



Judikatūras krājums

ĢENERĀLADVOKĀTA MANUELA KAMPOSA SANČESA-BORDONAS [MANUEL CAMPOS SÁNCHEZ-BORDONA] SECINĀJUMI,
sniegti 2020. gada 15. janvārī¹

Apvienotās lietas C-511/18 un C-512/18

***La Quadrature du Net u.c.
French Data Network,
Fédération des fournisseurs d'accès à Internet associatifs,
Igwant.net (C-511/18)***
pret
***Premier ministre,
Garde des Sceaux, ministre de la Justice,
Ministre de l'Intérieur,
Ministre des Armées***

(*Conseil d'État* (Valsts padome, Francija), kas rīkojas Augstākās administratīvās tiesas statusā, lūgums
sniegt prejudiciālu nolēmumu)

Lūgums sniegt prejudiciālu nolēmumu – Personas datu apstrāde un privātās dzīves aizsardzība
elektronisko komunikāciju nozarē – Valsts drošības aizsardzība un terorisma apkarošana –
Direktīva 2002/58/EK – Piemērošanas joma – 1. panta 3. punkts – 15. panta 3. punkts – LES 4. panta
2. punkts – Eiropas Savienības Pamattiesību harta – 6., 7., 8., 11., 47. pants un 52. panta 1. punkts –
Pieslēguma datu un datu, kas ļauj identificēt satura veidotājus, visaptveroša un nediferencēta
saglabāšana – Informācijas par datu plūsmu un atrašanās vietas datu vākšana – Piekļuve datiem

1. Jautājumā par personas datu saglabāšanu un piekļuvi tiem Tiesa pēdējos gados ir ieturējusi pastāvīgu
judikatūras kursu, kuru iezīmē šie ievēribas cienīgi nolēmumi:

- 2014. gada 8. aprīļa spriedums *Digital Rights Ireland u.c.*², kurā tā atzina Direktīvas 2006/24/EK³
spēkā neesamību, jo ar to bija atļauta nesamērīga ieviešana Eiropas Savienības Pamattiesību
hartas (turpmāk tekstā – “Harta”) 7. un 8. pantā nostiprinātajās tiesībās;
- 2016. gada 21. decembra spriedums *Tele2 Sverige* un *Watson u.c.*⁴, kurā tā interpretēja
Direktīvas 2002/58/EK⁵ 15. panta 1. punktu;
- 2018. gada 2. oktobra spriedums *Ministerio Fiscal*⁶, kurā tā apstiprināja Direktīvas 2002/58 šīs pašas
tiesību normas interpretāciju.

¹ Oriģinālvaloda – spāņu.

² Lietas C-293/12 un C-594/12, turpmāk tekstā – “spriedums *Digital Rights*”, EU:C:2014:238.

³ Eiropas Parlamenta un Padomes Direktīva (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.).

⁴ Lietas C-203/15 un C-698/15, turpmāk tekstā – “spriedums *Tele2 Sverige* un *Watson*”, EU:C:2016:970.

⁵ Eiropas Parlamenta un Padomes Direktīva (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.).

⁶ Lieta C-207/16, turpmāk tekstā – “spriedums *Ministerio Fiscal*”, EU:C:2018:788.

2. Šie spriedumi (it īpaši otrais no tiem) rada bažas dažu dalībvalstu iestādēm, jo, viņuprāt, tādējādi tām esot liegts kāds rīks, kuru tās uzskata par nepieciešamu, lai aizsargātu valsts drošību un apkarotu noziedzību un terorismu. Tāpēc dažas no šīm dalībvalstīm iestājas par šīs judikatūras atcelšanu vai niansēšanu.

3. Vairākas dalībvalstu tiesas šīs bažas ir paidušas četros lūgumos sniegt prejudiciālu nolēmumu⁷, par kuriem sniedzu secinājumus šajā pašā dienā.

4. Visās četrās lietās galvenokārt tiek aplūkota problēma saistībā ar Direktīvas 2002/58 piemērojamību ar valsts drošību un terorisma apkarošanu saistītām darbībām. Ja šī direktīva šajā jomā būtu piemērojama, tad pēc tam būtu jānoskaidro, cik tādā dalībvalstīs var ierobežot tajā aizsargātās tiesības uz privātumu. Visbeidzot, būtu jāanalizē, cik lielā mērā šajos dažādajos (Apvienotās Karalistes⁸, Beļģijas⁹ un Francijas¹⁰) šīs jomas tiesiskajos regulējumos ir ievērotas Savienības tiesības, kā tās ir interpretējusi Tiesa.

I. Atbilstošās tiesību normas

A. Savienības tiesības

1. Direktīva 2002/58

5. Saskaņā ar 1. pantu ("Darbības joma un mērķis"):

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

[..]

3. Šī direktīva neattiecas uz darbībām, uz kurām neattiecas Eiropas Kopienas dibināšanas līgums, tādām kā tās, kas iekļautas Līguma par Eiropas Savienību V un VI sadaļā, un jebkurā gadījumā uz darbībām, kas attiecas uz sabiedrības drošību, aizsardzību, valsts drošību (tostarp valsts ekonomisko labklājību, ja darbības attiecas uz valsts drošības jautājumiem) un uz valsts darbībām krimināltiesību jomā."

6. Direktīvas 3. pantā ("Attiecīgie pakalpojumi") ir norādīts:

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

⁷ Neskaitot šīs abas lietas (C-511/18 un C-512/18), tas ir darīts arī lietās C-623/17, *Privacy International*, un C-520/18, *Ordre des barreaux francophones et germanophone* u.c.

⁸ Lieta *Privacy International*, C-623/17.

⁹ Lieta *Ordre des barreaux francophones et germanophone* u.c., C-520/18.

¹⁰ Lietas *La Quadrature du Net* u.c., C-511/18 un C-512/18.

7. Direktīvas 5. panta (“Komunikāciju konfidencialitāte”) 1. punktā ir noteikts:

“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.”

8. Direktīvas 6. pantā (“Informācija par datu plūsmu”) ir paredzēts:

“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. pantu 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.”

9. Direktīvas 15. panta (“Direktīvas 95/46/EK ^[11] dažu noteikumu piemērošana”) 1. punktā ir norādīts:

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

2. Direktīva 2000/31/EK¹²

10. Direktīvas 14. pantā ir noteikts:

“1. Ja tiek piedāvāts informācijas sabiedrības pakalpojums, kas sastāv no pakalpojuma saņēmēja piedāvātās informācijas glabāšanas, dalībvalstis nodrošina, ka pakalpojuma sniedzējs nav atbildīgs par informāciju, kas glabāta pēc pakalpojuma saņēmēja pieprasījuma, ar noteikumu, ka:

[..]

3. Šis pants neietekmē tiesas vai administratīvās iestādes tiesības saskaņā ar dalībvalstu juridisko sistēmu pieprasīt pakalpojuma sniedzējam izbeigt vai novērst likuma pārkāpumu, kā arī neietekmē dalībvalstu tiesības izveidot procedūras, kas regulē informācijas izņemšanu vai pieejas liegšanu tai.”

11 Eiropas Parlamenta un Padomes Direktīva (1995. gada 24. oktobris) par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV 1995, L 281, 31. lpp.).

12 Eiropas Parlamenta un Padomes Direktīva (2000. gada 8. jūnijs) par dažiem informācijas sabiedrības pakalpojumu tiesiskiem aspektiem, jo īpaši elektronisko tirdzniecību, iekšējā tirgū (Direktīva par elektronisko tirdzniecību) (OV 2000, L 178, 1. lpp.).

11. Saskaņā ar 15. pantu:

“1. Dalībvalstis neuzliek vispārējas saistības pakalpojuma sniedzējiem, piedāvājot 12., 13. un 14. pantā minētos pakalpojumus, pārraudzīt informāciju, ko tie pārraida vai uzglabā, kā arī neuzliek pienākumu aktīvi meklēt faktus un apstākļus, kas norāda uz nelegālu darbību.

2. Dalībvalstis var paredzēt pienākumu informācijas sabiedrības pakalpojumu sniedzējiem nekavējoties informēt kompetentās valsts iestādes par iespējamām veiktajām nelegālajām darbībām vai informāciju, ko sniedz pakalpojumu sniedzēju pakalpojumu saņēmēji, vai pienākumu kompetentajām iestādēm pēc to pieprasījuma darīt zināmu informāciju, kas ļauj identificēt tos pakalpojumu saņēmējus, ar kuriem pakalpojumu sniedzējiem ir glabāšanas līgumi.”

3. Regula (ES) 2016/679¹³

12. Saskaņā ar 2. pantu (“Materiālā darbības joma”):

“1. Šo regulu piemēro personas datu apstrādei, kas pilnībā vai daļēji veikta ar automatizētiem līdzekļiem, un tādu personas datu apstrādei, kuri veido daļu no kartotēkas vai ir paredzēti, lai veidotu daļu no kartotēkas, ja apstrādi neveic ar automatizētiem līdzekļiem.

2. Šo regulu nepiemēro personas datu apstrādei:

- a) tādas darbības gaitā, kas neietilpst Savienības tiesību aktu darbības jomā;
- b) ko īsteno dalībvalstis, veicot darbības, kas ir LES V sadaļas 2. nodaļas darbības jomā;
- c) ko veic fiziska persona tikai personiska vai mājsaimnieciska pasākuma gaitā;
- d) ko veic kompetentas iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu kriminālsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu.

[..]”

13. Atbilstoši 23. panta 1. punktam (“Ierobežojumi”):

“Saskaņā ar Savienības vai dalībvalsts tiesību aktiem, kas piemērojami datu pārzinim vai apstrādātājam, ar leģislatīvu pasākumu var ierobežot to pienākumu un tiesību darbības jomu, kas paredzēti 12.–22. pantā un 34. pantā, kā arī 5. pantā, ciktāl tā noteikumi atbilst 12.–22. pantā paredzētajām tiesībām un pienākumiem, – ja ar šādu ierobežojumu tiek ievērota pamattiesību un pamatbrīvību būtība un tas demokrātiskā sabiedrībā ir nepieciešams un samērīgs, lai garantētu:

- a) valsts drošību;
- b) aizsardzību;
- c) sabiedrisko drošību;

¹³ Eiropas Parlamenta un Padomes Regula (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.).

- d) noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu vai saukšanu pie atbildības par tiem vai kriminālsodu izpildi, tostarp aizsardzību pret sabiedriskās drošības apdraudējumiem un to novēršanu;
- e) citus svarīgus Savienības vai dalībvalsts vispārējo sabiedrības interešu mērķus, jo īpaši Savienībai vai dalībvalstij svarīgas ekonomiskās vai finanšu intereses, tostarp monetāros, budžeta un nodokļu jautājumus, sabiedrības veselību un sociālo nodrošinājumu;
- f) tiesu neatkarības un tiesvedības aizsardzību;
- g) reglamentētu profesiju ētikas kodeksu pārkāpumu novēršanu, izmeklēšanu, atklāšanu un saukšanu pie atbildības par tiem;
- h) uzraudzības, pārbaudes vai regulatīvo funkciju, kas – pat, ja tikai epizodiski – ir saistīta ar oficiālu pilnvaru īstenošanu a) līdz e) un g) apakšpunktā minētajos gadījumos;
- i) datu subjekta aizsardzību vai citu personu tiesību un brīvību aizsardzību;
- j) civilprasību izpildi.”

14. Regulas 95. pantā (“Saistība ar Direktīvu 2002/58/EK”) ir noteikts:

“Šī regula neuzliek papildu pienākumus fiziskām vai juridiskām personām attiecībā uz apstrādi saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu publiskos komunikāciju tīklos Savienībā jautājumos, saistībā ar kuriem tām ir piemērojami Direktīvas 2002/58/EK īpašie noteikumi ar to pašu mērķi.”

B. Valsts tiesības

1. *Code de la sécurité intérieure (Iekšējās drošības kodekss)*

15. Saskaņā ar L. 851-1. pantu:

“Šīs daļas II sadaļas 1. nodaļā paredzētajos apstākļos no elektronisko komunikāciju operatoriem un no personām, kas ir minētas *code des postes et des communications électroniques* [(Pasta un elektronisko komunikāciju kodekss)] L. 34-1. pantā, kā arī personām, kas ir minētas *Loi n.º 2004-575 [...] pour la confiance dans l'économie numérique* [(...) Likums Nr. 2004-575 par uzticēšanās veicināšanu digitālajā ekonomikā)] 6. panta I punkta 1. un 2. apakšpunktā, var vākt informāciju vai dokumentus, kas tiek apstrādāti vai saglabāti to tīklos vai elektronisko komunikāciju pakalpojumos, tai skaitā tehniskus datus saistībā ar abonenta vai pieslēguma elektronisko komunikāciju pakalpojumiem numuru noteikšanu, konkrētas personas visu abonenta vai pieslēguma numuru uzskaiti, izmantoto galaiekārtu atrašanās vietas datus, kā arī informāciju par abonenta komunikācijām, kas ietver izejošo un ienākošo zvanu numurus, komunikāciju ilgumu un datumu [..].”

16. L. 851-2. un L. 851-4. pantā ir reglamentēts, kā iestādes dažādiem mērķiem un dažādā kārtībā reāllaikā var piekļūt šādi saglabātiem pieslēguma datiem.

17. Ar L.851-2. pantu ir atļauts savākt L. 851-1. pantā minēto informāciju vai dokumentus no šīm pašām personām tikai un vienīgi terorisma novēršanas vajadzībām. Šī informācijas vai dokumentu savākšana attiecībā uz tikai vienu vai vairākām personām, kas iepriekš identificētas kā personas, kuras tiek turētas aizdomās par saikni ar terorisma draudiem, ir veicama reāllaikā. Tas pats ir sakāms arī par šā paša kodeksa L. 851-4. pantu, ar ko operatoriem reāllaikā ir ļauts pārsūtīt tikai tehniskus datus par

galaiekārtu atrašanās vietu¹⁴.

