Judikatūras krājums

ĢENERĀLADVOKĀTA MANUELA KAMPOSA SANČESA-BORDONAS
[*MANUEL CAMPOS SÁNCHEZ-BORDONA*]
SECINĀJUMI,
sniegti 2023. gada 20. aprīlī [1]

Lieta C-548/21

C. G.
pret
Bezirkshauptmannschaft Landeck

(*Landesverwaltungsgericht Tirol* (Tiroles federālās zemes Administratīvā tiesa, Austrija) lūgums sniegt prejudiciālu nolēmumu)

Lūgums sniegt prejudiciālu nolēmumu – Telekomunikācijas – Personas datu aizsardzība – Direktīva (ES) 2016/680 – Kriminālprocess – Valsts iestāžu mēģinājums piekļūt mobilajā tālrunī saglabātajiem datiem bez tiesas vai neatkarīgas administratīvas iestādes atļaujas

1. Lūgums sniegt prejudiciālu nolēmumu būtībā ir par nosacījumiem, kas ir jāizpilda policijas iestādēm, lai piekļūtu tādas personas mobilajā tālrunī saglabātajiem datiem, attiecībā uz kuru tiek veikta krimināllizmeklēšana.

2. Kā mēģināšu izskaidrot, šis lūgums sniegt prejudiciālu nolēmumu ir visnotaļ problemātisks pieņemamības ziņā. Ja Tiesa tomēr nolemtu izskatīt lietu pēc būtības, tai būs jālemj par Direktīvas 2002/58/EK [2] un Direktīvas (ES) 2016/680 [3] piemērošanas jomām.

[1] Oriģinālvaloda – spāņu.

[2] 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.).

[3] Eiropas Parlamenta un Padomes Direktīva (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI (OV 2016, L 119, 89. lpp.).

I. Atbilstošās tiesību normas

A. Savienības tiesības

1. Regula (ES) 2016/679[4]

3. VDAR 2. panta (“Materiālā darbības joma”) 2. punkts noteic:

“Šo regulu nepiemēro personas datu apstrādei:

[..]

d) ko veic kompetentas iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu krimināsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu.”

2. Direktīva 2016/680

4. Direktīvas 2. apsvērumā ir teikts:

“Noteikumiem par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un tās principiem [..] būtu jāievēro pamattiesības un pamatbrīvības, jo īpaši tiesības uz personas datu aizsardzību. Šīs direktīvas mērķis ir palīdzēt izveidot brīvības, drošības un tiesiskuma telpu.”

5. Tās 46. apsvērumā ir teikts:

“Jānodrošina datu subjekta jebkādu tiesību ierobežojumu atbilstība hartai un ECTK, kā tas interpretēts attiecīgi Tiesas un Eiropas Cilvēktiesību tiesas [5] judikatūrā, un jo īpaši jānodrošina minēto tiesību un brīvību būtības ievērošana.”

6. Šīs direktīvas 49. apsvērums ir formulēts šādi:

“Ja personas dati tiek apstrādāti krimināllizmeklēšanas un tiesvedības krimināllietās gaitā, dalībvalstīm būtu jāvar noteikt, ka tiesības uz informāciju, piekļuvi personas datiem vai to labošanu vai dzēšanu un apstrādes ierobežošanu īsteno saskaņā ar valsts noteikumiem par tiesvedību.”

7. Tās 1. pants (“Priekšmets un mērķi”) noteic:

“1. Šajā direktīvā ir paredzēti noteikumi par fizisko personu aizsardzību attiecībā uz personas datu apstrādi, ko kompetentās iestādes veic, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, vai izpildītu krimināsodus, tostarp lai pasargātu no draudiem sabiedriskajai drošībai un tos novērstu.

[4] 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.). Turpmāk tekstā – “VDAR”.

[5] Turpmāk tekstā – “ECT”.

2. Saskaņā ar šo direktīvu dalībvalstis:

a) aizsargā fizisko personu pamattiesības un pamatbrīvības, un jo īpaši viņu tiesības uz personas datu aizsardzību; un

[..].

3. Šī direktīva dalībvalstīm neliedz paredzēt lielākas garantijas nekā tās, kas noteiktas šajā direktīvā, lai aizsargātu datu subjekta tiesības un brīvības attiecībā uz kompetento iestāžu veiktu personas datu apstrādi."

8. Direktīvas 2. panta ("Darbības joma") 1. punkts noteic:

"Šo direktīvu piemēro personas datu apstrādei, ko veic kompetentās iestādes 1. panta 1. punktā izklāstītajos nolūkos."

9. Tās 3. pants ("Definīcijas") noteic:

"Šajā direktīvā:

[..]

2) "apstrāde" ir jebkura ar personas datiem vai personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, piemēram, vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana;

[..]

7) "kompetentā iestāde":

   a) jebkura publiska iestāde, kuras kompetencē ir novērst, izmeklēt, atklāt noziedzīgus nodarījumus vai saukt pie atbildības par tiem, vai izpildīt krimināls odus, tostarp pasargāt no draudiem sabiedriskajai drošībai un tos novērst; vai

[..]."

10. Minētās direktīvas 4. panta ("Principi, kas saistīti ar personas datu apstrādi") 1. punkts noteic:

"Dalībvalstis paredz, ka personas dati:

a) tiek apstrādāti likumīgi un godprātīgi;

b) tiek vākti konkrētos, skaidros un leģitīmos nolūkos, un tie netiek apstrādāti ar minētajiem nolūkiem nesaderīgā veidā;

c) ir atbilstīgi, būtiski un nav pārmērīgi, ņemot vērā nolūkus, kādos tos apstrādā;

[..]

e) tiek glabāti veidā, kas pieļauj datu subjektu identifikāciju, ne ilgāk, kā tas ir nepieciešams tiem nolūkiem, kādos tos apstrādā;

f) tiek apstrādāti tā, lai tiktu nodrošināta atbilstīga personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstīgus tehniskos vai organizatoriskos pasākumus."

11. Minētās direktīvas 8. pantā ("Apstrādes likumīgums") ir norādīts:

"1. Dalībvalstis paredz, ka apstrāde ir likumīga tikai tad un tiktāl, ciktāl šī apstrāde ir nepieciešama tā uzdevuma izpildei, ko kompetentā iestāde veic 1. panta 1. punktā minētajos nolūkos, un ka tā balstās uz Savienības vai dalībvalsts tiesībām.

2. Dalībvalsts tiesībās, ar ko regulē apstrādi šīs direktīvas darbības jomā, precizē vismaz apstrādes mērķus, apstrādājamos personas datus un apstrādes nolūkus."

12. Tās 13. pantā ("Informācija, ko dara pieejamu vai sniedz datu subjektam") ir noteikts:

"1. Dalībvalstis paredz, ka pārzinis datu subjektam dara pieejamu vismaz šādu informāciju:

[..]

d) tiesības iesniegt sūdzību uzraudzības iestādē un uzraudzības iestādes kontaktinformācija;

[..].

3. Dalībvalstis var pieņemt leģislatīvus pasākumus, lai atliktu, ierobežotu vai nesniegtu informāciju datu subjektam, ievērojot 2. punktu, ciktāl un kamēr šāds pasākums ir nepieciešams un samērīgs demokrātiskā sabiedrībā, pienācīgi ņemot vērā attiecīgās fiziskās personas pamattiesības un leģitīmās intereses, lai:

a) novērstu, ka tiek traucētas oficiālas vai juridiskas pārbaudes, izmeklēšanas vai procedūras;

b) novērstu, ka tiek kaitēts noziedzīgu nodarījumu novēršanai, atklāšanai, izmeklēšanai vai saukšanai pie atbildības par tiem, vai kriminālsodu izpildei;

c) aizsargātu sabiedrisko drošību;

d) aizsargātu valsts drošību;

e) aizsargātu citu personu tiesības un brīvības.

