Judikatūras krājums

ĢENERĀLADVOKĀTA MANUELA KAMPOSA SANČESA BORDONAS [*MANUEL CAMPOS SÁNCHEZ-BORDONA*]
SECINĀJUMI,
sniegti 2020. gada 15. janvārī[1]

Lieta C-623/17

Privacy International
pret
Secretary of State for Foreign and Commonwealth Affairs,
Secretary of State for the Home Department,
Government Communications Headquarters,
Security Service,
Secret Intelligence Service

(*Investigatory Powers Tribunal* (Izmeklēšanas pilnvaru tiesa, Apvienotā Karaliste) lūgums sniegt prejudiciālu nolēmumu)

Lūgums sniegt prejudiciālu nolēmumu – Personas datu apstrāde un privātās dzīves aizsardzība elektronisko komunikāciju nozarē – Direktīva 2002/58/EK – Piemērošanas joma – 1. panta 3. punkts – 15. panta 3. punkts – Eiropas Savienības Pamattiesību harta – 7., 8., 51. pants un 52. panta 1. punkts – LES 4. panta 2. punkts – Elektronisko komunikāciju pakalpojuma lietotāju pieslēguma datu visaptveroša un nediferencēta nosūtīšana drošības dienestiem

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

– 2014. gada 8. aprīļa spriedums *Digital Rights Ireland* u.c.[2], kurā tā atzina Direktīvas 2006/24/EK[3] spēkā neesamību, jo ar to bija atļauta nesamērīga iejaukšanās Eiropas Savienības Pamattiesību hartas 7. un 8. pantā nostiprinātajās tiesībās;

– 2016. gada 21. decembra spriedums *Tele2 Sverige* un *Watson* u.c.[4], kurā tā interpretēja Direktīvas 2002/58/EK[5] 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 paudušas četros lūgumos sniegt prejudiciālu nolēmumu [7], 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, ciktāl dalībvalstis var ierobežot tajā aizsargātās tiesības uz privātumu. Visbeidzot, būtu jāanalizē, cik lielā mērā šajos dažādajos (Apvienotās Karalistes [8], Beļģijas [9] un Francijas [10]) šīs jomas tiesiskajos regulējumos ir ievērotas Savienības tiesības, kā tās ir interpretējusi Tiesa.

I. Atbilstošās tiesību normas

A. Savienības tiesības

5. Lūdzu skatīt attiecīgo sadaļu manos secinājumos lietās C-511/18 un C-512/18.

B. Valsts tiesības (kas piemērojamas šajā lietā)

1. Telecommunications Act 1984 [11]

6. Saskaņā ar 94. pantu ministrs var sniegt publiskā elektronisko komunikāciju tīkla operatoram tādus vispārīgus vai specifiskus norādījumus, kādus ministrs uzskata par nepieciešamiem vai nu valsts drošības, vai attiecību ar kādas citas valsts vai ārpus Apvienotās Karalistes esošas teritorijas valdību interesēs.

2. Data Retention and Investigatory Powers Act 2014 [12]

7. Šā likuma 1. pantā ir noteikts:

"(1) Ministrs var ar saglabāšanas rīkojumu pieprasīt publisko telekomunikāciju operatoram saglabāt attiecīgus komunikāciju datus, ja viņš uzskata, ka šis pieprasījums ir nepieciešams un samērīgs, ievērojot vienu vai vairākus mērķus, kas ir noteikti *Regulation of Investigatory Powers Act 2000* [(2000. gada Likums par izmeklēšanas pilnvaru regulējumu; turpmāk tekstā – "*RIPA*")] 22. panta 2. punkta a) līdz h) apakšpunktā.

(2) Saglabāšanas rīkojums var:

(a) attiekties uz kādu konkrētu operatoru vai uz visu veidu operatoriem,

7 Neskaitot šo lietu, tas ir darīts arī lietās C-511/18 un C-512/18, *La Quadrature du Net* u.c., 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.

