apkarotu noziedzību vispār. Šajos apstākļos jāprecizē, ka nedz šai direktīvai, nedz kādam citam Savienības tiesību aktam nav pretrunā tādi uz smagas noziedzības apkarošanu vērsti valsts tiesību akti, saskaņā ar kuriem elektroniskās komunikācijas līdzekļa, piemēram, priekšapmaksas *SIM* kartes, iegāde ir pakārtota prasībai par pircēja identitāti apliecinošu dokumentu pārbaudi un pārdevēja pienākumam reģistrēt no tās izrietošo informāciju, kā arī vajadzības gadījumā dot kompetentajām valsts iestādēm piekļuvi šai informācijai (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 72. punkts).

100 Turklāt jāatgādina, ka savienojuma avota IP adrešu visaptveroša glabāšana rada smagu iejaukšanos Hartas 7. un 8. pantā nostiprinātajās pamattiesībās, jo šīs IP adreses ļauj izdarīt precīzus secinājumus par attiecīgā elektronisko komunikāciju līdzekļa lietotāja privāto dzīvi, un tai var būt atturoša ietekme uz Hartas 11. pantā garantētās vārda brīvības izmantošanu. Taču jautājumā par šādu glabāšanu Tiesa ir konstatējusi: lai nodrošinātu nepieciešamo attiecīgo tiesību un leģitīmo interešu salāgošanu, kā prasīts šā sprieduma 65.–68. punktā minētajā judikatūrā, ir jāņem vērā, ka tiešsaistē izdarīta noziedzīga nodarījuma gadījumā – it īpaši, iegādājoties, izplatot, pārsūtot vai augšupielādējot bērnu pornogrāfiju Eiropas Parlamenta un Padomes Direktīvas 2011/93/ES (2011. gada 13. decembris) par seksuālas vardarbības pret bērniem, bērnu seksuālas izmantošanas un bērnu pornogrāfijas apkarošanu un ar kuru aizstāj Padomes Pamatlēmumu 2004/68/TI (OV 2011, L 335, 1. lpp.; labojums – OV 2012, L 18, 7. lpp.) 2. panta c) punkta izpratnē – IP

adrese var izrādīties esam vienīgais izmeklēšanas līdzeklis, kas ļauj identificēt personu, kurai šī adrese ir piešķirta noziedzīgā nodarījuma izdarīšanas brīdī (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 73. punkts).

101 Šādos apstākļos – lai arī leģislatīvais pasākums, kurā paredzēta visu to fizisko personu IP adrešu glabāšana, kurām pieder tāda galaiekārta, no kuras var tikt veikta piekļuve internetam, patiešām var attiekties uz personām, kurām šā sprieduma 70. punktā minētās judikatūras izpratnē pirmšķietami nav tiešas saiknes ar sasniedzamajiem mērķiem, un interneta lietotājiem atbilstoši šā sprieduma 54. punktā konstatētajam saskaņā ar Hartas 7. un 8. pantu patiešām ir tiesības sagaidīt, ka principā viņu identitāte netiks atklāta – tāds leģislatīvais pasākums, kurā paredzēta visaptveroša un nediferencēta vienīgi to IP adrešu glabāšana, kuras ir piešķirtas savienojuma avotam, principā nav pretrunā Direktīvas 2002/58 15. panta 1. punktam, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, ja šī iespēja ir pakļauta stingrai materiāltiesisko un tādu procesuālo nosacījumu ievērošanai, kam jāreglamentē šo datu izmantošana (spriedums, 2020. gada 6. oktobris, *La Quadrature du Net* u.c., C-511/18, C-512/18 un C-520/18, EU:C:2020:791, 155. punkts).

102 Ņemot vērā, ka šādas glabāšanas ceļā notiek smaga iejaukšanās Hartas 7. un 8. pantā garantētajās pamattiesībās, šo iejaukšanos tāpat kā valsts drošības aizsardzība var pamatot vienīgi smagas noziedzības apkarošana un nopietnu sabiedrības drošības apdraudējumu novēršana. Turklāt glabāšanas ilgums nedrīkst pārsniegt to, kas ir absolūti nepieciešams izvirzītā mērķa sasniegšanai. Visbeidzot, šāda veida pasākumā ir jāparedz stingri nosacījumi un garantijas attiecībā uz šo datu izmantošanu, it īpaši, izsekojot datu subjektu tiešsaistes komunikācijas un darbības (spriedums, 2020. gada 6. oktobris, *La Quadrature du Net* u.c., C-511/18, C-512/18 un C-520/18, EU:C:2020:791, 156. punkts).

