Zbirka odločb sodne prakse

SKLEPNI PREDLOGI GENERALNEGA PRAVOBRANILCA
MANUELA CAMPOSA SÁNCHEZ-BORDONE,
predstavljeni 20. aprila 2023 [1]

Zadeva C-548/21

C. G.
proti
Bezirkshauptmannschaft Landeck

(Predlog za sprejetje predhodne odločbe, ki ga je vložilo Landesverwaltungsgericht Tirol (deželno upravno sodišče za Tirolsko, Avstrija))

„Predhodno odločanje – Telekomunikacije – Varstvo osebnih podatkov – Direktiva (EU) 2016/680 – Kazenski postopek – Poskus dostopa javnih organov do podatkov, zabeleženih v mobilnem telefonu, brez dovoljenja sodišča ali neodvisnega upravnega organa“

1. Ta predlog za sprejetje predhodne odločbe se v bistvu nanaša na pogoje, ki jih morajo policijski organi upoštevati za dostop do podatkov, shranjenih v mobilnem telefonu osebe, zoper katero poteka kazenska preiskava.

2. Kot bom pojasnil, je predlog za sprejetje predhodne odločbe zelo pomanjkljiv glede njegove dopustnosti. Če se bo Sodišče vseeno odločilo, da bo zadevo vsebinsko preučilo, se bo moralo izreči o področju uporabe Direktive 2002/58/ES [2] in Direktive (EU) 2016/680. [3]

[1] Jezik izvirnika: španščina.

[2] Direktiva 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) (UL, posebna izdaja v slovenščini, poglavje 13, zvezek 29, str. 514).

[3] Direktiva Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ (UL 2016, L 119, str. 89).

I. Pravni okvir

A. Pravo Unije

1. Uredba (EU) 2016/679[4]

3. Člen 2, naslovljen „Področje uporabe“, v odstavku 2 določa:

„Ta uredba se ne uporablja za obdelavo osebnih podatkov:

[…]

(d) s strani pristojnih organov za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem.“

2. Direktiva 2016/680

4. V uvodni izjavi 2 je navedeno:

„Načela in pravila o varstvu posameznikov pri obdelavi njihovih osebnih podatkov bi morali ne glede na njihovo državljanstvo ali prebivališče zagotavljati spoštovanje temeljnih pravic in svoboščin posameznikov, zlasti pravico do varstva osebnih podatkov. Ta direktiva naj bi prispevala k dokončnemu oblikovanju območja svobode, varnosti in pravice.“

5. V uvodni izjavi 46 je navedeno:

„Vsaka omejitev pravic posameznika, na katerega se nanašajo osebni podatki, mora biti skladna z Listino in EKČP, kot ju razlaga sodna praksa Sodišča in Evropskega sodišča za človekove pravice,[5] zlasti glede vsebine teh pravic in svoboščin.“

6. V uvodni izjavi 49 je navedeno:

„Kadar se osebni podatki obdelujejo med kazensko preiskavo in v sodnem kazenskem postopku, bi moralo biti državam članicam omogočeno, da zagotovijo, da se uresničevanje pravic do informacij, dostopa in popravka ali izbrisa osebnih podatkov in omejitve obdelave izvajajo v skladu z nacionalnimi predpisi o sodnih postopkih.“

7. Člen 1, naslovljen „Predmet urejanja in cilji“, določa:

„1. V tej direktivi so določena pravila o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo za namene preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem.

[4] Uredba Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL 2016, L 119, str. 1; v nadaljevanju: SUVP).

[5] V nadaljevanju: ESČP.

2. Države članice v skladu s to direktivo:

(a) varujejo temeljne pravice in svoboščine posameznikov ter zlasti njihovo pravico do varstva osebnih podatkov, in

[…]

3. Ta direktiva državam članicam ne preprečuje, da za varovanje pravic in svoboščin posameznikov, na katere se nanašajo osebni podatki, ki jih obdelujejo pristojni organi, sprejmejo višjo raven zaščitnih ukrepov od ravni, določene v tej direktivi.“

8. Člen 2, naslovljen „Področje uporabe“, v odstavku 1 določa:

„Ta direktiva se uporablja za obdelavo osebnih podatkov, ki jih pristojni organi obdelujejo za namene iz člena 1(1).“

9. Člen 3, naslovljen „Opredelitev pojmov“, določa:

„V tej direktivi:

[…]

2. ‚obdelava‘ pomeni vsako dejanje ali niz dejanj, ki se izvaja v zvezi z osebnimi podatki ali nizi osebnih podatkov z avtomatiziranimi sredstvi ali brez njih, kot je zbiranje, beleženje, urejanje, strukturiranje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s posredovanjem, razširjanje ali drugačno omogočanje dostopa, prilagajanje ali kombiniranje, omejevanje, izbris ali uničenje;

[…]

7. ‚pristojni organ‘ pomeni:

(a) kateri koli javni organ, ki je pristojen za preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem, ali

[…]“

10. Člen 4, naslovljen „Načela v zvezi z obdelavo osebnih podatkov“, v odstavku 1 določa:

„Države članice zagotovijo, da se osebni podatki:

(a) obdelujejo zakonito in pošteno;

(b) so zbrani za določene, izrecne in zakonite namene ter da se ne obdelujejo na način, ki je nezdružljiv s temi nameni;

(c) so ustrezni, relevantni in ne prekomerni glede na namene, za katere se obdelujejo;

[…]

(e) se hranijo v obliki, ki dopušča identifikacijo posameznikov, na katere se osebni podatki nanašajo, in le toliko časa, kolikor je potrebno za namene, za katere se obdelujejo;

(f) se obdelujejo na način, ki zagotavlja ustrezno varnost osebnih podatkov, vključno z zaščito pred nedovoljeno ali nezakonito obdelavo ter pred nenamerno izgubo, uničenjem ali poškodbo, in sicer z ustreznimi tehničnimi ali organizacijskimi ukrepi.“

11. Člen 8, naslovljen „Zakonitost obdelave“, določa:

„1. Države članice zagotovijo, da obdelava velja za zakonito le, če je potrebna, in v obsegu, v katerem je potrebna, za opravljanje naloge, ki jo izvaja pristojni organ za namene iz člena 1(1) in temelji na pravu Unije ali države članice.

2. Pravo držav članic, ki ureja obdelavo v okviru področja uporabe te direktive, določa vsaj cilje obdelave, kateri osebni podatki se obdelajo in namene obdelave.“

12. Člen 13, naslovljen „Informacije, ki se dajo na voljo ali zagotovijo posamezniku, na katerega se nanašajo osebni podatki“, določa:

„1. Države članice določijo, da upravljavec posamezniku, na katerega se nanašajo osebni podatki, [da] na voljo vsaj naslednje informacije:

[…]

(d) o pravici do vložitve pritožbe pri nadzornem organu in njegove kontaktne podatke;

[…]

3. Države članice lahko sprejmejo zakonodajne ukrepe za zadržanje, omejitev ali opustitev zagotovitve informacij posamezniku, na katerega se nanašajo osebni podatki, na podlagi odstavka 2, če in dokler je takšen ukrep, ki mora spoštovati temeljne pravice in zakonite interese zadevnega posameznika, nujen in sorazmeren ukrep v demokratični družbi za:

(a) preprečitev oviranja uradnih ali zakonitih preiskav, poizvedb ali postopkov;

(b) preprečitev vplivanja na preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij;

(c) zaščito javne varnosti;

(d) zaščito varnosti države;

(e) zaščito pravic in svoboščin drugih.