11 1984. gada Telekomunikāciju likums; turpmāk tekstā – "1984. gada likums".

12 2014. gada Likums par datu saglabāšanu un izmeklēšanas pilnvarām; turpmāk tekstā – "DRIPA".

(b) noteikt visu datu vai visas kādas datu kategorijas saglabāšanu,

(c) precizēt laikposmu vai laikposmus, kuros ir jāsaglabā dati,

(d) noteikt citas prasības vai ierobežojumus attiecībā uz datu saglabāšanu,

(e) paredzēt atšķirīgus noteikumus dažādiem mērķiem,

(f) attiekties uz saglabāšanas rīkojuma pieņemšanas vai spēkā stāšanās laikā jau esošiem vai vēl neesošiem datiem.

(3) Ministrs var noteikumu formā sīkāk reglamentēt attiecīgo komunikāciju datu saglabāšanu.

(4) Šis regulējums var attiekties tostarp uz:

(a) prasībām pirms saglabāšanas rīkojuma pieņemšanas,

(b) maksimālo laikposmu, cik ilgi dati ir saglabājami saskaņā ar saglabāšanas rīkojumu,

(c) saglabāšanas rīkojuma saturu, pieņemšanu, spēkā stāšanos, pārskatīšanu, grozīšanu vai atcelšanu,

(d) saskaņā ar šo pantu saglabāto datu integritāti, drošību vai aizsardzību, piekļuvi datiem, kā arī to izpaušanu vai iznīcināšanu,

(e) attiecīgo prasību un ierobežojumu izpildi vai kontroli pār to ievērošanu,

(f) rīcības kodeksu darbam ar attiecīgajām prasībām, ierobežojumiem vai pilnvarām,

(g) atlīdzinājumu, ko ministrs (pakārtoti noteiktiem nosacījumiem vai bez tiem) veic attiecībā uz izmaksām, kas publisko telekomunikāciju operatoriem radušās, izpildot attiecīgās prasības un ierobežojumus,

[..]

(5) Maksimālais laikposms, kas ir paredzēts saskaņā ar 4. punkta b) apakšpunktu, nedrīkst pārsniegt 12 mēnešus no datuma, kas ir norādīts attiecībā uz datiem, uz kuriem attiecas 3. punktā minētie noteikumi.

(6) Publisko telekomunikāciju operators, kas saskaņā ar šo pantu saglabā attiecīgus datus par komunikācijām, nedrīkst izpaust šos datus, izņemot:

(a) kad tas tiek darīts saskaņā ar:

(i) [*RIPA*] 1. daļas 2. nodaļu vai

(ii) tiesas rīkojumu vai jebkādu citu tiesas atļauju vai orderi, vai

(b) kad tas ir paredzēts 3. punktā minētajos noteikumos.

(7) Ministrs var noteikumu formā pieņemt regulējumu, kas atbilst tam, kas ir pieņemts (vai var tikt pieņemts) saskaņā ar 4. punkta (d)–(g) apakšpunktu vai 6. punktu, attiecībā uz komunikāciju datiem, ko telekomunikāciju pakalpojumu sniedzēju saglabājuši saskaņā ar 2001. gada Likuma par cīņu pret terorismu, noziedzību un par drošību [*Anti-terrorism, Crime and Security Act 2001*] 102. pantā paredzēto rīcības kodeksu."

3. RIPA

8. Šā likuma 21. pantā ir noteikts:

"[..]