103 Tādējādi – pretēji iesniedzējtiesas teiktajam – 2020. gada 6. oktobra sprieduma *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791) 155. un 168. punkta starpā disonanses nav. Proti, kā secinājumu 81. un 82. punktā būtībā norāda ģenerāladvokāts, no minētā sprieduma 155. punkta, lasot to kopsakarā ar tā 156. un 168. punktu, izriet, ka tikai smagas noziedzības apkarošana un nopietnu sabiedrības drošības apdraudējumu novēršana var – tāpat kā valsts drošības aizsardzība – attaisnot savienojuma avotam piešķirto IP adrešu visaptverošu glabāšanu neatkarīgi no tā, vai attiecīgo datu subjekti var būt kaut vai vismaz netieši saistīti ar izvirzītajiem mērķiem.

104 Trešām kārtām, runājot par leģislatīvajiem pasākumiem, kas paredz informācijas par datu plūsmu un atrašanās vietas datu mērķorientētu glabāšanu un operatīvu saglabāšanu, daži apsvērumi, ko dalībvalstis ir paudušas pret šādiem pasākumiem, liecina, ka šo pasākumu tvērums tiek izprasts šaurāk, nekā tas darīts šā sprieduma 75. punktā atgādinātajā judikatūrā. Proti, lai arī – kā atgādināts šā sprieduma 57. punktā – šiem glabāšanas pasākumiem Direktīvas 2002/58 ieviestajā sistēmā ir jābūt izņēmumam, iespēja izdot rīkojumu par mērķorientētu glabāšanu šajā direktīvā, lasot to Hartas 7., 8. un 11. pantā, kā arī 52. panta 1. punktā nostiprināto pamattiesību gaismā, netiek pakārtota nosacījumam, ka pirms tam būtu jābūt zināmām vietām, kur iespējami tiks izdarīts smags noziegums, vai personām, kuras tiek turētas aizdomās par iesaisti šādā nodarījumā. Minētajā direktīvā netiek arī prasīts, lai rīkojums par operatīvo saglabāšanu attiektos tikai uz aizdomās turētajām personām, kas ir identificētas pirms šāda rīkojuma (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 75. punkts).

105 Jautājumā, pirmkārt, par mērķorientētu glabāšanu Tiesa ir nospriedusi, ka Direktīvas 2002/58 15. panta 1. punktam nav pretrunā valsts tiesību akti, kuru pamatā ir objektīvi kritēriji, kas ļauj, no vienas puses, vērsties pret personām, kuru gadījumā informācija par datu plūsmu un atrašanās vietas dati var norādīt uz – kaut vai netiešu – saikni ar smagiem noziegumiem, veicināt smagas noziedzības apkarošanu vai novērst nopietnu sabiedrības drošības apdraudējumu vai valsts drošības apdraudējumu (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 76. punkts, kā arī tajā minētā judikatūra).

106 Šajā ziņā Tiesa ir precizējusi, ka, lai gan šie objektīvie kritēriji var atšķirties atkarībā no veiktajiem pasākumiem smagas noziedzības novēršanas, izmeklēšanas, atklāšanas un kriminālvajāšanas nolūkā, personu loks, uz kurām tie attiecas, var ietvert konkrēti tās, kuras piemērojamās valsts procedūrās un pamatojoties uz objektīviem kritērijiem iepriekš ir identificētas kā tādas, kas apdraud attiecīgās dalībvalsts sabiedrības drošību vai valsts drošību (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 77. punkts).

107 Tādējādi dalībvalstis var veikt glabāšanas pasākumus saistībā ar personām, attiecībā uz kurām šādas identifikācijas rezultātā tiek veikta izmeklēšana vai citi novērošanas pasākumi vai par kurām ir izdarīts ieraksts valsts sodu reģistrā ar norādi uz agrāku sodāmību par smagu noziegumu izdarīšanu, kas var nozīmēt paaugstinātu recidīva risku. Ja šāda identifikācija ir balstīta uz valsts tiesībās noteiktiem objektīviem un nediskriminējošiem kritērijiem, mērķorientēta glabāšana attiecībā uz šādi identificētajām personām ir attaisnota (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 78. punkts).

108 No otras puses, informācijas par datu plūsmu un atrašanās vietas datu mērķorientētas glabāšanas pasākumu pēc valsts likumdevēja izvēles un stingri ievērojot samērīguma principu var balstīt arī uz ģeogrāfisku kritēriju, kad kompetentās valsts iestādes, pamatojoties uz objektīviem un nediskriminējošiem kritērijiem, uzskata, ka vienā vai vairākās ģeogrāfiskajās zonās pastāv augsts gatavošanās smagu noziegumu izdarīšanai vai to izdarīšanas risks. Šīs zonas tostarp var būt vietas, kurās raksturīgs liels smagu noziegumu skaits, vietas, kurās ir īpaši augsts smagu noziegumu izdarīšanas risks, piemēram, vietas vai infrastruktūras objekti, ko regulāri apmeklē ļoti liels personu skaits, vai arī stratēģiskas vietas, piemēram, lidostas, dzelzceļa stacijas, jūras ostas vai autoceļu lietošanas maksas iekasēšanas vietas (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 79. punkts, kā arī tajā minētā judikatūra).