[..]"

13. Saskaņā ar 15. panta ("Piekļuves tiesību ierobežojumi") 1. punktu:

"Dalībvalstis var pieņemt leģislatīvus pasākumus, ar ko pilnībā vai daļēji ierobežo datu subjekta piekļuves tiesības, ciktāl un tik ilgi, kamēr šāds daļējs vai pilnīgs ierobežojums ir nepieciešams un samērīgs pasākums demokrātiskā sabiedrībā, pienācīgi ņemot vērā attiecīgās fiziskās personas pamattiesības un leģitīmās intereses, lai:

a) novērstu, ka tiek traucētas oficiālas vai juridiskas pārbaudes, izmeklēšanas vai procedūras;

b) novērstu, ka tiek kaitēts noziedzīgu nodarījumu novēršanai, atklāšanai, izmeklēšanai vai saukšanai pie atbildības par tiem, vai kriminālsodu izpildei;

c) aizsargātu sabiedrisko drošību;

d) aizsargātu valsts drošību;

e) aizsargātu citu personu tiesības un brīvības."

14. Saskaņā ar 27. pantu ("Novērtējums par ietekmi uz datu aizsardzību"):

"1. Ja apstrādes veids, jo īpaši, izmantojot jaunās tehnoloģijas un ņemot vērā apstrādes raksturu, apmēru, kontekstu un nolūkus, varētu radīt augstu risku fizisko personu tiesībām un brīvībām, dalībvalstis paredz, ka pārzinis pirms apstrādes veic novērtējumu par to, kā plānotās apstrādes darbības ietekmēs personas datu aizsardzību.

2. Šā panta 1. punktā minētajā novērtējumā ietver vismaz plānoto apstrādes darbību vispārīgu aprakstu, novērtējumu par riskiem datu subjektu tiesībām un brīvībām, pasākumus, kas paredzēti minēto risku novēršanai, garantijas, drošības pasākumus un mehānismus, ar kuriem nodrošina personas datu aizsardzību un uzskatāmi parāda, ka ir ievērota šī direktīva, ņemot vērā datu subjektu un citu attiecīgo personu tiesības un leģitīmās intereses."

15. Direktīvas 28. pants ("Iepriekšēja apspriešanās ar uzraudzības iestādi") noteic:

"1. Dalībvalstis paredz, ka pārzinis vai apstrādātājs pirms tādu personas datu apstrādes, ko ietvers jaunizveidotā kartotēkā, apspriežas ar uzraudzības iestādi gadījumos, ja:

a) šīs direktīvas 27. pantā paredzētajā novērtējumā par ietekmi uz datu aizsardzību ir norādīts, ka gadījumā, ja pārzinis neveiktu pasākumus riska mazināšanai, apstrāde radītu augstu risku; vai

b) apstrādes veids, jo īpaši, izmantojot jaunas tehnoloģijas, mehānismus vai procedūras, ir saistīts ar augstu risku datu subjektu tiesībām un brīvībām.

[..]"

16. Tās 54. pantā ("Tiesības uz efektīvu tiesību aizsardzību tiesā pret pārzini vai apstrādātāju") ir noteikts:

"Neskarot pieejamos administratīvos vai ārpustiesas tiesību aizsardzības līdzekļus, tostarp tiesības iesniegt sūdzību uzraudzības iestādē, ievērojot 52. pantu, dalībvalstis datu subjektiem paredz tiesības uz efektīvu tiesību aizsardzību tiesā, ja viņš uzskata, ka viņa tiesības, kas izklāstītas

saskaņā ar šo direktīvu pieņemtos noteikumos, ir aizskartas personas datu apstrādes rezultātā, kura neatbilst minētajiem noteikumiem."

B. Valsts tiesības

17. *Strafprozessordnung*[6] 18. pants uzliek kriminālpolicijai pienākumus tiesu varas īstenošanā krimināllietās (1. punkts). Kriminālpolicijas izmeklēšanas ir drošības iestāžu kompetencē (2. punkts). Sabiedriskās drošības dienesta iestādes veic kriminālpolicijas izpilddarbības, kas ietver noziedzīgu nodarījumu izmeklēšanu un kriminālvajāšanu par tiem (3. punkts).

18. Saskaņā ar *StPO* 99. pantu kriminālpolicija veic izmeklēšanu pēc savas ierosmes vai uz sūdzības pamata un tai ir jāievēro prokuratūras un tiesu rīkojumi (1. punkts). Ja izmeklēšanas pasākumam ir nepieciešams prokuratūras rīkojums, nenovēršama apdraudējuma gadījumā kriminālpolicija var veikt attiecīgās darbības arī bez šāda rīkojuma. Tādā gadījumā tai nekavējoties ir jāpieprasa atļauja (2. punkts).

19. Saskaņā ar *StPO* 111. panta 2. punktu, ja datu nesējos saglabāto informāciju ir nepieciešams izgūt, katrai personai ir pienākums atļaut piekļuvi šai informācijai un pēc pieprasījuma nodot elektronisko datu nesēju parasti izmantojamā datu arhivēšanas formātā vai ļaut to izgatavot. Turklāt personai jāatļauj izgatavot datu nesējos saglabātās informācijas rezerves kopiju.

II. Fakti, pamatlieta un prejudiciālie jautājumi

20. C. G. ir Vācijas pilsonis, kas strādā un dzīvo Austrijā.

21. 2021. gada 23. februārī, veicot narkotisko vielu klātesamības pārbaudi, Insbrukas (Austrija) muitas iestādes amatpersonas izņēma prasītājam adresētu paku, kurā bija 85 grami kanabisa.

22. 2021. gada 6. martā divi policijas darbinieki nopratināja C. G. par pakas nosūtītāju un veica kratīšanu viņa dzīvesvietā. Kratīšanas laikā tika izņemts viņa mobilais tālrunis (kurā bija *SIM* karte un *SD* karte) un viņam tika izsniegts izņemšanas protokols.

23. C. G. tika pieprasīts sniegt piekļuvi viņa mobilā tālruņa savienojuma datiem, taču viņš attiecās izpaust tālruņa piekļuves kodu.

24. *Bezirkspolizeikommando Landeck* (Landekas rajona policijas iecirknis, Austrija) neizdevās atbloķēt mobilo tālruni. Tas tika nosūtīts *Bundeskriminalamt* (Federālais kriminālpolicijas birojs) Vīnē (Austrija), kurā atkal tika nesekmīgi mēģināts atbloķēt tālruni un iegūt tajā saglabātos datus.

25. Brīdī, kad policija veica šīs darbības, to pamatā nebija nedz prokuratūras rīkojuma, nedz tiesas nolēmuma.

26. 2021. gada 31. martā C. G. cēla prasību *Landesverwaltungsgericht Tirol* (Tiroles federālās zemes Administratīvā tiesa, Austrija) par viņam piemēroto piespiedu pasākumu un apstrīdēja viņa mobilā tālruņa izņemšanu. Tas viņam tika atdots 2021. gada 20. aprīlī.

[6] Kriminālprocesa kodekss. Turpmāk tekstā – "*StPO*". *BGBl* Nr. 631/1975, redakcijā, kas piemērojama lietā (*BGBl* I, Nr. 24/2020).

27. C. G. netika informēts par mēģinājumiem analizēt viņa mobilā tālruņa saturu; to viņš uzzināja tāpēc, ka policijas darbinieks, kas bija veicis izņemšanu un pēc tam sācis digitālo analīzi, tika nopratināts kā liecinieks, kuram ir pienākums teikt patiesību. Šie mēģinājumi arī netika dokumentēti kriminālpolicijas lietā.