[…]“

13. Člen 15, naslovljen „Omejitev pravice do dostopa“, v odstavku 1 določa:

„Države članice lahko sprejmejo zakonodajne ukrepe, s katerimi posamezniku, na katerega se nanašajo osebni podatki, popolnoma ali delno omejijo pravico do dostopa, in sicer če in dokler je taka delna ali popolna omejitev, ki mora spoštovati temeljne pravice in zakonite interese zadevnega posameznika, nujen in sorazmeren ukrep v demokratični družbi za:

(a) preprečitev oviranja uradnih ali zakonitih preiskav, poizvedb ali postopkov;

(b) preprečitev vplivanja na preprečevanje, preiskovanje, odkrivanje ali pregon kaznivih dejanj ali izvrševanje kazenskih sankcij;

(c) zaščito javne varnosti;

(d) zaščito varnosti države;

(e) zaščito pravic in svoboščin drugih.“

14. Člen 27, naslovljen „Ocena učinka v zvezi z varstvom podatkov“, določa:

„1. Kadar je možno, da bi lahko vrsta obdelave, zlasti z uporabo novih tehnologij, ob upoštevanju narave, obsega, okoliščin in namenov obdelave, povzročila veliko tveganje za pravice in svoboščine posameznikov, države članice določijo, da upravljavec pred obdelavo opravi oceno učinka predvidenih dejanj obdelave na varstvo osebnih podatkov.

2. Ocena iz odstavka 1 obsega vsaj splošni opis predvidenih dejanj obdelave, oceno tveganja za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki, ukrepe, namenjene obvladovanju teh tveganj, zaščitne ukrepe, varnostne ukrepe ter mehanizme za zagotavljanje varstva osebnih podatkov in za dokazovanje skladnosti s to direktivo, pri čemer se upoštevajo pravice in zakoniti interesi posameznikov, na katere se nanašajo osebni podatki, ter drugih zadevnih oseb.“

15. Člen 28, naslovljen „Predhodno posvetovanje z nadzornim organom“, določa:

„1. Države članice določijo, da se upravljavec ali obdelovalec pred obdelavo osebnih podatkov, ki bodo del nove zbirke, posvetuje z nadzornim organom, kadar:

(a) ocena učinka na varstvo podatkov iz člena 27 kaže, da bi obdelava povzročila veliko tveganje, če upravljavec ne bi sprejel ukrepov za ublažitev tveganja, ali

(b) vrsta obdelave, zlasti v primeru uporabe novih tehnologij, mehanizmov ali postopkov, pomeni veliko tveganje za pravice in svoboščine posameznikov, na katere se nanašajo osebni podatki.

[…]“

16. Člen 54, naslovljen „Pravica do učinkovitega pravnega sredstva zoper upravljavca ali obdelovalca“, določa:

„Brez poseganja v katero koli razpoložljivo upravno ali izvensodno sredstvo, vključno s pravico do vložitve pritožbe pri nadzornem organu na podlagi člena 52, države članice določijo, da ima vsak

posameznik, na katerega se nanašajo osebni podatki, pravico do učinkovitega pravnega sredstva, kadar meni da so bile njegove pravice iz predpisov, sprejetih na podlagi te direktive, kršene zaradi obdelave njegovih osebnih podatkov, ki ni bila v skladu z navedenimi predpisi.“

B. Nacionalno pravo

17. Člen 18 Strafprozessordnung[6] določa, da kriminalistična policija opravlja naloge pri izvajanju sodne oblasti v kazenskih zadevah (odstavek 1). Za preiskave kriminalistične policije so odgovorni varnostni organi (odstavek 2). Organi javne varnosti zagotavljajo izvrševanje nalog kriminalistične policije, ki obsegajo preiskovanje in pregon kaznivih dejanj (odstavek 3).

18. V skladu s členom 99 StPO kriminalistična policija preiskave izvaja po uradni dolžnosti ali na podlagi prijave, pri tem pa upošteva odredbe državnega tožilstva in sodišča (odstavek 1). Če je za preiskovalni ukrep potrebna odredba državnega tožilstva, lahko kriminalistična policija v primeru neposredne nevarnosti izvaja ustrezna pooblastila tudi brez take odredbe. V takem primeru mora nemudoma zaprositi za dovoljenje (odstavek 2).

19. Člen 111(2) StPO določa, da mora vsakdo – če je treba zbrati informacije, shranjene na nosilcih podatkov – omogočiti dostop do teh informacij in na zahtevo izročiti ali omogočiti izdelavo elektronskega nosilca podatkov v datotečni obliki, ki se običajno uporablja. Poleg tega mora omogočiti izdelavo varnostne kopije informacij, shranjenih na nosilcih podatkov.

II. Dejansko stanje, spor in vprašanja za predhodno odločanje

20. C. G. je nemški državljan, ki dela in prebiva v Avstriji.

21. Uradniki carinskega urada v Innsbrucku (Avstrija) so 23. februarja 2021 med izvajanjem nadzora nad prepovedanimi drogami zasegli paket, ki je bil naslovljen na C. G. in je vseboval 85 gramov marihuane.

22. Policijska uslužbenca sta 6. marca 2021 C. G. zaslišala glede pošiljatelja paketa in preiskala njegovo stanovanje. Med preiskavo sta zasegla njegov mobilni telefon (vključno s kartico SIM in kartico SD) in mu izročila zapisnik o zasegu.

23. Ko je bil C. G. pozvan, naj dovoli vpogled v podatke o povezavah svojega mobilnega telefona, tega ni hotel storiti, prav tako ni hotel razkriti kode za dostop do telefona.

24. Bezirkspolizeikommando Landeck (policijska uprava v Landecku, Avstrija) ni uspelo odkleniti mobilnega telefona. Poslan je bil na Bundeskriminalamt (zvezna uprava kriminalistične policije) na Dunaj (Avstrija), kjer so ga še enkrat neuspešno poskušali odkleniti in pridobiti vpogled v shranjene podatke.

25. Za te ukrepe v trenutku, ko jih je policija izvedla, ni bilo niti odredbe državnega tožilstva niti sklepa sodišča.

[6] Zakonik o kazenskem postopku. V nadaljevanju: StPO. BGBl št. 631/1975, v različici, ki se uporablja v času dejanskega stanja (BGBl I št. 24/2020).

26. C. G. je 31. marca 2021 pri Landesverwaltungsgericht Tirol (deželno upravno sodišče za Tirolsko, Avstrija) vložil tožbo zoper prisilni ukrep, ki mu je bil izrečen, in izpodbijal zaseg mobilnega telefona. Ta mu je bil 20. aprila 2021 vrnjen.