(4) Šajā nodaļā par "komunikāciju datiem" uzskata jebkuru no turpmāk minētā:

(a) jebkura informācija par datu plūsmu, ko (sūtītājs vai kāds cits) iekļauj komunikācijā vai pievieno tai jebkura pasta pakalpojuma vai telekomunikāciju sistēmas vajadzībām, ar ko šī komunikācija tiek vai var tikt nosūtīta,

(b) jebkura informācija, kas neietver nekādu komunikācijas saturu (izņemot jebkuru (a) apakšpunktā minēto informāciju) un attiecas uz jebkuras personas veiktu:

(i) jebkāda pasta vai telekomunikāciju pakalpojuma izmantošanu; vai

(ii) telekomunikāciju sistēmas daļas izmantošanu saistībā ar kāda telekomunikāciju pakalpojuma sniegšanu kādai personai vai šāda pakalpojuma izmantošanu, ko veic kāda persona,

(c) jebkura (a) vai (b) apakšpunktā neminēta informācija, kas pasta vai telekomunikāciju pakalpojumu sniedzošas personas rīcībā vai nu jau atrodas, vai tiek iegūta saistībā ar personām, kas saņem no tās pakalpojumu.

[..]

(6) Šajā pantā jēdziens "informācija par datu plūsmu" saistībā ar jebkuru komunikāciju nozīmē:

(a) jebkādus datus, kas identificē vai var identificēt jebkuru personu, ierīci vai vietu, kurai vai no kuras tiek nosūtīta komunikācija;

(b) jebkādus datus, kas identificē vai atlasa vai var identificēt vai atlasīt ierīci, pa kuru vai ar kuras palīdzību tiek vai var tikt nosūtīta komunikācija;

(c) jebkādus datus, kas ietver signālus telekomunikāciju sistēmas vajadzībām izmantotās ierīces iedarbināšanai jebkādas komunikācijas nosūtīšanai, un

(d) jebkādus datus, kas identificē konkrētā komunikācijā ietvertus vai tai pievienotus datus vai citus datus kā konkrētā komunikācijā ietvertus vai tai pievienotus datus.

[..]"

9. Likuma 22. pantā ir noteikts:

"(1) Šo pantu piemēro, ja šīs nodaļas vajadzībām par atbildīgo izraudzītā persona uzskata, ka šā panta 2. punktā uzskaitīto iemeslu dēļ ir nepieciešams iegūt jebkādus komunikāciju datus.

(2) Komunikāciju dati šajā punktā noteikto iemeslu dēļ ir jāiegūst, ja tie ir nepieciešami:

(a) valsts drošības interesēs,

(b) noziedzības novēršanas vai atklāšanas vai sabiedriskās kārtības traucējumu novēršanas mērķiem,

(c) Apvienotās Karalistes ekonomiskās labklājības interesēs, ja vien tās ir nozīmīgas arī valsts drošības interesēm,

(d) sabiedrības drošības interesēs,

(e) sabiedrības veselības aizsardzības mērķiem,

(f) jebkādu valsts administrācijas nodokļu, nodevu vai citu maksājumu, iemaksu vai maksu aprēķināšanas vai iekasēšanas mērķiem,

(g) fiziskas personas nāves, miesas bojājumu vai jebkāda kaitējuma tās fiziskajai vai garīgajai veselībai novēršanai vai fiziskas personas miesas bojājumu vai jebkāda kaitējuma tās fiziskajai vai garīgajai veselībai mazināšanai neatliekamos gadījumos,

(h) jebkādam citam mērķim (kas nav norādīts (a)–(g) apakšpunktā), kurš ir noteikts ministra izdotā rīkojumā saskaņā ar [*DRIPA*] 22. panta 2. punkta h) apakšpunktu.

(4) Ja vien 5. punktā nav noteikts citādi, atbildīgā persona – ja tai šķiet, ka telekomunikāciju vai pasta operatora rīcībā ir vai varētu būt komunikāciju dati, vai tas varētu šādus datus iegūt, – var pieprasīt telekomunikāciju vai pasta operatoram, lai tas:

(a) iegūst datus, ja tie ja nav operatora rīcībā, un

(b) katrā ziņā izpauž jebkādus savā rīcībā esošos vai vēlāk iegūtos datus.