18. Ar L. 851-3. pantu ir atļauts likt elektronisko komunikāciju operatoriem un tehnisko pakalpojumu sniedzējiem “savos tīklos veikt automātiskas apstrādes, kuru mērķis ir atbilstoši atļaujā norādītajiem parametriem atklāt pieslēgumus, kas var liecināt par terorisma draudiem”¹⁵.

19. L. 851-5. pantā ir precizēts, ka noteiktos apstākļos “var atļaut izmantot tehnisku aprīkojumu, kas ļauj reāllaikā noteikt personas, transportlīdzekļa vai priekšmeta atrašanās vietu”.

20. L. 851-6. panta I punktā ir noteikts, ka ar zināmiem nosacījumiem ir atļauts “ar *code pénal* [(Kriminālkodekss)] 226-3. panta 1. punktā minētā tehniskā aprīkojuma vai ierīces palīdzību tieši savākt [...] tehniskus pieslēguma datus, kas ļauj noteikt galaiekārtu vai tās lietotāja abonenta numuru, kā arī izmantoto galaiekārtu atrašanās vietas datus”.

2. Pasta un elektronisko komunikāciju kodekss

21. Saskaņā ar L. 34-1. pantu, tā redakcijā, kas ir piemērojama faktiem:

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

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

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

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

III. Lai veiktu noziedzīgu nodarījumu vai *code de la propriété intellectuelle* [(Intelektuālā īpašuma kodekss)] L. 336-3. pantā noteiktā pienākuma neizpildes gadījumu izmeklēšanu, atklāšanu un kriminālvajāšanu par tiem vai lai novērstu Kriminālkodeksa 323-1. līdz 323-3-1. pantā minētos sodāmos uzbrukumus datu automātiskās apstrādes sistēmām, konkrētu datu kategoriju dzēšanas vai anonimizēšanas operācijas var atlikt uz laiku, kas nepārsniedz vienu gadu, ar vienīgo mērķi vajadzības gadījumā nodrošināt tos tiesu iestādei vai augstajai iestādei, kas minēta Intelektuālā īpašuma kodeksa L. 331-12. pantā, vai nacionālajai informācijas sistēmu drošības iestādei, kas minēta *code de la défense* [(Aizsardzības kodekss)] L. 2321-1. pantā. *Conseil d'État* [(Valsts padome)] izspriestā dekrētā, kas ir pieņemts pēc *Commission nationale de l'informatique et des libertés* [(Nacionālā informātikas un brīvību komisija)] atzinuma, VI punktā paredzētajās robežās tiek noteiktas šīs datu kategorijas un to saglabāšanas ilgums atkarībā no operatoru darbības un komunikāciju rakstura, kā arī vajadzības gadījumā kārtība, kādā ir kompensējamas identificējamās un konkrētās papildizmaksas, kas rodas saistībā ar pakalpojumiem, kurus operatori tālab sniedz pēc valsts pieprasījuma.

[..]

¹⁴ Iesniedzējtiesa norāda, ka šīs metodes attiecīgajiem pakalpojumu sniedzējiem neuzliek papildu saglabāšanas pienākumu salīdzinājumā ar to, kas ir nepieciešams, lai izrakstītu rēķinus par saviem pakalpojumiem un veiktu šo pakalpojumu tirdzniecību, kā arī sniegtu pakalpojumus ar pievienoto vērtību.

¹⁵ Pēc iesniedzējtiesas domām, šī metode, kas neietver visaptverošu un nediferencētu saglabāšanu, ir vērsta tikai uz to, lai noteiktā laikposmā no visiem šo personu apstrādātajiem datiem tiktu atlasīti tie dati, kuriem varētu būt saikne ar šādu smagu noziegumu.

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

Tie nekādā gadījumā un nekādā veidā neattiecas uz saziņas saturu vai šo komunikāciju laikā izmantoto informāciju.

Datu saglabāšanu un apstrādi veic saskaņā ar noteikumiem, kas paredzēti 1978. gada 6. janvāra Likumā Nr. 78-17 par informātiku, datnēm un brīvībām.

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

22. Saskaņā ar R. 10-13. panta I punktu operatori noziedzīgu nodarījumu izmeklēšanas, atklāšanas un kriminālvajāšanas nolūkos saglabā šādus datus:

- “a) informācija, kas ļauj identificēt lietotāju;
- b) informācija par izmantotajām komunikāciju galaiekārtām;
- c) tehniskie parametri, kā arī katras komunikācijas datums, laiks un ilgums;
- d) dati par pieprasītajiem vai izmantotajiem papildu pakalpojumiem un šo pakalpojumu sniedzējiem;
- e) dati, kas ļauj identificēt komunikācijas adresātu vai adresātus.”

23. Saskaņā ar šīs tiesību normas II punktu operatoram saistībā ar telefonijas darbībām arī ir jāsaglabā dati, kas palīdz noteikt komunikācijas izcelsmi un atrašanās vietu.

24. Saskaņā ar šā panta III punktu minētos datus saglabā vienu gadu no to reģistrācijas dienas.

3. *Loi n.º 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique* (2004. gada 21. jūnijs Likums Nr. 2004-575 par uzticēšanās veicināšanu digitālajā ekonomikā)

25. Likuma Nr. 2004-575 6. panta II punkta pirmajā daļā ir noteikts, ka personām, kas nodarbojas ar piekļuves komunikāciju pakalpojumiem tiešsaistē piedāvāšanu sabiedrībai, un fiziskām un juridiskām personām, kuras – pat bez maksas –, lai darītu tos pieejamus sabiedrībai, izmantojot publiskos komunikāciju pakalpojumus, nodrošina jebkāda veida signālu, teksta, attēlu, skaņu un ziņojumu, ko ir snieguši šo pakalpojumu adresāti, glabāšanu, “ir jātur un jāsaglabā dati, kas ļauj identificēt jebkuru personu, kura ir piedalījusies to sniegto pakalpojumu satura vai tā daļas radīšanā”.

26. Šīs pašas tiesību normas II punkta trešajā daļā ir noteikts, ka tiesu iestāde var pieprasīt šīm personām paziņot pirmajā daļā minētos datus.

27. Saskaņā ar II punkta pēdējo daļu *Conseil d'État* (Valsts padome) ar dekrētu “nosaka pirmajā daļā minēto datu loku un to saglabāšanas ilgumu un kārtību”¹⁶.

II. Fakti un prejudiciālie jautājumi

A. Lieta C-511/18

28. *La Quadrature du Net, French Data Network, Igwan.net* un *Fédération des fournisseurs d'accès à Internet associatifs* (turpmāk tekstā – “prasītāji”) vērsās *Conseil d'État* (Valsts padome), lūdzot atcelt dažus Iekšējās drošības kodeksa noteikumu istenošanas dekrētus¹⁷.

29. Prasītāji būtībā apgalvoja, ka gan apstrīdētie dekrēti, gan šie Iekšējās drošības kodeksa noteikumi neesot saderīgi ar tiesībām uz privātās dzīves neaizskaramību, personas datu aizsardzību un efektīvu tiesību aizsardzību tiesā, kas ir garantētas attiecīgi Hartas 7., 8. un 47. pantā.

30. Šajos apstākļos *Conseil d'État* (Valsts padome) uzdod Tiesai šādus prejudiciālus jautājumus:

- “1) Vai visaptverošas un nediferencētās saglabāšanas pienākums, kas pakalpojumu sniedzējiem ir uzlikts, pamatojoties uz [Direktīvas 2002/58] 15. panta 1. punkta atļaujošajām normām, kontekstā, kurā pastāv būtiski un pastāvīgi valsts drošības apdraudējumi un it īpaši terorisma risks, ir uzskatāms par iejaukšanos, ko attaisno [Hartas] 6. pantā garantētās tiesības uz drošību un valsts drošības prasības, par kurām atbilstoši [LES] 4. pantam ir atbildīgas vienīgi dalībvalstis?
- 2) Vai [Direktīva 2002/58], to lasot [Hartas] gaismā, ir jāinterpretē tādējādi, ka tajā ir atļauti tādi likumdošanas pasākumi kā informācijas par datu plūsmu un noteiktu personu atrašanās vietas datu vākšana reāllaikā, kuri, lai gan tie ietekmē elektronisko komunikāciju pakalpojumu sniedzēju tiesības un pienākumus, tiem tomēr neuzliek konkrētu pienākumu saglabāt viņu datus?
- 3) Vai [Direktīva 2002/58], to lasot [Hartas] gaismā, ir jāinterpretē tādējādi, ka tajā visos gadījumos pieslēguma datu vākšanas likumība ir pakļauta prasībai par attiecīgo personu informēšanu, kad šāda informācija vairs nevar apdraudēt kompetento iestāžu veiktās izmeklēšanas, vai arī šādas procedūras var tikt uzskatītas par likumīgām, ņemot vērā visas pārējās pastāvošās procesuālās garantijas, ciktāl tās nodrošina, ka tiesības uz tiesību aizsardzību ir efektīvas?”

16 Definīcija ir sniegta *décret n.° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne* (2011. gada 25. februāra Dekrēts Nr. 2011-219 par to datu saglabāšanu, ar kuriem iespējams identificēt personas, kas ir piedalījušās tiešsaistes satura veidošanā). Var minēt šā dekrēta: a) 1. panta 1. punktu, saskaņā ar kuru tiem, kas piedāvā piekļuvi komunikāciju pakalpojumiem tiešsaistē, ir jāsaglabā šādi dati: pieslēguma identifikators, abonentam piešķirtais identifikators, pieslēgumam izmantotās gala iekārtas identifikators, pieslēguma datums, pieslēguma sākuma un beigu datums un laiks un abonenta līnijas parametri; b) 1. panta 2. punktu, saskaņā ar kuru tiem, kas, lai piedāvātu sabiedrībai komunikāciju pakalpojumus tiešsaistē – tostarp pa velti –, saglabā jebkāda veida signālus, tekstus, attēlus, skaņas vai ziņojumus, kurus nodrošina komunikāciju pakalpojumu lietotāji, ir jāsaglabā attiecībā uz katru darbību šādi dati: pieslēguma identifikators, komunikācijas avotā, darbības saturam piešķirtais identifikators, protokolu veidi, kas izmantoti, lai pieslēgtos pakalpojumam un pārsūtīšanu saturu, darbības veids, datums un laiks, darbības veicēja izmantotais identifikators, un visbeidzot c) 1. panta 3. punktu, kurā ir noteikts, ka abos iepriekšējos punktos minētajām personām ir jāsaglabā šāda informācija, ko ir sniedzis lietotājs, noslēdzot līgumu vai izveidojot kontu: pieslēguma identifikators, izveidojot kontu; vārds, uzvārds vai uzņēmuma nosaukums; piesaistītās pasta adreses, izmantotie pseidonīmi, elektroniskā pasta vai konta adreses, tālruņa numuri, atjaunotā parole un dati, kas ļauj to pārbaudīt vai mainīt.

17 Apstrīdēti tiek šie dekrēti: a) *décret n.° 2015-1885 du 28 septembre 2015 portant désignation des services spécialisés de renseignement* (2015. gada 28. septembra Dekrēts Nr. 2015-1185 par specializēto izlūkdienestu noteikšanu); b) *décret n.° 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en oeuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'État* (2015. gada 1. oktobra Dekrēts Nr. 2015-1211 par prāvām saistībā ar tādu izlūkdatu vākšanas metožu izmantošanu, kurām ir nepieciešama atļauja, un valsts drošības jautājumiem saistītajām datnēm); c) *décret n.° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure* (2015. gada 11. decembra Dekrēts Nr. 2015-1639 par tādu dienestu noteikšanu, kuri nav specializētie izlūkdienesti, bet kuriem ir tiesības izmantot Iekšējās drošības kodeksa VIII daļas V sadaļā minētās metodes), un d) *décret n.° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement* (2016. gada 29. janvāra Dekrēts Nr. 2016-67 par izlūkdatu vākšanas metodēm).

B. Lieta C-512/18

31. Arī prasītāji lietā C-511/18, izņemot *Igwan.net*, lūdza *Conseil d'État* (Valsts padome) atcelt (klusuciešot pieņemto) lēmumu, ar ko tika noraidīts viņu pieteikums atcelt *code des postes et des communications électroniques* (Pasta un elektronisko komunikāciju kodekss) R. 10-13. pantu un 2011. gada 25. februāra Dekrētu Nr. 2011-219.

32. Pēc šo prasītāju domām, ar apstrīdētajām tiesību normām ir uzlikts pienākums saglabāt informāciju par datu plūsmu, atrašanās vietas un pieslēguma datus, ar kuru šā lēmuma vispārīguma dēļ ir nesamērīgi aizskartas Hartas 7., 8. un 11. pantā aizsargātās tiesības uz privātās un ģimenes dzīves neaizskaramību, personas datu aizsardzību un vārda brīvību, kā arī pārkāpts Direktīvas 2002/58 15. panta 1. punkts.

33. Šajā tiesvedībā *Conseil d'État* (Valsts padome) uzdod šādus prejudiciālos jautājumus:

- “1) Vai visaptverošas un nediferencētās saglabāšanas pienākums, kas pakalpojumu sniedzējiem ir uzlikts, pamatojoties uz [Direktīvas 2002/58] 15. panta 1. punkta atļaujošajām normām, it īpaši ņemot vērā garantijas un kontroles, kam šo datu vākšana un izmantošana ir pēc tam pakārtotas, ir uzskatāms par iejaukšanos, ko attaisno [Hartas] 6. pantā garantētās tiesības uz drošību un valsts drošības prasības, par kurām atbilstoši [LES] 4. pantam ir atbildīgas vienīgi dalībvalstis?
- 2) Vai Direktīvas 2000/31 noteikumi, tos lasot [Hartas] 6., 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, ir jāinterpretē tādējādi, ka tajos valstij ir ļauts paredzēt valsts tiesisko regulējumu, ar ko personām, kuru darbība sastāv no komunikāciju pakalpojumu piedāvāšanas sabiedrībai tiešsaistē, un fiziskām vai juridiskām personām, kuras – pat bez maksas –, lai darītu tos pieejamus sabiedrībai, izmantojot publiskos komunikāciju pakalpojumus, nodrošina jebkāda veida signālu, teksta, attēlu, skaņu vai ziņojumu glabāšanu, ir likts saglabāt datus, kas var ļaut identificēt jebkādu personu, kura ir piedalījusies tās sniegto pakalpojumu saturā vai tā daļas radīšanā, lai tiesu iestāde vajadzības gadījumā no tām varētu pieprasīt šo datu paziņošanu nolūkā nodrošināt, ka tiek ievēroti noteikumi par civiltiesisko atbildību vai kriminālatbildību?”