109 Jāuzsver, ka saskaņā ar šo judikatūru kompetentās valsts iestādes attiecībā uz iepriekšējā punktā minētajām zonām drīkst veikt mērķorientētas glabāšanas pasākumu, pamatojoties uz ģeogrāfisku kritēriju, piemēram, vidējo noziedzības rādītāju kādā ģeogrāfiskajā zonā, un tālab nav obligāti nepieciešams, lai tām būtu zināmas konkrētas pazīmes, kas liecina par to, ka attiecīgajās zonās notiek gatavošanās smagu noziegumu izdarīšanai vai tie tiek izdarīti. Ciktāl, balstoties uz šo kritēriju, veiktā mērķorientētā glabāšana – atkarībā no konkrētajiem smagajiem noziegumiem un attiecīgajās dalībvalstīs esošās konkrētās situācijas – iespējami skar gan vietas, kam raksturīgs liels smagu noziegumu skaits, gan vietas, kurās jo īpaši iespējama šādu nodarījumu izdarīšana, tā turklāt principā nav diskriminējoša, jo kritērijs, kas balstīts uz vidējo smagās noziedzības rādītāju, pats par sevi nav nekādi saistīts ar faktoriem, kas iespējami varētu būt diskriminējoši (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 80. punkts).

110 Turklāt un vispār mērķorientētas glabāšanas pasākums, kurš tiek veikts attiecībā uz vietām vai infrastruktūras objektiem, ko regulāri apmeklē ļoti liels personu skaits, vai arī stratēģiskām vietām, piemēram, lidostām, dzelzceļa stacijām, jūras ostām vai autoceļu lietošanas maksas iekasēšanas vietām, ļauj kompetentajām iestādēm ievākt informāciju par datu plūsmu, un konkrēti – atrašanās vietas datus par visām personām, kas kādā konkrētā brīdī kādā no šīm vietām lieto elektroniskās komunikācijas līdzekli. Tādējādi šāds mērķorientētas glabāšanas pasākums iespējami ļauj minētajām iestādēm, piekļūstot šādi glabātajiem datiem, iegūt informāciju par šo personu atrašanos vietās vai ģeogrāfiskajās zonās, attiecībā uz kurām tiek veikts šis pasākums, kā arī par šo personu pārvietošanos starp šīm vietām un zonām vai to robežās, un smagas noziedzības apkarošanas nolūkos šīs glabāšanas laikā no šīs informācijas izdarīt secinājumus par viņu atrašanos un aktivitātēm šajās vietās vai ģeogrāfiskajās zonās kādā konkrētā laikā (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 81. punkts).

111 Vēl jānorāda, ka ģeogrāfiskās zonas, attiecībā uz kurām tiek veikta šāda mērķorientēta glabāšana, var mainīt un vajadzības gadījumā tas ir jādara atkarībā no tā, kā mainās nosacījumi, uz kuru pamata tās ir izvēlētas, šādi ļaujot tostarp reaģēt uz notikumu attīstības gaitu smagas noziedzības apkarošanā. Proti, Tiesa jau ir nospriedusi, ka šā sprieduma 105.–110. punktā aprakstīto mērķorientēto glabāšanas pasākumu ilgums nedrīkst pārsniegt to, kas ir absolūti nepieciešams, ņemot vērā ar tiem sasniedzamo mērķi, kā arī tos pamatojošos apstākļus, ar iespēju tos pagarināt gadījumā, ja šāda glabāšana joprojām ir nepieciešama (spriedumi, 2020. gada 6. oktobris, *La Quadrature du Net* u.c., C-511/18, C-512/18 un C-520/18, EU:C:2020:791, 151. punkts, kā arī 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 82. punkts).

112 Runājot par iespēju informācijas par datu plūsmu un atrašanās vietas datu mērķorientētas glabāšanas nolūkiem paredzēt citus nošķirošus kritērijus – kas nav saistīti ar konkrētu personu loku vai ģeogrāfiski –, nav izslēdzams, ka var tikt ņemti vērā citi objektīvi un nediskriminējoši kritēriji, lai nodrošinātu, ka mērķorientētas glabāšanas apjoms tiek ierobežots līdz absolūti nepieciešamajam, un konstatētu vismaz netiešu saikni starp smagajiem noziegumiem un personām, kuru dati ir glabāti. Tomēr, ņemot vērā, ka Direktīvas 2002/58 15. panta 1. punktā ir runa par dalībvalstu leģislatīvajiem pasākumiem, tieši dalībvalstīm, nevis Tiesai ir jānosaka šie kritēriji, protams, izslēdzot iespēju, ka šādā ceļā varētu tikt atjaunota informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencētu glabāšana (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 83. punkts).