28. Šajā kontekstā *Landesverwaltungsgericht Tirol* (Tiroles federālās zemes Administratīvā tiesa) uzdeva Tiesai šādus prejudiciālus jautājumus:

"1) Vai Direktīvas 2002/58 – redakcijā ar grozījumiem, kas izdarīti ar Direktīvu 2009/136/EK, – 15. panta 1. punkts (vajadzības gadījumā lasot to kopsakarā ar 5. pantu) [..] Hartas 7. un 8. panta gaismā ir jāinterpretē tādējādi, ka valsts iestāžu piekļuve mobilajos tālruņos saglabātajiem datiem ir uzskatāma par tādu iejaukšanos šajos Hartas pantos nostiprinātajās pamattiesībās, kas ir tik būtiska, ka noziedzīgu nodarījumu prevencijas, izmeklēšanas, atklāšanas un kriminālvajāšanas jomā šī piekļuve ir atļaujama tikai smagas noziedzības apkarošanas mērķiem?

2) Vai Direktīvas 2002/58 – redakcijā ar grozījumiem, kas izdarīti ar Direktīvu 2009/136/EK, – 15. panta 1. punkts, lasot to Pamattiesību hartas 7., 8. un 11. panta, kā arī 52. panta 1. punkta gaismā, ir jāinterpretē tādējādi, ka ar to netiek pieļauts tāds valsts tiesiskais regulējums kā [*StPO*] 18. pants, lasot to kopsakarā ar šā likuma 99. panta 1. punktu, atbilstoši kuram drošības iestādes kriminālizmeklēšanas gaitā bez tiesas vai neatkarīgas iestādes atļaujas pašas sev piešķir visaptverošu un nekontrolētu piekļuvi visiem mobilajā tālrunī saglabātajiem digitālajiem datiem?

3) Vai [..] Hartas 47. pants, vajadzības gadījumā lasot to kopsakarā ar 41. un 52. pantu, no pušu procesuālo tiesību vienlīdzības un efektīva tiesību aizsardzības līdzekļa viedokļa ir jāsaprot tādējādi, ka tam ir pretrunā tāds valsts tiesiskais regulējums, ar kuru, kā [*StPO*] 18. pantā, lasot to kopsakarā ar šā likuma 99. panta 1. punktu, tiek pieļauts, ka mobilais tālrunis tiek digitāli izvērtēts, par šo faktu neinformējot datu subjektu pirms tam vai vismaz pēc šā pasākuma veikšanas?"

III. Tiesvedība Tiesā

29. Lūgums sniegt prejudiciālu nolēmumu Tiesā tika reģistrēts 2021. gada 6. septembrī.

30. 2021. gada 20. oktobrī Tiesa lūdza iesniedzējtiesu paust viedokli, vai Direktīvai 2016/680 šajā lietā varētu būt nozīme.

31. 2021. gada 11. novembrī iesniedzējtiesa atbildēja, ka pamatlietā Direktīva 2016/680 ir piemērojama.

32. Rakstveida apsvērumus ir iesniegušas Vācijas, Austrijas, Kipras, Dānijas, Igaunijas, Francijas, Ungārijas, Īrijas, Nīderlandes, Norvēģijas, Polijas un Zviedrijas valdības, kā arī Eiropas Komisija.

33. 2023. gada 16. janvāra tiesas sēdē piedalījās gan visas rakstveida apsvērumus iesniegušās valdības – izņemot Vācijas, Ungārijas un Polijas valdību –, kā arī Somijas valdība. Tiesa tās visas aicināja koncentrēt savus argumentus uz Direktīvu 2016/680 un mutiski atbildēt uz vairākiem jautājumiem par šo direktīvu.

IV. Juridiskā analīze

A. Nepieņemamība

34. Jautājumu sākotnējā formulējumā iesniedzējtiesa lūdza interpretēt tikai Direktīvu 2002/58. Tomēr gandrīz visas personas, kas iestājušās lietā, ir vienisprātis, ka attiecīgā direktīva šajā lietā nav piemērojama un tādējādi tās interpretācija nav nepieciešama, lai atrisinātu strīdu.

35. Direktīva 2002/58 – kā teikts tās 3. pantā – reglamentē "[..] personas datu apstrādi saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu publiskos komunikāciju tīklos [Savienībā], tostarp publiskos komunikāciju tīklos, kuros var izmantot datu vākšanas un identifikācijas ierīces".

36. Tiesa ir atzinusi, ka tad, "ja dalībvalstis tieši īsteno pasākumus, ar kuriem tiek izdarīta atkāpe no elektronisko komunikāciju konfidencialitātes, neuzliekot apstrādes pienākumus šādas komunikācijas pakalpojumu sniedzējiem, datu subjektu datu aizsardzība ir atkarīga nevis no Direktīvas 2002/58, bet gan vienīgi no valsts tiesībām, neskarot [Direktīvu 2016/680]"[7].

37. Šajā lietā piekļūt datiem mēģināja tieši policijas iestādes kriminālizmeklēšanas gaitā. Elektronisko komunikāciju pakalpojumu sniedzēji tajā nepiedalījās, un tiem netika pieprasīta personas datu izpaušana. Tāpēc Direktīva 2002/58 nav piemērojama.

38. Savienības tiesību akts, kas reglamentē šo situāciju, ir Direktīva 2016/680, kura saskaņā ar tās 2. panta 1. punktu ir piemērojama personas datu apstrādei, ko veic kompetentās iestādes, "lai [..] izmeklētu [..] noziedzīgus nodarījumus".

39. Iepriekšminētais būtu pietiekams pamats, lai lūgumu sniegt prejudiciālu nolēmumu, kādu to bija formulējusi valsts tiesa, atzītu par nepieņemamu, jo Savienības tiesību norma, kuras interpretācija tika lūgta, lietā nav piemērojama.

40. Tomēr LESD 267. pants ļauj Tiesai pārformulēt tai uzdotos jautājumus vai norādīt uz citām lietā iespējami nozīmīgām Savienības tiesību normām, lai tā varētu sniegt valsts tiesai noderīgu atbildi[8].

41. Tiesa vērsās pie iesniedzējtiesas, lai tā paustu viedokli par Direktīvas 2016/680 iespējamo piemērojamību. Tādējādi tā šai tiesai deva iespēju pašai papildināt vai pārformulēt savus jautājumus. Tomēr iesniedzējtiesa vienīgi norādīja, ka "šajā lietā katrā ziņā ir jāievēro Direktīvas 2016/680 noteikumi", taču neminēja, par kurām normām tai ir šaubas, un neizklāstīja nekādus citus apsvērumus par lietas būtību[9].

[7] Spriedums, 2020. gada 6. oktobris, *La Quadrature du Net* u.c. (C-511/18, C-512/18 un C-520/18, EU:C:2020:791; turpmāk tekstā – "spriedums *La Quadrature du Net*"), 103. punkts.

[8] Tostarp spriedums, 2016. gada 28. aprīlis, *Oniors Bio* (C-233/15, EU:C:2016:305), 30. punkts.

[9] Tiesa uzskatīja, ka ir jāuzaicina lietas dalībniekus izteikties, "kādas, pēc to viedokļa, ir lietā nozīmīgās Direktīvas 2016/680 normas, kuras ņemot vērā Tiesai būtu vajadzības gadījumā jāpārformulē iesniedzējtiesas iesniegtie trīs prejudiciālie jautājumi" (ceturtais no uzdotajiem jautājumiem mutiskai atbildēšanai tiesas sēdē).