(5) Atbildīgā persona nedrīkst izsniegt atļauju saskaņā ar 3. punktu vai iesniegt pieprasījumu saskaņā ar 4. punktu, ja vien tā neuzskata, ka attiecīgo datu iegūšana ar rīcību, kura atļauta vai prasīta atļaujā vai pieprasījumā, ir samērīga ar mērķi, kas ir sasniedzams ar datu iegūšanu."

10. Likuma 65. pantā ir noteikts, ka gadījumā, ja ir pamats uzskatīt, ka dati ir iegūti nepienācīgā veidā, var iesniegt sūdzību *Investigatory Powers Tribunal* (Izmeklēšanas pilnvaru tiesa, Apvienotā Karaliste).

II. Fakti un prejudiciālie jautājumi

11. Iesniedzējtiesa apgalvo, ka pamatlieta ir par masveida komunikāciju datu iegūšanu un izmantošanu, ko īsteno *United Kingdom Security and Intelligence Agencies* (Apvienotās Karalistes drošības un izlūkošanas aģentūras, turpmāk tekstā – "DIA").

12. Šādi dati ir par to "kas" un "kad, kur, kā un ar ko" lieto tālruni un internetu. Tie ietver datus par to, kur atrodas mobilo un fiksēto tālruņa līnijas, no kurām tiek veikti vai saņemti zvani, kā arī to, kur atrodas interneta piekļuvei izmantotie datori. Tie neietver šo komunikāciju saturu, ko var iegūt tikai ar tiesas rīkojumu.

13. Prasītāja pamatlietā (*Privacy International*, nevalstiska cilvēktiesību aizsardzības organizācija) ir cēlusi prasību iesniedzējtiesā, jo uzskata, ka ar DIA veikto minēto datu iegūšanu un izmantošanu tiek pārkāptas Eiropas Cilvēktiesību [un pamatbrīvību aizsardzības] konvencijas (turpmāk tekstā – "ECPAK") 8. pantā nostiprinātās tiesības uz privātās dzīves neaizskaramību un šīs darbības ir pretrunā Savienības tiesībām.

14. Atbildētājas iestādes [13] apgalvo, ka to veiktā šādu pilnvaru izmantošana ir likumīga un būtiska, tostarp valsts drošības aizsardzībai.

15. Iesniedzējtiesas nolēmumā ir teikts, ka saskaņā ar ministra sniegtajiem norādījumiem atbilstoši 1984. gada likuma 94. pantam DIA saņem masveida komunikāciju datus no elektronisko komunikāciju publisko tīklu operatoriem.

16. Minētie dati ietver informāciju par lietotāju datu plūsmu un atrašanās vietu, kā arī par sociālām, komerciālām un finansiālām aktivitātēm, komunikācijām un braucieniem. Kad dati nonāk DIA rīcībā, tās nodrošina to drošu saglabāšanu, izmantojot vispārīgas metodes (piemēram, filtrēšana un apkopošana), proti, tādas, kas nav vērstas uz specifiskiem un zināmiem mērķiem.

17. Iesniedzējtiesa uzskata, ka ir pierādīts, ka šīs metodes ir būtiskas DIA darbam cīņā pret nopietniem sabiedrības drošības apdraudējumiem, tostarp terorismu, spiegošanu un kodolieroču izplatīšanu. DIA spēja iegūt un izmantot datus ir būtiski svarīga Apvienotās Karalistes valsts drošības aizsardzībai.

18. Iesniedzējtiesa uzskata, ka strīdīgie pasākumi atbilst valsts tiesībām un ECPAK 8. pantam. Tomēr tai ir šaubas par šo pasākumu atbilstību Savienības tiesībām, ņemot vērā spriedumu *Tele2 Sverige* un *Watson*.

