Zbirka odločb sodne prakse

SKLEPNI PREDLOGI GENERALNEGA PRAVOBRANILCA
GIOVANNIJA PITRUZZELLE,
predstavljeni 21. januarja 2020 [1]

Zadeva C-746/18

H. K.
proti
Prokuratuur

(Predlog za sprejetje predhodne odločbe, ki ga je vložilo Riigikohus (vrhovno sodišče, Estonija))

„Predhodno odločanje – Obdelava osebnih podatkov na področju elektronskih komunikacij – Zaupnost komunikacij – Ponudniki elektronskih komunikacijskih storitev – Splošna in neselektivna hramba podatkov o prometu in o lokaciji – Kazenske preiskave – Dostop preiskovalnega organa do hranjenih podatkov za obdobja, dolga od enega dneva do enega leta – Soglasje državnega tožilstva – Uporaba podatkov kot dokazov v okviru kazenskega postopka – Direktiva 2002/58/ES – Člen 1(3), člen 3 in člen 15(1) – Listina Evropske unije o temeljnih pravicah – Členi 7, 8 in 11 ter člen 52(1)“

I. Uvod

1. Obravnavani predlog za sprejetje predhodne odločbe se nanaša na razlago člena 15(1) Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) [2], kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009, [3] v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine Evropske unije o temeljnih pravicah [4].

2. Ta predlog je bil vložen v okviru kazenskega postopka, uvedenega zoper H. K., ker naj bi ta storila več tatvin, uporabila bančno kartico, ki je pripadala drugi osebi, in storila dejanja nasilja zoper udeleženca sodnega postopka.

3. Zapisniki, na katere se opira ugotovitev teh kaznivih dejanj, so bili sestavljeni zlasti na podlagi osebnih podatkov, pridobljenih v okviru zagotavljanja elektronskih komunikacijskih storitev. Riigikohus (vrhovno sodišče, Estonija) izraža dvome glede združljivosti pogojev, pod katerimi so imele preiskovalne službe dostop do teh podatkov, s pravom Unije.

4. Ti dvomi se nanašajo, prvič, na vprašanje, ali je dolžina obdobja, za katero so imele preiskovalne službe dostop do podatkov, merilo, na podlagi katerega je mogoče oceniti težo posega v temeljne pravice zadevnih oseb, ki ga pomeni ta dostop.

1 Jezik izvirnika: francoščina.

2 UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 514.

3 UL 2009, L 337, str. 11. V nadaljevanju: Direktiva 2002/58.

4 V nadaljevanju: Listina.

5. Drugič, predložitveno sodišče želi izvedeti, ali je Prokuratuur (državno tožilstvo, Estonija) ob upoštevanju različnih nalog, ki so mu zaupane z estonskimi predpisi, „neodvisen“ upravni organ v smislu sodbe z dne 21. decembra 2016, Tele2 Sverige in Watson in drugi [5].

II. Pravni okvir

A. Direktiva 2002/58

6. V skladu s členom 1(3) Direktive 2002/58 se ta „ne uporablja za dejavnosti, ki so zunaj obsega Pogodbe o ustanovitvi Evropske skupnosti, kot na primer tiste, zajete v Oddelkih [naslovih] V in VI Pogodbe o Evropski uniji in v vsakem primeru za dejavnosti v zvezi z javno varnostjo, obrambo, državno varnostjo (vključno z gospodarsko blaginjo države, kadar se dejavnosti nanašajo na zadeve v zvezi z državno varnostjo) ter dejavnosti države na področju kazenskega prava“.

7. Poleg tega člen 15(1) te direktive določa, da „[d]ržave članice lahko sprejmejo zakonske ukrepe, s katerimi omejijo obseg pravic in obveznosti, določenih v členu 5, členu 6, členu 8(1), (2), (3) in (4) ter členu 9 te direktive, kadar takšna omejitev pomeni potreben, primeren in ustrezen ukrep znotraj demokratične družbe za zaščito državne varnosti (to je Državne varnosti), obrambe, javne varnosti in preprečevanje, preiskovanje, odkrivanje in pregon kriminalnih dejanj ali nedovoljene uporabe elektronskega komunikacijskega sistema iz člena 13(1) Direktive 95/46/ES[[6]]. V ta namen lahko države članice med drugim sprejmejo zakonske ukrepe, ki določajo zadrževanje podatkov za določeno obdobje, upravičeno iz razlogov iz tega odstavka. Vsi ukrepi iz tega odstavka so v skladu s splošnimi načeli zakonodaje [Unije], vključno s tistimi iz člena 6(1) in (2) Pogodbe o Evropski uniji.“

B. Estonsko pravo

1. Zakon o elektronskih komunikacijah

8. Elektroonilise side seadus (zakon o elektronskih komunikacijah) [7] z dne 8. decembra 2004 v različici, ki se uporabi za spor o glavni stvari, v členu 111^1, naslovljenem „Obveznost hrambe podatkov“, določa:

„[…]

(2) Ponudniki telefonskih storitev in storitev mobilne telefonije ter storitev telefonskih omrežij in omrežij mobilne telefonije so dolžni hraniti te podatke:

1. številko kličočega priključka ter ime in naslov naročnika;

2. številko klicanega priključka ter ime in naslov naročnika;

3. pri uporabi dodatnih storitev, kot je transfer ali preusmeritev klica, izbrano številko ter ime in naslov naročnika;

4. datum in uro začetka in konca klica;

5. uporabljeno telefonsko storitev ali storitev mobilne telefonije;

5 C-203/15 in C-698/15, v nadaljevanju: sodba Tele2 Sverige in Watson in drugi, EU:C:2016:970 (točka 120 in izrek, točka 2).

6 Direktiva Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 15, str. 355).

7 RT I 2004, 87, 593.

6. mednarodno identiteto mobilnega naročnika (*International Mobile Subscriber Identity* – IMSI) kličočega in klicanega priključka;

7. mednarodno identiteto mobilnega terminala (*International Mobile Equipment Identity* – IMEI) kličočega in klicanega priključka;

8. lokacijsko oznako (ID celice) na začetku klica;

9. podatke, ki določajo zemljepisno lego celic, z navedbo njihovih lokacijskih oznak (ID celice) med obdobjem, za katero se hranijo podatki o komunikaciji;

10. v primeru predplačniških anonimnih storitev datum in uro začetka uporabe storitve in lokacijsko oznako (ID celice), kjer je bila storitev izvedena.

[…]

(4) Podatki iz odstavkov 2 in 3 tega člena se hranijo eno leto od komunikacije, če so bili ti podatki pridobljeni ali obdelani med zagotavljanjem komunikacijske storitve. […]

[…]

(11) Podatki iz odstavkov 2 in 3 tega člena se posredujejo:

1. na podlagi kriminaalmenetluse seadustik [zakon o kazenskem postopku [8]] preiskovalnemu organu, organu, ki je pooblaščen za izvajanje nadzornih ukrepov, državnemu tožilstvu in sodišču;

[…]“

2. Zakon o kazenskem postopku

9. Zakon o kazenskem postopku v različici, ki se uporabi za spor o glavni stvari, v členu 17, naslovljenem „Udeleženci sodnega postopka“, v odstavku 1 določa:

„Udeleženci sodnega postopka so državno tožilstvo, […]“

10. Člen 30 zakona o kazenskem postopku, naslovljen „Državno tožilstvo v kazenskem postopku“, določa:

„(1) Državno tožilstvo vodi predkazenski postopek, katerega zakonitost in učinkovitost zagotavlja, in zastopa obtožbo pred sodiščem.

(2) Pooblastila državnega tožilstva v kazenskem postopku v imenu državnega tožilstva izvaja državni tožilec, ki ravna neodvisno in ga zavezuje samo zakon.“

8 RT I 2003, 27, 166.

11. Člen 90[1] zakona o kazenskem postopku, naslovljen „Zahteva za podatke, ki se naslovi na podjetje za elektronske komunikacije“, v odstavkih 2 in 3 določa:

„(2) Preiskovalni organ lahko v predkazenskem postopku s soglasjem državnega tožilstva ali v sodnem postopku s soglasjem sodišča od ponudnika elektronskih komunikacijskih storitev zahteva podatke, ki so našteti v členu 111[1](2) in (3) zakona o elektronskih komunikacijah, ki v odstavku 1 tega člena niso navedeni. V soglasju k zahtevi se z natančnimi datumi navede obdobje, za katero se dovoli zahteva za podatke.

(3) V skladu s tem členom se lahko podatki zahtevajo samo, če je to nujno za uresničitev cilja kazenskega postopka.“

12. Člen 211 zakona o kazenskem postopku, naslovljen „Cilj predkazenskega postopka“, določa:

„(1) Cilj predkazenskega postopka je zbrati dokaze in vzpostaviti druge pogoje za začetek sodnega postopka.

(2) Preiskovalni organ in državno tožilstvo v predkazenskem postopku razjasnita razbremenilne in obremenilne okoliščine za osumljenca ali obdolženca.“

3. Zakon o državnem tožilstvu

13. Prokuratuuriseadus (zakon o državnem tožilstvu)[9] z dne 22. aprila 1998 v različici, ki se uporabi za spor o glavni stvari, v členu 1, naslovljenem „Državno tožilstvo“, določa:

„(1) Državno tožilstvo je organ, za katerega je pristojno Justiitsministeeriumi [ministrstvo za pravosodje, Estonija], ki sodeluje pri načrtovanju nadzornih ukrepov, ki so potrebni za preprečevanje in razjasnitev kaznivih dejanj, vodi predkazenski postopek, katerega zakonitost in učinkovitost zagotavlja, zastopa obtožbo pred sodiščem in opravlja druge naloge, ki jih zanj določa zakon.

(1[1]) Državno tožilstvo je pri opravljanju svojih zakonskih nalog neodvisno in ravna v skladu s tem zakonom, drugimi zakoni in pravnimi predpisi, sprejetimi na podlagi teh zakonov.