27. C. G. ni bil obveščen o poskusu pregleda vsebine mobilnega telefona; zanj je izvedel, ker je bil policist, ki je opravil zaseg in nato sprožil digitalni pregled, zaslišan kot priča pod prisego. Ta poskus ni bil dokumentiran niti v spisu kriminalistične policije.

28. V teh okoliščinah je Landesverwaltungsgericht Tirol (deželno upravno sodišče za Tirolsko) Sodišču v predhodno odločanje predložilo ta vprašanja:

„1. Ali je treba člen 15(1) (morebiti v povezavi s členom 5) Direktive 2002/58, kakor je bila spremenjena z Direktivo 2009/136/ES, v povezavi s členoma 7 in 8 Listine razlagati tako, da dostop javnih organov do podatkov, ki so shranjeni na mobilnih telefonih, pomeni poseg v temeljne pravice, določene v teh členih Listine, ki je tako resen, da je treba ta dostop na področju preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj omejiti na boj proti hudim oblikam kriminalitete?

2. Ali je treba člen 15(1) Direktive 2002/58, kakor je bila spremenjena z Direktivo 2009/136, v povezavi s členi 7, 8, 11 in 52(1) Listine razlagati tako, da nasprotuje nacionalni ureditvi, kot je ta iz člena 18 v povezavi s členom 99(1) [StPO], v skladu s katero si varnostni organi med postopkom kazenskega preiskovanja brez dovoljenja sodišča ali neodvisnega upravnega organa sami sebi zagotovijo vseobsežen in nenadzorovan dostop do vseh digitalnih podatkov, shranjenih na mobilnem telefonu?

3. Ali je treba člen 47 Listine, morebiti v povezavi s členom 41 in členom 52 Listine, z vidika enakosti orožij in z vidika pravice do učinkovitega pravnega sredstva razlagati tako, da nasprotuje ureditvi države članice, ki – kot člen 18 v povezavi s členom 99(1) [StPO] – omogoča, da se mobilni telefon digitalno pregleda, ne da bi bil [posameznik, na katerega se nanašajo osebni podatki,] s tem predhodno [seznanjen] ali bi [bil seznanjen] vsaj po sprejetju ukrepa?“

III. Postopek pred Sodiščem

29. Predlog za sprejetje predhodne odločbe je na Sodišče prispel 6. septembra 2021.

30. Sodišče je 20. oktobra 2021 predložitveno sodišče pozvalo, naj navede, ali bi bila v tej zadevi lahko upoštevna Direktiva (EU) 2016/680.

31. Predložitveno sodišče je 11. novembra 2021 odgovorilo, da je treba Direktivo 2016/680 uporabiti v postopku v glavni stvari.

32. Pisna stališča so predložile nemška, avstrijska, ciprska, danska, estonska, francoska, madžarska, irska, nizozemska, norveška, poljska in švedska vlada ter Evropska komisija.

33. Navedene stranke so se, razen nemške, madžarske in poljske vlade, ki so – enako kot finska vlada – predložile pisna stališča, udeležile tudi obravnave 16. januarja 2023. Sodišče jih je pozvalo, naj se v svojih trditvah osredotočijo na Direktivo (EU) 2016/680 in ustno odgovorijo na nekatera vprašanja v zvezi z njo.

IV. Analiza

A. Nedopustnost

34. Predložitveno sodišče je svoja vprašanja najprej oblikovalo tako, da se nanašajo le na razlago Direktive 2002/58. Vendar se skoraj vsi udeleženci tega postopka strinjajo, da se ta direktiva ne uporablja za obravnavano zadevo in da zato njena razlaga ni potrebna za rešitev spora.

35. Direktiva 2002/58 v skladu s členom 3 ureja „[…] obdelavo osebnih podatkov v zvezi z zagotavljanjem javno razpoložljivih elektronskih komunikacijskih storitev v javnih komunikacijskih omrežjih v [Uniji], vključno z javnimi komunikacijskimi omrežji, ki podpirajo zbiranje podatkov in identifikacijske naprave“.

36. Sodišče je razsodilo, da „[k]adar […] države članice neposredno izvajajo ukrepe, ki odstopajo od načela zaupnosti elektronskih komunikacij, ne da bi ponudnikom takih komunikacijskih storitev naložile obveznosti obdelave, varstvo podatkov zadevnih oseb ne spada na področje uporabe Direktive 2002/58, temveč zgolj na področje uporabe nacionalnega prava, s pridržkom uporabe [Direktive 2016/680]“.[7]

37. V tem primeru so do podatkov poskušali neposredno dostopati organi kazenskega pregona v okviru kazenske preiskave. Ponudniki elektronskih komunikacijskih storitev, ki niso bili pozvani k posredovanju osebnih podatkov, niso bili vključeni. Direktiva 2002/58 zato ni upoštevna.

38. Zakonodajni akt prava Unije, ki ureja ta položaj, je Direktiva (EU) 2016/680, ki se v skladu s členom 2(1) uporablja za obdelavo osebnih podatkov s strani pristojnih organov „za namene […] preiskovanja […] kaznivih dejanj“.

39. To bi zadostovalo za ugotovitev nedopustnosti predloga za sprejetje predhodne odločbe, kot ga je oblikovalo nacionalno sodišče, saj se zakonodajni akt prava Unije, katerega razlago je zahtevalo, v tej zadevi ne uporablja.

40. Res pa je, da člen 267 PDEU Sodišču omogoča, da preoblikuje vprašanja, ki so mu bila predložena, ali da navede morebitne druge upoštevne določbe prava Unije, da bi nacionalnemu sodišču dalo koristen odgovor.[8]

41. Sodišče je predložitveno sodišče pozvalo, naj se izreče o morebitni upoštevnosti Direktive 2016/680. Dalo mu je torej možnost, da samo dopolni ali preoblikuje svoja vprašanja. Namesto tega je predložitveno sodišče zgolj navedlo, da „je treba v obravnavani zadevi vsekakor upoštevati določbe Direktive (EU) 2016/680“, ne da bi opredelilo določbe te direktive, o katerih dvomi, ali se podrobneje opredelilo do drugih vsebinskih vprašanj.[9]

[7] Sodba z dne 6. oktobra 2020, La Quadrature du Net in drugi (C-511/18, C-512/18 in C-520/18, EU:C:2020:791, točka 103; v nadaljevanju: sodba La Quadrature du Net in drugi).

[8] Med drugim sodba z dne 28. aprila 2016, Oniors Bio (C-233/15, EU:C:2016:305, točka 30).

[9] Sodišče je moralo stranke pozvati, naj navedejo, „katere so po njihovem mnenju upoštevne določbe Direktive (EU) 2016/680, glede na katere bi moralo Sodišče po potrebi preoblikovati tri vprašanja za predhodno odločanje predložitvenega sodišča“ (četrto vprašanje za ustni odgovor na obravnavi).