19. Šajā kontekstā minētā tiesa uzdod Tiesai šādus jautājumus:

"1) Vai, ņemot vērā LES 4. pantu un [Direktīvas 2002/58] 1. panta 3. punktu, ministra rīkojumā elektroniskā komunikāciju tīkla operatoram izteiktā prasība sniegt masveida komunikāciju datus dalībvalsts drošības un izlūkošanas aģentūrām (DIA) ietilpst Savienības tiesību aktu un [Direktīvas 2002/58] piemērošanas jomā?

2) Ja atbilde uz 1. jautājumu ir apstiprinoša, vai uz šādu ministra rīkojumu attiecināmas kādas no *Watson* [14] prasībām vai citas prasības papildus ECPAK noteiktajām? Gadījumā, ja tas tā ir, kā un kādā mērā šīs prasības ir attiecināmas, ņemot vērā DIA būtisko nepieciešamību izmantot masveida iegūšanas un automatizētas apstrādes metodes, lai aizsargātu valsts drošību, un to, cik lielā mērā šādas iespējas, ja tās atbilstu ECPAK, var tikt būtiski ierobežotas, izvirzot šādas prasības?"

20. Iesniedzējtiesa uzdod savus jautājumus šādā kontekstā:

"a) [DIA] iespējas izmantot tām sniegtos [masveida komunikāciju datus] ir būtiskas, lai aizsargātu Apvienotās Karalistes valsts drošību, tostarp pretterorisma, pretizlūkošanas un kodolieroču izplatīšanas apkarošanas jomās;

b) DIA veiktas [šo datu] izmantošanas būtiska iezīme ir iepriekš nezināmu apdraudējumu valsts drošībai atklāšana, izmantojot neselektīvas masveida metodes, kas ir balstītas uz [šo datu] apkopošanu vienā vietā. Tā galvenokārt ir noderīga tam, lai ātri identificētu un izvērstu mērķi, kā arī rastu rīcības pamatu tūlītēja apdraudējuma gadījumā;

c) tāpēc elektronisko komunikāciju tīkla operatoram netiek prasīts saglabāt [masveida komunikāciju datus] (ilgāk par laikposmu, kādam tas nepieciešams parastajām komercdarbības vajadzībām), ko saglabā tikai valsts (DIA);

13 *Secretary of State for Foreign and Commonwealth Affairs* (ārlietu un sadraudzības lietu ministrs), *Secretary of State for the Home Department* (iekšlietu ministrs) un trīs Apvienotās Karalistes DIA, proti, *Government Communications Headquarters* (Valdības komunikāciju galvenā pārvalde; *GCHQ*), *Security Service* (Drošības dienests; *MI5*), un *Secret Intelligence Service* (Slepenais izlūkošanas dienests; *MI6*).

14 Proti, sprieduma *Tele2 Sverige* un *Watson* judikatūra.

d) valsts tiesa (pakārtoti vairākiem vēl izspriežamiem jautājumiem) ir konstatējusi, ka ar DIA veikto [šo datu] izmantošanu saistītās garantijas atbilst ECPAK, un

e) valsts tiesa ir konstatējusi, ka prasību, kas paredzētas [spriedumā *Tele2 Sverige* un *Watson*], izvirzīšana attiecīgajā gadījumā padarītu neefektīvus pasākumus, ko DIA veic, lai aizsargātu valsts drošību, un līdz ar to pakļautu Apvienotās Karalistes valsts drošību riskam."

III. Tiesvedība Tiesā

21. Lūgums sniegt prejudiciālu nolēmumu tika reģistrēts Tiesā 2017. gada 31. oktobrī.

22. Rakstveida apsvērumus ir iesniegušas Vācijas, Beļģijas, Apvienotās Karalistes, Čehijas, Kipras, Spānijas, Igaunijas, Francijas, Ungārijas, Īrijas, Latvijas, Nīderlandes, Norvēģijas, Polijas, Portugāles un Zviedrijas valdības, kā arī Komisija.