III. Tiesvedība Tiesā un lietas dalībnieku apsvērumi

34. Lūgumi sniegt prejudiciālu nolēmumu Tiesā tika reģistrēti 2018. gada 3. augustā.

35. Rakstveida apsvērumus iesniedza *La Quadrature du Net*, *Fédération des fournisseurs d'accès à Internet associatifs*, *French Data Network*, Vācijas, Beļģijas, Apvienotās Karalistes, Čehijas, Kipras, Dānijas, Spānijas, Igaunijas, Francijas, Ungārijas, Īrijas, Polijas un Zviedrijas valdības, kā arī Komisija.

36. 2019. gada 9. septembrī notika tiesas sēde, kas tika rīkota kopā ar tiesas sēdēm lietās C-623/17, *Privacy International*, un C-520/18, *Ordre des barreaux francophones et germanophone u.c.*, un tajā piedalījās visu četru prejudiciālā nolēmuma tiesvedību dalībnieki, iepriekš minēto valstu, Nīderlandes un Norvēģijas valdības, kā arī Komisija un Eiropas Datu aizsardzības uzraudzītājs.

IV. Vērtējums

37. *Conseil d'État* (Valsts padome) vaicāto var apkopot trīs jautājumos:

- pirmkārt, vai ar Savienības tiesībām ir saderīgs valsts tiesiskais regulējums, ar ko elektronisko komunikāciju pakalpojumu sniedzējiem ir noteikts pienākums visaptveroši un nediferencēti saglabāt pieslēguma datus (pirmais jautājums lietā C-511/18 un lietā C-512/18), it īpaši datus, kuri ļauj identificēt šo pakalpojumu sniedzēju piedāvātā satura veidotājus (otrais jautājums lietā C-512/18);
- otrkārt, vai nosacījums pieslēguma datu vākšanas procedūru likumībai katrā ziņā ir prasība informēt attiecīgās personas, ja vien netiek apdraudēta izmeklēšana (trešais jautājums lietā C-511/18);
- treškārt, vai un ar kādiem nosacījumiem informācijas par datu plūsmu un atrašanās vietas datu vākšana reāllaikā, neparedzot pienākumu tos saglabāt, ir saderīga ar Direktīvu 2002/58 (otrais jautājums lietā C-511/18).

38. Īsumā sakot, ir jānoskaidro, vai ar Savienības tiesībām ir saderīgs valsts tiesiskais regulējums, ar ko elektronisko komunikāciju pakalpojumu sniedzējiem ir noteikti divējādi pienākumi: a) pirmkārt, *vākt*, bet ne saglabāt konkrētus datus; b) otrkārt, *saglabāt* pieslēguma datus un datus, kas ļauj identificēt šo pakalpojumu sniedzēju sniegto pakalpojumu satura veidotājus.

39. Vispirms ir jānoskaidro, vai tieši izveidojušās situācijas dēļ¹⁸, kurā tika pieņemts šis valsts tiesiskais regulējums (proti, apstākļos, kad iespējami tiek apdraudēta valsts drošība), ir piemērojama Direktīva 2002/58.

A. Par Direktīvas 2002/58 piemērojamību

40. Iesniedzējtiesa vadās no pieņēmuma, ka izskatāmajā lietā aplūkotais tiesiskais regulējums ietilpst Direktīvas 2002/58 piemērošanas jomā. Pēc tās domām, tas izriet no spriedumā *Tele2 Sverige* un *Watson* izstrādātās judikatūras, kas apstiprināta spriedumā *Ministerio Fiscal*.

41. Turpretim dažas no valdībām, kas ir iestājušās lietā, apgalvo, ka strīdīgais tiesiskais regulējums neietilpst minētajā piemērošanas jomā. Lai pamatotu šo nostāju, tās tostarp atsaucas uz 2006. gada 30. maija spriedumu Parlaments/Padome un Komisija¹⁹.

42. Piekritu *Conseil d'État* (Valsts padome), ka spriedumā *Tele2 Sverige* un *Watson* ir sniegta atbilde uz šajā debašu daļā aplūkoto jautājumu, apstiprinot, ka principā Direktīva 2002/58 ir piemērojama gadījumā, ja elektronisko pakalpojumu sniedzējiem tiesību aktos ir noteikts pienākums saglabāt savu abonentu datus, lai nodrošinātu valsts iestādēm piekļuvi tiem. Šo apgalvojumu nemaina arī tas, ka pakalpojumu sniedzējiem pienākumi ir noteikti valsts drošības apsvērumu dēļ.

43. Uzreiz jau tagad jānorāda, ka, ja spriedums *Tele2 Sverige* un *Watson* kādā ziņā izrādītos esam pretrunā agrāk pasludinātajiem spriedumiem, par prevalējošu būtu atzīstams šis spriedums, jo tas ir pasludināts vēlāk un apstiprināts ar spriedumu *Ministerio Fiscal*. Tomēr uzskatu, ka šādas pretrunas nav, un turpinājumā mēģināšu to izskaidrot.

¹⁸ "Kontekstā, kurā pastāv būtiski un pastāvīgi valsts drošības apdraudējumi un it īpaši terorisma risks", kā norādīts pirmajā jautājumā lietā C-511/18.

¹⁹ Lietas C-317/04 un C-318/04, turpmāk tekstā – "spriedums Parlaments/Padome un Komisija", EU:C:2006:346.

1. Spriedums Parlaments/Padome un Komisija

44. Lietas, kurās ir taisīts spriedums Parlaments/Padome un Komisija, attiecās uz:

- Nolīgumu starp Eiropas Kopienu un Amerikas Savienotajām Valstīm par PDR [pasažieru datu reģistrs] datu apstrādi un pārsūtīšanu, ko aviopārvadātāji veic Amerikas Savienoto Valstu iestādēm²⁰;
- pasažieru datu reģistros iekļauto personas datu, kas pārsūtīti minētajām iestādēm, aizsardzības atbilstīgumu²¹.

45. Tiesa nosprieda, ka šo datu pārsūtīšana ir apstrāde, kuras mērķis ir sabiedriskā drošība un valsts pasākumi krimināltiesību jomā. Saskaņā ar Direktīvas 95/46 3. panta 2. punkta pirmo ievilkumu abi apstrīdētie lēmumi neietilpst Direktīvas 95/46 piemērošanas jomā.

46. Aviosabiedrības sākotnēji bija savākušas datus saistībā ar savu darbību – aviobiļešu pārdošanu –, kas ietilpst Savienības tiesību piemērošanas jomā. Tomēr to apstrāde, kā paredzēts apstrīdētajā lēmumā, ir nevis tāda, “kas ir nepieciešama pakalpojumu sniegšanai, bet gan [tāda], kas nepieciešama, lai nodrošinātu sabiedrisko drošību, un represīvos nolūkos”²².

47. Tādējādi Tiesa izmantoja teleoloģisku pieeju, atsaucoties uz datu apstrādes mērķi: ja ar tās palīdzību būtu jāpanāk sabiedrības drošība, tā būtu jāuzskata par izslēgtu no Direktīvas 95/46 piemērošanas jomas. Tomēr šis mērķis nebija vienīgais izšķirošais kritērijs²³, tāpēc spriedumā tika uzsvērts, ka tā “ietilpst valsts varas noteiktajos ietvaros un attiecas uz sabiedrisko drošību”²⁴.

48. Tādējādi spriedums Parlaments/Padome un Komisija ļauj noskaidrot atšķirību starp Direktīvā 95/46 paredzēto izslēdzošu noteikumu un ierobežojošiem vai sašaurinošiem noteikumiem (kas ir analogiski Direktīvā 2002/58 paredzētajiem). Tomēr ir taisnība, ka gan vieni, gan otri attiecas uz līdzīgiem vispārējo interešu mērķiem, kas rada neskaidrības par to attiecīgo tvērumu, kā savulaik norādīja ģenerālvokāts Ī. Bots [*Y. Bot*]²⁵.

20 Padomes Lēmums 2004/496/EK (2004. gada 17. maijs) par nolīguma noslēgšanu starp Eiropas Kopienu un Amerikas Savienotajām Valstīm attiecībā uz personas datu apstrādi un pārsūtīšanu, ko aviopārvadātāji veic ASV Nacionālās drošības ministrijas Muitas un robezsardzes departamentam (OV 2004, L 183, 83. lpp., un labojumi – OV 2005, L 255, 168. lpp.) (lieta C-317/04).

21 Komisijas Lēmums 2004/535/EK (2004. gada 14. maijs) par pietiekamu aizsardzību *Passenger Name Record* iekļautajiem lidmašīnu pasažieru personas datiem, kas nosūtīti Amerikas Savienoto Valstu Muitas un robežapsardzes birojam (OV 2004, L 235, 11. lpp.) (lieta C-318/04).

22 Spriedums Parlaments/Padome un Komisija, 57. punkts. Sprieduma 58. punktā ir uzsvērts, ka apstāklis, ka “privātie uzņēmēji ir apkopojuši [...] datus komercdarbības nolūkā un organizē to pārsūtīšanu uz trešajām valstīm” nenožīmē, ka šī pārsūtīšana nav viens no Direktīvas 95/46 3. panta 2. punkta pirmajā ievilkumā minētajiem šīs direktīvas nepiemērošanas gadījumiem, jo “ši pārsūtīšana ietilpst valsts varas noteiktajos ietvaros un attiecas uz sabiedrisko drošību”.

23 Vēlāk to uzsvēra mūžībā aizgājušais ģenerālvokāts Ī. Bots secinājumos lietā Īrija/Parlaments un Padome (C-301/06, EU:C:2008:558). Viņš apgalvoja, ka spriedums Parlaments/Padome un Komisija “nenožīmē [...] ka ar personas datu apstrādes mērķa pārbaudi vien pietiek, lai šādu apstrādi iekļautu vai izslēgtu no datu aizsardzības sistēmas, kas tika noteikta ar Direktīvu 95/46, piemērošanas jomas. Ir jāpārbauda arī, kāda veida pasākumu ietvaros notiek datu apstrāde. Tikai gadījumā, kad ir veikta šāda apstrāde, lai īstenotu valsts vai valsts iestāžu pasākumus, kas neietilpst privātpersonu darbības lokā, tā ir izslēgta no Kopienas personu datu aizsardzības sistēmas, kas noteikta Direktīvā 95/46, piemērojot šīs direktīvas 3. panta 2. punkta pirmo ievilkumu” (122. punkts).

24 Spriedums Parlaments/Padome un Komisija, 58. punkts. Nolīguma galvenais mērķis bija pieprasīt aviosabiedrībām, kas sniedz pasažieru pārvadāšanas pakalpojumus starp Savienību un Amerikas Savienotajām Valstīm, piešķirt Amerikas Savienoto Valstu iestādēm elektronisku piekļuvi PDR pasažieru datu reģistra datiem aviosabiedrību automatiskajās rezervāciju un izlidošanas kontroles sistēmās. Tādējādi tika nodibināta zināma veida starptautiska sadarbība starp Savienību un Amerikas Savienotajām Valstīm, lai apkarotu terorismu un citus smagus noziegumus, mēģinot salāgot šo mērķi ar pasažieru personas datu aizsardzību. Šajos apstākļos šīm sabiedrībām uzliktais pienākums būtiski neatšķiras no tiesas datu apmaiņas starp valsts iestādēm.

25 Ģenerālvokāta Ī. Bota secinājumi lietā Īrija/Parlaments un Padome (C-301/06, EU:C:2008:558), 127. punkts.

49. Iespējams, ka šī neskaidriība ir pamatā to dalībvalstu nostājai, kuras uzskata, ka šajā kontekstā Direktīva 2002/58 nav piemērojama. To ieskatā, valsts drošības intereses tiek aizsargātas tikai ar izslēgšanu, kas ir paredzēta Direktīvas 2002/58 1. panta 3. punktā. Tomēr patiesībā ir tā, ka tām pašām interesēm kalpo arī minētās direktīvas 15. panta 1. punktā atļautie ierobežojumi, tostarp attiecībā uz valsts drošību. Šī nupat minētā tiesību norma būtu lieka, ja Direktīva 2002/58 nebūtu piemērojama ikreiz, kad tiek piesaukta valsts drošība.

2. Spriedums “Tele2 Sverige un Watson”

50. Spriedumā *Tele2 Sverige* un *Watson* bija jālemj par to, vai ar Savienības tiesībām bija saderīgas vairāku dalībvalstu sistēmas, kurās sabiedrībai pieejamu elektronisko komunikāciju pakalpojumu sniedzējiem tika uzlikts vispārējs pienākums saglabāt ar šīm komunikācijām saistītos datus. Tāpēc lietas apstākļi tajā bija būtībā identiski šajos lūgumos sniegt prejudiciālu nolēmumu izklāstītajiem.

51. Kad Tiesai atkārtoti tika vaicāts par Savienības tiesību – tagad jau Direktīvas 2002/58 – piemērojamību, tā vispirms norādīja, ka “Direktīvas 2002/58 piemērošanas joma ir jāizvērtē, it īpaši ņemot vērā tās vispārējo struktūru”²⁶.