42. Tiesa ir vairākkārt atzinusi: "Kā noteikts Reglamenta 94. panta c) punktā, pašā lūgumā sniegt prejudiciālu nolēmumu noteikti ir jāietver to iemeslu izklāsts, kuri likuši iesniedzējtiesai šaubīties par noteiktu Savienības tiesību normu interpretāciju vai spēkā esamību, kā arī saikne, ko tā konstatējusi starp šīm tiesību normām un pamatlietai piemērojamajiem valsts tiesību aktiem." [10]

43. No iepriekšminētā ir skaidri redzams, ka šajā lūgumā Tiesas Reglamenta 94. panta nosacījumi nav izpildīti. Pat ja Tiesa šajā ziņā izrāda zināmu elastību, sadarbībai ar iesniedzējtiesu jābūt savstarpējai, proti, ja iesniedzējtiesa nepamatoti nesadarbojas un neizklāsta savas šaubas par to, kā interpretējamas Savienības tiesību normas, kuras tā uzskata par piemērojamām (šajā gadījumā Direktīva 2016/680), man šķiet loģiski šo lūgumu sniegt prejudiciālu nolēmumu noraidīt kā nepieņemamu [11].

44. Turklāt iesniedzējtiesa:

– neprecizē policijas iestāžu mēģinātās apstrādes vai konkrēti meklēto personas datu iedabu. Sākotnēji tā šķiet norādām, ka runa ir tikai par savienojuma datiem (proti, par datu plūsmu un atrašanās vietu), taču pēc tam tā neizslēdz, ka tālruņa atbloķēšana sniegtu piekļuvi "visiem [..] saglabātajiem digitālajiem datiem" [12] un tostarp ar tā starpniecību veiktās saziņas un elektronisko ziņojumu saturam [13];

– norāda gan uz tālruņa izņemšanu un piekļuvi vai piekļuves mēģinājumu tajā saglabātajiem datiem, gan uz šo datu turpmāku "izvērtēšanu" (*Auswertung*), proti, to analizēšanu un interpretēšanu. Tā piebilst, ka šī izvērtēšana "nozīmē pilnīgi nekontrolētu piekļuvi visai datu subjekta digitālajai saziņai", kas ļauj "iegūt ļoti detalizētu un pamatīgu priekšstatu gandrīz par visām privātās dzīves jomām".

45. Šajos apstākļos Tiesa nevis *pārformulētu* iesniedzējtiesas jautājumus, bet gan patiesībā gluži *pārveidotu* lūgumu sniegt prejudiciālu nolēmumu, turklāt daļēji balstoties uz hipotētiskiem apsvērumiem, nevis uz konstatētiem faktiem. Turklāt jāņem vērā, kā jau teicu, ka iesniedzējtiesai jau tika sniegta iespēja pašai papildināt vai pārformulēt savus jautājumus.

46. Tādēļ ierosinu šo lūgumu sniegt prejudiciālu nolēmumu atzīt par nepieņemamu, kā to aicina darīt vairākas šajā lietā iestājušās valstis.

47. Nepieņemamība būtu atzīstama arī Tiesas sēdē norādītā apstākļa dēļ, ka iesniedzējtiesa vairs nesaskaras ar īstenu strīdu, kura izspriešanai būtu nepieciešama Savienības tiesību normu interpretācija.

48. Proti, Austrijas valdība (kuras pakļautībā ir policijas iestādes, kas piedalījās izmeklēšanā) atzīst, ka šo iestāžu darbība bija nelikumīga un radīja attiecīgās personas tiesību aizskārumu. Tā kā – atbilstoši iesniedzējtiesas nolēmumā teiktajam – prasītāja prasījums administratīvajā tiesā attiecās tieši uz tiem policijas pasākumiem, kurus atbildētāja iestāde atzīst par nelikumīgiem, izskatīšanai iesniedzējtiesā iesniegtais strīds ir zudis.

[10] Spriedums, 2021. gada 6. oktobris, *Consorzio Italian Management* un *Catania Multiservizi* (C-561/19, EU:C:2021:799), 69. punkts.

[11] Šajā ziņā piekrītu Francijas valdībai (tās rakstveida apsvērumu 36.–41. punkts).

[12] Tā norādīts otrajā prejudiciālajā jautājumā.

[13] Iesniedzējtiesa apgalvo, ka, "izmantojot savienojuma datus, var iegūt informāciju gandrīz par visu saziņu pēc tās biežuma, laika un ilguma, savukārt saistībā ar saziņu, kas ir notikusi ar *SMS* vai citu ziņu nosūtīšanas pakalpojumu starpniecību, var iegūt informāciju pat par tās saturu; arī analizējot saglabātās fotogrāfijas un navigācijas vēsturi, var iegūt ļoti intīmu ieskatu datu subjekta privātajā dzīvē".

49. Katrā ziņā, ja Tiesa uzskatītu citādi, turpmāk pakārtoti izskatīšu prejudiciālo jautājumu pamatā esošo materiāltiesisko problemātiku.

50. Tomēr pirms tam, manuprāt, ir jāizslēdz, ka pastāvētu vēl kāds cits nepieņemamības pamats, kuru izvirza dažas no personām, kas iestājušās lietā [14]. To ieskatā, ņemot vērā, ka Direktīva 2016/680 attiecas uz fizisko personu aizsardzību saistībā ar viņu datu *apstrādi*, tā nebūtu jāpiemēro tādos gadījumos kā šajā lietā, kurā nav notikusi apstrāde, bet gan vienkāršs *mēģinājums piekļūt* datiem, kurus galu galā tā arī nav izdevies iegūt.

51. Komisija savukārt uzskata, ka Direktīvas 2016/680 lietderīgās iedarbības labad būtu jādod priekšroka tādai šīs direktīvas priekšmeta interpretācijai, kas neaprobežotos ar datu apstrādi šaurā nozīmē, bet gan aptvertu arī situācijas, kas ir tieši saistītas ar to. Viena no tādām situācijām esot mēģinājums piekļūt datiem, kurus paredzēts apstrādāt [15].

52. Manuprāt, bez vajadzības paplašināt Direktīvas 2016/680 piemērošanas jomas robežas [16] tās piemērošana šajā gadījumā ir pamatota nevis tāpēc, ka ir bijis izņemts tālrunis [17], bet gan tā iemesla dēļ, kā policijas iestādes ir rīkojušās pēc tam, lai iegūtu no šā tālruņa kādus datu subjekta personas datus, un tālab mēģinājušas šo tālruni atbloķēt un piekļūt tā saturam.

53. Viena no darbībām, kuras Direktīvas 2016/680 3. panta 2. punktā ir definētas kā "apstrāde", ir kriminālizmeklēšanas gaitā veikta personas datu izpaušana, "citādi darot tos pieejamus". Uzskatu, ka tad, ja policijas iestāde izņem tālruni, kurā ir saglabāti šie dati, un rīkojas ar to, lai datus no tā iegūtu, tā uzsāk apstrādes "darbību", lai cik nesekmīga tā arī izrādās ar kriptogrāfisko drošību saistītu tehnisku faktoru dēļ.

54. Kriminālizmeklēšanas gaitā nesekmīgi veikts mēģinājums piekļūt mobilajā tālrunī saglabātajiem personas datiem ietilpst Direktīvas 2016/680 piemērošanas jomā to pašu iemeslu dēļ, kuru dēļ Tiesa ir atzinusi, ka Direktīva 2002/58 ir piemērojama *mēģinājumam* (arī nesekmīgam) saņemt tiesas atļauju, lai piekļūtu kādiem aizdomās turētās personas datiem, kas ir elektronisko komunikāciju pakalpojumu sniedzēja rīcībā [18].

55. Šajos apstākļos, ja iesniedzējtiesai būtu jālemj par policijas darbības nelikumīgumu (kuru, kā jau teicu, Austrijas valdība atzīst), tās vērtējums varētu būt atkarīgs no tā nolūka likumības, kurā apstrādi bija paredzēts veikt, gan tad, ja pasākums būtu izdevies, gan tad, ja tas ir vienīgi uzsākts un nav bijis sekmīgs.