23. 2019. gada 9. septembrī notika tiesas sēde, kas tika rīkota kopā ar tiesas sēdēm lietās C-511/18, C-512/18 un C-520/18, kurās piedalījās četru prejudiciālā nolēmuma tiesvedību dalībnieki, iepriekš minētās valdības, kā arī Komisija un Eiropas Datu aizsardzības uzraudzītājs.

IV. Analīze

A. Par Direktīvas 2002/58 piemērošanas jomu un valsts drošības izslēgšanu (pirmais prejudiciālais jautājums)

24. Secinājumos, ko šajā pašā datumā sniedzu lietās C-511/18 un C-512/18, skaidroju iemeslus, kādēļ, manuprāt, "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" [15].

25. Savu argumentu izklāstā aplūkoju 2006. gada 30. maija Tiesas sprieduma Parlaments/Padome un Komisija [16] un sprieduma *Tele2 Sverige* un *Watson* ietekmi, atbalstot interpretāciju, kas tos abus saskaņo [17].

26. Šajos pašos secinājumos pēc tam, kad ir apstiprināta Direktīvas 2002/58 piemērojamība, aplūkoju tajā paredzēto valsts drošības izslēgšanu un LES 4. panta 2. punkta ietekmi [18].

27. Neskarot turpinājumā izklāstīto, lūdzu skatīt manis teikto gan jau nupat minētajos, gan lietā C-520/18 sniegtajos secinājumos.

15 Secinājumi lietās C-511/18 un C-512/18, 42. punkts.

16 Lietas C-317/04 un C-318/04, EU:C:2006:346.

17 Secinājumi lietās C-511/18 un C-512/18, 44.–76. punkts.

18 Turpat, 77.–90. punkts.

1. Direktīvas 2002/58 piemērošana šajā lietā

28. Saskaņā ar šajā tiesvedībā aplūkotajām tiesību normām elektronisko komunikāciju pakalpojumu sniedzējiem ir pienākums ne tikai saglabāt datus, bet arī apstrādāt datus, kas ir to rīcībā tāpēc, ka tie sniedz pakalpojumu Savienības publisko komunikāciju tīklu lietotājiem [19].

29. Proti, minētajiem operatoriem ir obligāti jānosūta šie dati DIA. Šajā lietā tiek vaicāts par to, vai Direktīvas 2002/58 15. panta 1. punkts atļauj šādu nosūtīšanu, ņemot vērā tās mērķi, automātiski izslēgt no Savienības tiesību piemērošanas jomas.

30. Manuprāt, tā tas nav. Tā kā minēto datu saglabāšana un tās tālāka nosūtīšana var tikt uzskatīta par personas datu apstrādi, ko veic elektronisko telekomunikāciju pakalpojumu sniedzēji, tā dabiski iekļaujas Direktīvas 2002/58 piemērošanas jomā.

31. Nav tā, ka šo konstatējumu atsvērtu valsts drošības apsvērumi – kā to uzskata iesniedzējtiesa – un tādējādi attiecīgais pienākums neietilptu Savienības tiesību piemērošanas jomā. Manuprāt, kā jau teicu, pakalpojumu sniedzējiem tiek uzlikts pienākums apstrādāt datus saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu Savienības publiskos komunikāciju tīklos, kas tieši atbilst Direktīvas 2002/58 piemērošanas jomai, kā noteikts tās 3. panta 1. punktā.

32. Balstoties uz šo premisu, runa ir vairs ne par DIA darbībām (kas, kā jau teicu, varētu ietilpt Savienības tiesību piemērošanas jomā, ja tās neskartu elektronisko komunikāciju operatorus), bet gan par šo operatoru rīcībā esošu datu saglabāšanu un tālāku nosūtīšanu. Raugoties no šā viedokļa, uz kārts ir liktas Savienības garantētās pamattiesības.

33. Arī šajā strīdā izšķirošā nozīme ir pienākumam visaptveroši un nediferencēti saglabāt datus, kuriem valsts iestādēm tiek sniegta piekļuve.