52. No šā skatpunkta, Tiesa noteica, ka, “protams, Direktīvas 2002/58 15. panta 1. punktā paredzētie tiesību akti ir valsts vai valsts iestāžu atbilstošās darbības, kas nepieder pie fizisko personu darbības jomām [...]. Turklāt mērķi, kuri saskaņā ar šo tiesību normu ir jāsasniedz ar šādiem tiesību aktiem, konkrētaj[ā] gadījumā – valsts drošības [...] nodrošināšana [...], būtiski sakrīt ar mērķiem, kas sasniedzami ar šīs direktīvas 1. panta 3. punktā paredzētajām darbībām”²⁷.

53. Tādējādi to pasākumu mērķis, kurus saskaņā ar Direktīvas 2002/58 15. panta 1. punktu var pieņemt dalībvalstis, lai ierobežotu tiesības uz privātumu, (šajā ziņā) atbilst to pasākumu mērķim, kas pamato dažu valsts darbību izslēgšanu no direktīvas sistēmas saskaņā ar tās 1. panta 3. punktu.

54. Tomēr Tiesa uzskatīja, ka, “ņemot vērā Direktīvas 2002/58 vispārējo struktūru”, šis apstāklis neļauj “secināt, ka Direktīvas 2002/58 15. panta 1. punktā paredzētie tiesību akti ir izslēgti no šīs direktīvas piemērošanas jomas, pretējā gadījumā šī tiesību norma pavisam zaudētu lietderību. Proti, minētā tiesību norma obligāti nozīmē, ka tajā noteiktie valsts pasākumi [...] ietilpst šīs direktīvas piemērošanas jomā, jo šajā pēdējā minētajā direktīvā dalībvalstīm ir tieši atļauts šos tiesību aktus pieņemt vienīgi, ievērojot tajā paredzētos nosacījumus”²⁸.

55. Tā arī piebilda, ka ierobežojumi, kas paredzēti Direktīvas 2002/58 15. panta 1. punktā, “saskaņā ar šajā tiesību normā paredzētajiem mērķiem reglamentē elektronisko sakaru pakalpojumu sniedzēju darbību”. Tāpēc šis 15. panta 1. punkts, skatot to kopsakarā ar minētās direktīvas 3. pantu, “ir jāinterpretē tādējādi, ka šādi tiesību akti ietilpst šīs pašas direktīvas piemērošanas jomā”²⁹.

56. Līdz ar to Tiesa norādīja, ka Direktīvas 2002/58 piemērošanas jomā ietilpst gan tiesību akts, ar ko pakalpojuma sniedzējiem ir noteikts “pienākum[s] saglabāt informāciju par datu plūsmu un atrašanās vietas datus, jo šāda darbība noteikti nozīmē, ka šie pakalpojumu sniedzēji apstrādās personas datus”³⁰, gan tiesību akts, kas reglamentē valsts iestāžu piekļuvi šo pakalpojumu sniedzēju saglabātajiem datiem³¹.

26 Spriedums *Tele2 Sverige* un *Watson*, 67. punkts.

27 Turpat, 72. punkts.

28 Turpat, 73. punkts.

29 Turpat, 74. punkts.

30 Turpat, 75. punkts.

31 Turpat, 76. punkts.

57. Direktīvas 2002/58 interpretācija, kuru Tiesa ir sniegusi spriedumā *Tele2 Sverige* un *Watson*, tika apstiprināta spriedumā *Ministerio Fiscal*.

58. Vai var apgalvot, ka spriedums *Tele2 Sverige* un *Watson* nozīmē vairāk vai mazāk implicītu pavērsienu attiecībā uz judikatūru, kas ir izstrādāta spriedumā Parlaments/Padome un Komisija? Tā uzskata, piemēram, Īrijas valdība, pēc kuras domām, tikai šis pēdējais no minētajiem spriedumiem ir saderīgs ar Direktīvas 2002/58 juridisko pamatu un LES 4. panta 2. punktu³².

59. Savukārt Francijas valdība uzskata, ka pretrunu varētu novērst, ja ņem vērā to, ka spriedumā *Tele2 Sverige* un *Watson* izstrādātā judikatūra attiecas uz dalībvalstu darbību krimināltiesību jomā, savukārt spriedumā Parlaments/Padome un Komisija izstrādātajā judikatūrā ir runa par valsts drošību un aizsardzību. Tādējādi sprieduma *Tele2 Sverige* un *Watson* judikatūra neesot piemērojama pašlaik aplūkojamajā gadījumā, kurā būtu jāņem vērā spriedumā Parlaments/Padome un Komisija rastais risinājums³³.

60. Kā jau esmu norādījis, uzskatu, ka abus šos spriedumus var saskaņot veidā, kas atšķiras no Francijas valdības piedāvātā risinājuma. Šim risinājumam nepiekrītu, jo, manuprāt, spriedumā *Tele2 Sverige* un *Watson* paustie apsvērumi, kas skaidri attiecas uz terorisma apkarošanu³⁴, ir attiecināmi arī uz jebkuru citu valsts drošības apdraudējumu (terorismam esot tikai vienam no tiem).

3. Iespēja spriedumu Parlaments/Padome un Komisija interpretēt saskaņoti ar spriedumu “Tele2 Sverige un Watson”

61. Manuprāt, spriedumā *Tele2 Sverige* un *Watson* un spriedumā *Ministerio Fiscal* Tiesa ir ņēmusi vērā izslēdzošo un ierobežojošo noteikumu esības jēgu, kā arī sistēmisko saikni starp abu noteikumu veidu.

62. Ja lietā Parlaments/Padome un Komisija Tiesa apgalvoja, ka attiecīgā datu apstrāde neietilpst Direktīvas 95/46 piemērošanas jomā, tas, kā jau esmu atgādinājis, tā bija tāpēc, ka Eiropas Savienības sadarbības ar Amerikas Savienotajām Valstīm kontekstā, proti, tipiski starptautiskā ietvarā, darbības valstiskajam aspektam bija jāprevalē pār to, ka apstrādei varētu būt arī komerciāls vai privāts aspekts. Viens no toreiz iztīrītajiem jautājumiem bija par to, kāds tieši ir atbilstīgais apstrīdētā lēmuma juridiskais pamats.

63. Savukārt attiecībā uz spriedumā *Tele2 Sverige* un *Watson* un spriedumā *Ministerio Fiscal* aplūkotajiem valsts pasākumiem Tiesa priekšplānā izvirzīja datu apstrādes tvērumu valsts tiesībās, proti, tā kā apstrādes tiesisko ietvaru veidoja tikai valsts tiesību normas, tai nepiemita ārējais aspekts, kas bija raksturīgs apstrādei, kura tika aplūkota spriedumā Parlaments/Padome un Komisija.

64. Datu apstrādes starptautiskā aspekta un iekšējā (komerciālā un privātā) aspekta atšķirīgā nozīmīguma dēļ pirmajā gadījumā Savienības tiesību izslēdzošais noteikums tika atzīts par atbilstīgāko, lai aizsargātu vispārējās intereses, kas izpaudās kā valsts drošība. Turpretim otrajā gadījumā šīs intereses varēja efektīvi īstenot, piemērojot Direktīvas 2002/58 15. panta 1. punktā paredzēto ierobežojošo noteikumu.

65. Ir manāma vēl viena atšķirība, kas ir saistīta ar atšķirīgo normatīvo kontekstu: katrā no šiem spriedumiem tika interpretētas divas tiesību normas, kas, neraugoties uz to šķietamo līdzību, tomēr atšķiras.

32 Īrijas valdības rakstveida apsvērumu 15. un 16. punkts.

33 Francijas valdības rakstveida apsvērumu 34.–50. punkts.

34 Spriedums *Tele2 Sverige* un *Watson*, 103. un 119. punkts.

66. Tādējādi spriedumā Parlaments/Padome un Komisija tā lēma par Direktīvas 95/46 3. panta 2. punkta interpretāciju, savukārt spriedums *Tele2 Sverige* un *Watson* bija par Direktīvas 2002/58 1. panta 3. punktu. Rūpīgi iepazīstoties ar šiem pantiem, kļūst redzama atšķirība, kas ļauj pamatot Tiesas nolēmumu nozīmi vienā un otrā gadījumā.

67. Saskaņā ar Direktīvas 95/46 3. panta 2. punktu “ši direktīva neattiecas uz *personas datu apstrādi*: [...] tādu pasākumu gaitā, uz kuru neattiecas Kopienas tiesību akti [...] 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”³⁵.

68. Savukārt saskaņā ar Direktīvas 2002/58 1. panta 3. punktu minētā direktīva “*neattiecas uz darbībām*, uz kurām neattiecas Eiropas Kopienas dibināšanas līgums [...], 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”³⁶.

69. Ar Direktīvas 95/46 3. panta 2. punktu ir izslēgta *datu apstrāde*, kas – ciktāl tam ir nozīme šajā lietā – attiecas uz valsts drošību, savukārt ar Direktīvas 2002/58 1. panta 3. punktu ir izslēgtas *darbības*, kuru mērķis ir saglabāt – arī ciktāl tam ir nozīme šajā lietā – valsts drošību.

70. Atšķirība nav nebūtiska. No Direktīvas 95/46 piemērošanas jomas tika izslēgta darbība (“personas datu apstrāde”), kuru var veikt ikviens. Šīs darbības ietvaros it īpaši bija izslēgta apstrāde, kas veikta tostarp valsts drošības vajadzībām. Savukārt datu apstrādes *veicēja* statusam nebija nozīmes. Tāpēc izslēgto darbību noteikšanas nolūkā tika pieņemta teleoloģiska un uz mērķi vērsta pieeja, neveicot nošķiršanu atkarībā no šo darbību veicējiem.

71. Tādējādi var uzskatīt, ka lietā Parlaments/Padome un Komisija Tiesa galvenokārt ņēma vērā mērķi, kādam dati tiek apstrādāti. Netika piešķirta nozīme apstāklim, ka “privātie uzņēmēji ir apkopājuši [...] datus komercdarbības nolūkā un organizē to pārsūtīšanu uz trešajām valstīm”, jo būtiska nozīme bija tam, ka “ši pārsūtīšana ietilpst valsts varas noteiktajos ietvaros un attiecas uz sabiedrisko drošību”³⁷.

72. Turpretī “darbības, kas attiecas uz valsts drošību”, kuras nav iekļautas Direktīvas 2002/58 piemērošanas jomā, kas izvērtēts lietā *Tele2 Sverige* un *Watson*, nevar veikt jebkurš subjekts, bet vienīgi pati valsts. Turklāt tajās neietilpst valsts normatīvās vai regulatīvās funkcijas, bet gan tikai valsts iestāžu faktiskās darbības.

73. Proti, Direktīvas 2002/58 1. panta 3. punktā minētās *darbības* “visos gadījumos ir valstu vai valstu iestāžu darbības, kas neietilpst privātpersonu darbības lokā”³⁸. Tomēr šīs “darbības” nedrīkst būt normatīva rakstura. Ja tas tā būtu, visas tiesību normas, kuras dalībvalstis pieņemtu attiecībā uz personas datu apstrādi, neietilptu Direktīvas 2002/58 piemērošanas jomā, līdzko tiktu mēģināts tās attaisnot kā valsts drošības garantēšanai nepieciešamas.

74. Pirmkārt, tas nozīmētu, ka minētā direktīva būtiski zaudētu savu efektivitāti, jo pietiktu vien atsaukties uz tik nenoteiktu juridisku jēdzienu kā valsts drošība, lai pret dalībvalstīm nebūtu piemērojamas garantijas, ko Savienības likumdevējs iecerējis, lai aizsargātu pilsoņu personas datus. Šo aizsardzību nevar nodrošināt bez dalībvalstu līdzdarbības, un katram pilsonim tiek garantēta arī aizsardzība pret valsts iestādēm.

³⁵ Mans izcēlums.

³⁶ Mans izcēlums.

³⁷ Spriedums Parlaments/Padome un Komisija, 58. punkts.

³⁸ Spriedums *Ministerio Fiscal*, 32. punkts. Tāda pati nostāja ir pausta arī spriedumā *Tele2 Sverige* un *Watson*, 72. punkts.

75. Otrkārt, ja jēdzienu “valsts darbības” interpretētu tādējādi, ka tas ietver darbības, kuru rezultātā tiek pieņemtas tiesību normas, savu jēgu zaudētu Direktīvas 2002/58 15. pants, ar ko dalībvalstīm – tostarp valsts drošības aizsardzības apsvērumu dēļ – tieši ir piešķirtas pilnvaras pieņemt “tiesību aktus”, lai ierobežotu konkrētu šajā direktīvā paredzēto tiesību un pienākumu tvērumu³⁹.

76. Ka Tiesa norādīja lietā *Tele2 Sverige* un *Watson*, “Direktīvas 2002/58 piemērošanas joma ir jāizvērtē, it īpaši ņemot vērā tās vispārējo struktūru”⁴⁰. No šā skatupunkta, Direktīvas 2002/58 1. panta 3. punkta un 15. panta 1. punkta jēgpilna interpretācija, neatņemot tiem efektivitāti, ir šāda: pirmajā no abām tiesību normām ir paredzēta dalībvalstu *darbību* valsts drošības jomā (un līdzīgās jomās) materiāla izslēgšana, un ar otro tiesību normu dalībvalstis ir apveltītas ar tiesībām pieņemt *tiesību aktus* (proti, vispārpiemērojamas normas), kas valsts drošības nolūkā ietekmē dalībvalstu *imperium* pakļautu indivīdu darbības, ierobežojot Direktīvā 2002/58 garantētās tiesības.

4. Valsts drošības izslēgšana no Direktīvas 2002/58 piemērošanas jomas

77. Nacionālā drošība (jeb direktīvas 15. panta 1. punktā izmantotais sinonīms “valsts drošība”) Direktīvā 2002/58 ir ņemta vērā divējādi. Pirmkārt, tā ir iemesls, lai (no šīs direktīvas piemērošanas jomas) *izslēgtu* visas tās dalībvalstu darbības, kas konkrēti “attiecas uz” šo drošību. Otrkārt, tā ir iemesls, lai Direktīvā 2002/58 paredzētās tiesības un pienākumus likumiski *ierobežotu*, proti, attiecībā uz valsts varas darbības sfērā neietilpstošām privātām vai komerciālām darbībām⁴¹.