113 Katrā ziņā – kā secinājumu 50. punktā norādījis ģenerāladvokāts – iespējamās grūtības precīzi noteikt gadījumus, kad var tikt veikta mērķorientēta glabāšana, un nosacījumus, saskaņā ar kuriem tā veicama, neļauj dalībvalstīm, padarot atkāpi par principu, paredzēt informācijas par datu plūsmu un atrašanās vietas datu visaptverošu un nediferencētu glabāšanu (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 84. punkts).

114 Otrkārt, jautājumā par tās informācijas par datu plūsmu un to atrašanās vietas datu glabāšanu, kurus elektronisko komunikāciju pakalpojumu sniedzēji apstrādā un uzglabā, pamatojoties vai nu uz Direktīvas 2002/58 5., 6. un 9. pantu, vai uz leģislatīvajiem pasākumiem, kas pieņemti saskaņā ar tās 15. panta 1. punktu, jāatgādina, ka šie dati principā katrā konkrētajā gadījumā ir jādzēš vai jāpadara anonīmi, beidzoties termiņam, kas minētās direktīvas transponēšanai pieņemtajās valsts tiesību normās ir likumiski noteikts to apstrādei un uzglabāšanai. Tomēr Tiesa ir nospriedusi, ka šīs apstrādes un uzglabāšanas laikā var rasties situācijas, kad ir nepieciešams glabāt minētos datus

arī pēc šiem termiņiem, lai atklātu smagus noziegumus vai valsts drošības apdraudējumus, un tas var notikt gan situācijā, kad šie noziedzīgie nodarījumi vai apdraudējumi jau ir tikuši konstatēti, gan gadījumā, kad par to esamību pēc visu lietā nozīmīgo apstākļu objektīvas pārbaudes var rasties pamatotas aizdomas (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 85. punkts).

115 Šādā situācijā dalībvalstis, ņemot vērā šā sprieduma 65.–68. punktā minēto nepieciešamību salāgot attiecīgās tiesības un leģitīmās intereses, var saskaņā ar Direktīvas 2002/58 15. panta 1. punktu pieņemtajos tiesību aktos paredzēt iespēju ar kompetentās iestādes lēmumu, kas ir pakļauts efektīvai pārbaudei tiesā, uzdot elektronisko komunikāciju pakalpojumu sniedzējiem uz noteiktu laiku operatīvi saglabāt to rīcībā esošo informāciju par datu plūsmu un atrašanās vietas datus (spriedumi, 2020. gada 6. oktobris, *La Quadrature du Net* u.c., C-511/18, C-512/18 un C-520/18, EU:C:2020:791, 163. punkts, kā arī 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 86. punkts).

116 Ciktāl šādas operatīvās saglabāšanas mērķis vairs neatbilst mērķiem, kuriem šie dati tika sākotnēji ievākti un glabāti, un tā kā datu apstrādei saskaņā ar Hartas 8. panta 2. punktu ir jāatbilst noteiktiem mērķiem, dalībvalstīm savos tiesību aktos ir jāprecizē, kādam mērķim var tikt veikta datu operatīvā saglabāšana. Ievērojot to, cik nopietnu Hartas 7. un 8. pantā nostiprināto pamattiesību aizskārumu spēj radīt šāda glabāšana, šis aizskārums var būt attaisnojams tikai ar mērķi apkarot smagu noziedzību vai – *a fortiori* – aizsargāt valsts drošību, ja vien šis pasākums, kā arī piekļuve šādi glabātajiem datiem aprobežojas ar to, kas ir absolūti nepieciešams, kā noteikts 2020. gada 6. oktobra sprieduma *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791) 164.–167. punktā (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 87. punkts).