[14] Domātas konkrēti Austrijas, Francijas, Nīderlandes un Norvēģijas valdības.

[15] Komisija uzskata, ka "nav nozīmes tam, vai mēģinājumi ir vai nav bijuši sekmīgi. Tehnisku grūtību rašanās, kas liedz piekļuves mēģinājumu sekmīgu izdošanos, ir iepriekš neparedzams apstāklis, kas neietekmē personas datu aizsardzības riskus".

[16] Konkrēti, Komisijas rakstveida apsvērumos ierosinātā atsaukšanās uz Direktīvas 2016/680 27. un 28. pantu, manuprāt, ir lieka. Tās 27. pantā minētais "novērtējums par ietekmi uz datu aizsardzību" attiecas vispārīgi uz "apstrādes veidu", nevis uz konkrētu jeb individuālu apstrādi. No Direktīvas 2016/680 58. apsvēruma izriet, ka "ietekmes novērtējumiem *būtu jāaptver nevis atsevišķi gadījumi*, bet attiecīgās apstrādes darbību sistēmas un procesi" (mans izcēlums). Tiesas sēdē Komisija paskaidroja, ka abas šīs normas tā ir minējusi tikai tālab, lai norādītu, ka Direktīva 2016/680 attiecas arī uz situācijām pirms datu apstrādes šā jēdziena tiešajā nozīmē.

[17] Direktīva 2016/680 nereglamentē tālruņa izņemšanu, kas veikta pierādījumu iegūšanai kriminālizmeklēšanā.

[18] Spriedums, 2018. gada 2. oktobris, *Ministerio Fiscal* (C-207/16, EU:C:2018:788).

B. Par lietas būtību

1. Pirmais prejudiciālais jautājums

56. Iesniedzējtiesa vēlas noskaidrot, vai saskaņā ar Direktīvas 2002/58 15. panta 1. punktu (vajadzības gadījumā kopsakarā ar tās 5. pantu) un Hartas 7. un 8. panta gaismā "valsts iestāžu piekļuve mobilajos tālruņos saglabātajiem datiem ir uzskatāma par tādu iejaukšanos šajos Hartas pantos nostiprinātajās pamattiesībās, kas ir tik būtiska, ka noziedzīgu nodarījumu prevencijas, izmeklēšanas, atklāšanas un kriminālvajāšanas jomā šī piekļuve ir atļaujama tikai smagas noziedzības apkarošanas mērķiem".

57. Ja lūgums sniegt prejudiciālu nolēmumu būtu pieņemams, Direktīvas 2002/58 nepiemērojamības dēļ pirmais jautājums būtu jāpārformulē tā, lai Tiesas atbildē tiktu interpretēta Direktīva 2016/680.

58. Šajā atbildē būtu secīgi jānoskaidro vispirms, vai tādos gadījumos kā šeit aplūkotais var būt runa par iejaukšanos, un tad, ja šāda iejaukšanās pastāv, – vai Direktīvā 2016/680 ir prasīts, lai piekļuve datiem aprobežotos ar smagas noziedzības apkarošanas gadījumiem.

59. Datu apstrādes darbības pēc savas iedabas var radīt tiesību uz privātās dzīves neaizskaramību (Hartas 7. pants) un personas datu aizsardzības tiesību (Hartas 8. pants) aizskārumu. Tāpēc valsts iestādēm ir jāizpilda Hartas 52. panta 1. punktā paredzētie nosacījumi, lai pamatotu savu iejaukšanos šo pamattiesību izmantošanā.

60. Iejaukšanās Hartas 7. un 8. pantā aizsargātajās tiesībās ir vēl būtiskāka, ja ar to: a) tiek mēģināts piekļūt sensitīviem datiem, kuri parasti tiek ierakstīti mobilajos tālruņos un kuru uzzināšana var atklāt to īpašnieku dzīves aspektus, kas trešām personām nav jāzina; un b) tiek radīta iespēja piekļūt saziņas saturam.

61. Tomēr Direktīva 2016/680 – vispārīgi un ņemot vērā tās saturu – nav interpretējama tādējādi, ka tā attiektos tikai uz tādām datu apstrādes darbībām, kas aprobežojas ar smagas noziedzības apkarošanas gadījumiem vien.

62. Direktīvas 2016/680 priekšmets ir jebkura personas datu apstrādes darbība[19], ko veic kompetentās iestādes, lai novērstu, izmeklētu un atklātu *visu veidu* noziedzīgus nodarījumus vai sauktu pie atbildības par tiem.

63. No principiem, ko Direktīva 2016/680 noteic attiecībā uz personas datu apstrādi šajā nolūkā (4. pants), vai tās veikšanas likumīguma nosacījumiem (8. pants) neizriet, ka datu apstrāde būtu pieļaujama tikai smagas noziedzības gadījumos.

64. Pamatojums šādai ierobežošanai tikai attiecībā uz smagas noziedzības apkarošanas gadījumiem nebūtu rodams arī Tiesas judikatūras par Direktīvu 2002/58[20] automātiskā attiecināšanā uz tādām situācijām kā šajā lietā aplūkotā.

[19] Direktīvas 2016/680 3. panta 2. punktā minēto "darbību" tipoloģija ir ļoti plaša. Šī norma citēta šo secinājumu 9. punktā.

[20] Spriedumi *La Quadrature du Net* un 2016. gada 21. decembris, *Tele2 Sverige* un *Watson* u.c. (C-203/15 un C-698/15, EU:C:2016:970; turpmāk tekstā – "spriedums *Tele2 Sverige* un *Watson*"); 2018. gada 2. oktobris, *Ministerio Fiscal* (C-207/16, EU:C:2018:788); 2020. gada 6. oktobris, *Privacy International* (C-623/17, EU:C:2020:790); un 2021. gada 2. marts, *Prokuratuur* (Piekļuves elektronisko komunikāciju datiem nosacījumi) (C-746/18, EU:C:2021:152; turpmāk tekstā – "spriedums *Prokuratuur*").

65. Manuprāt, to darīt nav iespējams tāpēc, ka – ar turpinājumā izklāstīto atrunu – minētā judikatūra attiecas uz vispārīga un nenoteikta personu loka datu visaptverošu un nediferencētu glabāšanu, ko elektronisko komunikāciju pakalpojumu sniedzēji veic sistemātiski. Tas, ka Tiesa ir bijusi īpaši stingra, aizliedzot šo glabāšanu un paredzot atkāpes no šā aizlieguma, ir izskaidrojams ar apstākli, ka šāda datu glabāšana rada vērienīgu iejaukšanos, kas skar sabiedrību kopumā.

66. Tā savukārt nenotiek tad, ja paredzētā piekļuve attiecas nevis uz visiem iedzīvotājiem vai lielām iedzīvotāju grupām (proti, vispārīga un nenoteikta personu loka personas datiem), bet gan uz konkrētā mobilā tālrunī saglabātu informāciju konkrētas krimināllizmeklēšanas gaitā, uz kuru attiecas tieši Direktīva 2016/680.

67. Direktīvas 2016/680 priekšmets nav nekas cits kā datu apstrāde, ko veic kompetentās iestādes, lai novērstu, izmeklētu un atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem, proti, apstrāde saistībā ne tikai ar smagiem, bet gan ar visu veidu noziedzīgiem nodarījumiem.

68. Turklāt – kā uzsvērušas vairākas no personām, kas iestājušās šajā prejudiciālajā tiesvedībā –, ņemot vērā, ka Direktīvā 2016/680 nav nekādu norāžu uz noziedzīgu nodarījumu smagumu, tā dalībvalstīs iespējami varētu netikt piemērota vienveidīgi, jo katras valsts tiesību vērtējums par sodāmas rīcības smaguma pakāpi būtiski atšķiras [21].