[…]“

14. Člen 2 zakona o državnem tožilstvu, naslovljen „Državni tožilec“, v odstavku 2 določa:

„Državni tožilec je pri opravljanju svojih nalog neodvisen in ravna izključno po zakonu in svojem prepričanju.“

III. Dejansko stanje, postopek v glavni stvari in vprašanja za predhodno odločanje

15. Viru Maakohus (prvostopenjsko sodišče v Viruju, Estonija) je s sodbo z dne 6. aprila 2017 obsodilo H. K. na kazen zapora dveh let, ker je v obdobju od 4. avgusta 2015 do 1. februarja 2016 storila osem tatvin živil in drugih predmetov v vrednosti od 3 do 40 EUR ter denarnih zneskov v višini od 5,20 do 2100 EUR, ker je uporabila bančno kartico druge osebe za dvigovanje gotovine z bankomata, s čimer je tej osebi povzročila škodo v višini 3941,82 EUR, in ker je storila dejanja nasilja zoper udeleženca sodnega postopka.[10]

9 RT I 1998, 41, 625.

10 Predložitveno sodišče pojasnjuje, da je bila po združitvi te kazni s kaznijo zapora štirih let in sedmih mesecev, na katero je bila H. K. obsojena s sodbo Viru Maakohus (prvostopenjsko sodišče v Viruju) z dne 22. marca 2016, obsojenki izrečena enotna kazen zapora petih let in enega meseca.

16. Da je Viru Maakohus (prvostopenjsko sodišče v Viruju) obsodilo H. K. zaradi teh kaznivih dejanj, se je med drugim oprlo na več zapisnikov, ki so bili sestavljeni na podlagi podatkov o elektronskih komunikacijah iz člena 111^1(2) zakona o elektronskih komunikacijah, ki jih je preiskovalni organ v predkazenskem postopku zbral pri ponudniku telekomunikacijskih storitev, potem ko je na podlagi člena 90^1(2) zakona o kazenskem postopku pridobil soglasja državnega tožilca Viru Ringkonnaprokuratuur (okrožno državno tožilstvo v Viruju, Estonija).

17. Tako je državni tožilec okrožnega državnega tožilstva v Viruju 2. novembra 2015 dal soglasje, da preiskovalni organ od telekomunikacijskega podjetja zahteva predložitev podatkov iz člena 111^1(2) zakona o elektronskih komunikacijah, da bi se s pomočjo dveh številk mobilnega telefona H. K. ugotovili prenos klicev in sporočil, njihovo trajanje, način prenosa, osebni podatki in lokacija kličoče osebe oziroma pošiljatelja in klicane osebe oziroma prejemnika dne 21. septembra 2015.

18. Preiskovalni organ je 4. novembra 2015 o podatkih, pridobljenih od telekomunikacijskega podjetja na podlagi tega soglasja, sestavil zapisnik, v katerem so navedeni oddajniki, v dometu katerih je bila 21. septembra 2015 po 19. uri uporabljena naročniška številka, ki jo je uporabljala H. K. Državno tožilstvo je želelo s tem zapisnikom in drugimi dokazi pred sodiščem dokazati, da je H. K. storila tatvino, storjeno 21. septembra 2015.

19. Državni tožilec okrožnega državnega tožilstva v Viruju je 25. februarja 2016 dal soglasje, da preiskovalni organ od telekomunikacijskega podjetja zahteva, da ta za preiskavo kaznivega dejanja po členu 303(1) Karistusseadustik (kazenski zakonik)[11] predloži podatke iz člena 111^1(2) zakona o elektronskih komunikacijah v zvezi s sedmimi naročniškimi številkami, ki jih je H. K. uporabljala v obdobju od 1. marca 2015 do 19. februarja 2016.

20. Preiskovalni organ je 15. marca 2016 o podatkih, pridobljenih od telekomunikacijskega podjetja na podlagi tega soglasja, sestavil zapisnik, v katerem so navedeni datumi, na katere je H. K. poklicala soobdolžence in od njih prejela klice, ter datumi, na katere je H. K. soobdolžencem poslala in od njih prejela sporočila. Državno tožilstvo je želelo s tem zapisnikom in drugimi dokazi pred sodiščem dokazati, da je H. K. od pomladi 2015 večkrat po telefonu grozila soobdolžencem.

21. Preiskovalni organ je 20. aprila in 6. maja 2016 o podatkih, pridobljenih od telekomunikacijskega podjetja na podlagi istega soglasja, sestavil še dva zapisnika. V teh zapisnikih so navedene bazne postaje, v dometu katerih so bili 4., 27. in 31. avgusta 2015 ter od 1. do 3. septembra 2015 oddani in sprejeti klici z uporabo šestih naročniških številk, ki jih je uporabljala H. K. Državno tožilstvo je želelo s tema zapisnikoma in sklopom drugih dokazov pred sodiščem dokazati, da je H. K. storila šest tatvin, ki so bile storjene na navedene datume.

22. Preiskovalni organ je 20. aprila 2016 sestavil zapisnik, ki zajema podatke o dveh naročniških številkah, ki ju je uporabljala H. K. Natančneje, v tem zapisniku so navedene bazne postaje, v dometu katerih so bili od 16. do 19. januarja 2015 oddani in sprejeti klici z uporabo teh naročniških številk. Državno tožilstvo je želelo s tem zapisnikom in drugimi dokazi dokazati, da je H. K. med 17. in 19. januarjem 2015 z bančno kartico oškodovanca dvigovala gotovino z bankomata.

23. Podatki, na katerih temelji navedeni zapisnik, so bili od telekomunikacijskega podjetja pridobljeni na podlagi soglasij, ki ju je 28. januarja in 2. februarja 2015 dal državni tožilec okrožnega državnega tožilstva v Viruju v drugi kazenski zadevi. Ta zadeva se je nanašala na kaznivi dejanji po členu 200(2), točke 7, 8 in 9, kazenskega zakonika, in sicer na ropa, ki ju je 23. in 27. januarja 2015 storila neka

11 Gre za kaznivo dejanje vplivanja na izvajanje sodne oblasti. Navesti moram, da je Viru Maakohus (prvostopenjsko sodišče v Viruju) dejanja, očitana H. K., v tej točki prekvalificiralo v nasilje zoper udeleženca sodnega postopka po členu 323(1) kazenskega zakonika.

skupina ob uporabi orožja in z vlomom. Preiskovalni organ je lahko na podlagi teh soglasij od telekomunikacijskega podjetja zahteval predložitev podatkov iz člena 111^1(2) zakona o elektronskih komunikacijah v zvezi z dvema naročniškima številkama in različnimi mednarodnimi identitetami mobilnega terminala, ki so pripadale H. K, za obdobje od 1. januarja do 2. februarja 2015.

24. Iz tega opisa dejanskega stanja v postopku v glavni stvari je razvidno, da je državno tožilstvo v skladu s členom 90^1(2) zakona o kazenskem postopku dalo soglasja, da preiskovalni organ v predkazenskem postopku na telekomunikacijsko podjetje naslovi zahteve za predložitev podatkov. Soglasja, ki so se nanašala na podatke o naročniških številkah obdolženke, so bila zaradi preiskave različnih kaznivih dejanj dana za obdobje enega dneva, približno enega meseca oziroma približno enega leta.

25. H. K. je zoper sodbo Viru Maakohus (prvostopenjsko sodišče v Viruju) vložila pritožbo pri Tartu Ringkonnakohus (pritožbeno sodišče v Tartuju, Estonija), ki je s sodbo z dne 17. novembra 2017 to pritožbo zavrnilo. Nato je H. K. vložila kasacijsko pritožbo pri Riigikohus (vrhovno sodišče), pri čemer je predlagala razveljavitev sodb prvostopenjskega in pritožbenega sodišča, končanje kazenskega pregona zoper njo ter svojo oprostitev.

26. H. K. trdi, da zapisniki, ki zajemajo podatke, pridobljene od telekomunikacijskega podjetja, niso dopustni dokazi in da njena obsodba na podlagi teh zapisnikov ni utemeljena. V skladu s sodbo Tele2 Sverige in Watson in drugi naj bi bili pravila člena 111^1 zakona o elektronskih komunikacijah, ki določajo obveznost za te ponudnike storitev, da hranijo podatke o komunikacijah, in uporaba teh podatkov za njeno obsodbo v nasprotju s členom 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine.

27. Po mnenju predložitvenega sodišča se tako postavlja vprašanje, ali je zadevne zapisnike, ki jih je preiskovalni organ sestavil na podlagi podatkov iz člena 111^1(2) zakona o elektronskih komunikacijah, ki so bili zahtevani od telekomunikacijskega podjetja s soglasji državnega tožilstva, mogoče šteti za dopustne dokaze.

28. Podatki, ki naj bi jih ponudniki elektronskih komunikacijskih storitev morali hraniti eno leto, naj bi zajemali med drugim številko kličočega in klicanega priključka, ime in naslov naročnika, datum in uro začetka in konca klica, uporabljeno telefonsko storitev ali storitev mobilne telefonije, mednarodno identiteto mobilnega naročnika in mednarodno identiteto mobilnega terminala kličočega in klicanega priključka ter lokacijsko oznako (ID celice) na začetku klica in podatke, ki določajo zemljepisno lego celic. Predložitveno sodišče poudarja, da gre za podatke o tem, da se je zgodil prenos klicev in sporočil po telefonu ali mobilnem telefonu, in o lokaciji uporabe mobilnega terminala, da pa ti podatki ne zagotavljajo informacij o vsebini komunikacij.

29. Kot naj bi izhajalo iz sodbe Tele2 Sverige in Watson in drugi ter iz sodbe z dne 2. oktobra 2018, Ministerio Fiscal [12], naj bi nacionalni predpisi, ki urejajo hrambo podatkov o prometu in podatkov o lokaciji ter dostop do teh podatkov v okviru kazenskega postopka, kot sta člen 111^1(2) in (4) zakona o elektronskih komunikacijah ter člen 90^1(2) zakona o kazenskem postopku, spadali na področje uporabe Direktive 2002/58/ES.

30. Dopustnost dokazov naj bi bila odvisna od tega, ali so bili upoštevani postopkovni predpisi o zbiranju dokazov. Tako naj bi bilo treba pri presoji, ali so zapisniki iz postopka v glavni stvari dopustni kot dokazi, preučiti tudi vprašanje, v kolikšni meri so bili podatki, na katerih ti zapisniki temeljijo, pri telekomunikacijskem podjetju zbrani v skladu s členom 15(1) te direktive v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine.