42. Sodišče je večkrat razsodilo, da „je nujno, kot določa člen 94(c) Poslovnika, da predložitvena odločba vsebuje razloge, ki so predložitvenemu sodišču vzbudili dvom o razlagi ali veljavnosti nekaterih določb prava Unije, in pojasnitev zveze, ki po mnenju predložitvenega sodišča obstaja med temi določbami in nacionalno zakonodajo, ki jo je treba uporabiti v sporu o glavni stvari“. [10]

43. Iz zgoraj navedenega je razvidno, da zahteve iz člena 94 Poslovnika v okviru tega predloga za sprejetje predhodne odločbe niso bile upoštevane. Čeprav je Sodišče v zvezi s tem do neke mere prožno, mora biti sodelovanje s predložitvenim sodiščem vzajemno: ker to brez utemeljitve ni sodelovalo in predložilo svojih dvomov glede razlage akta prava Unije, za katerega meni, da se uporablja (v tem primeru Direktive 2016/680), se mi zdi logično, da se ugotovi nedopustnost predloga za sprejetje predhodne odločbe. [11]

44. Poleg zgoraj navedenega predložitveno sodišče:

– ni navedlo vrste obdelave, ki so jo poskušali izvesti policijski organi, niti osebnih podatkov, ki so jih pri tem iskali. Na prvi pogled se zdi, da naj bi bila obdelava omejena na podatke o povezavah (to je podatke o prometu in lokaciji), v nadaljevanju pa ni izključeno, da bi odklepanje telefona omogočilo dostop do „vseh [shranjenih] digitalnih podatkov“ [12] in celo do vsebine komunikacij in elektronskih sporočil, izmenjanih prek telefona; [13]

– se sklicuje tako na zaseg telefona kot tudi na dostop ali poskus dostopa do podatkov, ki jih vsebuje, in njihovo poznejšo „uporabo“ (*Auswertung*), to je analizo in branje. Dodaja, da to „pomeni povsem nenadzorovan dostop do celotne digitalne korespondence osebe, na katero se podatki nanašajo“, s čimer je mogoče „rekonstruirati zelo podrobno in natančno sliko na skoraj vseh področjih zasebnega življenja“.

45. V teh okoliščinah bi Sodišče namesto *preoblikovanja* prvotnih vprašanj predložitvenega sodišča izvedlo pravo *rekonstrukcijo* predloga za sprejetje predhodne odločbe, ki bi poleg tega delno temeljila na hipotetičnih preudarkih in ne na ugotovljenih dejstvih. Vse to, ponavljam, po tem, ko je bila pravosodnemu organu dana možnost, da sam dopolni ali preoblikuje svoja vprašanja.

46. Predlagam torej, naj se predlog za sprejetje predhodne odločbe razglasi za nedopusten, kot je predlagalo več držav intervenientk.

47. Dejstvo, ki je bilo poudarjeno na obravnavi, da pred predložitvenim sodiščem ni več dejanskega spora, ki bi zahteval razlago pravil prava Unije, bi prav tako moralo voditi do takšne ugotovitve nedopustnosti.

48. Avstrijska vlada (ki je odgovorna za policijske organe, ki so sodelovali v preiskavi) namreč priznava, da je bilo ravnanje teh organov nezakonito in so bile z njim kršene pravice zadevne osebe. Ker je bil v skladu s predložitveno odločbo zahtevek tožeče stranke pred upravnim sodiščem usmerjen prav proti policijskim ukrepom, ki jih tožena uprava šteje za nezakonite, spor pred predložitvenim sodiščem ne obstaja več.

[10] Sodba z dne 6. oktobra 2021, Consorzio Italian Management in Catania Multiservizi (C-561/19, EU:C:2021:799, točka 69).

[11] V zvezi s to presojo se strinjam s francosko vlado (točke od 36 do 41 njenega pisnega stališča).

[12] Kot je navedeno v drugem vprašanju za predhodno odločanje.

[13] Predložitveno sodišče navaja, da je, „kar zadeva podatke o povezavah, […] mogoče rekonstruirati skoraj vse stike glede na pogostost, čas in trajanje pogovorov, kar zadeva pogovore, ki so izvedeni prek sporočil SMS in drugih storitev sporočil, pa tudi vsebino; prav tako se z analiziranjem shranjenih slik in zgodovine brskanja doseže zelo intimni vpogled v zasebno življenje osebe, na katero se podatki nanašajo“.

49. Kljub vsemu bom, če se Sodišče ne bi strinjalo z mojim stališčem, v nadaljevanju podredno obravnaval vsebinska vprašanja, na katerih temeljijo vprašanja za predhodno odločanje.

50. Vendar menim, da je treba najprej izključiti obstoj še enega ugovora nedopustnosti, ki so ga navedle nekatere intervenientke v postopku.[14] Ker se Direktiva (EU) 2016/680 nanaša na varstvo fizičnih oseb pri *obdelavi* njihovih podatkov, naj po njihovem mnenju ne bi urejala primerov, kot je ta, v katerem ni prišlo do obdelave, temveč le do *poskusa dostopa* do podatkov, ki jih na koncu ni bilo mogoče pridobiti.

51. Nasprotno pa bi bilo treba po mnenju Komisije zaradi polnega učinka Direktive (EU) 2016/680 dati prednost razlagi njenega cilja, ki ne bi bila omejena na obdelavo podatkov v ožjem smislu, temveč bi zajemala tudi vprašanja, ki so z njo neposredno povezana. Eno od teh naj bi bil poskus dostopa do podatkov, katerih obdelava se načrtuje.[15]

52. Menim, da je uporaba Direktive 2016/680 v obravnavani zadevi, ne da bi bilo treba prestopiti meje njenega področja uporabe,[16] upravičena, ne zaradi zasega mobilnega telefona,[17] temveč zaradi poznejših poskusov policijskih organov, da bi iz njega pridobili nekatere osebne podatke zadevnega posameznika, na katerega se osebni podatki nanašajo, zaradi česar so ga poskušali odkleniti in omogočiti dostop do njegove vsebine.

53. Med postopki, ki so v členu 3(2) Direktive (EU) 2016/680 opredeljeni kot „obdelava“, je tudi „drugačno omogočanje dostopa“ do osebnih podatkov, ki se izvaja v okviru kazenske preiskave. Razumem, da ko policijski organ zaseže telefon, v katerem so shranjeni takšni podatki, in z njim manipulira, da bi jih iz njega pridobil, začne „dejanje“ obdelave, tudi če je ta onemogočena zaradi tehničnih razlogov v zvezi s kriptografsko varnostjo.

54. Neuspeli poskus dostopa do osebnih podatkov, shranjenih v mobilnem telefonu, v okviru kazenske preiskave ureja Direktiva (EU) 2016/680 iz podobnih razlogov kot so razlogi, zaradi katerih je Sodišče ugotovilo, da se Direktiva 2002/58 uporablja za (prav tako neuspeli) *poskus* pridobitve sodnega dovoljenja za dostop do nekaterih podatkov preiskovane osebe, ki jih je hranil operater elektronskih komunikacij.[18]

55. Če bi predložitveno sodišče v tem okviru odločalo o nezakonitosti policijskega ukrepa (kar je priznala tudi avstrijska vlada, kot sem že pojasnil), bi bila lahko njegova presoja odvisna od zakonitosti cilja, ki se mu je sledilo, ne glede na to, ali je bil ukrep uspešen ali pa se je šele začel izvajati, vendar neuspešno.