78. Uz kādām darbībām attiecas Direktīvas 2002/58 1. panta 3. punkts? Manuprāt, pati *Conseil d'État* (Valsts padome) sniedz labu piemēru, minēdama uz Iekšējās drošības kodeksa L. 851-5. un L. 851-6. pantu, atsaucoties uz “informācijas vākšanas metodēm, kuras valsts izmanto tieši, bet kuras nereglamentē elektronisko komunikāciju pakalpojumu sniedzēju darbību, uzliekot tiem īpašus pienākumus”⁴².

79. Uzskatu, ka šeit ir rodama atslēga Direktīvas 2002/58 1. panta 3. punkta izslēgšanas jomas tvēruma noskaidrošanai. Tās regulējumam nav pakļautas *darbības*, kuras valsts drošības saglabāšanas nolūkā veic pašas valsts iestādes, neprasot privātpersonu palīdzību un tādējādi neuzliekot tām pienākumus viņu uzņēmējdarbības pārvaldībā.

80. Tomēr valsts iestāžu darbību kopums, kas ir izslēgts no personas datu apstrādes vispārējā regulējuma, ir jāinterpretē šauri. Proti, jēdzienu *valsts drošība*, par kuru rūpēties saskaņā ar LES 4. panta 2. punktu ir tikai un vienīgi katras dalībvalsts ziņā, nevar attiecināt uz citām ar sabiedrības dzīvi vairāk vai mazāk saistītām jomām.

81. Tā kā šie prejudiciālie jautājumi attiecas nevis uz tikai un vienīgi valsts iestāžu iejaukšanos, bet gan uz privātpersonu (proti, personu, kas sniedz lietotājiem elektronisko komunikāciju pakalpojumus) iesaistīšanos, pie valsts drošības jēdziena tvēruma *stricto sensu* noteikšanas nav jāpakavējas ilgāk.

39 Proti, būtu grūti apgalvot, ka Direktīvas 2002/58 15. panta 1. punkts ļauj ierobežot tiesības un pienākumus, ko tas nosaka tādā jomā kā valsts drošība, kas saskaņā ar šīs direktīvas 1. panta 3. punktu principā neietilptu tās piemērošanas jomā. Direktīvas 2002/58 15. panta 1. punkts, kā Tiesa apgalvoja sprieduma *Tele2 Sverige* un *Watson* 73. punktā, “obligāti nozīmē, ka tajā noteiktie valsts pasākumi [...] ietilpst šīs direktīvas piemērošanas jomā, jo šajā pēdējā minētajā direktīvā dalībvalstīm ir tieši atļauts šos tiesību aktus pieņemt vienīgi, ievērojot tajā paredzētos nosacījumus”.

40 Spriedums *Tele2 Sverige* un *Watson*, 67. punkts.

41 Kā tostarp norādīja ģenerālvokāts H. Saugmandsgors Ēe [*H. Saugmandsgaard Oe*] secinājumu lietā *Ministerio Fiscal* (C-207/16, EU:C:2018:300) 47. punktā, “personas datus, kas tiek *tieši* apstrādāti valsts darbībā ar valsts varas raksturu [...] – krimināltiesību jomā [...], nedrīkst sajaukt ar datiem, kas tiek apstrādāti elektronisko sakaru pakalpojumu sniedzēja komerciāla rakstura darbību ietvaros, kurus kompetentās valsts iestādes izmanto *pēc tam*”.

42 Lūgums sniegt prejudiciālu nolēmumu lietā C-511/18, 18. un 21. punkts.

82. Tomēr uzskatu, ka vērtīgu norādi var sniegt kritējs, kas noteikts Pamatlēmumā 2006/960/TI⁴³, kura 2. panta a) punktā tiesībaizsardzības iestādes plašā nozīmē – kas ir “valsts policija, muita vai cita iestāde, kura ar valsts tiesību aktiem ir pilnvarota konstatēt, novērst un izmeklēt nodarījumus vai noziedzīgas darbības, kā arī īstenot varu un izmantot piespiedu līdzekļus saistībā ar tādām darbībām” – tiek nošķirtas no “aģentūrām vai vienībām, kas īpaši nodarbojas ar valsts drošības jautājumiem”⁴⁴.

83. Direktīvas 2002/58 11. apsvērumā ir teikts, ka “tāpat kā Direktīva 95/46[...], arī šī direktīva neattiecas uz pamattiesību un pamatbrīvību aizsardzības jautājumiem, kas saistīti ar darbībām, kuras neregulē [Savienības] tiesību akti”. Tādējādi Direktīva 2002/58 “nemainā esošo līdzsvaru starp fizisku personu tiesībām uz privāto dzīvi un iespēju dalībvalstīm pieņemt šīs direktīvas 15. panta 1. punktā minētos pasākumus, kas nepieciešami [...] valsts drošībai [...]”.

84. Proti, attiecībā uz dalībvalstu pilnvarām valsts drošības jautājumos gan Direktīvā 95/46, gan Direktīvā 2002/58 ir ievērota kontinuitāte. Neviena no abām neattiecas uz pamattiesību aizsardzību šajā īpašajā jomā, kurā dalībvalstu darbību “neregulē [Savienības] tiesību akti”.

85. Šajā apsvērumā minētais “līdzsvars” izriet no nepieciešamības ievērot dalībvalstu pilnvaras valsts drošības jomā, kad tā īsteno tās *tieši un ar saviem spēkiem*. Turpretim, ja pat to pašu valsts drošības apsvērumu dēļ ir nepieciešama privātpersonu palīdzība un tām tiek uzlikti kādi pienākumi, šā apstākļa dēļ nonākam Savienības tiesībās reglamentētā jomā (šo privātpersonu pienākums ievērot privātumu).

86. Gan ar Direktīvu 95/46, gan ar Direktīvu 2002/58 tiek mēģināts panākt šo līdzsvaru, atļaujot ierobežot privātpersonu tiesības, valstīm pieņemot tiesību aktus saskaņā attiecīgi ar pirmās minētās direktīvas 13. panta 1. punktu un otrās minētās direktīvas 15. panta 1. punktu. Šajā ziņā nav nekādas atšķirības starp abām direktīvām.

87. Savukārt Regulas 2016/679, kurā ir paredzēts (jauns) vispārējs regulējums personas datu aizsardzības jomā, 2. panta 2. punktā ir noteikts, ka to nepiemēro “personas datu apstrādei”, ko īsteno dalībvalstis “veicot darbības, kas ir LES V sadaļas 2. nodaļas darbības jomā”.

88. Direktīvā 95/46 personas datu apstrāde bija raksturota, tikai atsaucoties uz tās mērķi, neatkarīgi no tās veicēja, savukārt no Regulas 2016/679 izslēgtā apstrāde ir identificēta, definējot gan tās mērķi, gan veicējus: ir izslēgta apstrāde, ko dalībvalstis veic tādas *darbības* gaitā, kas neietilpst Savienības tiesību aktu darbības jomā (2. panta 2. punkta a) un b) apakšpunkts), un darbības, kuras veic iestādes, lai *apkarotu noziedzīgus nodarījumus un aizsargātu pret sabiedriskās drošības apdraudējumiem*⁴⁵.

89. Šo valsts iestāžu darbību noteikšanai obligāti ir jābūt ierobežojošai, pretējā gadījumā Savienības tiesiskais regulējums privātās dzīves aizsardzības jomā kļūtu neefektīvs. Regulas 2016/679 23. pantā – tāpat kā Direktīvas 2002/58 15. panta 1. punktā – ir minēts tajā noteikto tiesību un pienākumu ierobežojums *ar legislatīvu pasākumu*, ja tas ir nepieciešams, lai tostarp sasniegtu tādus mērķus kā valsts drošība, aizsardzība vai sabiedrības drošība. Arī šajā gadījumā, ja šo mērķu aizsardzība būtu pietiekama, lai paredzētu izslēgšanu no Regulas 2016/679 piemērošanas jomas, atsaukšanās uz valsts drošību kā ar šo regulu garantēto tiesību ierobežojuma pamatojumu, nosakot legislatīvus pasākumus, būtu lieka.

43 Padomes Pamatlēmums (2016. gada 18. decembris) par Eiropas Savienības dalībvalstu tiesībaizsardzības iestāžu informācijas un izlūkdatu apmaiņas vienkāršošanu (OV 2006, L 386, 89. lpp.).

44 Līdzīgi arī Padomes Pamatlēmuma 2008/977/TI (2008. gada 27. novembris) par tādu personas datu aizsardzību, ko apstrādā, policijas un tiesu iestādēm sadarbojoties krimināllietās (OV 2008, L 350, 60. lpp.), 1. panta 4. punktā bija paredzēts, ka tas “neskar būtiskas valsts drošības intereses un īpašas izlūkošanas darbības valsts drošības jomā”.

45 Proti, no Regulas 2016/679 ir izslēgta datu apstrāde, ko veic dalībvalstis, īstenojot *darbību*, kura neietilpst Savienības tiesību piemērošanas jomā, kā arī darbību, kuru veic iestādes sabiedrības drošības *aizsardzības nolūkos*.

90. Tāpat, kā tas ir Direktīvas 2002/58 gadījumā, nebūtu konsekvences, ja Regulas 2016/679 23. pantā (ar kuru, jāatgādina, valstīm ir atļauts ierobežot pilsoņu tiesības uz privātās dzīves neaizskaramību valsts drošības apsvērumu dēļ) paredzētie leģislatīvie pasākumi būtu tās piemērošanas jomā un vienlaikus valsts drošības nodrošināšanas dēļ pati regula automātiski kļūtu nepiemērojama, kas nozīmētu, ka netiek atzītas nevienas subjektīvās tiesības.

B. Tele 2 Sverige un Watson izstrādātās judikatūras apstiprinājums un tās tālākās attīstības iespējas

91. Secinājumos lietā C-520/18 es sīki izvērtēju Tiesas judikatūru šajā jomā⁴⁶ un šā izvērtējuma rezultātā ierosinu šo judikatūru apstiprināt, kā arī piedāvāju veidu, kā tā būtu interpretējama, lai sīkāk izskaidrotu tās saturu.

92. Lūdzu skatīt šo izvērtējumu, kurš lakonisma labad šeit, manuprāt, nav jāatkārto. Tāpēc turpinājumā izklāstītie apsvērumi par *Conseil d'État* (Valsts padome) uzdotajiem prejudiciālajiem jautājumiem ir lasāmi kopsakarā ar attiecīgajām sadaļām secinājumos lietā C-520/18.

C. Atbilde uz prejudiciālajiem jautājumiem

1. Par pienākumu saglabāt datus (pirmais prejudiciālais jautājums lietās C-511/18 un C-512/18 un otrais prejudiciālais jautājums lietā C-512/18)

93. Runājot par elektronisko komunikāciju pakalpojumu sniedzējiem uzlikto pienākumu saglabāt datus iesniedzējtiesa būtībā vēlas noskaidrot:

- vai šis ar Direktīvas 2002/58 15. panta 1. punktu uzliktais pienākums ir iejaukšanās, kuru var attaisnot Hartas 6. pantā garantētās “tiesības uz drošību” un valsts drošības prasības (pirmais jautājums lietās C-511/18 un C-512/18, kā arī trešais jautājums lietā C-511/18);
- vai ar Direktīvu 2000/31 ir atļauts saglabāt datus, kuri ļauj identificēt tos, kas ir piedalījušies sabiedrībai tiešsaistē pieejama satura veidošanā (otrais jautājums lietā C-512/18).

a) Ievada apsvērumi

94. *Conseil d'État* (Valsts padome) atsaucas uz pamattiesībām, kas ir nostiprinātas Hartas 7. pantā (tiesības uz privātās un ģimenes dzīves neaizskaramību), 8. pantā (personas datu aizsardzība) un 11. pantā (vārda un informācijas brīvība). Šīs tiesības, pēc Tiesas domām, ir tās, kuras iespējami var tikt aizskartas, ja valsts iestādes elektronisko komunikāciju pakalpojumu sniedzējiem nosaka pienākumu saglabāt informāciju par datu plūsmu⁴⁷.

95. Iesniedzējtiesa min arī tiesības uz drošību, kas ir aizsargātas ar Hartas 6. pantu. Tā atsaucas uz tām nevis kā tiesībām, kas var tikt aizskartas, bet kā uz faktoru, kas var pamatot šāda pienākuma noteikšanu.

96. Piekritu Komisijai, ka šī atsauce uz 6. pantu var būt maldinoša. Tāpat kā Komisija es uzskatu, ka šī tiesību norma nav jāinterpretē tādējādi, ka ar to var “uzlikt Savienībai pozitīvu pienākumu pieņemt pasākumus, lai aizsargātu personas pret noziedzīgiem nodarījumiem”⁴⁸.

⁴⁶ 27.–68. punkts.

⁴⁷ Spriedums *Tele2 Sverige* un *Watson*, 92. punkts, kurā pēc analogijas ir minēts spriedums *Digital Rights*, 25. un 70. punkts.

⁴⁸ Komisijas rakstveida apsvērumu 37. punkts.

97. Šajā Hartas pantā garantētā drošība nav tas pats, kas sabiedrības drošība. Jeb, citiem vārdiem sakot, tai ir tikpat cieša saikne ar sabiedrības drošību kā ar jebkurām citām pamattiesībām, jo sabiedrības drošība ir obligāts nosacījums, lai varētu baudīt pamattiesības un pamatbrīvības.