12 C-207/16, v nadaljevanju: sodba Ministerio Fiscal, EU:C:2018:788.

31. Ob upoštevanju sodb Tele2 Sverige in Watson in drugi [13] ter Ministerio Fiscal [14] se predložitveno sodišče sprašuje, ali je treba člen 15(1) Direktive 2002/58/ES v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine razlagati tako, da dostop nacionalnih organov do podatkov, ki omogočajo, da se v zvezi s telefonsko komunikacijo ali komunikacijo po mobilnem telefonu osumljenca ugotovijo izhodiščni in ciljni kraj, datum, ura in trajanje, vrsta komunikacijske storitve, uporabljeni terminal in lokacija uporabe mobilnega terminala, pomeni poseg v temeljne pravice, določene v teh členih Listine, ki je tako hud, da je treba ta dostop omejiti na boj proti hudemu kriminalu, ne glede na obdobje, za katero so ti nacionalni organi zahtevali dostop do hranjenih podatkov.

32. V zvezi s tem predložitveno sodišče meni, da je obdobje, za katero se zahtevajo zadevni podatki, bistvena okoliščina za oceno teže posega v temeljne pravice, ki naj bi ga pomenil dostop do teh podatkov. Zato naj bi bilo mogoče, da se ta poseg ne bi smel šteti za hud, če bi se zahtevani podatki nanašali le na zelo kratko obdobje, kot je en dan. V tem primeru naj praviloma na podlagi teh podatkov ne bi bilo mogoče priti do natančnih ugotovitev o zasebnem življenju zadevne osebe, zaradi česar naj bi lahko bil dostop nacionalnih organov do navedenih podatkov upravičen s ciljem preiskovanja in pregona kaznivih dejanj na splošno.

33. Poleg tega se predložitveno sodišče sprašuje, ali je ob upoštevanju spoznanj, ki izhajajo iz sodbe Ministerio Fiscal [15], dostop do podatkov, kot so ti v postopku v glavni stvari, lahko upravičen s tem istim ciljem, če je količina podatkov, do katerih imajo organi dostop, majhna in poseg v temeljne pravice zato ni hud. Kar zadeva količino podatkov, naj bi bilo bistveno upoštevati vrsto podatkov (kot so podatki o naslovniku komunikacije ali lokaciji terminala) in dolžino zadevnega obdobja (na primer en dan, en mesec ali eno leto). Predložitveno sodišče meni, da hujše kot bi bilo kaznivo dejanje, hujši bi lahko bil dovoljeni poseg v temeljne pravice v okviru postopka, kar pomeni, da bi bila količina podatkov, do katerih lahko nacionalni organi dostopajo, toliko večja.

34. Nazadnje se predložitveno sodišče sprašuje, ali je državno tožilstvo mogoče šteti za „neodvisen“ upravni organ v smislu sodbe Tele2 Sverige in Watson in drugi [16]. Navaja, da v Estoniji državno tožilstvo vodi predkazenski postopek, katerega cilj je med drugim zbrati dokaze. Poleg tega poudarja, da morata preiskovalni organ in državno tožilstvo razjasniti obremenilne in razbremenilne okoliščine za osumljenca. Na koncu opozarja, da pooblastila državnega tožilstva v njegovem imenu izvaja državni tožilec, ki je pri opravljanju svojih nalog neodvisen, kar izhaja iz člena 30(1) in (2) zakona o kazenskem postopku ter iz člena 1(1) in (1^1) in člena 2(2) zakona o državnem tožilstvu.

35. V tem okviru predložitveno sodišče poudarja, da so njegovi dvomi glede neodvisnosti, zahtevane s pravom Unije, predvsem posledica tega, da državno tožilstvo, če je po predkazenskem postopku prepričano, da so zbrani vsi potrebni dokazi, in če obstajajo razlogi za to, vloži obtožni akt zoper zadevno osebo. Kot navaja predložitveno sodišče, v tem primeru državno tožilstvo zastopa obtožbo pred sodiščem in je tako tudi udeleženec sodnega postopka. Predložitveno sodišče tudi opozarja, da je Evropsko sodišče za človekove pravice že priznalo, da se lahko pri nadzornih ukrepih pod določenimi pogoji ne izvede predhodni sodni nadzor, če se sodni nadzor izvede pozneje. [17]

13 Izrek, točka 2, te sodbe.

14 Točki 53 in 57 te sodbe.

15 Točke od 55 do 57 te sodbe.

16 Točka 120 in izrek, točka 2, te sodbe.

17 Predložitveno sodišče v zvezi s tem navaja sodbi ESČP z dne 2. septembra 2010, Uzun proti Nemčiji (CE:ECHR:2010:0902JUD003562305, točke od 71 do 74), ter z dne 12. januarja 2016, Szabó in Vissy proti Madžarski (CE:ECHR:2016:0112JUD003713814, točka 77).

36. V teh okoliščinah je Riigikohus (vrhovno sodišče) prekinilo odločanje in Sodišču v predhodno odločanje predložilo ta vprašanja:

„1. Ali je treba člen 15(1) Direktive [2002/58] v povezavi s členi 7, 8, 11 in 52(1) [Listine] razlagati tako, da v kazenskem postopku dostop nacionalnih organov, ki omogoča, da se v zvezi s telefonsko komunikacijo ali komunikacijo po mobilnem telefonu obdolženca ugotovijo izhodiščni in ciljni kraj, datum, ura in trajanje, vrsta komunikacijske storitve, uporabljeni terminal in lokacija uporabe mobilnega terminala, pomeni tako resen poseg v temeljne pravice, določene v navedenih členih Listine, da je treba ta dostop na področju preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj omejiti na boj proti hudemu kriminalu, ne glede na to, na kako dolgo obdobje se nanašajo hranjeni podatki, do katerih imajo dostop nacionalni organi?

2. Ali je treba člen 15(1) Direktive [2002/58] ob upoštevanju načela sorazmernosti, ki je bilo poudarjeno v točkah od 55 do 57 sodbe [Ministerio Fiscal], razlagati tako, da je lahko, če količina podatkov, navedenih v prvem vprašanju, do katerih imajo dostop nacionalni organi, (niti glede na vrsto niti glede na obdobje, za katero se dajejo na razpolago) ni velika, poseg v temeljne pravice, ki je povezan s tem, na splošno upravičen s ciljem preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj, in da morajo biti kazniva dejanja, ki naj bi se preprečila s tem posegom, toliko hujša, kolikor je večja količina podatkov, do katerih imajo dostop nacionalni organi?

3. Ali zahteva iz točke 2 izreka sodbe [Tele2 Sverige in Watson in drugi], da mora sodišče ali neodvisni upravni organ predhodno opraviti nadzor nad dostopom pristojnih nacionalnih organov do podatkov, pomeni, da je treba člen 15(1) Direktive [2002/58] razlagati tako, da se lahko državno tožilstvo, ki vodi predkazenski postopek, pri čemer je po zakonu dolžno ravnati neodvisno in ga zavezuje samo zakon ter v predkazenskem postopku razjasnjuje obremenilne in tudi razbremenilne okoliščine za obdolženca, vendar pozneje v sodnem postopku zastopa obtožbo, šteje za neodvisni upravni organ?“

IV. Analiza

37. Predložitveno sodišče želi s prvim in drugim vprašanjem za predhodno odločanje v bistvu izvedeti, ali je treba člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine razlagati tako, da merila, na podlagi katerih je mogoče presoditi težo posega v temeljne pravice, ki ga pomeni dostop pristojnih nacionalnih organov do osebnih podatkov, ki jih morajo v skladu z nacionalnimi predpisi hraniti ponudniki elektronskih komunikacijskih storitev, vključujejo vrste zadevnih podatkov in dolžino obdobja, za katero se zahteva dostop.

38. Preden odgovorim na to vprašanje, bom podal dva sklopa uvodnih ugotovitev, na podlagi katerih bom lahko odgovoril na eni strani na trditve, ki jih navajajo nekatere države članice glede področja uporabe Direktive 2002/58, in na drugi strani na predlog Evropske komisije, naj se v okviru tega predloga za sprejetje predhodne odločbe preizkusi združljivost estonskih predpisov s pravom Unije v delu, v katerem ti predpisi ponudnikom elektronskih komunikacijskih storitev nalagajo, da hranijo več vrst osebnih podatkov, pridobljenih v okviru teh storitev.

A. Uvodne ugotovitve

1. Področje uporabe Direktive 2002/58

39. Irska, madžarska in poljska vlada izpostavljajo vprašanja glede področja uporabe Direktive 2002/58.

40. Zdi se, da irska vlada meni, da so nacionalni predpisi o dostopu organov, pristojnih za kazenske zadeve, do hranjenih podatkov v skladu s členom 1(3) Direktive 2002/58 izključeni s področja uporabe te direktive.

41. To trditev je treba zavrniti na podlagi sodne prakse Sodišča, ki izhaja iz sodb Tele2 Sverige in Watson in drugi ter Ministerio Fiscal.

42. V zvezi s tem je treba navesti, da je Sodišče odločilo, da zakonski ukrepi iz člena 15(1) Direktive 2002/58 „na področje uporabe te direktive spadajo tudi, če se nanašajo na dejavnosti držav ali drugih državnih organov, ki niso povezane s področji dejavnosti posameznikov, in če so nameni, ki jim morajo slediti ti ukrepi, v bistvu enaki namenom, ki jim sledijo dejavnosti iz člena 1(3) Direktive 2002/58“.[18] Kot je presodilo Sodišče, „[č]len 15(1) te direktive namreč nujno predpostavlja, da nacionalni ukrepi, ki so v njej navedeni, spadajo na področje uporabe navedene direktive, ker ta državam članicam izrecno dopušča, da jih sprejmejo le ob upoštevanju pogojev, ki jih določa. Poleg tega zakonski ukrepi iz člena 15(1) Direktive 2002/58 za namene, navedene v tej določbi, urejajo dejavnost ponudnikov elektronskih komunikacijskih storitev“[19].

43. Sodišče je na podlagi tega ugotovilo, da „je treba navedeni člen 15(1) v povezavi s členom 3 Direktive 2002/58 razlagati tako, da na področje uporabe te direktive zlasti spada ne le zakonski ukrep, ki ponudnikom elektronskih komunikacijskih storitev nalaga, da hranijo podatke o prometu in podatke o lokaciji, temveč tudi zakonski ukrep, ki se nanaša na dostop nacionalnih organov do podatkov, ki jih hranijo ti ponudniki“[20].