117 Tiesa ir precizējusi, ka šāda veida glabāšanas pasākums var tikt attiecināts ne tikai uz to personu datiem, kuras pirms tam ir identificētas kā tādas, kas apdraud attiecīgās dalībvalsts sabiedrības drošību vai valsts drošību, vai kuras konkrēti tiek turētas aizdomās par smaga nozieguma izdarīšanu vai valsts drošības apdraudējumu. Proti, Tiesa ir atzinusi, ka, ievērojot Direktīvas 2002/58 15. panta 1. punktā, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, noteiktos ietvarus un ņemot vērā šā sprieduma 70. punktā minētos apsvērumus, šādu pasākumu – atkarībā no valsts likumdevēja izvēles un ievērojot absolūti nepieciešamā robežas – var attiecināt arī uz informāciju par datu plūsmu un atrašanās vietas datiem saistībā ar personām, kas nav tās, kuras tiek turētas aizdomās par to, ka tās ir plānojušas vai izdarījušas smagu noziegumu vai valsts drošības apdraudējumu, ciktāl šie dati, pamatojoties uz objektīviem un nediskriminējošiem kritērijiem, var veicināt šāda noziedzīga nodarījuma vai valsts drošības apdraudējuma atklāšanu, piemēram, cietušās personas dati, kā arī dati par tās sociālo vai profesionālo vidi veidojošo personu loku (spriedumi, 2020. gada 6. oktobris, *La Quadrature du Net* u.c., C-511/18, C-512/18 un C-520/18, EU:C:2020:791, 165. punkts, kā arī 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 88. punkts).

118 Tādējādi ar leģislatīvu pasākumu var atļaut izdot rīkojumu elektronisko komunikāciju pakalpojumu sniedzējiem veikt informācijas par datu plūsmu un atrašanās vietas datu operatīvo saglabāšanu attiecībā tostarp uz personām, ar kurām pirms nopietna sabiedrības drošības apdraudējuma vai smaga nozieguma izdarīšanas cietusī persona bija sazinājusies, izmantojot savus elektronisko komunikāciju līdzekļus (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 89. punkts).

119 Šādu operatīvo saglabāšanu saskaņā ar šā sprieduma 117. punktā atgādināto judikatūru un ar tādiem pašiem nosacījumiem kā minētajā punktā noteiktie var attiecināt arī uz noteiktām ģeogrāfiskajām zonām, piemēram, vietām, kur izdarīts attiecīgais noziedzīgais nodarījums vai valsts drošības apdraudējums un notikusi gatavošanās to izdarīšanai. Jāprecizē, ka šādu pasākumu var veikt arī ar informāciju par datu plūsmu un atrašanās vietas datiem attiecībā uz vietu, kur ir pazudusi persona, kas iespējami ir cietusi smagā noziegumā, ja vien šis pasākums, kā arī piekļuve šādi glabātajiem datiem aprobežojas ar to, kas ir absolūti nepieciešams smagas noziedzības apkarošanas vai valsts drošības aizsardzības mērķiem, kā noteikts 2020. gada 6. oktobra sprieduma *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791) 164.–167. punktā (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 90. punkts).

120 Jāprecizē arīdzan, ka Direktīvas 2002/58 15. panta 1. punktam nav pretrunā, ka kompetentās valsts iestādes izdod rīkojumu veikt operatīvo saglabāšanu jau kopš brīža, kad tiek sākta izmeklēšana jautājumā par nopietnu sabiedriskās drošības apdraudējumu vai iespējamu smagu noziegumu, proti, līdzko šīs iestādes saskaņā ar piemērojamajām valsts tiesību normām var sākt šādu izmeklēšanu (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 91. punkts).

121 Runājot vēl par šā sprieduma 75. punktā minēto dažādo informācijas par datu plūsmu un atrašanās vietas datu glabāšanas pasākumu klāstu, jāprecizē, ka šos dažādos pasākumus atkarībā no valsts likumdevēja izvēles un ievērojot absolūti nepieciešamā robežas var piemērot kopā. Šajos apstākļos Direktīvas 2002/58 15. panta 1. punktam - lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā un atbilstoši tam, kā tas interpretēts judikatūrā, kas izriet no 2020. gada 6. oktobra sprieduma *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791), - nav pretrunā, ka šie pasākumi tiek apvienoti (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 92. punkts).

122 Visbeidzot, ceturtām kārtām, jāuzsver, ka, lai saskaņā ar Direktīvas 2002/58 15. panta 1. punktu pieņemtie pasākumi būtu samērīgi, tiem saskaņā ar Tiesas pastāvīgo judikatūru, kas atreferēta 2020. gada 6. oktobra spriedumā *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791), ir jāatbilst ne tikai piemērotības un nepieciešamības prasībām, bet arī prasībai par šo pasākumu samērīgumu ar izvirzīto mērķi (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 93. punkts).

123 Šajā kontekstā jāatgādina, ka 2014. gada 8. aprīļa sprieduma *Digital Rights Ireland* u.c. (C-293/12 un C-594/12, EU:C:2014:238) 51. punktā Tiesa ir nospriedusi, ka, lai gan smagas noziedzības apkarošana ir ārkārtīgi svarīga sabiedriskās drošības garantēšanai un tās efektivitāte lielā mērā var būt atkarīga no moderno izmeklēšanas metožu izmantošanas, tomēr šis vispārējo interešu mērķis, lai cik būtisks tas būtu, pats par sevi nevar pamatot tāda informācijas par datu plūsmu un atrašanās vietas datu visaptverošas un nediferencētas glabāšanas pasākuma kā Direktīvā 2006/24 noteiktais nepieciešamību (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 94. punkts).