98. Kā atgādina Komisija, Hartas 6. pants atbilst Eiropas Cilvēktiesību [un pamatbrīvību aizsardzības] konvencijas (turpmāk tekstā – “ECPAK”) 5. pantam, kā redzams tai pievienotajos paskaidrojumos. No ECPAK 5. panta interpretācijas izriet, ka ar to aizsargātā “drošība” ir personiskā drošība tiešā nozīmē, ko saprot kā garantiju tiesībām uz fizisku brīvību attiecībā uz patvaļīgu aizturēšanu vai apcietināšanu. Īsumā sakot, tā ir drošība, ka nevienam nevar atņemt brīvību, izņemot likumā paredzētajos gadījumos un tajos noteiktajā kārtībā.

99. Tādējādi runa ir par *personisku drošību*, kuras kontekstā nozīme ir nosacījumiem, kādos var ierobežot personu fizisko brīvību⁴⁹, nevis no valsts pastāvēšanas izrietošo *sabiedrības drošību*, kas ir obligāts nosacījums attīstītā sabiedrībā, lai valsts varas īstenošanu saskaņotu ar individuālo tiesību īstenošanu.

100. Dažas valdības tomēr lūdz aplūkot tiesības uz drošību otrajā no šīm nozīmēm. Patiesībā Tiesa to ne tikai ir ņēmusi tās vērā, bet arī skaidri minējusi savos spriedumos⁵⁰ un atzinumos⁵¹. Tā nekad nav noliegusi tādu vispārējo interešu mērķu nozīmīgumu kā valsts drošība un sabiedriskā kārtība⁵², starptautiskā terorisma apkarošana, uzturot starptautisko mieru un drošību, kā arī smagu noziegumu apkarošana, lai garantētu sabiedrības drošību⁵³, ko tā pamatoti ir kvalificējusi kā “būtisku”⁵⁴. Savulaik tā norādīja, ka “sabiedrības drošības aizsardzība veicina arī citu personu tiesību un brīvību aizsardzību”⁵⁵.

101. Saistībā ar šiem lūgumiem sniegt prejudiciālu nolēmumu radušos iespēju varētu izmantot, lai mudinātu aktīvāk meklēt līdzsvaru starp tiesībām uz drošību, no vienas puses, un tiesībām uz privātās dzīves neaizskaramību un tiesībām personas datu aizsardzību, no otras puses. Tas ļautu izvairīties no kritikas, ka otrās no tām tiek nodrošinātas, kaitējot pirmajām.

102. Šis līdzsvars, manuprāt, ir minēts Direktīvas 2002/58 11. apsvērumā un 15. panta 1. punktā, runājot par pasākumu nepieciešamību un samērīgumu *demokrātiskā sabiedrībā*. Tiesībām uz drošību, kā jau teicu, ir būtiska nozīme demokrātijas pastāvēšanā un saglabāšanā, un tāpēc tās ir pilnībā jāņem vērā, veicot šo samērīguma izvērtējumu. Citiem vārdiem sakot, ja demokrātiskā sabiedrībā ir ļoti būtiska nozīme datu konfidencialitātes principa ievērošanai, par zemu nebūtu jānovērtē arī drošības nozīmīgums šajā sabiedrībā.

103. Tādējādi apstākļos, kad ir nopietni un pastāvīgi apdraudēta valsts drošība, konkrēti, pastāv terorisma draudi, ir jāņem sprieduma *Tele2 Sverige un Watson* 119. punkta pēdējā teikumā paustā atziņa. Valsts sistēmā var tikt paredzēta samērīga atbilde uz apdraudējumu un tā intensitāti, un ne vienmēr tās atbildei ir jābūt identiskai atbildēm, kas ir rastas citās dalībvalstīs.

49 Tā to interpretē ECT. Skat. tostarp spriedumu, 2016. gada 5. jūlijs, *Buzadji* pret Moldovas Republiku, ECHR:2016:0705JUD002375507, kura 84. punktā ir apgalvots, ka ECPAK 5. pantā nostiprināto tiesību galvenais mērķis ir novērst patvaļīgu vai nepamatotu individuālas brīvības atņemšanu.

50 Spriedums *Digital Rights*, 42. punkts.

51 Atzinums 1/15 (ES un Kanādas PDR nolīgums), 2017. gada 26. jūlijs (turpmāk tekstā – “Atzinums 1/15”, EU:C:2017:592), 149. punkts un tajā minētā judikatūra.

52 Spriedums, 2016. gada 15. februāris, N. (C-601/15 PPU, EU:C:2016:84), 53. punkts

53 Spriedums *Digital Rights*, 42. punkts un tajā minētā judikatūra.

54 Turpat, 51. punkts.

55 Atzinums 1/15, 149. punkts.

104. Visbeidzot ir jāpiebilst, ka iepriekš izklāstītie apsvērumi neliedz – patiesi *ārkārtējās* situācijās, kuras raksturo tūlītēji draudi vai ārkārtīgs risks, kas attaisno oficiālu ārkārtas situācijas pasludināšanu dalībvalstī, – valsts tiesību aktos paredzēt iespēju uz noteiktu laiku uzlikt tik plašu un vispārēju datu saglabāšanas pienākumu, cik tas ir uzskatāms par nepieciešamu⁵⁶.

105. Tādējādi pirmais jautājums abos lūgumos sniegt prejudiciālu nolēmumu būtu jāpārformulē un drīzāk būtu jāaplūko iespēja attaisnot iejaukšanos valsts drošības apsvērumu dēļ. Tādējādi jautājums būtu par to, vai elektronisko komunikāciju pakalpojumu sniedzējiem uzliktais pienākums ir saderīgs ar Direktīvas 2002/58 15. panta 1. punktu.

b) Vērtējums

1) Lūgumos sniegt prejudiciālu nolēmumu aplūkoto valsts tiesību normu raksturojums Tiesas judikatūras gaismā

106. No lūgumiem sniegt prejudiciālu nolēmumu izriet, ka pamatlietās aplūkotajos tiesiskajos regulējumos pienākums saglabāt datus ir:

- elektronisko komunikāciju pakalpojumu sniedzējiem, it īpaši tiem, kas nodrošina sabiedrībai komunikāciju pakalpojumus tiešsaistē, un
- fiziskām vai juridiskām personām, kas nolūkā padarīt tos pieejamus sabiedrībai tiešsaistē – pat bez maksas – glabā jebkāda veida signālus, tekstus, skaņas, attēlus vai ziņojumus, kurus sniedz šo pakalpojumu adresāti⁵⁷.

107. Operatoriem ir pienākums saglabāt datus vienu gadu no to reģistrācijas dienas, informāciju, kas ļauj identificēt lietotāju, informāciju par izmantotajām komunikāciju galaiekārtām, tehniskos parametrus, ikvienas komunikācijas datumu, laiku un ilgumu, informāciju par pieprasītajiem vai izmantotajiem papildu pakalpojumiem un to sniedzējiem, kā arī informāciju, kas ļauj identificēt komunikācijas adresātu un telefonijas darbību gadījumā – komunikācijas izcelsmi un atrašanās vietu⁵⁸.

108. Runājot konkrēti par interneta piekļuves pakalpojumiem un glabāšanas pakalpojumiem, valsts tiesiskajā regulējumā, šķiet, ir noteikts, ka ir jāsaglabā IP adreses⁵⁹, paroles un, ja tiek noslēgts abonenta līgums vai atvērts maksājuma konts, maksāšanas veids, kā arī darījuma references numurs, summa, tā veikšanas datums un laiks⁶⁰.

109. Šis pienākums saglabāt datus ir noteikts noziedzīgu nodarījumu izmeklēšanas, konstatēšanas un kriminālvajāšanas nolūkos⁶¹. Proti, atšķirībā no pienākuma *vākt* informāciju par datu plūsmu un atrašanās vietas datus – kā tas tiks norādīts turpinājumā – terorisma novēršana nav vienīgais pienākuma *tos saglabāt* mērķis⁶².

⁵⁶ Skat. manus secinājumus lietā C-520/18, 105.–107. punkts.

⁵⁷ Tas izriet no Iekšējās drošības kodeksa L. 851-1. panta, kurā ir atsauce uz Pasta un elektronisko komunikāciju kodeksa L. 34-1. pantu un Likuma Nr. 2004-575 par uzticēšanās veicināšanu digitālajā ekonomikā 6. pantu.

⁵⁸ Tā ir teikts Pasta un elektronisko komunikāciju kodeksa R. 10-13. pantā.

⁵⁹ Šo jautājumu, par kuru tiesas sēdē tika pausti atšķirīgi viedokļi, noskaidrot ir iesniedzējtiesas ziņā.

⁶⁰ Dekrēta Nr. 2011-219 1. pants.

⁶¹ Pasta un elektronisko komunikāciju kodeksa R. 10-13. pants.

⁶² Gan *Quadrature du Net*, gan *Fédération des fournisseurs d'accès à Internet associatifs* uzsver datu saglabāšanas mērķu dažādību, iestādēm piešķirto novērtējuma brīvību, objektīvu kritēriju neesamību tās noteikšanā un nozīmi, kas ir piešķirta noziedzīgiem nodarījumiem, kas nav kvalificējami par smagiem noziegumiem.

110. No lūgumos sniegt prejudiciālu nolēmumu sniegtās informācijas izriet, ka nosacījumi par *piekļuvi* saglabātajiem datiem ir vai nu paredzēti vispārējā kārtībā (tiesu iestādes iesaistīšanās), vai arī šī piekļuve tiek piešķirta tikai individuāli izraudzītiem un pilnvarotiem pārstāvjiem, saņemot premjerministra atļauju, kas ir izsniegta, pamatojoties uz neatkarīgas administratīvas iestādes nesaistošu atzinumu⁶³.

111. Kā norāda Komisija⁶⁴, ir visai acīmredzami, ka dati, kurus saglabāšanas pienākums ir noteikts valsts tiesību normās, būtībā ir dati, ko Tiesa ir aplūkojusi spriedumā *Digital Rights* un spriedumā *Tele2 Sverige* un *Watson*⁶⁵. Gluži tāpat kā minētajās lietās aplūkoto datu gadījumā, arī uz šiem datiem attiecas “pienākums veikt visaptverošu un nediferencētu saglabāšanu”, kā sava lūguma sniegt prejudiciālu nolēmumu sākumā uz to visnotaļ atklāti norāda *Conseil d'État* (Valsts padome).

112. Ja tas tā ir – un tas galu galā ir jāizvērtē iesniedzējtiesai – atliek vienīgi secināt, ka attiecīgais tiesiskais regulējums ietver “iejaukšan[os] ar Hartas 7. un 8. pantu paredzētajās pamattiesībās[, kas] ir atzīstama par ļoti plašu un tā ir jāuzskata par īpaši nopietnu”⁶⁶.

113. Neviens no lietas dalībniekiem nav apšaubījis to, ka šāds tiesiskais regulējums rada iejaukšanos šajās tiesībās. Tagad tas nav jāiztirzā, pat ne tālab, lai atgādinātu, ka šo tiesību neievērošana nenovēršami pašos pamatos apdraud sabiedrību, kura līdzās citām vērtībām tiecas respektēt arī Hartā nostiprinātās tiesības uz privātās dzīves neaizskaramību.

114. Ja tiktu piemērota spriedumā *Tele2 Sverige* un *Watson* izstrādātā un spriedumā *Ministerio Fiscal* apstiprinātā judikatūra, noteikti būtu jāatzīst, ka tāds tiesiskais regulējums kā šajā lietā aplūkots “pārsniedz to, kas ir absolūti nepieciešams[,] un nevar tikt uzskatīts par pamatotu demokrātiskā sabiedrībā, kā arī to prasa Direktīvas 2002/58 15. panta 1. punkts, lasot to Hartas 7., 8., 11. panta un 52. panta 1. punkta gaismā”⁶⁷.

115. Proti, tāpat kā spriedumā *Tele2 Sverige* un *Watson* izvērtētais tiesiskais regulējums arī pašlaik aplūkojamais “vispārīgi attiecas uz visiem abonentiem un reģistrētajiem lietotājiem un attiecas uz visiem elektronisko sakaru līdzekļiem, kā arī visu informāciju par datu plūsmu – [un tajā] nav paredzēta nekāda diferencēšana, ierobežojumi vai izņēmumi atkarībā no sasniedzamā mērķa”⁶⁸. Līdz ar to tas ir “piemērojams pat attiecībā uz personām, par kurām nepastāv nekādas norādes, kas var ļaut uzskatīt, ka to rīcībai varētu būtu kaut netieša vai attālināta saikne ar smagiem noziegumiem”, nepieļaujot nekādu izņēmumu, “kā rezultātā to piemēro pat personām, uz kuru sakariem saskaņā ar valsts tiesību normām attiecas dienesta noslēpums”⁶⁹.

116. Šāds tiesiskais regulējums “neprasa nekādu saikni starp datiem, kurus ir paredzēts saglabāt, un draudiem sabiedrības drošībai. Tostarp tajā nav paredzēta vienīgi ierobežota saglabāšana, kas attiecas vai nu uz datiem saistībā ar kādu laikposmu un/vai ģeogrāfisku teritoriju un/vai personu loku, kuras var vienā vai otrā veidā būt iesaistītas smagā noziegumā, vai arī uz personām, kuru datu saglabāšana citu iemeslu dēļ varētu dot ieguldījumu noziegumu apkarošanā”⁷⁰.

63 *Commission nationale de contrôle des techniques de renseignement* (Nacionālā izlūkdatu vākšanas metožu kontroles komisija). Šajā sakarā skat. Francijas valdības rakstveida apsvērumu 145.–148. punktu.

64 Komisijas rakstveida apsvērumu 60. punkts.

65 Faktiski tiek aplūkoti arī citi dati, jo šķiet, ka interneta piekļuves pakalpojumu gadījumā ir paredzēts saglabāt IP adreses vai paroles.