[14] Sklicujem se zlasti na avstrijsko, francosko, nizozemsko in norveško vlado.

[15] Po mnenju Komisije „ni pomembno, ali je bil poskus uspešen ali ne. Pojav tehničnih težav, ki preprečijo uspeh poskusov dostopa, je okoliščina, ki je ni mogoče vnaprej poznati in ne vpliva na tveganja v zvezi z varstvom osebnih podatkov.“

[16] Zlasti se mi ne zdi potrebna uporaba členov 27 in 28 Direktive (EU) 2016/680, ki jo predlaga Komisija v svojem pisnem stališču. „Ocena učinka v zvezi z varstvom na podatkov“ iz člena 27 se na splošno nanaša na „vrsto obdelave“, ne pa na konkretne ali posamične obdelave. To je razvidno iz uvodne izjave 58 Direktive 2016/680: „Ocene učinka bi morale zajemati ustrezne sisteme in dejanja obdelave, *ne pa tudi posameznih primerov*“ (moj poudarek). Komisija je na obravnavi omilila svoje sklicevanje na ti določbi, ki naj bi ju navedla le zato, da bi poudarila, da so v Direktivi 2016/680 predvideni tudi položaji pred obdelavo podatkov v pravem pomenu besede.

[17] Direktiva 2016/680 ne ureja zasega telefona kot dokaznega sredstva v okviru kazenske preiskave.

[18] Sodba z dne 2. oktobra 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788).

B. Vsebinska presoja

1. Prvo vprašanje za predhodno odločanje

56. Predložitveno sodišče želi izvedeti, ali v skladu s členom 15(1) Direktive 2002/58 (morebiti v povezavi s členom 5 te direktive) v povezavi s členoma 7 in 8 Listine „dostop javnih organov do podatkov, ki so shranjeni na mobilnih telefonih, pomeni poseg v temeljne pravice, določene v teh členih Listine, ki je tako resen, da je treba ta dostop na področju preprečevanja, preiskovanja, odkrivanja in pregona kaznivih dejanj omejiti na boj proti hudim oblikam kriminalitete“.

57. Če bi bil predlog za sprejetje predhodne odločbe dopusten, bi bilo treba zaradi neuporabe Direktive 2002/58 prvo vprašanje preoblikovati tako, da bi Sodišče v odgovoru razložilo Direktivo 2016/680.

58. V tem odgovoru bi bilo treba pojasniti, ali je v zadevah, kot je obravnavana, mogoče govoriti o posegu v podatke, in, če poseg obstaja, ali je z Direktivo (EU) 2016/680 zahtevano, da se dostop do podatkov omeji na primere boja proti hudim kaznivim dejanjem.

59. Dejanja obdelave podatkov lahko že po definiciji ogrozijo pravici do spoštovanja zasebnega življenja (člen 7 Listine) in varstva osebnih podatkov (člen 8 Listine). Javni organi morajo zato izpolnjevati pogoje iz člena 52(1) Listine, da bi upravičili svoj poseg v uresničevanje teh temeljnih pravic.

60. Poseg v pravice, varovane s členoma 7 in 8 Listine, je še toliko večji, če se (a) namerava dostopati do občutljivih podatkov, ki so običajno zabeleženi v mobilnih telefonih in katerih poznavanje lahko razkrije vidike življenja njihovih imetnikov, ki bi morali ostati neznani tretjim osebam, in (b) omogoči dostop do vsebine komunikacij.

61. Vendar pa Direktive (EU) 2016/680 s splošnega vidika in ob upoštevanju njene vsebine ni mogoče razlagati v smislu, da je obdelava podatkov, na katero se nanaša, omejena samo na primere boja proti hudim kaznivim dejanjem.

62. Direktiva (EU) 2016/680 se nanaša na vsako dejanje obdelave[19] osebnih podatkov, ki ga izvajajo pristojni organi zaradi preprečevanja, preiskovanja, odkrivanja ali pregona *vseh vrst* kaznivih dejanj.

63. Iz načel, ki jih Direktiva (EU) 2016/680 za to (člen 4) določa glede obdelave osebnih podatkov, ali iz pogojev za njeno zakonitost (člen 8) ne izhaja, da je obdelava podatkov praviloma izvedljiva le v primerih hudih kaznivih dejanj.

64. Omejitve na primere boja proti hudim kaznivim dejanjem tudi ni mogoče utemeljiti s preprostim prenosom sodne prakse Sodišča v zvezi z Direktivo 2002/58[20] na primere, kot je ta v obravnavani zadevi.

[19] Tipologija „dejanj“ iz člena 3(2) Direktive (EU) 2016/680 je zelo široka. Glej navedbo te določbe v točki 9 teh sklepnih predlogov.

[20] Sodba La Quadrature du Net in sodbe z dne 21. decembra 2016, Tele2 Sverige in Watson in drugi (C-203/15 in C-698/15, EU:C:2016:970; v nadaljevanju: sodba Tele2 Sverige in Watson); z dne 2. oktobra 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788); z dne 6. oktobra 2020, Privacy International (C-623/17, EU:C:2020:790), in z dne 2. marca 2021, Prokuratuur (Pogoji za dostop do podatkov o elektronskih komunikacijah) (C-746/18, EU:C:2021:152; v nadaljevanju: sodba Prokuratuur).

65. Po mojem mnenju tega ni mogoče storiti, ker se ta sodna praksa, brez poseganja v to, kar bom navedel v nadaljevanju, nanaša na splošno in neselektivno hrambo osebnih podatkov splošne in nedoločljive skupine, ki ga sistematično izvajajo ponudniki elektronskih komunikacijskih storitev. Obseg posega, ki ga takšna hramba pomeni za družbo kot celoto, pojasnjuje, zakaj je bilo Sodišče pri njegovi prepovedi in določanju izjem od te prepovedi še posebej strogo.

66. Drugače pa je, če se nameravani dostop ne nanaša na celotno ali veliko skupino prebivalstva (torej na osebne podatke splošne in nedoločljive skupine), temveč na informacije, shranjene v posameznem mobilnem telefonu, v okviru postopka posamezne kazenske preiskave, kar je posebej urejeno z Direktivo (EU) 2016/680.

67. Predmet Direktive (EU) 2016/680 ni nič drugega kot obdelava podatkov, ki jo izvajajo pristojni organi zaradi preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj. In sicer vseh vrst kaznivih dejanj, ne le hudih.