44. Kot je presodilo Sodišče, se „[v]arstvo zaupnosti elektronskih komunikacij in z njimi povezanih podatkov o prometu, ki ga zagotavlja člen 5(1) Direktive 2002/58, […] namreč uporablja za ukrepe, ki so jih sprejele katere koli osebe razen uporabnikov, ne glede na to, ali gre za posameznike, zasebne subjekte ali državne organe. Kot je potrjeno v uvodni izjavi 21 te direktive, je njen namen preprečiti nedovoljen ‚dostop‘ do sporočil, vključno ‚z vsemi podatki glede teh sporočil‘, da se zagotovi zaupnost elektronskih sporočil“[21].

45. Tem argumentom je Sodišče dodalo, da „zakonski ukrepi, ki ponudnikom elektronskih komunikacijskih storitev nalagajo, da hranijo osebne podatke ali da pristojnim nacionalnim organom odobrijo dostop do teh podatkov, nujno pomenijo obdelavo navedenih podatkov s strani teh ponudnikov […]. Takih ukrepov v delu, v katerem urejajo dejavnosti navedenih dobaviteljev, zato ni mogoče šteti za dejavnosti držav iz člena 1(3) Direktive 2002/58“[22].

46. Po zgledu odločitve Sodišča v sodbi Ministerio Fiscal[23] je treba iz vseh teh argumentov sklepati, da zahteva za dostop do osebnih podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev, podana v okviru kazenskega preiskovalnega postopka, spada na področje uporabe Direktive 2002/58.

47. Poleg tega madžarska in poljska vlada trdita, da pravo Unije ne ureja vprašanja dopustnosti dokazov v kazenskih postopkih.

48. Res je, da to pravo v sedanjem stanju svojega razvoja ne ureja pravil o dopustnosti dokazov v kazenskem postopku, vendar je predložitveno sodišče jasno poudarilo, zakaj je razlaga prava Unije, za katero prosi, potrebna, da bi lahko odločilo o dopustnosti dokazov. Ta je namreč odvisna od tega, ali so bili upoštevani pogoji in postopkovni predpisi za zbiranje teh dokazov. Tako mora predložitveno

18 Sodba Ministerio Fiscal (točka 34 in navedena sodna praksa).

19 Prav tam.

20 Sodba Ministerio Fiscal (točka 35 in navedena sodna praksa).

21 Sodba Ministerio Fiscal (točka 36 in navedena sodna praksa).

22 Sodba Ministerio Fiscal (točka 37 in navedena sodna praksa).

23 Glej sodbo Ministerio Fiscal (točki 38 in 39).

sodišče pri presoji, ali so zapisniki iz postopka v glavni stvari dopustni kot dokazi, preučiti predhodno vprašanje, v kolikšni meri so bili podatki, na katerih ti zapisniki temeljijo, pri telekomunikacijskem podjetju zbrani v skladu s členom 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine. To predhodno vprašanje pa se nanaša na vidik, ki je, kot sem že poudaril, urejen s pravom Unije. S tega vidika morajo biti nacionalna pravila, ki se uporabijo na področju izvajanja dokazov, torej v skladu z zahtevami, ki izhajajo iz temeljnih pravic, zagotovljenih s pravom Unije.[24] V teh okoliščinah trditev, ki jo navajata madžarska in poljska vlada, po mojem mnenju ni upoštevna.

2. Hramba podatkov o prometu in o lokaciji

49. Čeprav se vprašanja, ki jih postavlja predložitveno sodišče, nanašajo na pogoje dostopa do podatkov, Komisija Sodišču predlaga, naj se v okviru tega predloga za sprejetje predhodne odločbe opredeli tudi do problematike, povezane s hrambo podatkov. V zvezi s tem ta institucija v bistvu ugotavlja, da je za zakonit dostop do hranjenih podatkov potrebno, da nacionalni predpisi, ki ponudnikom elektronskih komunikacijskih storitev nalagajo hrambo podatkov, pridobljenih v okviru teh storitev, izpolnjujejo zahteve, določene v členu 15(1) Direktive 2002/58 v povezavi z Listino, ali da so ti ponudniki zadevne podatke hranili na lastno pobudo, zlasti v poslovne namene, v skladu s to direktivo.

50. Komisija glede postopka v glavni stvari ugotavlja, da podatkov, do katerih je preiskovalni organ imel dostop, ponudniki elektronskih komunikacijskih storitev niso hranili na lastno pobudo v poslovne namene, temveč zaradi obveznosti hrambe, ki jim jo nalaga člen 111^1 zakona o elektronskih komunikacijah. Navaja tudi, da H. K. izpodbija zakonitost nacionalnih pravil o dostopu do podatkov in o njihovi hrambi.[25]

51. Ob tem poudarjam, da se enako kot v okviru predloga za sprejetje predhodne odločbe, na podlagi katerega je bila izrečena sodba Ministerio Fiscal[26], z vprašanji, ki jih postavlja predložitveno sodišče v okviru obravnavane zadeve, ne želi ugotoviti, ali so ponudniki elektronskih komunikacijskih storitev osebne podatke iz postopka v glavni stvari hranili ob upoštevanju pogojev iz člena 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine. Ta vprašanja se nanašajo samo na združljivost pogojev, pod katerimi je v skladu z estonskimi predpisi nacionalnim preiskovalnim organom dovoljen dostop do takih podatkov, z zgoraj navedenimi določbami. Zato je razprava, ki se je razvila pred Sodiščem, zadevala skoraj izključno te pogoje dostopa.

52. Vsekakor se lahko predložitveno sodišče, če meni, da je za rešitev spora o glavni stvari treba odločiti o združljivosti člena 111^1 zakona o elektronskih komunikacijah s pravom Unije, opre na sodno prakso, ki izhaja iz sodbe Tele2 Sverige in Watson in drugi.

53. V zvezi s tem bom samo spomnil, da je Sodišče odločilo, da „je treba člen 15(1) Direktive 2002/58 glede na člene 7, 8, 11 in 52(1) Listine razlagati tako, da nasprotuje nacionalni ureditvi, ki z namenom boja proti kriminalu določa splošno in neselektivno hrambo vseh podatkov o prometu in podatkov o lokaciji vseh naročnikov in registriranih uporabnikov glede vseh elektronskih komunikacijskih sredstev“[27].

24 Glej po analogiji zlasti sodbo z dne 10. aprila 2003, Steffensen (C-276/01, EU:C:2003:228, točka 71). V tej sodbi Sodišče to problematiko obravnava tudi z vidika načela učinkovitosti kot meje procesne avtonomije držav članic (točke od 66 do 68).

25 Komisija v tem okviru poudarja, da se obravnavana zadeva razlikuje od zadeve, v kateri je bila izrečena sodba Ministerio Fiscal.

26 Glej sodbo Ministerio Fiscal (točki 49 in 50).

27 Sodba Tele2 Sverige in Watson in drugi (točka 112).

54. Predložitveno sodišče mora po potrebi preveriti, ali estonski predpisi ponudnikom elektronskih komunikacijskih storitev nalagajo takšno splošno in neselektivno obveznost hrambe podatkov, ter iz tega izpeljati posledice za rešitev spora o glavni stvari. Če bi bilo ureditev hrambe podatkov, ki jo je uvedla Republika Estonija, treba šteti za neskladno s pravom Unije zaradi njene nesorazmernosti glede na uresničevani cilj, tudi dostop do tako hranjenih podatkov ne bi mogel biti upravičen s tem ciljem.

55. Ta obveznost hrambe bo preizkus sorazmernosti lahko prestala le, če jo spremljajo ustrezne omejitve, zlasti kar zadeva vrste zadevnih podatkov in trajanje hrambe, na podlagi ureditve, ki je selektivna glede na uresničevani cilj in nujno potrebna za doseganje tega cilja.

56. V okviru teh sklepnih predlogov ne bom natančneje obravnaval pojma „omejena hramba podatkov“, ki ga je podrobno preučil generalni pravobranilec M. Campos Sánchez-Bordona v sklepnih predlogih, ki jih je predstavil 15. januarja 2020 v zadevi Ordre des barreaux francophones et germanophone [28].

B. Dostop pristojnih nacionalnih organov do hranjenih podatkov

1. Spoznanja iz sodbe Tele2 Sverige in Watson in drugi

57. Sodišče problematiko dostopa pristojnih nacionalnih organov do hranjenih podatkov razume „neodvisno od obsega obveznosti hrambe podatkov, ki naj bi bila naložena ponudnikom elektronskih komunikacijskih storitev“, in zlasti neodvisno od splošne ali ciljne narave hrambe podatkov. [29] Ta ugotovitev je povezana z dejstvom, da Sodišče šteje hrambo podatkov in dostop do njih za ločena posega v temeljne pravice, varovane z Listino.

58. Dostop do hranjenih podatkov mora „dejansko in strogo ustrezati kateremu od […] ciljev“ iz člena 15(1), prvi stavek, Direktive 2002/58. Poleg tega mora obstajati ujemanje med težo posega in uresničevanim ciljem. Če je poseg opredeljen kot „hud“, je lahko upravičen le z bojem proti hudemu kriminalu. [30]

59. Enako kot velja za hrambo podatkov, je dostop do njih s strani pristojnih nacionalnih organov mogoče dovoliti le v mejah tistega, kar je nujno potrebno. [31] Poleg tega morajo zakonski ukrepi „določiti jasna in natančna pravila, ki določajo, v katerih okoliščinah in pod kakšnimi pogoji morajo ponudniki elektronskih komunikacijskih storitev pristojnim nacionalnim organom omogočiti dostop do podatkov. Tak ukrep mora biti tudi zakonsko zavezujoč v nacionalnem pravu.“ [32] Natančneje, nacionalni predpisi morajo „določiti […] vsebinske in postopkovne pogoje, ki urejajo dostop pristojnih nacionalnih organov do hranjenih podatkov“ [33].

60. Iz navedenega je mogoče sklepati, da „ni mogoče šteti, da je splošni dostop do vseh hranjenih podatkov, neodvisno od kakršne koli vezi, tudi posredne, s ciljem, ki se mu sledi, omejen na nujno potrebno“ [34].