66 Spriedums *Tele2 Sverige* un *Watson*, 100. punkts.

67 Turpat, 107. punkts.

68 Turpat, 105. punkts.

69 Minēts iepriekš.

70 Spriedums *Tele2 Sverige* un *Watson*, 106. punkts.

117. No iepriekš minētā izriet, ka šis tiesiskais regulējums “pārsniedz to, kas ir absolūti nepieciešams[,] un nevar tikt uzskatīts par pamatotu demokrātiskā sabiedrībā, kā arī to prasa Direktīvas 2002/58 15. panta 1. punkts, lasot to Hartas 7., 8., 11. panta un 52. panta 1. punkta gaismā”⁷¹.

118. Ar iepriekš minēto bija pietiekami, lai Tiesa secinātu, ka attiecīgās valsts tiesību normas nav saderīgas ar Direktīvas 2002/58 15. panta 1. punktu, ciktāl tajās “noziedzības apkarošanas nolūkā ir paredzēta visaptveroša un nediferencēta visas informācijas par datu plūsmu un atrašanās vietas datu saglabāšana attiecībā uz visiem abonentiem un reģistrētiem lietotājiem un attiecībā uz visiem elektronisko sakaru līdzekļiem”⁷².

119. Tagad jautājums rodas par to, vai Tiesas judikatūra personas datu saglabāšanas jomā būtu, ja ne pārskatāma, tad vismaz niansējama gadījumā, ja šis “visaptverošas un nediferencētas” saglabāšanas mērķis ir terorisma apkarošana. Pirmais jautājums lietā C-511/18 ir uzdots tieši “kontekstā, kurā pastāv būtiski un pastāvīgi valsts drošības apdraudējumi un it īpaši terorisma risks”.

120. Tomēr, lai arī pienākums saglabāt datus ir uzlikts šajā *faktiskajā kontekstā*, patiesība ir tāda, ka tā *normatīvais konteksts* attiecas ne tikai un vienīgi uz terorismu. *Conseil d'État* (Valsts padome) notiekošajā tiesvedībā aplūkots regulējums par datu saglabāšanu un piekļuvi tiem nosaka, ka šis pienākums ir vispārīgi pakārtots noziedzīgu nodarījumu izmeklēšanas, konstatēšanas un kriminālvajāšanas mērķiem.

121. Katrā ziņā atgādināšu, ka terorisma apkarošana tika minēta arī sprieduma *Tele2 Sverige* un *Watson* argumentācijā, tomēr toreiz Tiesa neuzskatīja, ka šis noziedzīgu nodarījumu veids radītu vajadzību jebkādi pielāgot tās judikatūru⁷³.

122. Tāpēc principā uzskatu, ka uz iesniedzējtiesas jautājumu, kas balstīts uz terorisma draudu īpatnībām, būtu jāatbild tāpat, kā Tiesa ir nospriedusi spriedumā *Tele2 Sverige* un *Watson*.

123. Kā esmu norādījis secinājumos lietā *Stichting Brein*, “noteiktība tiesību piemērošanā uzliek tiesām pienākumu nevis piemērot *stare decisis* absolūtā veidā, bet būt rūpīgām un ievērot to, ko tās pašas ir nolēmušas pēc nopietnām pārdomām par attiecīgo juridisko problēmu”⁷⁴.

2) Ierobežota datu glabāšana, ņemot vērā draudus valsts drošībai, tostarp terorisma draudus

124. Tomēr vai būtu iespējams niansēt vai papildināt šo judikatūru, ņemot vērā tās ietekmi uz terorisma apkarošanu vai valsts aizsardzību pret citiem līdzīgiem valsts drošības apdraudējumiem?

⁷¹ Turpat, 107. punkts.

⁷² Turpat, 112. punkts.

⁷³ Turpat, 103. punkts.

⁷⁴ Lieta C-527/15, EU:C:2016:938, 41. punkts.

125. Esmu jau uzsvēris, ka personas datu glabāšana jau pati par sevi rada iejaukšanos Hartas 7., 8. un 11. pantā nostiprinātajās tiesībās⁷⁵. Neatkarīgi no tā, ka beigu beigās ar to tiek mēģināts konkrētā brīdī nodrošināt iespēju vēlāk vai tajā pašā laikā *piekļūt* datiem⁷⁶, datu glabāšana tādā apjomā, kurš pārsniedz to, kas ir stingri nepieciešams saziņas nodrošināšanai vai rēķinu izrakstīšanai par pakalpojumu sniedzēja sniegtajiem pakalpojumiem, jau pati par sevi ir Direktīvas 2002/58 5. un 6. pantā paredzēto ierobežojumu neievērošana.

126. Šo pakalpojumu lietotājiem (kuru kopumu patiesībā veido gandrīz visi attīstītāko sabiedrību līdzpilsoņi) ir vai jābūt tiesiskajai palāvēībai, ka bez viņu piekrišanas tiks saglabāti tikai tie dati, kurus glabā saskaņā ar šīm tiesību normām. Direktīvas 2002/58 15. panta 1. punktā paredzētie izņēmumi ir jāinterpretē, balstoties uz šo premisu.

127. Kā jau esmu paskaidrojis, personas datu visaptverošu un nediferencētu saglabāšanu Tiesa spriedumā *Tele2 Sverige* un *Watson* noraidīja arī saistībā ar terorisma apkarošanu⁷⁷.

128. Atbildot uz pausto kritiku, neuzskatu, ka minētajā spriedumā izstrādātajā judikatūrā nebūtu pietiekami novērtēti terorisma draudi kā īpaši smagu noziegumu veids, kas ietver skaidru mērķi apšaubīt valsts varu un destabilizēt vai iznīcināt tās institūcijas. Terorisma apkarošana burtiski ir vitāli svarīga valstij un tās sekmīgai pastāvēšanai, tas ir vispārējo interešu mērķis, no kura tiesiska valsts nevar atteikties.

129. Praktiski visas tiesvedībā pārstāvētās valdības, kā arī Komisija vienprātīgi norādīja, ka daļēja un diferencēta personas datu saglabāšana radītu ne tikai tehniskas grūtības, bet arī liegtu valsts izlūkdienestiem iespēju piekļūt informācijai, kas ir vajadzīga, lai identificētu draudus sabiedrības drošībai un valsts aizsardzībai, kā arī veiktu teroristu uzbrukumu organizatoru kriminālvajāšanu⁷⁸.

130. Atbildot uz šo nostāju, manuprāt, ir jānorāda, ka terorisma apkarošana nav jāaplūko tikai no tās efektivitātes skatupunkta. Tādējādi tā ir grūta, bet arī cildena, ja tās līdzekļi un metodes tiek pielāgoti tiesiskas valsts prasībām, kas pirmkārt jau ir varas un spēka pakļautība likumā noteiktajiem ierobežojumiem un it īpaši tiesību sistēmai, kuras esības iemesls un mērķis ir nodrošināt pamattiesību aizsardzību.

131. Terorismā līdzekļu attaisnošanai tiek izmantots tikai pastāvošajai kārtībai veikto uzbrukumu tīras (un maksimālas) efektivitātes kritējs, turpretim tiesiska valsts efektivitāti mēra tādējādi, ka tās aizsardzībā nav atļauts neievērot procedūras un garantijas, kas to padara par leģitīmu kārtību. Ja vadītos tikai no efektivitātes apsvērumiem vien, tiesiska valsts zaudētu savas raksturiezīmes un ārkārtas gadījumos, iespējams, pati kļūtu par apdraudējumu pilsoņiem. Ja valsts vara būtu apbruņota ar pārmērīgiem kriminālvajāšanas rīkiem, kas ļautu tai neievērot vai pārkāpt pamattiesības, nebūtu nekādas garantijas, ka tās nekontrolētā un nekādi neierobežotā rīcība beigu beigās nekaitētu ikvienas personas brīvībai.

⁷⁵ Kā Tiesa atgādināja Atzinuma 1/15 124. punktā, "personas datu izpaušana trešajai personai, piemēram, valsts iestādei, ir iejaukšanās Eiropas Savienības Pamattiesību hartas 7. pantā noteiktajās pamattiesībās, lai kāda būtu izpaustās informācijas vēlāka izmantošana. Tas pats attiecas uz personas datu saglabāšanu, kā arī piekļuvi šiem datiem, lai valsts iestādes varētu tos izmantot. Šajā ziņā nav svarīgi, vai attiecīgā informācija par privāto dzīvi ir vai nav sensitīva, vai tas, ka attiecīgajām personām ir vai nav radītas iespējamās neērtības šīs iejaukšanās dēļ".

⁷⁶ Kā norādīja ģenerālvokāts P. Kruss Viljalons [*P. Cruz Villalón*] secinājumos lietā *Digital Rights*, C-293/12 un C-594/12 (EU:C:2013:845), 72. punktā, "daudzu datu, kas ir iegūti vai apstrādāti lielākajā Eiropas Savienības pilsoņu parasto elektronisko komunikāciju daļā [...], savākšana [...], un it īpaši saglabāšana [...], ļoti apjomīgās datu bāzēs, ir būtiska iejaukšanās viņu privātajā dzīvē, lai arī tas tikai rada nosacījumus iespējai *a posteriori* veikt kontroli pār viņu personisko un profesionālo darbību. Šādu datu vākšana rada apstākļus uzraudzībai, kas, lai arī var tikt veikta tikai *a posteriori* tad, kad šie dati tiek izmantoti, tomēr pastāvīgi – visā datu saglabāšanas laikā – apdraud Savienības pilsoņu tiesības uz viņu privātās dzīves noslēpumu. Radītā kļiedētā sajūta par uzraudzību [...] padara īpaši aktuālu jautājumu par datu saglabāšanas ilgumu".

⁷⁷ Spriedums *Tele2 Sverige* un *Watson*, 103. punkts: "nevar pamatot, ka valsts tiesiskais regulējums, kurā paredzēta visas informācijas par datu plūsmu un atrašanās vietas datu visaptveroša un nediferencēta saglabāšana, tiek uzskatīts par nepieciešamu minētās apkarošanas mērķiem".

⁷⁸ Šādi to interpretē, piemēram, Francijas valdība, kas šo apgalvojumu pamato ar konkrētiem piemēriem, kuri liecina par visaptverošas saglabāšanas noderīgumu, kas ir ļāvusi valstij reaģēt uz šajā valstī pēdējos gados notikušajiem nopietnajiem teroristu uzbrukumiem (Francijas valdības rakstveida apsvērumu 107. un 122.–126. punkts).

132. Valsts varas efektivitātei nepārkāpjama robeža, kā jau teicu, ir pilsoņu pamattiesības, kuru ierobežojumus, kā tas ir noteikts Hartas 52. panta 1. punktā, var ieviest tikai ar tiesību aktiem un, ievērojot to būtisko saturu, “ja tie ir nepieciešami un patiešām atbilst vispārējo interešu mērķiem, ko atzinusi Savienība, vai vajadzībai aizsargāt citu personu tiesības un brīvības”⁷⁹.

133. Par apstākļiem, kādos atbilstoši spriedumam *Tele2 Sverige* un *Watson* būtu pieļaujama datu selektīva saglabāšana, lūdzu skatīt manus secinājumus lietā C-520/18⁸⁰.

134. Apstākļi, kuros drošības dienestu rīcībā esošā informācija ļauj pamatot aizdomas par teroraktu sagatavošanu, var būt gadījums, kad likumīgi var uzlikt pienākumu saglabāt kādus datus. Vēl jo vairāk to var noteikt, ja uzbrukums ir faktiski noticis. Šajā nupat minētajā gadījumā noziedzīga nodarījuma izdarīšana jau pati par sevi var būt šāda pasākuma noteikšanu attaisnojošs faktors, savukārt gadījumā, kad ir tikai aizdomas par iespējamu uzbrukumu, apstākļiem, kas to pamato, būtu jābūt vismaz minimālai ticamības pakāpei, kas nepieciešama, lai varētu objektīvi izvērtēt pazīmes, kuru dēļ pasākums varētu būt attaisnots.

135. Lai gan ir grūti, tomēr nav neiespējami precīzi un saskaņā ar objektīviem kritērijiem noteikt gan to datu kategorijas, kuru saglabāšana tiek uzskatīta par nepieciešamu, gan attiecīgo personu loku. Protams, *praktiskāk un efektīvāk* būtu, ja elektronisko komunikāciju pakalpojumu sniedzēji varētu veikt visu datu visaptverošu un nediferencētu saglabāšanu, bet, kā jau teicu, šis jautājums ir risināms nevis no *praktiskas efektivitātes*, bet *juridiskās efektivitātes* viedokļa un tiesiskas valsts kontekstā.

136. Šī noteikšana parasti ir veicama likumdošanas ceļā, ievērojot Tiesas judikatūrā noteiktās robežas. Šajā ziņā atkal lūdzu skatīt manis izklāstīto secinājumus lietā C-520/18⁸¹.

3) Piekļuve saglabātajiem datiem

137. Balstoties uz premisu, ka operatori ir savākuši datus, ievērojot Direktīvā 2002/58 noteikto, un ka tie ir saglabāti saskaņā ar tās 15. panta 1. punktu⁸², kompetento iestāžu piekļuve šai informācijai ir jānodrošina, ievērojot Tiesas izvirzītos nosacījumus, kuru izvērtējumu lūdzu skatīt manus secinājumus lietā C-520/18⁸³.

138. Līdz ar to arī šajā gadījumā valsts tiesiskajā regulējumā ir jāparedz materiāltiesiskie un procesuālie nosacījumi, kas reglamentē kompetento valsts iestāžu piekļuvi saglabātajiem datiem⁸⁴. Lūgumos sniegt prejudiciālu nolēmumu aplūkotojamos gadījumos šīs prasības atļautu piekļūt to personu datiem, kuras tiek turētas aizdomās par terorakta plānošanu, sagatavošanos tam vai tā izdarīšanu vai arī kuras varētu būt tajā iesaistītas⁸⁵.