68. Poleg tega, kot so opozorile nekatere intervenientke v postopku predhodnega odločanja, bi se lahko sicer Direktiva (EU) 2016/680, ker v njej ni nobenih navedb o resnosti kaznivih dejanj, v državah članicah uporabljala neenotno, saj se presoje glede večje ali manjše resnosti kaznivih dejanj v posameznih nacionalnih zakonodajah precej razlikujejo. [21]

69. Skratka, Direktiva (EU) 2016/680 kot pogoj za zakonitost ne določa, da se sme obdelava osebnih podatkov, ki se ureja z njo, izvajati le zaradi boja proti hudim kaznivim dejanjem.

70. To ne posega v dejstvo, da je treba obdelavo podatkov, ki jo nameravajo pristojni organi izvajati v skladu z Direktivo (EU) 2016/680, v skladu z načelom sorazmernosti in za vsak primer posebej prilagoditi glede na: (a) naravo preganjanih kaznivih dejanj in (b) vrsto osebnih podatkov, na katere se nanaša ta obdelava.

71. V zvezi s tem se strinjam z nekaterimi izjavami nemške vlade o omejitvi dostopa do podatkov iz zaseženih telefonov, če ti glede na digitalno vsebino telefonov omogočajo oblikovanje popolnega profila osebnosti njihovih imetnikov. Po mnenju nemške vlade bi moral biti tak dostop omejen na podatke, ki so potrebni kot dokazi v konkretnem primeru, in bi bil lahko neprimeren zaradi dejavnikov, kot sta „manj huda narava preiskovanega kaznivega dejanja ali šibka dokazna vrednost podatkov, ki se poskušajo pridobiti“. [22]

72. Iz Direktive (EU) 2016/680 torej *abstraktno* gledano ne izhaja, da je dostop do osebnih podatkov, shranjenih v mobilnem telefonu, zaradi olajšanja preiskave o dejanjih, ki se lahko štejejo za dejanja splošne ali običajne kriminalitete, sistematično nezakonit. Ali je *v konkretnem primeru* takšen dostop primeren, pa mora zadevni organ presoditi za vsak primer posebej ob upoštevanju njegove nujnosti in merila sorazmernosti, ki sem ga pravkar navedel.

73. To po mojem mnenju izhaja iz določb Direktive (EU) 2016/680, ki določajo pogoje veljavnosti obdelave osebnih podatkov v okviru boja proti kriminalu:

– člena 4(1)(a), v skladu s katerim je treba zagotoviti, da se podatki „obdelujejo zakonito“;

[21] Francoska vlada kot primer navaja kazniva dejanja v zvezi s posedovanjem drog in trgovino z njimi, katerih resnost se v avstrijskem in francoskem kazenskem pravu razlikuje. Podobno meni tudi švedska vlada.

[22] Pisno stališče nemške vlade (točka 20).

– člena 8(1), v katerem je poudarjeno, da se mora obdelava izkazati za *potrebno* in mora temeljiti na pravu Unije ali države članice.

2. Drugo vprašanje za predhodno odločanje

74. Predložitveno sodišče želi z drugim vprašanjem za predhodno odločanje izvedeti, ali člen 15(1) Direktive 2002/58 v povezavi s členi 7, 8, 11 in 52(1) Listine „nasprotuje nacionalni ureditvi, kot je ta iz člena 18 v povezavi s členom 99(1) [StPO], v skladu s katero si varnostni organi med postopkom kazenskega preiskovanja brez dovoljenja sodišča ali neodvisnega upravnega organa sami sebi zagotovijo vseobsežen in nenadzorovan dostop do vseh digitalnih podatkov, shranjenih na mobilnem telefonu“.

75. Besedilo vprašanja je nekoliko dvoumno. Predložitveno sodišče:

– priznava, da člen 110(2) StPO določa, da je za zaseg premoženja načeloma potrebno dovoljenje državnega tožilstva. Policijski organ lahko brez takšnega dovoljenja opravi tak zaseg le v izrednih okoliščinah iz odstavka 3 istega člena (za katere se zdi, da v obravnavani zadevi niso podane);

– vendar dodaja, da analiza podatkov, shranjenih v mobilnih telefonih, „[v StPO] ni nedvoumno urejena“ in da jo lahko varnostni organi izvajajo na lastno pobudo brez predhodnega dovoljenja.

76. Avstrijska vlada je podala razlago nacionalne zakonodaje, ki ni enaka razlagi iz predložitvene odločbe. Zlasti navaja, da sta po nacionalnem pravu tako zaseg telefona (razen v nujnih primerih) kot analiza podatkov, shranjenih v njem, mogoča le z dovoljenjem državnega tožilstva.[23] Brez odredbe državnega tožilstva je to, da policija uporabi podatke, shranjene v takem telefonu, nezakonito.

77. Pogoje nacionalne zakonodaje mora preveriti predložitveno sodišče. Sodišče v okviru postopka iz člena 267 PDEU ni pristojno za razlago nacionalnega prava, zato mora izključno predložitveno sodišče natančno opredeliti področje uporabe nacionalnih zakonov in drugih predpisov.[24]

78. Ne da bi se želel spuščati v polemiko glede razlage avstrijskega prava, menim, da je težko samo iz določb, ki jih navaja predložitveno sodišče (člen 18 StPO v povezavi s členom 99(1) istega zakona), izpeljati posledico, ki jo samo izpeljuje. Vendar ponavljam, da lahko o tem odloči le to sodišče.

79. Predložitveno sodišče pa meni, da je mogoče ugotovitev iz sodbe Prokuratuur,[25] ki se nanaša na predhodni preizkus dostopa sodišča ali neodvisnega organa do hranjenih podatkov, prenesti na primer, kot je ta v obravnavani zadevi.

[23] Točka 19 pisnega stališča avstrijske vlade. Ta vlada navaja odločbo vrhovnega sodišča (Oberster Gerichtshof, Avstrija) z dne 13. oktobra 2020 (zadeva 11 Os 56/20z), v kateri je analiza podatkov na mobilnem telefonu s strani kriminalistične policije brez dovoljenja državnega tožilstva opredeljena kot nezakonita, ker gre za poseg v subjektivne pravice zadevne osebe.

[24] Med drugim sodba z dne 28. aprila 2022, SeGEC in drugi (C-277/21, EU:C:2022:318, točka 21).

[25] Sodba Prokuratuur (točka 51): „[B]istveno [je], da pred dostopom pristojnih nacionalnih organov do hranjenih podatkov sodišče ali neodvisen upravni organ opravi predhoden preizkus in da se odločba tega sodišča ali tega organa izda na obrazložen predlog navedenih nacionalnih organov, ki se predloži, med drugim, v okviru postopkov preprečevanja, odkrivanja ali pregona kaznivih dejanj“.

80. Nasprotno pa je treba po mnenju nizozemske vlade to ugotovitev razlagati v okviru nacionalne zakonodaje, ki je omogočala *splošen* dostop pristojnih organov do *vseh* hranjenih podatkov o prometu in lokaciji. To bi pojasnilo zahtevo po predhodni sodni odobritvi, ki pa v primeru dostopa do podatkov enega samega mobilnega telefona morda ni upravičena.

81. Podobno norveška vlada trdi, da med številnimi jamstvi, določenimi z Direktivo 2016/680, [26] ni izrecno navedeno, da mora biti predhodno izdano dovoljenje neodvisnega sodnega ali upravnega organa.