124 Ar šādu pašu domu gājienu 2020. gada 6. oktobra sprieduma *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791) 145. punktā Tiesa ir precizējusi, ka pat dalībvalstu pozitīvie pienākumi, kuri var izrietēt attiecīgi no Hartas 3., 4. un 7. panta un kuri, kā norādīts šā sprieduma 64. punktā, attiecas uz tādu noteikumu ieviešanu, kas ļauj efektīvi apkarot noziedzīgus nodarījumus, nevar attaisnot tik nopietnu no valsts tiesību aktiem, kuros paredzēta informācijas par datu plūsmu un atrašanās vietas datu glabāšana, izrietošu iejaukšanos gandrīz

visu iedzīvotāju pamattiesībās, kas garantētas Hartas 7. un 8. pantā, ja attiecīgo personu datiem nav – kaut vai tikai netiešas – saiknes ar izvirzīto mērķi (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 95. punkts).

125 Turklāt ECT 2021. gada 25. maija spriedums *Big Brother Watch* u.c. pret Apvienoto Karalisti (CE:ECHR:2021:0525JUD005817013) un 2021. gada 25. maija spriedums *Centrum för Rättvisa* pret Zviedriju (CE:ECHR:2021:0525JUD003525208) – uz kuriem atsaucoties dažas valdības tiesas sēdē apgalvoja, ka ECPAK pieļauj valstu tiesiskos regulējumus, kas būtībā paredz visaptveroši un nediferencēti glabāt informāciju par datu plūsmu vai atrašanās vietas datus, – neliek apšaubīt no iepriekš izklāstītā izrietošo Direktīvas 2002/58 15. panta 1. punkta interpretāciju. Proti, minētajos spriedumos tika aplūkota ar starptautiskajām komunikācijām saistīto datu masveida pārtveršana. Tādējādi – kā tiesas sēdē norādīja Komisija – minētajos spriedumos Eiropas Cilvēktiesību tiesa nav spriedusi par to, vai ar ECPAK ir saderīga tāda informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta glabāšana, kas veikta valsts teritorijā, nedz pat šo datu masveida pārtveršana smagu noziegumu novēršanas, atklāšanas un izmeklēšanas nolūkos. Katrā ziņā jāatgādina, ka Hartas 52. panta 3. punkta mērķis ir nodrošināt nepieciešamo saskaņotību starp Hartā ietvertajām tiesībām un atbilstošajām ECPAK garantētajām tiesībām, neskarot Savienības tiesību un Eiropas Savienības Tiesas autonomiju, un tāpēc, interpretējot Hartu, atbilstošās ECPAK tiesības ir jāņem vērā tikai kā aizsardzības prasību minimums (spriedums, 2020. gada 17. decembris, *Centraal Israëlitisch Consistorie van België* u.c., C-336/19, EU:C:2020:1031, 56. punkts).

Par piekļuvi visaptveroši un nediferencēti glabātajiem datiem

126 Dānijas valdība tiesas sēdē apgalvoja, ka kompetentajām valsts iestādēm būtu jāvar smagas noziedzības apkarošanas nolūkos piekļūt visaptveroši un nediferencēti glabātajai informācijai par datu plūsmu un atrašanās vietas datiem atbilstoši no 2020. gada 6. oktobra sprieduma *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791, 135.–139. punkts) izrietošajai judikatūrai, lai reaģētu uz nopietnu valsts drošības apdraudējumu, kas izrādās patiess un faktisks vai paredzams.

127 Uzreiz jānorāda, ka smagas noziedzības apkarošanas nolūkos atļaut piekļuvi visaptveroši un nediferencēti glabātajai informācijai par datu plūsmu un atrašanās vietas datiem nozīmētu padarīt šo piekļuvi atkarīgu no apstākļiem, kuriem nav nekā kopīga ar šo mērķi, atkarībā no tā, vai attiecīgajā dalībvalstī pastāv vai nepastāv tāds nopietns valsts drošības apdraudējums kā iepriekšējā punktā minētais, lai gan, ievērojot to, ka šo datu glabāšanai un piekļuvei tiem ir jābūt pamatotai vienīgi ar mērķi apkarot smagu noziedzību, nekas neattaisnotu atšķirīgu attieksmi, it īpaši starp dalībvalstīm (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 97. punkts).