69. Īsāk sakot, Direktīvā 2016/680 paredzētās personas datu apstrādes likumība tajā nav pakārtota nosacījumam, ka šī apstrāde ir pieļaujama tikai smagas noziedzības apkarošanai.

70. Iepriekšminētais neizslēdz, ka saskaņā ar samērīguma principu katrā atsevišķā gadījumā datu apstrāde, kuru kompetentās iestādes paredz veikt saskaņā ar Direktīvu 2016/680, ir jāpielāgo, ņemot vērā: a) to noziedzīgo nodarījumu iedabu, par kuriem notiek kriminālvajāšana; un b) apstrādājamo personas datu veidu.

71. Šajā ziņā piekrītu vairākiem Vācijas valdības argumentiem par ierobežojumu piekļuvē izņemto tālruņu datiem, ja šie dati ļauj izveidot pilnīgu to īpašnieku personas profilu, ņemot vērā šo tālruņu digitālo saturu. Vācijas valdība uzskata, ka šai piekļuvei vajadzētu aprobežoties ar datiem, kas nepieciešami kā pierādīšanas līdzeklis konkrētā gadījumā, un tā varētu būt nepieļaujama, ņemot vērā tādus faktorus kā "izmeklējamā noziedzīgā nodarījuma maznozīmīgums vai iegūstamo personas datu vājais pierādījumu spēks" [22].

72. Tātad *teorētiski* Direktīva 2016/680 nenoteic, ka piekļuve mobilajā tālrunī saglabātajiem personas datiem pēc noklusējuma būtu nelikumīga, lai atvieglotu tādu darbību izmeklēšanu, kas var attiekties uz vispārīgo jeb parasto noziedzību. Tas, vai *praktiski* konkrētai iestādei ir jāpiešķir piekļuve, būs jāizvērtē katrā atsevišķā gadījumā, ņemot vērā tās nepieciešamību un samērīgumu, ko tikko pieminēju.

73. Manuprāt, tas ir secināms no Direktīvas 2016/680 normām, kas paredz personas datu apstrādes pieļaujamības nosacījumus noziedzības apkarošanas ietvaros, proti:

– no 4. panta 1. punkta a) apakšpunkta, saskaņā ar kuru dati tiek "apstrādāti likumīgi";

[21] Francijas valdība kā piemēru min nodarījumus saistībā ar narkotisko vielu glabāšanu un apriti, kas Austrijas un Francijas krimināltiesību normās tiek atzīti par atšķirīga smaguma nodarījumiem. Zviedrijas valdība ir paudusi līdzīgu viedokli.

[22] Vācijas valdības rakstveida apsvērumi, 20. punkts.

– no 8. panta 1. punkta, kurā uzsvērts, ka apstrādei jābūt *nepieciešamai* un jābalstās uz Savienības vai dalībvalsts tiesībām.

2. Otrais prejudiciālais jautājums

74. Ar otro prejudiciālo jautājumu iesniedzējtiesa vēlas noskaidrot, vai ar Direktīvas 2002/58 15. panta 1. punktu, lasot to Hartas 7., 8. un 11. panta un 52. panta 1. punkta gaismā, "netiek pieļauts tāds valsts tiesiskais regulējums kā [*StPO*] 18. pants, lasot to kopsakarā ar šā likuma 99. panta 1. punktu, atbilstoši kuram drošības iestādes kriminālizmeklēšanas gaitā bez tiesas vai neatkarīgas iestādes atļaujas pašas sev piešķir visaptverošu un nekontrolētu piekļuvi visiem mobilajā tālrunī saglabātajiem digitālajiem datiem".

75. Jautājuma formulējums ir visnotaļ neskaidrs. Iesniedzējtiesa:

– atzīst, ka *StPO* 110. panta 2. punkts paredz, ka mantas izņemšanai principā ir nepieciešama prokuratūras atļauja. Policijas iestāde bez atļaujas var veikt izņemšanu tikai šā paša panta 3. punktā paredzētajos ārkārtas apstākļos (kādu šajā gadījumā nav);

– tomēr piebilst, ka mobilajos tālruņos saglabātās informācijas analīzi "[*StPO*] nereglamentē viennozīmīgi" un ka tai var piekļūt drošības iestādes pēc savas ierosmes un bez iepriekšējas atļaujas.

76. Austrijas valdība valsts tiesisko regulējumu izklāsta atšķirīgi no tā, kā tas darīts iesniedzējtiesas nolēmumā. Konkrēti, tā apgalvo, ka saskaņā ar valsts tiesībām gan tālruņa izņemšana (atskaitot steidzamības gadījumus), gan tajā saglabāto datu analīze ir iespējama tikai ar prokuratūras atļauju[23]. Bez prokuratūras rīkojuma policijas veikta šajā tālrunī saglabāto datu izvērtēšana ir nelikumīga.

77. Valsts tiesisko regulējumu interpretēt ir iesniedzējtiesas ziņā. LESD 267. pantā paredzētajā procedūrā Tiesas kompetencē neietilpst valsts tiesību interpretēšana, un tikai un vienīgi iesniedzējtiesas ziņā ir noskaidrot valsts normatīvo un administratīvo aktu konkrēto tvērumu[24].

78. Lai gan nevēlos iesaistīties polemikā par Austrijas tiesību interpretāciju, manuprāt, no iesniedzējtiesas norādītajām normām (*StPO* 18. panta saistībā ar šā likuma 99. panta 1. punktu) vien ir grūti izsecināt iesniedzējtiesas atvedinātās sekas. Taču, kā jau teicu, par to lemt ir tikai iesniedzējtiesas ziņā.

79. Lai būtu kā būdams, iesniedzējtiesa uzskata, ka uz tādu gadījumu, kāds aplūkots šajā lietā, esot attiecināma sprieduma *Prokuratuur* judikatūra[25] par piekļuves saglabātajiem datiem iepriekšēju kontroli, ko īsteno tiesa vai neatkarīga administratīva iestāde.

[23] Austrijas valdības rakstveida apsvērumu 19. punkts. Tā atsaucas uz *Oberster Gerichtshof* (Augstākā tiesa, Austrija) 2020. gada 13. oktobra spriedumu (lieta 11 Os 56/20z), kas krimināpolicijas veiktu mobilā tālruņa datu analīzi bez prokuratūras atļaujas atzīst par nelikumīgu tāpēc, ka ar to ir pārkāptas attiecīgās personas subjektīvās tiesības.

[24] Tostarp spriedums, 2022. gada 28. aprīlis, *SeGEC* u.c. (C-277/21, EU:C:2022:318), 21. punkts.

[25] Spriedums *Prokuratuur*, 51. punkts: "Ir būtiski, ka kompetento valsts iestāžu piekļuve saglabātajiem datiem principā ir pakļauta iepriekšējai pārbaudei, ko veic tiesa vai neatkarīga administratīva iestāde, un ka šīs tiesas vai iestādes lēmums tiek pieņemts, pamatojoties uz šīs iestādes pieteikumu tostarp saistībā ar noziedzīga nodarījuma novēršanu, atklāšanu vai krimināvajāšanas procedūrām."

80. Savukārt Nīderlandes valdība uzskata, ka šī judikatūra ir jāskata valsts tiesiskā regulējuma kontekstā, kas atļautu kompetento iestāžu *vispārēju* piekļuvi *visai* saglabātajai informācijai par datu plūsmu un atrašanās vietas datiem. Tā būtu izskaidrojama iepriekšējas tiesas atļaujas prasība, kurai tomēr varētu trūkt pamatojuma gadījumā ar piekļuvi viena tālruņa datiem.