28 C-520/18, EU:C:2020:7. Glej zlasti točke od 72 do 107 teh sklepnih predlogov.

29 Glej sodbo Tele2 Sverige in Watson in drugi (točka 113).

30 Glej sodbo Tele2 Sverige in Watson in drugi (točka 115).

31 Glej sodbo Tele2 Sverige in Watson in drugi (točka 116).

32 Sodba Tele2 Sverige in Watson in drugi (točka 117).

33 Sodba Tele2 Sverige in Watson in drugi (točka 118).

34 Sodba Tele2 Sverige in Watson in drugi (točka 119).

61. Kot je odločilo Sodišče, „se mora zadevna nacionalna ureditev pri določitvi okoliščin in pogojev, pod katerimi se pristojnim nacionalnim organom omogoči dostop do podatkov naročnikov ali registriranih uporabnikov, opreti na objektivna merila. V zvezi s tem je dostop v povezavi z namenom boja proti kriminalu načeloma mogoče odobriti le do podatkov oseb, za katere obstaja sum, da nameravajo izvršiti ali da so izvršile hudo kaznivo dejanje ali da so tako ali drugače povezane s tem kaznivim dejanjem“ [35].

62. Z drugimi besedami, nacionalni predpisi, ki pristojnim nacionalnim organom omogočajo dostop do hranjenih podatkov, morajo imeti dovolj omejen obseg, da se prepreči, da bi se tak dostop lahko nanašal na veliko število oseb ali celo na vse osebe in vsa elektronska komunikacijska sredstva ter vse hranjene podatke. Zato je Sodišče določilo merilo vezi med zadevnimi osebami in uresničevanim ciljem.

63. Poleg tega je postavilo pogoje, ki jih mora izpolnjevati vsak dostop pristojnih nacionalnih organov do hranjenih podatkov.

64. Najprej, za ta dostop mora „načeloma, razen v nujnih primerih, ki so ustrezno utemeljeni, sodišče ali neodvisen upravni organ opravi[ti] predhoden nadzor“ [36]. Odločba tega sodišča ali tega organa mora biti izdana „na obrazložen predlog, ki se ga predloži v postopku preprečevanja, odkrivanja ali pregona kaznivih dejanj“ [37].

65. Dalje, kot je navedlo Sodišče, „je pomembno, da pristojni nacionalni organi, ki jim je bil odobren dostop do hranjenih podatkov, v okviru veljavnih nacionalnih postopkov o tem obvestijo zadevne osebe takoj, ko to sporočilo ne more ogroziti preiskav, ki jih vodijo ti organi“ [38].

66. Nazadnje, države članice morajo sprejeti pravila o varnosti in varstvu podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev, da se preprečijo zlorabe in kakršen koli nepooblaščen dostop do podatkov. [39]

2. Spoznanja iz sodbe Ministerio Fiscal

67. V navedeni zadevi je bilo Sodišču predloženo vprašanje, ali so nacionalni predpisi, s katerimi je predviden dostop pristojnih nacionalnih organov, kot je kriminalistična policija, do podatkov o osebni istovetnosti imetnikov nekaterih kartic SIM, združljivi s členom 15(1) Direktive 2002/58 v povezavi s členoma 7 in 8 Listine.

68. Sodišče je v sodbi poudarilo, da v zvezi s ciljem preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj člen 15(1), prvi stavek, Direktive 2002/58 tega cilja ne omejuje na boj proti hudim kaznivim dejanjem, ampak se nanaša na „kazniva dejanja“ na splošno. [40]

69. Razlogovanje, ki ga je razvilo Sodišče, jasno kaže, da mora v zvezi z dostopom pristojnih nacionalnih organov do podatkov obstajati ujemanje med težo posega in težo zadevnih kaznivih dejanj.

35 Prav tam.

36 Sodba Tele2 Sverige in Watson in drugi (točka 120).

37 Prav tam.

38 Sodba Tele2 Sverige in Watson in drugi (točka 121).

39 Glej sodbo Tele2 Sverige in Watson in drugi (točka 122).

40 Glej sodbo Ministerio Fiscal (točka 53).

70. Tako Sodišče ob sklicevanju na točko 99 svoje sodbe Tele2 Sverige in Watson in drugi opozarja, da je sicer res presodilo, da „lahko na področju preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj dostop javnih organov do osebnih podatkov, ki jih hranijo ponudniki elektronskih komunikacijskih storitev, upraviči le boj proti hudemu kriminalu, ker je na podlagi vseh teh podatkov mogoče izpeljati natančne ugotovitve o zasebnem življenju oseb, za podatke katerih gre“ [41].

71. Vendar Sodišče pojasnjuje, da je „to razlago utemeljilo s tem, da mora biti cilj, ki se uresničuje z ureditvijo, ki ta dostop ureja, povezan s težo posega v zadevne temeljne pravice, ki ga povzroči ta operacija“ [42].

72. „V skladu z načelom sorazmernosti lahko namreč na področju preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj hud poseg upraviči le cilj boja proti kriminalu, ki mora biti prav tako opredeljen kot ‚hud‘.“ [43]

73. Nasprotno pa se, „kadar poseg, ki ga pomeni tak dostop, ni hud, […] navedeni dostop lahko upraviči s ciljem preprečevanja, preiskovanja, odkrivanja in pregona ‚kaznivih dejanj‘ na splošno“ [44].

74. Zaradi teh premislekov je bilo torej treba presoditi, ali je treba na podlagi okoliščin obravnavanega primera poseg v temeljne pravice iz členov 7 in 8 Listine, ki bi ga povzročil dostop kriminalistične policije do podatkov iz postopka v glavni stvari, šteti za „hud“.

75. Sodišče pa v nasprotju s tem, kar je storilo v sodbi Tele2 Sverige in Watson in drugi, posega v pravice, varovane s členoma 7 in 8 Listine, ki ga je pomenil dostop do zadevnih podatkov, ni opredelilo kot „hudega“. [45] „[E]dini namen zahteve“ za dostop je bila namreč „identifikacija imetnikov kartic SIM, ki so bile v obdobju dvanajstih dni aktivirane s številko [mednarodne identitete mobilnega terminala] ukradenega mobilnega telefona“. [46] Šlo je „le [z]a dostop do telefonskih številk, ki [so] ustreza[le] tem karticam SIM, in do podatkov o osebni istovetnosti imetnikov navedenih kartic, kot so priimek, ime in po potrebi naslov. Nasprotno pa se […] ti podatki n[iso] nanaša[li] na komunikacije, ki so bile opravljene z ukradenim mobilnim telefonom, niti na njegovo lokacijo.“ [47]

76. Sodišče je iz tega sklepalo, da „podatki iz zahteve za dostop iz postopka v glavni stvari omogočajo zgolj povezavo – v nekem obdobju – med kartico ali karticami SIM, aktiviranimi z ukradenim mobilnim telefonom, in osebno istovetnostjo imetnikov teh kartic SIM. Brez prekrivanja s podatki, ki se nanašajo na komunikacije, opravljene z navedenimi karticami SIM, in podatki o lokaciji navedeni podatki ne omogočajo seznanitve z datumom, uro, trajanjem in prejemniki komunikacij, opravljenih z zadevno kartico ali karticami SIM, niti z okoljem, v katerem so bile te komunikacije opravljene, ali z njihovo pogostostjo z določenimi osebami v danem obdobju. Navedeni podatki zato ne omogočajo izpeljave natančnih ugotovitev o zasebnem življenju oseb, za podatke katerih gre.“ [48]

77. Ko je bila opredelitev dostopa kot „hudega posega“ izključena, je Sodišče lahko ugotovilo, da je zadevni poseg mogoče upravičiti s sklicevanjem na cilj preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj na splošno, tudi če ta niso huda. [49]

41 Sodba Ministerio Fiscal (točka 54).
42 Sodba Ministerio Fiscal (točka 55).
43 Sodba Ministerio Fiscal (točka 56).
44 Sodba Ministerio Fiscal (točka 57).
45 Sodba Ministerio Fiscal (točka 61).
46 Sodba Ministerio Fiscal (točka 59).
47 Prav tam.
48 Sodba Ministerio Fiscal (točka 60).
49 Sodba Ministerio Fiscal (točka 62).

78. Z vidika te sodne prakse predložitveno sodišče postavlja prvo in drugo vprašanje za predhodno odločanje, da bi se presodila teža posega, ki ga pomeni dostop do podatkov v kazenskem postopku v glavni stvari. Natančneje, izvedeti želi, ali se za upoštevni merili v tem pogledu štejejo vrste zadevnih podatkov in dolžina obdobja, za katero se zahteva dostop do teh podatkov.

3. Merila, ki omogočajo oceno teže posega

79. Kot izhaja iz sodne prakse Sodišča, več kot je vrst podatkov, do katerih se zahteva dostop, večja je možnost, da se poseg opredeli kot „hud“.

80. Ob tem bo v okviru prvega in drugega vprašanja, ki ju postavlja predložitveno sodišče, Sodišče moralo pojasniti, ali ima poleg vrst zadevnih podatkov vlogo pri ugotavljanju teže posega tudi dolžina obdobja, na katero se nanaša ta dostop.

81. Po mojem mnenju bi moral biti odgovor pritrdilen. Poleg tega je treba navesti, da je Sodišče v sodbi Ministerio Fiscal v okviru svoje presoje prav tako upoštevalo dolžino obdobja, na katero se je nanašal dostop, in sicer v navedenem primeru 12 dni.[50]

82. Povezava vrste zadevnih podatkov in dolžine obdobja, na katero se nanaša dostop, je tista, ki omogoča presojo teže posega. Na podlagi teh dveh vidikov je namreč mogoče preveriti, ali je merilo, ki določa težo posega, izpolnjeno, to je, ali lahko dostop do zadevnih podatkov pristojnim nacionalnim organom omogoči, da izpeljejo natančne ugotovitve o zasebnem življenju oseb, na podatke katerih se nanaša ta dostop. Da pa je mogoče ustvariti natančen portret neke osebe, je potrebno ne le, da dostop zadeva več vrst podatkov, kot so identifikacijski podatki, podatki o prometu in podatki o lokaciji, temveč tudi, da se ta dostop nanaša na dovolj dolgo obdobje, da se lahko dovolj natančno razkrijejo glavne značilnosti življenja osebe.

83. Enako kot število zadevnih vrst podatkov je dolžina obdobja, za katero se zahtevajo podatki v skladu s soglasjem za dostop, torej bistven element za presojo teže posega v temeljne pravice zadevnih oseb. Kot navaja Komisija, je treba upoštevati tudi kopičenje več zahtev za dostop v zvezi z eno in isto osebo, tudi če se te zahteve nanašajo na kratka obdobja.