2. Atsaukšanās uz valsts drošību

34. Tā kā šajā lietā iesniedzējtiesa liek īpašu uzvaru uz DIA darbību, kas skar valsts drošību, atļaušos citēt dažus punktus no saviem šajā pašā dienā sniegtajiem secinājumiem lietās C-511/18 un C-512/18 par šo jautājumu:

"77. Nacionālā 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 darbībām.

78. Uz kādām darbībām attiecas Direktīvas 2002/58 1. panta 3. punkts? Manuprāt, pati *Conseil d'État* (Valsts padome) sniedz labu piemēru, minēdama 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" [..].

19 Direktīvas 2002/58 2. pantā ir noteikts, ka tajā ir piemērojamas definīcijas, kas rodamas Direktīvā 95/46. Savukārt šīs nupat minētās direktīvas 2. panta b) punktā ir noteikts, ka "personu datu apstrāde" ir "jebkura ar personas datiem veikta darbība vai darbību kopums ar vai bez automatizētiem līdzekļiem – kā vākšana, reģistrēšana, organizēšana, uzglabāšana, piemērošana vai pārveidošana, labošana, konsultēšana, izmantošana, *atklāšana, pielietojot pārsūtīšanu*, izplatīšanu vai *darot tos pieejamus citādā veidā*, grupēšana vai savienošana, piekļuves noslēgšana, dzēšana vai iznīcināšana" (mans izcēlums).

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 viņām 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.

[..]

82. [..] uzskatu, ka vērtīgu norādi var sniegt kritērijs, kas noteikts Pamatlēmumā 2006/960/TI [..], 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" [..].

[..]

84. [..] 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. [Direktīvas 2002/58 11. 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.

[..]

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 leģislatīvu 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 leģislatīvus pasākumus, būtu lieka."

3. No sprieduma Tele2 Sverige un Watson piemērošanas šajā lietā izrietošās sekas

35. Iesniedzējtiesa ir koncentrējusies uz spriedumā *Tele2 Sverige* un *Watson* Tiesas sniegto interpretāciju un izklāsta, kādas grūtības, tās ieskatā, rastos, ja šī interpretācija būtu jāpiemēro šajā lietā.

36. Proti, spriedumā *Tele2 Sverige* un *Watson* tika izklāstīti nosacījumi, kādiem ir jāatbilst valsts tiesību aktiem, kuros tiek noteikts pienākums saglabāt informāciju par datu plūsmu un atrašanās vietas datus, lai tiem vēlāk varētu piekļūt valsts iestādes.

37. Tāpat kā lietās C-511/18 un C-512/18 un analoģisku iemeslu dēļ uzskatu, ka valsts tiesību normas, uz kurām attiecas šis lūgums sniegt prejudiciālo nolēmumu, neatbilst spriedumā *Tele2 Sverige* un *Watson* izklāstītajiem nosacījumiem, jo paredz personas datu visaptverošu un nediferencētu saglabāšanu, kas sniedz detalizētu pārskatu par attiecīgo personu dzīvi ilgstošā laikposmā.

38. Abu minēto lietu secinājumos apsvēru, vai būtu iespējams niansēt vai papildināt minētajā spriedumā rodamo judikatūru, ņemot vērā sekas, ko tā rada cīņai pret terorismu vai valsts aizsardzībai pret citiem līdzīgiem apdraudējumiem valsts drošībai.

39. Turpinājumā atļaujos arī citēt dažus šo secinājumu punktus, kuros būtībā apgalvoju – tā kā ir iespējams niansēt minēto judikatūru, tā būtu jāapstiprina pēc būtības:

"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 [..] 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. [..]

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. punktu [..], kompetento iestāžu piekļuve šai informācijai ir jānodrošina, ievērojot Tiesas izvirzītos nosacījumus, kuru izvērtējumu lūdzu skatīt manos secinājumos lietā C-520/18 [..].