81. Ar tādu pašu domu gājienu Norvēģijas valdība apgalvo, ka starp daudzajām Direktīvā 2016/680 noteiktajām garantijām [26] nav rodama skaidri noteikta prasība, ka jābūt tiesas vai neatkarīgas administratīvas iestādes iepriekšējai atļaujai.

82. Pamatodamās uz to, ka Direktīvas 2016/680 noteikumi jāinterpretē Hartas gaismā, Komisija apgalvo, ka šīs direktīvas 8. panta 1. punktā dalībvalstīm uzliktais pienākums (apstrādes likumīguma nosacījumi) ietver nepieciešamību ievērot Hartas 7. un 8. pantā garantētās pamattiesības.

83. Piekrītu Komisijai, ka, ievērojot šīs Hartas normas, valstu likumdevējiem ir jānosaka noteikumi, kas nepieciešami, lai nodrošinātu, ka piekļuve datiem ir pamatota katrā atsevišķā gadījumā un aprobežojas ar to, kas ir absolūti nepieciešams un samērīgs.

84. Tomēr šādiem valstu noteikumiem nav jāregulē konkrēti piekļuve personas datiem, kas, kā šajā gadījumā, atrodas mobilajā tālrunī, bet gan tie var būt noteikti valsts tiesību vispārīgajās normās par pierādījumu iegūšanu.

85. Šajā ziņā jau esmu citējis sprieduma *La Quadrature du Net* 103. punktu jautājumā par dalībvalstu pasākumiem, kas skar elektronisko komunikāciju konfidencialitāti, neuzliekot apstrādes pienākumus šādu komunikāciju pakalpojumu sniedzējiem [27].

86. Tāpēc no Direktīvas 2016/680 nav jāsecina kādi *speciāli* procesuāla rakstura noteikumi, kā nodrošināt piekļuves mobilajā tālrunī saglabātajiem datiem likumīgumu [28], bet gan šajā ziņā ir piemērojamas valsts tiesību normas, kas reglamentē kratīšanas un izņemšanas pilnvaru īstenošanu krimināllizmeklēšanā [29].

87. Atsaukšanās uz valsts tiesību normām, lai nodrošinātu piekļuves likumību saskaņā ar Direktīvu 2016/680, turklāt atbilst ECT judikatūrai. Tieši kādā ar Austrijas Republiku saistītā lietā par ECPAK 8. pantu (par tiesībām uz savas privātās un ģimenes dzīves, dzīvokļa un sarakstes neaizskaramību) ECT konstatēja, ka Austrijas tiesiskais regulējums par mantas, konkrētāk, dokumentu, izņemšanu ir piemērojams kratīšanas un datu nesējos saglabāto datu izņemšanas darbībām [30].

88. Ja – kā, atsaukdamās *Oberster Gerichtshof* (Augstākā tiesa, Austrija) judikatūru, apgalvo Austrijas valdība – policijas iestādēm patiešām nav tiesību piekļūt konkrētā tālrunī saglabātajiem datiem bez prokuratūras atļaujas, otrajam prejudiciālajam jautājumam liela mērā zūd jēga.

[26] Papildus 4. un 8. panta garantijām tās ir arī garantijas, kas ietvertas III nodaļā ("Datu subjekta tiesības"), IV nodaļā ("Pārzinis un apstrādātājs"), VI nodaļā ("Neatkarīgas uzraudzības iestādes") un VIII nodaļā ("Tiesību aizsardzības līdzekļi, atbildība un sankcijas").

[27] Skat. šo secinājumu 36. punktu.

[28] To, cik grūti šo uzdevumu ir paveikt, uzskatāmi parāda Komisijas centieni tās rakstveida apsvērumu 34.–39. punktā sekmēt skaidru un precīzu noteikumu noteikšanu, lai paredzētu atbilstošus ierobežojumus un garantijas saistībā ar piekļuvi mobilā tālruņa datiem.

[29] Normas, kuras, kā norāda, piemēram, Dānijas un Īrijas valdības, neietilpst Savienības tiesību piemērošanas jomā, bet var kalpot kādas no šīm tiesībām izrietošas prasības izpildei.

[30] ECT spriedums, 2007. gada 16. oktobris, *Wieser* un *Bicos Beteiligungen* pret Austriju (CE:ECHR:2007:1016JUD007433601), 54. punkts: "The Austrian Code of Criminal Procedure does not contain specific provisions for the search and seizure of electronic data. However, it contains detailed provisions for the seizure of objects and, in addition, specific rules for the seizure of documents. It is established in the domestic courts' case-law that these provisions also apply to the search and seizure of electronic data."

89. Katrā ziņā atbildē uz šo jautājumu nevar izslēgt, ka, piekļūstot izņemtajā tālrunī esošajiem personas datiem, var "gūt ļoti detalizētu un pamatīgu priekšstatu gandrīz par visām [datu subjekta] privātās dzīves jomām" [31]. Tādā gadījumā policijas iestādes nedrīkstētu rīkoties bez spriedumā *Prokuratuur* minētās iepriekšējās atļaujas.

90. Pirmšķietami šis arguments varētu likties nesavienojams ar manis iepriekš apgalvoto apstākli, ka Direktīva 2002/58 (kura interpretēta spriedumā *Prokuratuur*) šajā lietā nav piemērojama. Tomēr uzskatu, ka minētā sprieduma *ratio* atbalsta šo pašu risinājumu.

91. Strīdā, kurā tika taisīts spriedums *Prokuratuur*, lai gan piekļuve tika veikta, iegūstot datus (metadatus) no elektronisko komunikāciju pakalpojumu sniedzējiem, tāpat kā šajā lietā notika viena noziedzīga nodarījuma izmeklēšana attiecībā uz noteiktu personu. Tajā bija iecerēts ievākt "dat[us] par vairākiem [..] tālruņa numuriem un vairākiem starptautiskajiem mobilās galiekārtas identitātes identifikatoriem" [32].

92. Manuprāt, spriedumā *Prokuratuur* izšķirami divi aspekti: a) jautājums par to, vai ir pieļaujams dalībvalsts vispārīgs regulējums par datu visaptverošu un nediferencētu glabāšanu un turpmāku piekļuvi pakalpojumu sniedzēju rīcībā esošajiem datiem; un b) jautājums par piekļuves šiem metadatiem iepriekšēju kontroli katrā atsevišķā gadījumā, ja šie dati ļauj izveidot precīzu personas privātās dzīves profilu.

93. Tas apstāklis, ka šajā lietā privāto dzīvi atklājošie dati nav pakalpojumu sniedzēju valdījumā un tiek iegūti (vai tos tiek mēģināts iegūt) no viena vienīga izņemta tālruņa, man šķiet maznozīmīgs salīdzinājumā ar iepriekšējas kontroles prasības *ratio*, uz kuru atsaucas spriedums *Prokuratuur*.

94. Šīs iepriekšējas kontroles virspamatojums rodams vajadzībā nodrošināt Hartas 7. un 8. pantā garantēto aizsardzību. Šo kontroli īstenojošajai iestādei ir "[jāspēj] nodrošināt taisnīgu līdzsvaru starp interesēm, kas saistītas ar izmeklēšanas vajadzībām saistībā ar cīņu pret noziedzību, no vienas puses, un personu, kuru datiem tiek piekļūts, pamattiesībām uz privātās dzīves neaizskaramību un personas datu aizsardzību, no otras" [33].

3. Trešais prejudiciālais jautājums

95. Ar trešo prejudiciālo jautājumu iesniedzējtiesa vēlas noskaidrot, vai Hartas 47. pantam (vajadzības gadījumā kopsakarā ar tās 41. un 52. pantu) ir pretrunā tāds tiesiskais regulējums kā Austrijā esošais [34], ar kuru "tiek pieļauts, ka mobilais tālrunis tiek digitāli izvērtēts, par šo faktu neinformējot datu subjektu pirms tam vai vismaz pēc šā pasākuma veikšanas".