82. Komisija izhaja iz tega, da je treba določbe Direktive (EU) 2016/680 razlagati ob upoštevanju Listine, in trdi, da obveznost, ki jo državam članicam nalaga člen 8(1) te direktive (pogoji za zakonitost obdelave), vključuje potrebo po spoštovanju temeljnih pravic, zagotovljenih s členoma 7 in 8 Listine.

83. Strinjam se s Komisijo, da morajo nacionalni zakonodajalci ob spoštovanju teh določb Listine opredeliti pravila, potrebna za zagotovitev, da je dostop do podatkov utemeljen v vsakem posameznem primeru in omejen na to, kar je nujno potrebno in sorazmerno.

84. Vendar pa ni nujno, da so takšna nacionalna pravila specifična za dostop do osebnih podatkov, ki jih – kot v tem primeru – vsebuje mobilni telefon, temveč so lahko to pravila, ki so v nacionalnem pravu na splošno določena na področju pridobivanja dokazov.

85. V zvezi s tem sem že navedel točko 103 sodbe La Quadrature du Net v zvezi z ukrepi držav članic, ki vplivajo na zaupnost elektronskih komunikacij, ne da bi ponudnikom teh komunikacij nalagali obveznosti obdelave. [27]

86. Ker torej iz Direktive (EU) 2016/680 ni treba izpeljati *posebnih* postopkovnih pravil za zagotovitev zakonitosti dostopa do podatkov, shranjenih v mobilnem telefonu, [28] se uporablja nacionalna zakonodaja, ki ureja izvajanje pooblastil za preiskavo in zaseg v okviru kazenskih preiskav. [29]

87. Poleg tega je sklicevanje na določbe nacionalnega prava za zagotovitev zakonitosti dostopa na podlagi Direktive (EU) 2016/680 v skladu s sodno prakso ESČP. ESČP je v zadevi, ki se je nanašala prav na Republiko Avstrijo v zvezi s členom 8 EKČP (pravica do spoštovanja zasebnega in družinskega življenja, doma in dopisovanja), ugotovilo, da se avstrijska zakonodaja o zasegu predmetov, zlasti dokumentov, uporablja za preiskavo in zaseg podatkov, shranjenih na računalniških nosilcih. [30]

[26] Poleg tistih iz členov 4 in 8 tudi iz poglavij III („Pravice posameznika, na katerega se nanašajo osebni podatki“), IV („Upravljavec in obdelovalec“), VI („Neodvisni nadzorni organi“) in VIII („Pravna sredstva, odgovornost in kazni“).

[27] Glej točko 36 teh sklepnih predlogov.

[28] Težavnost te naloge se kaže v prizadevanjih Komisije v točkah od 34 do 39 njenega pisnega stališča, da bi prispevala k opredelitvi jasnih in natančnih pravil za določitev omejitev in ustreznih jamstev v zvezi z dostopom do podatkov v mobilnem telefonu.

[29] Zakonodaja, ki, kot na primer poudarjata danska in irska vlada, ne spada na področje uporabe prava Unije, vendar lahko služi izpolnjevanju zahteve, ki izhaja iz tega prava.

[30] Sodba ESČP z dne 16. oktobra 2007, Wieser in Bicos Beteiligungen proti Avstriji (CE:ECHR:2007:1016JUD007433601, točka 54): „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“.

88. Če organi kazenskega pregona, kot trdi avstrijska vlada in se pri tem sklicuje na sodno prakso Oberster Gerichtshof (vrhovno sodišče, Avstrija), brez dovoljenja državnega tožilstva nimajo pravice do dostopa do podatkov, shranjenih v določenem mobilnem telefonu, drugo vprašanje za predhodno odločanje v veliki meri izgubi svoj smisel.

89. Vsekakor odgovor na to vprašanje ne more izključiti možnosti, da bi bilo z dostopom do osebnih podatkov na zaseženem telefonu mogoče „rekonstruirati zelo podrobno in natančno sliko na skoraj vseh področjih zasebnega življenja“ zadevne osebe.[31] Če je tako, policijski organi ne bi smeli opustiti pridobitve predhodnega dovoljenja iz sodbe Prokuratuur.

90. Na prvi pogled se zdi, da je ta izjava v nasprotju z neuporabo Direktive 2002/58 (ki je razložena v sodbi Prokuratuur) v obravnavani zadevi, kot sem dokazoval zgoraj. Vendar razumem, da *smisel* te sodbe podpira enako rešitev.

91. Čeprav je bil v zadevi, v kateri je bila izdana sodba Prokuratuur, dostop omogočen s pridobitvijo podatkov (metapodatkov) ponudnikov elektronskih komunikacijskih storitev, je šlo – kot v obravnavani zadevi – za posamično kazensko preiskavo zoper določeno osebo. Šlo je za zbiranje „podatk[ov] v zvezi z več telefonskimi številkami […] in njenimi različnimi mednarodnimi identitetami mobilnega terminala“.[32]

92. V sodbi Prokuratuur je po mojem mnenju mogoče razlikovati dve ravni: (a) pomisleke glede splošne ureditve države članice o splošni in neselektivni hrambi podatkov, ki jih hranijo ponudniki storitev, in o poznejšem dostopu do njih, ter (b) predhodni preizkus dostopa do teh metapodatkov v posamičnem primeru, če omogočajo oblikovanje natančnega profila zasebnega življenja osebe.

93. Dejstvo, da v obravnavani zadevi podatki, ki razkrivajo zasebno življenje, niso v posesti ponudnikov storitev in so pridobljeni (ali se poskušajo pridobiti) iz enega samega zaseženega telefona, se mi zdi drugotnega pomena v primerjavi s *smislom* zahteve po predhodnem preizkusu, na katerega se sklicuje sodba Prokuratuur.

94. Ta predhodni preizkus ima končno podlago v varstvu, zagotovljenem s členoma 7 in 8 Listine. Organ, ki izvaja ukrep, mora „zagotoviti pravično ravnotežje med interesi, povezanimi s potrebami preiskave, ki se nanaša na boj proti kriminalu, na eni strani ter temeljnimi pravicami do spoštovanja zasebnega življenja in varstva osebnih podatkov posameznikov, do katerih podatkov se dostopa, na drugi“.[33]

3. Tretje vprašanje za predhodno odločanje

95. Predložitveno sodišče želi s tretjim vprašanjem za predhodno odločanje izvedeti, ali člen 47 Listine (morebiti v povezavi s členoma 41 in 52) nasprotuje zakonodaji, kot je avstrijska,[34] ki „omogoča, da se mobilni telefon digitalno pregleda, ne da bi bil [posameznik, na katerega se nanašajo osebni podatki,] s tem predhodno [seznanjen] ali bi [bil seznanjen] vsaj po sprejetju ukrepa“.

[31] Glej trditve predložitvenega sodišča, povzete v točki 44 teh sklepnih predlogov.

[32] Sodba Prokuratuur (točka 17).