84. Kot je razvidno iz predloga za sprejetje predhodne odločbe, so podatki, do katerih je preiskovalni organ imel dostop, tisti iz člena 111^{1}(2) zakona o elektronskih komunikacijah. Ti podatki omogočajo, da se v zvezi s telefonsko komunikacijo ali komunikacijo po mobilnem telefonu osebe ugotovijo izhodiščni in ciljni kraj, datum, ura in trajanje, vrsta komunikacijske storitve, uporabljeni terminal in lokacija uporabe mobilnega terminala. Ti podatki so bili preiskovalnemu organu posredovani za obdobja enega dneva, enega meseca in skoraj enega leta.

85. Presoja teže posega v temeljne pravice, ki ga pomeni dostop pristojnih nacionalnih organov do hranjenih osebnih podatkov, je rezultat konkretne preučitve okoliščin vsakega primera. Predložitveno sodišče mora v vsakem posameznem primeru presoditi, ali so lahko podatki, za dostop do katerih je bilo dano soglasje, glede na njihovo vrsto in dolžino obdobja, na katero se je ta dostop nanašal, omogočili izpeljavo natančnih ugotovitev o zasebnem življenju zadevnih oseb.

86. V primeru pritrdilnega odgovora bi moral biti poseg opredeljen kot „hud“ v smislu sodne prakse Sodišča ter bi torej lahko bil na področju preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj upravičen le s ciljem boja proti kriminalu, ki bi moral biti prav tako opredeljen kot „hud“.[51]

50 Glej sodbo Ministerio Fiscal (točka 59). Glej v istem smislu sklepne predloge generalnega pravobranilca H. Saugmandsgaarda Øeja v zadevi Ministerio Fiscal (C-207/16, EU:C:2018:300), ki ugotavlja, da se je predlog policijskih organov nanašal „na obdobje, ki je jasno opredeljeno in časovno omejeno, in sicer na dvanajst dni“ (točka 33, pa tudi točka 84).

51 Sodba Ministerio Fiscal (točka 56).

4. Ujemanje med težo posega in uresničevanim ciljem

87. Iz sodne prakse Sodišča izhaja, da poseg v temeljne pravice, ki je opredeljen kot „hud“, pomeni okrepljeno zahtevo po upravičenosti.

88. Kar zadeva težo domnevnih kaznivih dejanj, glede katerih je bilo dano soglasje za dostop do podatkov, Komisija ugotavlja, da je z nacionalnimi predpisi iz postopka v glavni stvari dostop dovoljen zlasti za boj proti kaznivim dejanjem na splošno.[52]

89. Predložitveno sodišče mora preveriti, ali glede na okoliščine primera dostop do podatkov, kot so ti iz postopka v glavni stvari, dejansko in strogo ustreza kateremu od ciljev iz člena 15(1) Direktive 2002/58. V zvezi s tem je treba spomniti, da ta določba cilja preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj ne omejuje na boj proti hudim kaznivim dejanjem, ampak se nanaša na „kazniva dejanja“ na splošno.[53]

90. Če predložitveno sodišče ugotovi, da je poseg treba opredeliti kot „hud“, mora presoditi, ali je zadevno kaznivo dejanje po nacionalnem kazenskem pravu prav tako mogoče opredeliti kot „hudo“.

91. V zvezi s tem menim, da je treba določitev tega, kaj se lahko opredeli kot „hudo kaznivo dejanje“, prepustiti presoji držav članic.

92. Glede na nacionalne pravne sisteme je namreč isto kaznivo dejanje lahko kaznovano bolj ali manj strogo. Tudi opredelitev obteževalnih okoliščin se lahko po državah članicah razlikuje.

93. Kot pravilno poudarja estonska vlada, pri določanju teže kaznivih dejanj kazen, ki se uporabi, ni edino merilo. Upoštevati je treba tudi naravo kaznivih dejanj, škodo, ki jo povzročijo družbi, škodljivost teh dejanj za pravne interese ter skupne posledice, ki jih imajo za nacionalni pravni red in za vrednote demokratične družbe. Zgodovinske, gospodarske in družbene okoliščine, ki so specifične za vsako državo članico, imajo tudi vlogo pri tem. Poleg tega se je treba v okviru obteževalnih okoliščin vprašati, ali so se na primer kazniva dejanja ponavljala oziroma so bila storjena zoper skupino ranljivih oseb.

94. Za presojo sorazmernosti dostopa je treba upoštevati tudi, da se v skladu s členom 90^1(3) zakona o kazenskem postopku „lahko podatki zahtevajo samo, če je to nujno za uresničitev cilja kazenskega postopka“. Kot navaja estonska vlada, merilo absolutne nujnosti[54] obvezuje tako preiskovalce kot osebe, odgovorne za dajanje soglasij, da upoštevajo in presodijo, kateri podatki so nujni za uspešno končanje kazenskega postopka in brez katerih v okviru dane zadeve ne bi bilo mogoče prizadevati si za ugotavljanje resnice ali prijeti domnevnega storilca kaznivega dejanja.

95. Naj dodam, da – kot je pravilno poudarila francoska vlada – teže kaznivega dejanja ali celo njegove točne pravne kvalifikacije ni mogoče vedno natančno ugotoviti, če soglasje za dostop do hranjenih podatkov nastopi v zgodnji fazi preiskave, tako da bi se lahko zdelo, da je v tej fazi še prezgodaj to kaznivo dejanje uvrščati v kategorijo hudih kaznivih dejanj oziroma v kategorijo kaznivih dejanj na splošno. Predložitveno sodišče mora to negotovost, ki je sestavni del kazenskih preiskav, katerih namen je prispevati k ugotavljanju resnice, upoštevati pri presoji sorazmernosti dostopa.

52 Člen 111^1(11) zakona o elektronskih komunikacijah in člen 90^1 zakona o kazenskem postopku.

53 Glej sodbo Ministerio Fiscal (točka 53).

54 Opredeljeno tudi kot „načelo *ultima ratio*“.

96. Vendar negotovost, ki lahko tako obstaja na začetku kazenske preiskave v zvezi s temi vidiki, ne more odpraviti potrebe po tem, da je vsaka zahteva za dostop obrazložena z nujnostjo poiskati dokaze o konkretnem kaznivem ravnanju na podlagi suma, podprtega z objektivnimi elementi. Tako namen zahteve za dostop ne more biti to, da se v danem obdobju preučijo vsa dejanja in poteze osebe, da bi se poiskala morebitna kazniva dejanja. Poleg tega, če se med preiskavo razkrijejo nova dejstva, bo moral biti dostop do podatkov, da bi se ta dejstva dokazala, predmet novega soglasja za dostop.

97. Ob upoštevanju zgornjih preudarkov Sodišču predlagam, naj odloči, da je treba člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine razlagati tako, da merila, na podlagi katerih je mogoče oceniti težo posega v temeljne pravice, ki ga pomeni dostop pristojnih nacionalnih organov do osebnih podatkov, ki jih morajo v skladu z nacionalnimi predpisi hraniti ponudniki elektronskih komunikacijskih storitev, vključujejo vrste zadevnih podatkov in dolžino obdobja, za katero se zahteva dostop. Predložitveno sodišče mora glede na težo posega presoditi, ali je bil navedeni dostop nujno potreben za doseganje cilja preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj.

C. Predhodni nadzor, ki ga opravi sodišče ali neodvisen upravni organ

98. Za zagotovitev, da je dostop pristojnih nacionalnih organov do hranjenih podatkov omejen na tisto, kar je nujno potrebno za doseganje uresničevanega cilja, je Sodišče presodilo, da je bistveno, da za ta dostop „načeloma, razen v nujnih primerih, ki so ustrezno utemeljeni, *sodišče ali neodvisen upravni organ* opravi predhoden nadzor in da se odločba tega sodišča ali tega organa izda na obrazložen predlog, ki se ga predloži v postopku preprečevanja, odkrivanja ali pregona kaznivih dejanj“. [55]

99. Predložitveno sodišče s tretjim vprašanjem za predhodno odločanje Sodišču predlaga, naj natančneje opredeli merila, ki jih mora izpolnjevati upravni organ, da se lahko šteje za „neodvisen“ v smislu sodbe Tele2 Sverige in Watson in drugi. Natančneje, predložitveno sodišče se sprašuje, ali je državno tožilstvo mogoče šteti za neodvisen upravni organ glede na to, da vodi predkazenski postopek in zastopa obtožbo pred sodiščem.

100. Za odgovor na to vprašanje se mi zdi koristno upoštevati dve področji sodne prakse Sodišča, in sicer, prvič, sodno prakso glede neodvisnosti nacionalnih nadzornih organov za varstvo osebnih podatkov in, drugič, sodno prakso glede neodvisnosti odreditvenega pravosodnega organa v okviru evropskega naloga za prijetje.

101. Po mnenju Sodišča je neodvisnost bistvena značilnost – potrjena med drugim v členu 8(3) Listine – organov, pristojnih za nadzor nad spoštovanjem pravil Unije o varstvu posameznikov pri obdelavi osebnih podatkov, da se zagotovita učinkovitost in zanesljivost tega nadzora ter da se okrepi varstvo oseb, na katere se nanašajo odločbe teh organov. [56]

102. Sodišče je v zvezi s členom 28(1), drugi pododstavek, Direktive 95/46 že odločilo, da „morajo biti nadzorni organi, pristojni za spremljanje obdelave osebnih podatkov, samostojni, tako da lahko svoje naloge izvajajo brez zunanjega vpliva. Ta samostojnost izključuje zlasti vsakršno navodilo in kakršenkoli drug zunanji vpliv, bodisi neposreden bodisi posreden, ki bi lahko usmerjal odločitve teh nadzornih organov in tako ogrožal njihovo opravljanje naloge ohranjanja pravega ravnotežja med pravnim varstvom zasebnosti in prostim pretokom osebnih podatkov“ [57].

55 Sodba Tele2 Sverige in Watson in drugi (točka 120 in navedena sodna praksa), moj poudarek. Glej v istem smislu mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017 (EU:C:2017:592, točki 202 in 208).

56 Glej zlasti sodbo z dne 6. oktobra 2015, Schrems (C-362/14, EU:C:2015:650, točki 40 in 41 ter navedena sodna praksa). Glej tudi mnenje 1/15 (Sporazum PNR med EU in Kanado) z dne 26. julija 2017 (EU:C:2017:592, točka 229).