128 Kā Tiesa jau nospriedusi, piekļuvi informācijai par datu plūsmu un atrašanās vietas datiem, ko elektronisko komunikāciju pakalpojumu sniedzēji glabā atbilstoši saskaņā ar Direktīvas 2002/58 15. panta 1. punktu pieņemtam leģislatīvam pasākumam, kuram pilnībā ir jāatbilst no šo direktīvu interpretējošās judikatūras izrietošajiem nosacījumiem, principā var pamatot vienīgi ar to vispārējo interešu mērķi, kura dēļ pakalpojumu sniedzējiem ir ticis uzdots veikt šādu glabāšanu. Citādi ir tikai gadījumā, ja piekļuves mērķis ir svarīgāks par mērķi, kas ir pamatojis glabāšanu (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 98. punkts).

129 Savukārt Dānijas valdības argumentācija attiecas uz situāciju, kad iecerētās piekļuves pieprasījuma mērķis, proti, smagas noziedzības apkarošana, vispārējo interešu mērķu hierarhijā ierindojas kā mazāk svarīgs nekā šo glabāšanu pamatojušais mērķis, proti, valsts drošības aizsardzība. Šādos apstākļos atļaut piekļuvi glabātajiem datiem būtu pretrunā šai vispārējo interešu mērķu hierarhijai, kas atgādināta šā sprieduma iepriekšējā punktā, kā arī 68., 71., 72. un 73. punktā (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 99. punkts).

130 Turklāt atbilstoši šā sprieduma 74. punktā atgādinātajai judikatūrai informāciju par datu plūsmu un atrašanās vietas datus visaptveroši un nediferencēti glabāt smagas noziedzības apkarošanas nolūkā nedrīkst vispār, un tāpēc ar šiem pašiem mērķiem nav pamatojama arī piekļuve šiem datiem. Taču tad, kad šie dati izņēmuma kārtā ir visaptveroši un nediferencēti glabāti, lai aizsargātu valsts drošību pret apdraudējumu, kas izrādās patiess un faktisks vai paredzams, ar šā sprieduma 71. punktā minētajiem nosacījumiem, valsts iestādes, kuru kompetencē ir krimināllizmeklēšana, nedrīkst šiem datiem piekļūt krimināltvajāšanas ietvaros, jo pretējā gadījumā tiktu atņemta visa lietderīgā iedarbība minētajā 74. punktā atgādinātajam aizliegumam veikt šādu glabāšanu smagas noziedzības apkarošanas nolūkos (spriedums, 2022. gada 5. aprīlis, *Commissioner of An Garda Síochána* u.c., C-140/20, EU:C:2022:258, 100. punkts).

131 Ņemot vērā visus iepriekš izklāstītos apsvērumus, uz prejudiciālo jautājumu ir atbildams, 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 ir pretrunā tādi valsts leģislatīvi pasākumi, kuros smagas noziedzības apkarošanai un nopietna sabiedrības drošības apdraudējuma novēršanai preventīvi tiek paredzēta informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta glabāšana. Minētais 15. panta 1. punkts, lasot to Hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, ir jāinterpretē tādējādi, ka tam savukārt nav pretrunā valsts leģislatīvi pasākumi, kas:

– ļauj ar rīkojumu uzdot elektronisko komunikāciju pakalpojumu sniedzējiem visaptveroši un nediferencēti glabāt informāciju par datu plūsmu un atrašanās vietas datus valsts drošības aizsardzības nolūkā situācijās, kad attiecīgā dalībvalsts sastopas ar nopietniem draudiem valsts drošībai, kuri izrādās patiesi un faktiski vai paredzami, ja lēmumu par šo rīkojumu var pakļaut efektīvai pārbaudei tiesā vai arī neatkarīgā administratīvā iestādē – kuras nolēmumam ir saistoša iedarbība –, lai pārbaudītu šādas situācijas esamību, kā arī paredzēto nosacījumu un garantiju ievērošanu, un minēto rīkojumu var izdot vienīgi uz laikposmu, kura ilgums aprobežojas ar absolūti nepieciešamo, taču kuru var pagarināt, ja šāds apdraudējums joprojām pastāv;

– valsts drošības aizsardzības, smagas noziedzības apkarošanas un nopietna sabiedrības drošības apdraudējuma novēršanas nolūkos paredz informācijas par datu plūsmu un atrašanās vietas datu mērķorientētu glabāšanu – kura, pamatojoties uz objektīviem un nediskriminējošiem elementiem, tiek ierobežota atkarībā no attiecīgo personu kategorijām vai pēc ģeogrāfiska kritērija – uz laikposmu, kura ilgums aprobežojas ar absolūti nepieciešamo, taču kuru var pagarināt;

– valsts drošības aizsardzības, smagas noziedzības apkarošanas un nopietna sabiedrības drošības apdraudējuma novēršanas nolūkos paredz savienojuma avotam piešķirto IP adrešu visaptverošu un nediferencētu glabāšanu uz laikposmu, kura ilgums aprobežojas ar absolūti nepieciešamo;