[33] Sodba Prokuratuur (točka 52).

[34] Ponovno je napoteno na člen 18 StPO v povezavi s členom 99 tega zakona.

96. Menim, da tako oblikovano vprašanje morda ni potrebno za rešitev spora, saj je posameznik, na katerega se nanašajo osebni podatki, lahko uveljavljal pravico iz člena 47 Listine in predložitveno sodišče pozval, naj razglasi ničnost policijskega ukrepa v zvezi z zaseženim telefonom, ki je vključeval poznejši (neuspešen) poskus uporabe podatkov, shranjenih na njem.

97. V zvezi s tema trenutkoma policijskega ukrepanja bi bilo treba razlikovati:

– v zvezi s samim zasegom telefona je iz podatkov v spisu razvidno, da je bil posameznik, na katerega se osebni podatki nanašajo, z njim seznanjen in da policijskim organom ob zasegu telefona ni želel posredovati kode za odklepanje;

– v zvezi s poskusom analize podatkov se zdi, da upravljavec podatkov posameznika, na katerega se nanašajo osebni podatki, ni obvestil o tej operaciji, čeprav avstrijska vlada navaja, da je bil ta seznanjen s poročilom, v katerem je bilo navedeno, kako je kriminalistična policija postopala s telefonom. [35]

98. Zato ostajajo nekatere nejasnosti glede uporabe podatkov in seznanjenosti posameznika, na katerega se osebni podatki nanašajo, ki bi jih moralo, kot sem že poudaril, predložitveno sodišče pojasniti v predložitveni odločbi in ki onemogočajo koristen odgovor na tretje vprašanje za predhodno odločanje.

99. Kljub temu bom to vprašanje obravnaval, če Sodišče ne bi ugotovilo, da ni dopustno. V tem primeru in ob upoštevanju nemožnosti uporabe Direktive 2002/58 bi bilo treba vprašanje preoblikovati ob upoštevanju Direktive 2016/680, katere členi 13, 15 in 54 vsebujejo iztočnice za odgovor nanj.

100. V skladu z Direktivo 2016/680 je treba posamezniku, na katerega se osebni podatki nanašajo, sporočiti informacije o obdelavi osebnih podatkov, ki so med drugim potrebne za to, da: (a) pri nadzornem organu vloži pritožbo (člen 13(1)(d)) in (b) si zagotovi učinkovito sodno varstvo pred kršitvijo pravic, zagotovljenih z Direktivo 2016/680, brez poseganja v razpoložljiva upravna ali izvensodna sredstva (člen 54).

101. Vendar se ne sme pozabiti, da tako člen 13(3) kot člen 15(1) Direktive 2016/680 državam članicam omogočata, da sprejmejo zakonodajne ukrepe, s katerimi:

– se zagotovitev informacij posamezniku, na katerega se osebni podatki nanašajo, zadrži, omeji ali opusti v skladu s členom 13(2);

– se pravica posameznika, na katerega se osebni podatki nanašajo, do dostopa do obdelanih podatkov v celoti ali delno omeji, če je takšna omejitev nujen in sorazmeren ukrep, da se *med drugim* prepreči oviranje uradnih ali sodnih preiskav ali postopkov ali vplivanje na preiskovanje kaznivih dejanj. [36]

102. Vsekakor zakonitost obdelave podatkov ni odvisna od tega, ali so pristojni organi izpolnili (poznejše) obveznosti, ki so jim bile naložene s členom 13 Direktive (EU) 2016/680, temveč od zakonitosti namena, ki je upravičeval obdelavo, torej od tega, ali so bili ti upravni organi upravičeni do obdelave osebnih podatkov.

[35] Točka 37 njenega pisnega stališča.

[36] Glej v tem smislu sodbo Tele2 Sverige in Watson (točka 121). To ugotovitev v zvezi z Direktivo 2002/58 je mogoče prenesti na Direktivo 2016/680 v okviru zagotavljanja sodnega varstva posameznikov, na katere se nanašajo osebni podatki.

103. S tega vidika dejstvo, ali je bil posameznik, na katerega se osebni podatki nanašajo, obveščen o poskusih dostopa do podatkov, shranjenih v telefonu, ki mu je bil zasežen, samo po sebi ni povezano z zakonitostjo policijskega ukrepa z vsebinskega vidika. Ravnanje upravljavca, ki je lahko v nasprotju z dolžnostmi, ki mu jih nalaga člen 13 Direktive (EU) 2016/680, ima lahko druge posledice, vendar, ponavljam, samo po sebi ne vpliva na zakonitost ali nezakonitost te obdelave.

104. Predložitveno sodišče mora preveriti, ali nacionalna ureditev zadevni osebi omogoča učinkovito uveljavljanje teh pravic.

V. Predlog

105. Glede na navedeno Sodišču predlagam, naj predlog za sprejetje predhodne odločbe, ki ga je vložilo Landesverwaltungsgericht Tirol (deželno upravno sodišče za Tirolsko, Avstrija), razglasi za nedopusten.

Podredno predlagam, naj se na ta predlog odgovori tako:

1. Člen 4(1)(a) in člen 8(1) Direktive (EU) 2016/680 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov, ki jih pristojni organi obdelujejo zaradi preprečevanja, preiskovanja, odkrivanja ali pregona kaznivih dejanj ali izvrševanja kazenskih sankcij, in o prostem pretoku takih podatkov ter o razveljavitvi Okvirnega sklepa Sveta 2008/977/PNZ v povezavi s členi 7, 8 in 52 Listine Evropske unije o temeljnih pravicah

   je treba razlagati tako, da

   dostop javnih organov do osebnih podatkov, shranjenih v mobilnem telefonu, zaradi njihove obdelave v okviru kazenske preiskave ni omejen na primere boja proti hudim kaznivim dejanjem.

   Tak dostop mora biti utemeljen v vsakem posameznem primeru ter omejen na to, kar je nujno potrebno in sorazmerno glede na naravo preganjanih kaznivih dejanj in osebnih podatkov, do katerih se namerava dostopati.

   Policijski organi v okviru kazenske preiskave ne smejo sami, brez predhodnega dovoljenja pravosodnega organa, pridobiti popolnega in nenadzorovanega dostopa do vseh podatkov, shranjenih v mobilnem telefonu, če je na njihovi podlagi mogoče izoblikovati natančno sliko o zasebnem življenju osebe.

2. Člene 13, 15 in 54 Direktive 2016/680 v povezavi s členoma 47 in 52 Listine

   je treba razlagati tako, da

   mora biti imetnik mobilnega telefona brez poseganja v omejitve, dovoljene s členom 15(1) Direktive (EU) 2016/680, ali v druga razpoložljiva upravna ali izvensodna sredstva obveščen o obdelavi osebnih podatkov, shranjenih v tem telefonu, od ustreznih organov, in sicer v času in pod pogoji, ki so potrebni za zagotovitev učinkovitega uveljavljanja njegove pravice, da zahteva sodno varstvo pred morebitno kršitvijo pravic, priznanih z Direktivo (EU) 2016/680.