57 Sodba z dne 8. aprila 2014, Komisija/Madžarska (C-288/12, EU:C:2014:237, točka 51 in navedena sodna praksa).

103. Sodišče je tudi poudarilo zahtevo, da morajo biti ob upoštevanju njihove vloge varuhov pravice do zasebnosti ti nadzorni organi „brez vsakega suma pristranskosti“. [58]

104. Ker tretje vprašanje, ki ga postavlja predložitveno sodišče, zadeva državno tožilstvo, je prav tako primerno upoštevati prispevek sodne prakse Sodišča v zvezi z neodvisnostjo odreditvenega pravosodnega organa v okviru evropskega naloga za prijetje. Tako je Sodišče odločilo, da mora biti nadzor v okviru sprejetja naloga za prijetje „izveden objektivno, ob upoštevanju vseh obremenilnih in razbremenilnih elementov, ter neodvisno, za kar morajo obstajati statusna in organizacijska pravila, ki izključujejo vsakršno tveganje, da bi na sprejetje odločitve o izdaji takega naloga za prijetje vplivala zunanja navodila, zlasti taka, ki jih da izvršilna veja oblasti“. [59]

105. Zadevni področji sodne prakse Sodišča sta si torej podobni v tem, da se na vsakem od teh področij poudarja, da mora biti pristojni nacionalni organ za preverjanje spoštovanja pravil prava Unije neodvisen, kar obsega dve zahtevi[60]. Prvič, ta organ ne sme prejemati navodil ali biti izpostavljen zunanjim pritiskom, ki bi lahko vplivali na njegove odločitve. Drugič, navedeni organ mora v skladu s svojim statusom in nalogami, ki so mu zaupane, izpolnjevati zahtevo po objektivnosti pri nadzoru, ki ga opravlja, to je ponujati jamstva nepristranskosti. Natančneje, presoja upravnega organa, ali je dostop do hranjenih podatkov sorazmeren, zahteva, da je sposoben vzpostaviti pravično ravnotežje med interesi, povezanimi z učinkovitostjo preiskave v okviru boja proti kriminalu, in interesi, povezanimi z varstvom osebnih podatkov oseb, ki jih zadeva dostop. Z zadnjenavedenega vidika je zahteva po nepristranskosti torej vgrajena v pojem „neodvisen upravni organ“, ki ga je Sodišče izpostavilo v sodbi Tele2 Sverige in Watson in drugi.

106. Preveriti je treba, ali državno tožilstvo ob upoštevanju različnih nalog, ki so mu dodeljene z estonskimi predpisi, izpolnjuje to merilo neodvisnosti v njegovih dveh razsežnostih, kadar mora nadzirati nujno potrebnost dostopa do podatkov. Tako ima pojem „neodvisnost“, ki mora opredeljevati upravni organ, pristojen za tak nadzor, funkcionalno razsežnost v smislu, da mora biti ta organ zmožen zagotavljati navedeni nadzor brez zunanjih posegov ali pritiskov, ki bi lahko vplivali na njegove odločitve, ter ob spoštovanju objektivnosti in stroge uporabe pravnih pravil. Skratka, pojem „neodvisen upravni organ“ v smislu sodbe Tele2 Sverige in Watson in drugi je namenjen temu, da se zagotovijo objektivnost, zanesljivost in učinkovitost tega nadzora.

107. To zahteva preučitev, ali lahko estonski predpisi, ki določajo status in naloge državnega tožilstva, pri zadevnih osebah ustvarijo legitimne dvome o zavarovanosti državnih tožilcev pred zunanjimi dejavniki in o njihovi nevtralnosti glede nasprotujočih si interesov, kadar morajo ti tožilci zagotoviti predhodni nadzor sorazmernosti dostopa do podatkov.

108. Državno tožilstvo ima bistveno vlogo pri vodenju kazenskega postopka, saj vodi predkazenski postopek in ima med drugim pristojnost, da sproži pregon zoper osebo, osumljeno storitve kaznivega dejanja, z namenom, da bi bila privedena pred sodišče. V tem pogledu ga je treba obravnavati kot organ, ki sodeluje pri izvajanju sodne oblasti v kazenskih zadevah. [61]

109. Kot je Sodišče dejalo v zvezi s Procura della Repubblica (državno tožilstvo, Italija) in v skladu s formulacijo, ki jo je, se mi zdi, mogoče prenesti na obravnavano zadevo, „naloga [državnega tožilca] ni, da popolnoma neodvisno odloči o sporu, temveč da ga po potrebi predloži v odločanje pristojnemu sodišču kot udeležencu v sodnem postopku, ki zastopa kazensko obtožbo“ [62].

58 Prav tam (točka 53 in navedena sodna praksa).

59 Glej sodbo z dne 9. oktobra 2019, NJ (Državno tožilstvo na Dunaju) (C-489/19 PPU, EU:C:2019:849, točka 38 in navedena sodna praksa).

60 Glede dveh vidikov zahteve po neodvisnosti glej po analogiji – v zvezi z nacionalnimi sodišči, ki odločajo o vprašanjih glede razlage in uporabe prava Unije – sodbo z dne 5. novembra 2019, Komisija/Poljska (Neodvisnost splošnih sodišč) (C-192/18, EU:C:2019:924, točke od 108 do 110 in navedena sodna praksa).

61 Glej zlasti sodbo z dne 27. maja 2019, PF (Generalni državni tožilec Litve) (C-509/18, EU:C:2019:457, točki 39 in 40).

62 Sodba z dne 12. decembra 1996, X (C-74/95 in C-129/95, EU:C:1996:491, točka 19).

110. Čeprav torej državno tožilstvo v svojem statusu, organizaciji in nalogah kaže posebne značilnosti, po katerih se razlikuje od sodišča in ki utemeljujejo, da je opredeljeno kot „organ, ki sodeluje pri izvajanju sodne oblasti v kazenskih zadevah v državah članicah“, to ne spremeni dejstva, da mora državno tožilstvo s funkcionalnega vidika – če nacionalno pravo določa, da je to tožilstvo organ, ki opravlja predhodni nadzor sorazmernosti dostopa, zahtevan s sodbo Tele2 Sverige in Watson in drugi – izkazovati v tem pogledu podobno raven neodvisnosti kot sodišče. Okoliščina, da to funkcijo namesto sodišča opravlja upravni organ, namreč ne sme vplivati na objektivnost, zanesljivost in učinkovitost tega nadzora.

111. V zvezi s tem je treba spomniti, da lahko v skladu s členom 90^1(2) zakona o kazenskem postopku preiskovalni organ v predkazenskem postopku s soglasjem državnega tožilstva ali v sodnem postopku s soglasjem sodišča od ponudnika elektronskih komunikacijskih storitev zahteva podatke, ki so našteti v členu 111^1(2) in (3) zakona o elektronskih komunikacijah.

112. Poleg tega iz estonskih predpisov izhaja, da državno tožilstvo v okviru kazenskega postopka vodi predkazenski postopek, katerega cilj je zbrati dokaze in vzpostaviti druge pogoje za začetek sodnega postopka. Preiskovalni organ in državno tožilstvo v predkazenskem postopku tudi razjasnita razbremenilne in obremenilne okoliščine za osumljenca ali obdolženca. Če je državno tožilstvo prepričano, da so zbrani vsi potrebni dokazi, in če obstajajo razlogi za to, vloži obtožni akt zoper osebo in v tem primeru sámo zastopa obtožbo pred sodiščem.

113. Predložitveno sodišče poleg tega opozarja, da mora državno tožilstvo v okviru kazenskega postopka sicer za ukrepe, ki pomenijo najhujši poseg v temeljne pravice, pridobiti soglasje preiskovalnega sodnika (na primer za večino nadzornih ukrepov in za odvzem prostosti), vendar je tudi državno tožilstvo pristojno za odločanje o nekaterih postopkovnih ukrepih, ki pomenijo hud poseg v več temeljnih pravic.[63]

114. Dvomi, ki jih predložitveno sodišče izraža glede opredelitve državnega tožilstva kot „neodvisnega upravnega organa“ v smislu sodbe Tele2 Sverige in Watson in drugi, so predvsem posledica tega, da mora državno tožilstvo, če je po predkazenskem postopku prepričano, da so v kazenski zadevi zbrani vsi potrebni dokazi, in če obstajajo razlogi za to, vložiti obtožni akt zoper zadevno osebo. V tem primeru državno tožilstvo zastopa obtožbo pred sodiščem in je tako tudi udeleženec sodnega postopka. Predvsem tožilski status državnega tožilstva je torej tisti, zaradi katerega predložitveno sodišče dvomi o opredelitvi tega tožilstva kot „neodvisnega upravnega organa“ v smislu sodbe Tele2 Sverige in Watson in drugi.

115. Če se dvomi predložitvenega sodišča izrazijo na ta način, se torej še posebej nanašajo na nepristranskost državnega tožilstva pri nadzoru sorazmernosti dostopa preiskovalnih služb do podatkov, ki naj bi ga to tožilstvo opravilo, preden da soglasje za tak dostop.

116. Preden se lotim tega vidika, povezanega z nepristranskostjo, poudarjam, da člen $1(1^1)$ zakona o državnem tožilstvu določa, da je to „pri opravljanju svojih zakonskih nalog neodvisno“. Poleg tega je v skladu s členom 2(2) tega zakona „[d]ržavni tožilec […] pri opravljanju svojih nalog neodvisen in ravna izključno po zakonu in svojem prepričanju“.[64]

117. V zvezi s tem estonska vlada navaja, da čeprav je državno tožilstvo organ, ki spada pod ministrstvo za pravosodje, estonski predpisi temu ministrstvu vseeno ne priznavajo nobene možnosti, da bi podalo presojo o konkretnem postopku ali poseglo v kazenski postopek, ki poteka. Ta vlada pojasnjuje, da poseganje v neodvisnost državnega tožilstva pomeni kršitev, za katero je predpisana sankcija.

63 Državno tožilstvo na primer da soglasje za prikrito opazovanje osebe, stvari ali kraja in v številnih primerih za hišno preiskavo.