79 Spriedums, 2016. gada 15. februāris, N. (C-601/15 PPU, EU:C:2016:84), 50. punkts. Tādējādi runa ir par manis jau minēto grūti sasniedzamo līdzsvaru starp sabiedrisko kārtību un brīvību, kuru principā tiecas nodrošināt viss Savienības tiesiskais regulējums. Kā piemēru var minēt Eiropas Parlamenta un Padomes Direktīvu (ES) 2017/541 (2017. gada 15. marts) par terorisma apkarošanu un ar ko aizstāj Padomes Pamatlēmumu 2002/475/TI un groza Padomes Lēmumu 2005/671/TI (OV 2017, L 88, 6. lpp.). Lai arī 20. panta 1. punktā ir noteikts, ka dalībvalstīm ir jāgarantē, ka personām, kas ir atbildīgas par tādu noziedzīgu nodarījumu kā terorisms izmeklēšanu vai kriminālvajāšanu, ir “pieejami [...] efektīvi izmeklēšanas līdzekļi”, tās 21. apsvērumā ir norādīts, ka šo efektīvo instrumentu izmantošanā “būtu jāņem vērā proporcionālītātes princips un izmeklējamu nodarījumu raksturs un smagums un jāievēro tiesības uz personas datu aizsardzību”.

80 87.–95. punkts.

81 100.–107. punkts.

82 Ciktāl tiek ievēroti sprieduma *Tele2 Sverige* un *Watson* 122. punktā minētie nosacījumi: Tiesa ir atgādinājusi, ka ar Direktīvas 2002/58 15. panta 1. punktu nav atļauts atkāpties no tās 4. panta 1. un 1.a punkta, saskaņā ar kuru pakalpojumu sniedzējiem ir jāveic pasākumi, kas ļauj nodrošināt saglabāto datu aizsardzību pret ļaunprātīgas izmantošanas un prettiesiskas piekļuves risku. Šajā ziņā tā nosprieda, ka, “ņemot vērā saglabāto datu apjomu, šo datu sensitīvo raksturu, kā arī prettiesiskas piekļuves šiem datiem risku, elektronisko sakaru pakalpojumu sniedzējiem minēto datu integritātes un konfidencialitātes nodrošināšanai pilnībā ir jāgarantē īpaši augsts aizsardzības līmenis ar piemērotiem tehniskiem un organizatoriskiem pasākumiem. It īpaši valsts tiesiskajā regulējumā ir jāparedz, ka [dati] netiek izpausti ārpus Savienības teritorijas, kā arī tas, ka dati pēc to saglabāšanas termiņa beigām tiek neatgriezeniski iznīcināti”.

83 52.–60. punkts.

84 Spriedums *Tele2 Sverige* un *Watson*, 118. punkts.

85 Turpat, 119. punkts.

139. Tomēr būtiskākais ir tas, ka, izņemot pienācīgi pamatotus neatliekamības gadījumus, piekļuve attiecīgajiem datiem ir pakārtota iepriekšējai pārbaudei, ko tiesa vai neatkarīga administratīva iestāde veic, pieņemot lēmumu attiecībā uz kompetento iestāžu pamatotu pieteikumu⁸⁶. Tādējādi jautājumos, kur likuma abstraktais vērtējums nesniedzas, vērtējumu *in concreto* nodrošina šī neatkarīgā iestāde, apņēmdamās vienlīdz garantēt valsts drošību un pilsoņu pamattiesību aizsardzību.

4) Pienākums glabāt datus, kas ļauj identificēt satura veidotājus, Direktīvas 2000/31 gaismā (otrais prejudiciālais jautājums lietā C-512/18)

140. Iesniedzējtiesa atsaucas uz Direktīvu 2000/31, lai noskaidrotu, vai ir iespējams konkrētām personām⁸⁷ un operatoriem, kas sniedz komunikāciju pakalpojumus sabiedrībai, uzlikt pienākumu saglabāt datus, “kuri var ļaut identificēt jebkuru personu, kas ir piedalījies tās sniegto pakalpojumu saturā vai tā daļas radīšanā, lai tiesu iestāde vajadzības gadījumā varētu pieprasīt šo datu paziņošanu nolūkā nodrošināt, ka tiek ievēroti noteikumi par civiltiesisko atbildību vai kriminālatbildību”.

141. Piekritu Komisijai, ka būtu nevietā pārbaudīt šā pienākuma saderību ar Direktīvu 2000/31⁸⁸, jo šī direktīva – saskaņā ar tās 1. panta 5. punkta b) apakšpunktā teikto – nav piemērojama “jautājumiem, kuri attiecas uz informācijas sabiedrības pakalpojumiem un kuri ietverti Direktīvā 95/46/EK un 97/66/EK”, proti, regulējumos, kas tagad atbilst Regulai 2006/679 un Direktīvai 2002/58⁸⁹, kuru attiecīgi 23. panta 1. punkts un 15. panta 1. punkts, manuprāt, ir jāinterpretē tā, kā izklāstīts iepriekš.

2. Par pienākumu reāllaikā vākt informāciju par datu plūsmu un atrašanās vietas datus (otrais prejudiciālais jautājums lietā C-511/18)

142. Iesniedzējtiesa uzskata, ka ar Iekšējās drošības kodeksa L. 851-2. pantu tikai terorisma novēršanas nolūkos ir atļauts reāllaikā vākt informāciju par personām, kuras iepriekš identificētas kā personas, kas tiek turētas aizdomās par saikni ar terorisma draudiem. Tāpat arī šā paša kodeksa L.851-4. pants operatoriem reāllaikā ļauj pārsūtīt tehniskos datus par galaiekārtu atrašanās vietu.

143. Pēc iesniedzējtiesas teiktā, šīs metodes neuzliek pakalpojumu sniedzējiem pienākumu glabāt datus papildus tam, kas nepieciešams viņu rēķinu izsniegšanai un pakalpojumu tirdzniecībai.

144. Turklāt saskaņā ar Iekšējās drošības kodeksa L. 851-3. pantu elektronisko komunikāciju operatoriem un tehnisko pakalpojumu sniedzējiem var būt pienākums “savos tiklos veikt automātiskas apstrādes, kuru mērķis ir atbilstoši atļaujā norādītajiem parametriem atklāt pieslēgumus, kas var liecināt par terorisma draudiem”. Šī metode neietver datu visaptverošu un nediferencētu glabāšanu, un tās mērķis ir ierobežotā laikā vākt tikai tos pieslēguma datus, kas, iespējams, ir saistīti ar teroristisku noziegumu.

145. Manuprāt, nosacījumi, lai iegūtu piekļuvi saglabātajiem personas datiem, ir jāpiemēro arī piekļuvei reāllaikā datiem, kas tiek ģenerēti elektronisko komunikāciju gaitā. Tāpēc lūdzu skatīt manis jau teikto šajā jautājumā. Nav nozīmes, vai tie ir saglabātie dati vai reāllaikā savāktie dati, jo abos gadījumos tiek uzzināti personas dati – neatkarīgi no tā, vai tie ir agrāki vai pašreizējie dati.

⁸⁶ Turpat, 120. punkts.

⁸⁷ Proti, personām, kuras, “lai darītu tos pieejamus sabiedrībai, izmantojot publiskos komunikāciju pakalpojumus, nodrošina jebkāda veida signālu, teksta, attēlu, skaņu un ziņojumu, ko ir snieguši šo pakalpojumu adresāti, glabāšanu [...]”.

⁸⁸ Iesniedzējtiesa uz šo direktīvu, vispārīgi un nenorādot konkrētas tiesību normas, atsaucas otrajā jautājumā lietā C-512/18.

⁸⁹ Komisijas rakstveida apsvērumu 112. un 113. punkts.

146. Konkrēti, ja piekļuve reāllaikā izriet no pieslēgumiem, kas ir noteikti automatizētas apstrādes rezultātā, kā tas ir paredzēts Iekšējās drošības kodeksa L. 851-3. pantā, ir jānodrošina, ka šīs apstrādes veikšanai iepriekš noteiktās metodes un kritēriji ir konkrēti, ticami un nediskriminējoši, lai ļautu identificēt personas, kas ir pamatoti turamas aizdomās par dalību teroristiskās darbībās⁹⁰.

3. Par pienākumu informēt attiecīgās personas (trešais prejudiciālais jautājums lietā C-511/18)

147. Tiesa ir norādījusi, ka iestādēm, kurām ir piešķirta piekļuve datiem, ir jāinformē par šo apstākli attiecīgās personas, ja vien šī informēšana netraucē notiekošajai izmeklēšanai. Šis pienākums ir noteikts tāpēc, ka minētā informācija ir nepieciešama, lai tiesību pārkāpuma gadījumā attiecīgās personas varētu izmantot savas tiesības uz efektīvu tiesību aizsardzību tiesā, kas ir skaidri minētas Direktīvas 2002/58 15. panta 2. punktā⁹¹.

148. *Conseil d'État* (Valsts padome) ar trešo jautājumu lietā C-511/18 vēlas noskaidrot, vai šī informēšanas prasība katrā ziņā ir obligāta vai arī ir iespējams no tās atbrīvot, ja tiek sniegtas tādas citas garantijas kā lūgumā sniegt prejudiciālu nolēmumu aprakstītās.

149. Kā izklāsta iesniedzējtiesa⁹², minētās garantijas izpaužas kā iespēja personām, kuras vēlas pārbaudīt, vai informēšanas metode tika piemērota nelikumīgi, vērsties pie pašas *Conseil d'État* (Valsts padome). Šī iestāde vajadzības gadījumā varētu atsaukt atļauju veikt pasākumu un varētu izdot rīkojumu iznīcināt savāktu informāciju procedūrā, kurā nav paredzēts tiesvedībās parasti piemērojamais sacīkstes princips.

150. Iesniedzējtiesa uzskata, ka ar šo tiesisko regulējumu nav pārkāptas tiesības uz efektīvu tiesību aizsardzību tiesā. Tomēr, manuprāt, lai arī tas tā teorētiski varētu būt to personu gadījumā, kas vēlas pārbaudīt, vai pret tām ir vērsta izlūkošanas darbība, šīs tiesības turpretim netiek ievērotas, ja, personas, pret kurām tiek vai ir tikusi vērsta šī darbība, par to netiek brīdinātas un tādējādi pat nevar apsvērt to, vai viņu tiesības tika pārkāptas.

151. Šķiet, ka iesniedzējtiesas minētās tiesiskās garantijas ir atkarīgas no tā, vai persona, kurai ir aizdomas, ka par viņu tiek vākta informācija, izrāda kādu iniciatīvu. Taču efektīvai iespējai vērsties tiesā, lai aizstāvētu savas tiesības, ir jābūt ikvienam, un tas nozīmē, ka ikvienam, kura personas dati tika apstrādāti, ir jābūt iespējai vērsties tiesā, lai apstrīdētu minētās apstrādes likumību, un tāpēc ir jābūt informētam par tās veikšanu.

152. Lai gan no sniegtās informācijas patiešām izriet, ka tiesvedību var uzsākt *ex officio* vai arī ar administratīvu sūdzību, bet katrā ziņā attiecīgajai personai ir jādod iespēja to ierosināt pašai, tāpēc minētā persona ir jāinformē par to, ka tās personas dati ir tikuši pakļauti konkrētai apstrādei. Attiecīgās personas tiesību aizstāvēšana nevar būt atkarīga no apstākļa, ka šī persona par šo apstrādi uzzina no kāda cita vai pati saviem spēkiem.

153. Tādējādi, ciktāl nav traucēta tās izmeklēšanas gaita, kuras vajadzībām ir tikusi piešķirta piekļuve saglabātajiem datiem, par minēto piekļuvi ir jāinformē attiecīgā persona.

154. Pavisam cita lieta ir – ja attiecīgā persona ir uzsākusi tiesvedību pēc tam, kad tai ir ticis darīts zināms par piekļuvi tās datiem, turpmākajā tiesvedībā ir jāievēro konfidencialitātes un slepenības prasības, kas ir raksturīgas valsts iestāžu darbības kontrolei tādās sensitīvās jomās kā valsts drošība un aizsardzība. Tomēr šajos lūgumos sniegt prejudiciālu nolēmumu šis jautājums nav iztirzāts, tādējādi, manuprāt, Tiesai par to nav jālemj.

⁹⁰ Spriedums *Digital Rights*, 59. punkts.

⁹¹ Spriedums *Tele2 Sverige* un *Watson*, 121. punkts.

⁹² Lūguma sniegt prejudiciālu nolēmumu 8.–11. punkts.

V. Secinājumi

155. Ņemot vērā iepriekš minēto, ierosinu Tiesai atbildēt *Conseil d'État* (Valsts padome, Francija) šādi:

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) 15. panta 1. punkts, skatot to kopsakarā ar Eiropas Savienības Pamattiesību hartas 7., 8., 11. pantu un 52. panta 1. punktu, ir jāinterpretē tādējādi, ka:

- 1) tam ir pretrunā tāds valsts tiesiskais regulējums, ar ko situācijā, kurā pastāv nopietni un pastāvīgi draudi valsts drošībai, it īpaši terorisma risks, elektronisko komunikāciju operatoriem un šo pakalpojumu sniedzējiem ir noteikts pienākums visaptveroši un nediferencēti saglabāt informāciju par datu plūsmu un atrašanās vietas datus attiecībā uz visiem abonentiem, kā arī datus, kas ļauj identificēt minēto pakalpojumu sniedzēju piedāvātā satura veidotājus;
- 2) tam ir pretrunā tāds valsts tiesiskais regulējums, ar ko nav noteikts pienākums informēt attiecīgās personas par to, ka kompetentās iestādes veic viņu personas datu apstrādi, ja vien šī informēšana netraucē minēto iestāžu darbību;
- 3) tam nav pretrunā tāds valsts tiesiskais regulējums, ar ko ir atļauts reāllaikā vākt informāciju par datu plūsmu un atrašanās vietas datus attiecībā uz atsevišķām personām, ciktāl šīs darbības ir veiktas saskaņā ar procedūrām, kuras ir noteiktas, lai likumīgi piekļūtu saglabātajiem personas datiem, un, sniedzot tādas pašas garantijas.