96. Uzskatu, ka šādi formulēts šis jautājums varētu izrādīties strīda atrisināšanai nevajadzīgs, jo datu subjekts varēja izmantot Hartas 47. pantā nostiprinātās tiesības, lūdzot iesniedzējtiesu atzīt par spēkā neesošu policijas rīcību ar izņemto tālruni, kas ietvēra turpmāku (un nesekmīgu) tajā saglabāto datu izvērtējumu.

[31] Skat. iesniedzējtiesas argumentus, kas atreferēti šo secinājumu 44. punktā.

[32] Spriedums *Prokuratuur*, 17. punkts.

[33] Spriedums *Prokuratuur*, 52. punkts.

[34] Tā atkal atsaucas uz *StPO* 18. pantu saistībā ar tā 99. pantu.

97. Saistībā ar šīm abām policijas rīcības epizodēm būtu jānorāda uz šādu atšķirību:

– par tālruņa izņemšanu kā tādu – kā redzams no lietas materiālos esošās informācijas – datu subjekts ir zinājis, un tālruņa izņemšanas brīdī tas ir atteicies sniegt policijas iestādēm šā tālruņa atbloķēšanas kodu;

– savukārt par datu analīzes mēģinājumu – kā viss norāda – pārzinis nav informējis datu subjektu, lai gan Austrijas valdība apgalvo, ka datu subjekts esot iepazinies ar ziņojumu, kurā bija norādīta kriminālpolicijas rīcība ar tālruni [35].

98. Tādēļ saistībā ar datu izvērtējumu un datu subjekta informētību par to ir zināmas neskaidrības, kuras, kā jau esmu norādījis, būtu bijis jāprecizē iesniedzējtiesai tās nolēmumā un kuras liedz sniegt noderīgu atbildi uz trešo prejudiciālo jautājumu.

99. Katrā ziņā gadījumam, ja Tiesa neuzskatītu šo jautājumu par nepieņemamu, paudīšu savu viedokli par to. Šādā gadījumā un ņemot vērā Direktīvas 2002/58 nepiemērojamību, jautājumu vajadzētu pārformulēt, ņemot vērā Direktīvu 2016/680, kuras 13., 15. un 54. pantā rodamas norādes, kā uz šo jautājumu atbildams.

100. Saskaņā ar Direktīvu 2016/680 datu subjektam ir jāsaņem tā informācija par viņa datu apstrādi, kas ir nepieciešama tostarp, lai tas: a) iesniegtu sūdzību uzraudzības iestādē (13. panta 1. punkta d) apakšpunkts); un b) izmantotu tiesības uz efektīvu tiesību aizsardzību tiesā par Direktīvā 2016/680 garantēto tiesību pārkāpumu, neskarot pieejamos administratīvos vai ārpustiesas tiesību aizsardzības līdzekļus (54. pants).

101. Tomēr nevar aizmirst, ka gan Direktīvas 2016/680 13. panta 3. punkts, gan 15. panta 1. punkts atļauj dalībvalstīm pieņemt leģislatīvus pasākumus:

– lai atliktu, ierobežotu vai nesniegtu informāciju datu subjektam, ievērojot 13. panta 2. punktu;

– lai pilnībā vai daļēji ierobežotu datu subjekta piekļuves tiesības, ciktāl un tik ilgi, kamēr šāds daļējs vai pilnīgs ierobežojums ir nepieciešams un samērīgs pasākums, lai *inter alia* novērstu, ka tās traucētu izmeklēšanai vai iestāžu vai tiesu procedūrām vai kaitētu noziedzīgu nodarījumu izmeklēšanai [36].

102. Katrā ziņā datu apstrādes likumība nav atkarīga no tā, vai kompetentās iestādes izpilda (turpmākus) pienākumus, ko tām noteic Direktīvas 2016/680 13. pants, bet gan no to pamatojošā nolūka likumīguma; proti, no tā, vai šīm administratīvajām iestādēm bija tiesības veikt personas datu apstrādi.

103. No šā viedokļa raugoties, tam, vai datu subjekts tika informēts par mēģinājumiem piekļūt viņa izņemtajā mobilajā tālrunī saglabātajiem datiem, pašam par sevi nav nekāda sakara ar policijas darbības materiāltiesisko likumību. Pārziņa rīcībai, kas eventuāli ir pretrunā pienākumiem, kurus tam noteic Direktīvas 2016/680 13. pants, var būt citas sekas, bet, kā jau teicu, tā pati par sevi neietekmē šīs apstrādes likumību vai nelikumību.

[35] Tās rakstveida apsvērumu 37. punkts.

[36] Šajā nozīmē skat. spriedumu *Tele2 Sverige* un *Watson*, 121. punkts. Attiecībā uz apstrādei pakļauto datu subjektu tiesību aizsardzības tiesā garantiju Tiesas judikatūra par Direktīvu 2002/58 ir attiecināma arī uz Direktīvu 2016/680.

104. Noskaidrot, vai valsts tiesiskais regulējums attiecīgajai personai ļauj efektīvi izmantot šīs tiesības, ir iesniedzējtiesas ziņā.

V. Secinājumi

105. Ņemot vērā izklāstīto, ierosinu Tiesai *Landesverwaltungsgericht Tirol* (Tiroles federālās zemes Administratīvā tiesa, Austrija) iesniegto lūgumu sniegt prejudiciālu nolēmumu atzīt par nepieņemamu.

Pakārtoti iesaku uz šo lūgumu atbildēt šādi:

1) Eiropas Parlamenta un Padomes Direktīvas (ES) 2016/680 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināsodus, un par šādu datu brīvu apriti, ar ko atceļ Padomes Pamatlēmumu 2008/977/TI, 4. panta 1. punkta a) apakšpunkts un 8. panta 1. punkts kopsakarā ar Eiropas Savienības Pamattiesību hartas 7., 8. un 52. pantu

   ir jāinterpretē tādējādi, ka

   valsts iestāžu iespēja krimināizmeklēšanas gaitā piekļūt mobilajā tālrunī saglabātajiem personas datiem tālab, lai šos datus apstrādātu, neaprobežojas ar smagas noziedzības apkarošanas gadījumiem vien.

   Minētajai piekļuvei jābūt pamatotai katrā atsevišķā gadījumā un jāaprobežojas ar to, kas ir absolūti nepieciešams un samērīgs, ņemot vērā gan izmeklējamo noziedzīgo nodarījumu, gan personas datu, kuriem gribēts piekļūt, iedabu.

   Policijas iestādes nevar pašas un bez iepriekšējas tiesas atļaujas noziedzīgu nodarījumu izmeklēšanas gaitā iegūt visaptverošu un nekontrolētu piekļuvi visiem mobilajā tālrunī saglabātajiem datiem, ja no tiem var gūt precīzu priekšstatu par personas privāto dzīvi.

2) Direktīvas 2016/680 13., 15. un 54. pants kopsakarā ar Hartas 47. un 52. pantu

   ir jāinterpretē tādējādi, ka,

   neskarot ierobežojumus, kurus atļauj Direktīvas 2016/680 15. panta 1. punkts, vai citus pieejamos administratīvos vai ārpustiesas tiesību aizsardzības līdzekļus, mobilā tālruņa īpašnieks ir jāinformē par šajā tālrunī saglabāto personas datu apstrādi, ko veikušas attiecīgas iestādes, tādā brīdī un veidā, kādos tas jādara, lai nodrošinātu attiecīgajai personai iespēju efektīvi izmantot savas tiesības uz aizsardzību tiesā pret iespējamu Direktīvā 2016/680 piešķirto tiesību pārkāpumu.