64 Glej v istem smislu tudi člen 30(2) zakona o kazenskem postopku.

118. Če torej o neodvisnosti državnega tožilstva ni treba dvomiti v okviru nalog, ki jih ima na podlagi estonskih predpisov, pa se mi zdi, da lahko ti predpisi vzbujajo legitimne dvome glede zmožnosti državnega tožilstva, da opravi nevtralen in objektiven predhodni nadzor sorazmernosti dostopa do podatkov, kadar mora v okviru neke zadeve hkrati opravljati naloge vodenja kazenske preiskave, odločanja o kazenskem pregonu in zastopanja obtožbe pred sodiščem.

119. Res je, da več elementov v estonskih predpisih pomeni jamstva, da državno tožilstvo v okviru nalog, za katere je odgovorno, ravna ob spoštovanju zahteve po nepristranskosti.

120. Tako mora v skladu s členom 211(2) zakona o kazenskem postopku državno tožilstvo razjasniti razbremenilne in obremenilne okoliščine za osumljenca ali obdolženca.

121. Poleg tega mora, kot izhaja iz člena 1(1) zakona o državnem tožilstvu, to zagotavljati zakonitost predkazenskega postopka, katerega vodenje je njegova naloga. Prav tako mora na podlagi člena $1(1^1)$ in člena 2(2) tega zakona državno tožilstvo svoje naloge opravljati v skladu z zakonom. To pomeni, da ko državno tožilstvo vodi predkazenski postopek, mora biti njegov cilj ne le skrbeti za učinkovitost tega postopka, ampak tudi zagotoviti, da se navedeni postopek ne izvaja ob nesorazmernem poseganju v pravico zadevnih oseb do zasebnosti. Šteti je namreč mogoče, da je soglasje za dostop do hranjenih podatkov sestavni del splošnejše naloge državnega tožilstva, to je nadzirati zakonitost sredstev, ki jih uporabijo preiskovalne službe, zlasti sorazmernost preiskovalnih dejanj glede na naravo in težo dejstev.

122. Zato bi se lahko trdilo, da je državno tožilstvo ravno zato, ker vodi predkazenski postopek, zmožno presoditi, ali je glede na posebnosti vsake zadeve dostop do podatkov, ki jih hranijo telekomunikacijski operaterji, ob neobstoju drugih dokazov nujno potreben, da bi se preiskava domnevnega kaznivega dejanja pomaknila naprej.

123. To ne spremeni dejstva, da lahko z vidika oseb, na katere se nanaša zahteva za dostop do podatkov, okoliščina, da je upravni organ, ki naj bi preverjal, ali je ta dostop v okviru preiskave nujno potreben, hkrati tudi organ, ki lahko zoper njih sproži pregon in nato zastopa obtožbo v morebitnem poznejšem sodnem postopku, po mojem mnenju oslabi jamstva nepristranskosti, določena v estonskih predpisih. S tega vidika lahko med temi nalogami državnega tožilstva na eni strani ter zahtevo po nevtralnosti in objektivnosti predhodnega nadzora sorazmernosti dostopa do podatkov na drugi strani obstaja morebitno navzkrižje.

124. Državno tožilstvo mora namreč v okviru svojih nalog zbrati dokaze, presoditi njihovo upoštevnost in oblikovati sklepe o krivdi zadevne osebe. Ta državni organ mora vložiti in podkrepiti obtožni akt v okviru obtožbe, ki jo mora zastopati pred sodiščem, pri čemer je torej udeleženec postopka. Zaradi teh nalog za državno tožilstvo velja dokazna zahteva, ki se lahko osebam, osumljenim storitve kaznivega dejanja, zdi nezdružljiva z zmožnostjo tega organa, da nevtralno in objektivno opravi predhodni nadzor sorazmernosti dostopa do podatkov.

125. Kot poudarja Komisija, je tveganje lahko v tem, da lahko zadevne osebe državno tožilstvo zaradi združenosti njegovih nalog dojemajo tako, kot da ima interes za obširno omogočanje dostopa do njihovih podatkov, naj so ti obremenilni ali razbremenilni. Poleg tega se lahko pri osebah, osumljenih storitve kaznivega dejanja, pojavijo legitimni dvomi glede nepristranskosti državnega tožilstva, ko daje soglasje za dostop do njihovih podatkov, ker lahko v poznejšem postopku nastopa proti njim v vlogi tožilca. Po mojem mnenju pa zahteva po nepristranskosti upravnega organa, ki je pristojen za predhodni nadzor, zahtevan s sodbo Tele2 Sverige in Watson in drugi, predpostavlja določeno oddaljenost in nevtralnost glede na interese, ki si lahko nasprotujejo v okviru predkazenskega postopka, in sicer na eni strani učinkovitost tega postopka in na drugi strani varstvo osebnih podatkov zadevnih oseb. Po mnenju Komisije bi bil položaj lahko drugačen, če bi bila notranja upravna organizacija državnega tožilstva taka, da državni tožilec, ki bi moral odločiti o zahtevi za dostop, ne bi imel nobene vloge v predkazenskem postopku in poznejših fazah postopka, vključno z zastopanjem obtožbe.

126. Ker so, kot je bilo potrjeno na obravnavi, državna tožilstva v Republiki Estoniji organizirana hierarhično, nisem prepričan, da lahko ta predlog Komisije odpravi nevšečnosti, nastale zaradi združenosti nalog, ki jih estonski predpisi nalagajo državnemu tožilstvu. Vsekakor to ne odvzame upoštevnosti ideji, na kateri ta predlog temelji, in sicer, da bi moral predhodni nadzor sorazmernosti dostopa do podatkov opravljati upravni organ, ki, prvič, ni neposredno vključen v vodenje zadevne kazenske preiskave in, drugič, ima nevtralno držo do udeležencev kazenskega postopka. Takemu organu, ločenemu od interesov, povezanih s preiskavo in zastopanjem obtožbe v zadevnem postopku, ne bi bilo mogoče očitati, da interesom preiskave daje prednost pred interesi, povezanimi v varstvom podatkov zadevnih oseb. Navedeni organ bi bil zato zmožen popolnoma nepristransko sprejeti odločitev, s katero bi se dostop do hranjenih podatkov omejil na tisto, kar bi bilo nujno potrebno za doseganje uresničevanega cilja, v skladu s tem, kar se zahteva s členom 15(1) Direktive 2002/58, kot ga je Sodišče razložilo v sodbi z dne 8. aprila 2014, Digital Rights Ireland in drugi [65], ter v sodbi Tele2 Sverige in Watson in drugi. Hkrati se zavedam, da do uvedbe nadzora, ki nima zveze z interesi, povezanimi z zadevnim postopkom, ne sme priti za ceno zmanjšanja učinkovitosti preiskovanja, pregona in preprečevanja kaznivih dejanj.

127. Zaradi spoštovanja procesne avtonomije držav članic se Sodišče ne bi smelo podrobneje vmešavati v splošno organizacijo izvajanja sodne oblasti v državah članicah kot tudi ne v notranjo organizacijo državnih tožilstev. Naloga držav članic je, da vzpostavijo primerna orodja za to, da bo predhodni nadzor dostopa do hranjenih podatkov zagotavljal pravično ravnotežje med interesi, povezanimi z učinkovitostjo kazenske preiskave, in pravico do varstva podatkov oseb, ki jih zadeva ta dostop.

128. Zaključil bom s pojasnilom, da po mojem mnenju neobstoja predhodnega nadzora, ki bi ga opravil „neodvisen“ upravni organ v smislu sodbe Tele2 Sverige in Watson in drugi, ni mogoče odtehtati z obstojem sodnega nadzora, ki se lahko opravi po tem, ko je bilo dano soglasje za dostop. [66] V nasprotnem primeru bi zahteva po predhodnosti nadzora izgubila svojo utemeljitev, to je preprečiti, da bi se soglasja dajala za tak dostop do hranjenih podatkov, ki bi bil nesorazmeren glede na cilj preiskovanja, pregona in preprečevanja kaznivih dejanj.

129. Glede na zgornje preudarke Sodišču predlagam, naj na tretje vprašanje za predhodno odločanje odgovori, da je treba člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine razlagati tako, da zahteva, v skladu s katero mora sodišče ali neodvisen upravni organ opraviti predhodni nadzor nad dostopom pristojnih nacionalnih organov do hranjenih podatkov, ni izpolnjena, če nacionalni predpisi določajo, da tak nadzor opravi državno tožilstvo, ki ima nalogo vodenja predkazenskega postopka, hkrati pa lahko zastopa obtožbo pred sodiščem.

V. Predlog

130. Glede na navedeno Sodišču predlagam, naj na vprašanja, ki jih je postavilo Riigikohus (vrhovno sodišče, Estonija), odgovori:

1. Člen 15(1) Direktive 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah), kakor je bila spremenjena z Direktivo 2009/136/ES Evropskega parlamenta in Sveta z dne 25. novembra 2009, v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine Evropske unije o temeljnih pravicah je treba razlagati tako, da merila, na podlagi katerih je mogoče oceniti težo posega v temeljne pravice, ki ga pomeni dostop pristojnih nacionalnih organov do osebnih podatkov, ki jih morajo v skladu z nacionalnimi predpisi hraniti ponudniki elektronskih komunikacijskih storitev, vključujejo vrste zadevnih podatkov in dolžino

65 C-293/12 in C-594/12, EU:C:2014:238.

66 Glede na podatke, zagotovljene Sodišču na obravnavi, lahko po estonskem pravu ta sodni nadzor nastopi ob koncu predkazenskega postopka, kadar se osumljenec, ki se mu posreduje spis, odloči izpodbijati dejanje iz tega postopka, ali tudi med sodnim postopkom.

obdobja, za katero se zahteva dostop. Predložitveno sodišče mora glede na težo posega presoditi, ali je bil navedeni dostop nujno potreben za doseganje cilja preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj.

2. Člen 15(1) Direktive 2002/58, kakor je bila spremenjena z Direktivo 2009/136, v povezavi s členi 7, 8 in 11 ter členom 52(1) Listine o temeljnih pravicah je treba razlagati tako, da zahteva, v skladu s katero mora sodišče ali neodvisen upravni organ opraviti predhodni nadzor nad dostopom pristojnih nacionalnih organov do hranjenih podatkov, ni izpolnjena, če nacionalni predpisi določajo, da tak nadzor opravi državno tožilstvo, ki ima nalogo vodenja predkazenskega postopka, hkrati pa lahko zastopa obtožbo pred sodiščem.