138. Līdz ar to arī šajā gadījumā valsts tiesiskajā regulējumā ir jāparedz materiāltiesiskie un procesuālie nosacījumi, kas reglamentē kompetento valsts iestāžu piekļuvi saglabātajiem datiem [..]. Lūgumos sniegt prejudiciālu nolēmumu aplūkotajos 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 iesaistītas [..].

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 pieteikumu [..]. Tādējādi jautājumos, kur likuma abstraktais vērtējums nesniedzas, vērtējumu *in concreto* nodrošina šī neatkarīgā iestāde, apņemdamās vienlīdz garantēt valsts drošību un pilsoņu pamattiesību aizsardzību."

B. Par otro prejudiciālo jautājumu

40. Iesniedzējtiesa formulē savu otro jautājumu gadījumam, ja atbilde uz pirmo jautājumu būtu apstiprinoša. Tādā gadījumā tā vēlētos zināt, kādas "citas prasības papildus ECPAK noteiktajām" vai prasības, kas izriet no sprieduma *Tele2 Sverige* un *Watson*, būtu piemērojamas.

41. Šajā ziņā tā apgalvo, ka sprieduma *Tele2 Sverige* un *Watson* nosacījumu piemērošana "padarītu neefektīvus pasākumus, ko DIA veic, lai aizsargātu valsts drošību".

42. Tā kā uz pirmo jautājumu ierosinu atbildēt noliedzoši, otro jautājumu nav vajadzības iztirzāt. Otrais jautājums, kā uzsver pati iesniedzējtiesa, ir pakārtots tam, vai visu Apvienotās Karalistes lietotāju personas datu, kas elektronisko komunikāciju operatoriem būtu jānosūta DIA, "masveida iegūšanas un automatizētas apstrādes metodes" tiek atzītas par saderīgām ar Savienības tiesībām.

43. Ja Tiesa uzskatītu par vajadzīgu atbildēt uz otro jautājumu, manuprāt, tai būtu jāapstiprina minētie no sprieduma *Tele2 Sverige* un *Watson* izrietošie nosacījumi attiecībā uz:

– vispārējas piekļuves datiem aizliegumu;

– nepieciešamību saņemt tiesas vai neatkarīgas administratīvas iestādes iepriekšēju atļauju, lai šo piekļuvi leģitimētu;

– pienākumu informēt attiecīgās personas, ja vien tas neapdraud pasākuma efektivitāti;

– datu saglabāšanu Savienības teritorijā.

44. Kā jau teicu, pietiktu vien ar to, ka šie saistošie nosacījumi tiktu apstiprināti to iemeslu dēļ, kurus esmu izklāstījis secinājumos lietās C-511/18 un C-512/18, kā arī C-520/18, un nebūtu vajadzības noteikt "citas" papildu prasības iesniedzējtiesas izpratnē.

V. Secinājumi

45. Pamatojoties uz visu iepriekš izklāstīto, ierosinu Tiesai atbildēt *Investigatory Powers Tribunal* (Izmeklēšanas pilnvaru tiesa, Apvienotā Karaliste) šādi:

LES 4. pants un 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) 1. panta 3. punkts ir interpretējami tādējādi, ka tiem ir pretrunā tāds valsts tiesiskais regulējums, ar kuru elektronisko komunikāciju tīklu operatoram tiek uzlikts pienākums sniegt dalībvalsts drošības un izlūkošanas aģentūrām "masveida komunikāciju datus", iepriekš tos visaptveroši un nediferencēti savācot.

Pakārtoti:

Dalībvalsts drošības un izlūkošanas aģentūru piekļuvei datiem, ko nosūta elektronisko komunikāciju tīklu operatori, ir jāatbilst 2016. gada 21. decembra spriedumā *Tele2 Sverige* un *Watson* (C-203/15 un C-698/15, EU:C:2016:970) paredzētajiem nosacījumiem.