– valsts drošības aizsardzības, noziedzības apkarošanas un sabiedrības drošības aizsardzības nolūkos paredz elektronisko komunikāciju līdzekļu lietotāju personas identitātes datu visaptverošu un nediferencētu glabāšanu; un

– smagas noziedzības apkarošanas un *a fortiori* valsts drošības aizsardzības nolūkos paredz ar kompetentās iestādes lēmumu, kas ir pakļauts efektīvai pārbaudei tiesā, noformēta rīkojuma izdošanu elektronisko komunikāciju pakalpojumu sniedzējiem uz noteiktu laiku veikt šo pakalpojumu sniedzēju rīcībā esošās informācijas par datu plūsmu un atrašanās vietas datu operatīvo saglabāšanu,

ja ar šiem pasākumiem, paredzot skaidrus un konkrētus noteikumus, tiek nodrošināts, ka attiecīgo datu glabāšana notiek atbilstoši tai paredzētajiem materiāltiesiskajiem un procesuālajiem nosacījumiem un ka datu subjektiem ir efektīvas garantijas pret ļaunprātīgas izmantošanas risku.

Par tiesāšanās izdevumiem

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

Ar šādu pamatojumu Tiesa (virspalāta) nospriež:

Eiropas Parlamenta un Padomes Direktīvas 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju), redakcijā ar grozījumiem, kas tajā 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 ir pretrunā tādi valsts leģislatīvie pasākumi, kuros smagas noziedzības apkarošanai un nopietna sabiedrības drošības apdraudējuma novēršanai preventīvi tiek paredzēta informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta glabāšana;

tam nav pretrunā valsts leģislatīvie pasākumi, kas:

– **ļauj ar rīkojumu uzdot elektronisko komunikāciju pakalpojumu sniedzējiem visaptveroši un nediferencēti glabāt informāciju par datu plūsmu un atrašanās vietas datus valsts drošības aizsardzības nolūkā situācijās, kad attiecīgā dalībvalsts sastopas ar nopietniem draudiem valsts drošībai, kuri izrādās patiesi un faktiski vai paredzami, ja lēmumu par šo rīkojumu var pakļaut efektīvai pārbaudei tiesā vai arī neatkarīgā administratīvā iestādē – kuras nolēmumam ir saistoša iedarbība –, lai pārbaudītu šādas situācijas esamību, kā arī paredzēto nosacījumu un garantiju ievērošanu, un minēto rīkojumu var izdot vienīgi uz laikposmu, kura ilgums aprobežojas ar absolūti nepieciešamo, taču kuru var pagarināt, ja šāds apdraudējums joprojām pastāv;**

– **valsts drošības aizsardzības, smagas noziedzības apkarošanas un nopietna sabiedrības drošības apdraudējuma novēršanas nolūkos paredz informācijas par datu plūsmu un atrašanās vietas datu mērķorientētu glabāšanu – kura, pamatojoties uz objektīviem un nediskriminējošiem elementiem, tiek ierobežota atkarībā no attiecīgo personu kategorijām vai pēc ģeogrāfiska kritērija – uz laikposmu, kura ilgums aprobežojas ar absolūti nepieciešamo, taču kuru var pagarināt;**

– **valsts drošības aizsardzības, smagas noziedzības apkarošanas un nopietna sabiedrības drošības apdraudējuma novēršanas nolūkos paredz savienojuma avotam piešķirto IP adrešu visaptverošu un nediferencētu glabāšanu uz laikposmu, kura ilgums aprobežojas ar absolūti nepieciešamo;**

– **valsts drošības aizsardzības, noziedzības apkarošanas un sabiedrības drošības aizsardzības nolūkos paredz elektronisko komunikāciju līdzekļu lietotāju personas identitātes datu visaptverošu un nediferencētu glabāšanu; un**

– **smagas noziedzības apkarošanas un *a fortiori* valsts drošības aizsardzības nolūkos paredz ar kompetentās iestādes lēmumu, kas ir pakļauts efektīvai pārbaudei tiesā, noformēta rīkojuma izdošanu elektronisko komunikāciju pakalpojumu sniedzējiem uz noteiktu laiku veikt šo pakalpojumu sniedzēju rīcībā esošās informācijas par datu plūsmu un atrašanās vietas datu operatīvo saglabāšanu,**

ja ar šiem pasākumiem, paredzot skaidrus un konkrētus noteikumus, tiek nodrošināts, ka attiecīgo datu glabāšana notiek atbilstoši tai paredzētajiem materiāltiesiskajiem un procesuālajiem nosacījumiem un ka datu subjektiem ir efektīvas garantijas pret ļaunprātīgas izmantošanas risku.

[Paraksti]