Zbornik sudske prakse

MIŠLJENJE NEZAVISNOG ODVJETNIKA
MANUELA CAMPOSA SÁNCHEZ-BORDONE
od 20. travnja 2023. [1]

Predmet C-548/21

C. G.
protiv
Bezirkshauptmannschaft Landeck

(zahtjev za prethodnu odluku koji je uputio Landesverwaltungsgericht Tirol (Zemaljski upravni sud u Tirolu, Austrija))

„Zahtjev za prethodnu odluku – Telekomunikacije – Zaštita osobnih podataka – Direktiva (EU) 2016/680 – Kazneni postupak – Pokušaj tijela javne vlasti da pristupe podacima pohranjenim pohranjenima na mobilnom telefonu bez odobrenja suda ili neovisnog upravnog tijela”

1. Predmetni se zahtjev za prethodnu odluku odnosi, ukratko, na uvjete koje trebaju ispuniti policijska tijela kako bi pristupila podacima pohranjenima na mobilnom telefonu osobe protiv koje se vodi kaznena istraga.

2. Kao što ću to pokušati objasniti, postoje znatni nedostaci u pogledu dopuštenosti zahtjeva za prethodnu odluku. Ako Sud ipak odluči ispitivati meritum, treba donijeti odluku o područjima primjene Direktive 2002/58/EZ [2] i Direktive (EU) 2016/680 [3].

[1] Izvorni jezik: španjolski

[2] Direktiva Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL 2002., L 201, str. 37.) (SL, posebno izdanje na hrvatskom jeziku, poglavlje 13., svezak 52., str. 111.)

[3] Direktiva Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP (SL 2016., L 119, str. 89. i ispravak SL 2018., L 127, str. 14.)

I. Pravni okvir

A. Pravo Unije

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

3. Člankom 2. („Glavno područje primjene”) stavkom 2. određuje se:

„Ova se Uredba ne odnosi na obradu osobnih podataka:

[…]

(d) koju obavljaju nadležna tijela u svrhu sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihova sprečavanja.”

2. Direktiva 2016/680

4. U uvodnoj izjavi 2. navodi se:

„Načela i pravila o zaštiti pojedinaca u vezi s obradom njihovih osobnih podataka trebala bi poštovati njihova temeljna prava i slobode, a posebno njihovo pravo na zaštitu osobnih podataka, bez obzira na državljanstvo ili boravište pojedinaca. Ovom Direktivom želi se doprinijeti uspostavi područja slobode, sigurnosti i pravde.”

5. U uvodnoj izjavi 46. navodi se:

„Svako ograničavanje prava ispitanika mora biti u skladu s Poveljom i Europskom konvencijom o zaštiti ljudskih prava, kako se tumače u sudskoj praksi Suda odnosno Europskog suda za ljudska prava[5], te se njime posebno mora poštovati bit tih prava i sloboda.”

6. Uvodna izjava 49. glasi:

„Ako se osobni podaci obrađuju u okviru kaznene istrage i sudskih postupaka u kaznenim predmetima, države članice trebale bi imati mogućnost predvidjeti da se ostvarivanje prava na informiranje, pristup i ispravak ili brisanje osobnih podataka i ograničavanje obrade obavlja u skladu s nacionalnim pravilima o sudskom postupku.”

7. Člankom 1. („Predmet i ciljevi”) određuje se:

„1. Ovom se Direktivom utvrđuju pravila povezana sa zaštitom pojedinaca u pogledu obrade osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje.

[4] Uredba Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL 2016., L 119, str. 1. i ispravci SL 2018., L 127, str. 2. i SL 2021., L 74, str. 35.). U daljnjem tekstu: OUZP.

[5] U daljnjem tekstu: ESLJP

2. U skladu s ovom Direktivom države članice:

(a) štite temeljna prava i slobode pojedinaca, a posebno njihovo pravo na zaštitu osobnih podataka; i

[…]

3. Ovom se Direktivom ne sprečava države članice da predvide snažnije zaštitne mjere za zaštitu prava i sloboda ispitanika u pogledu obrade osobnih podataka od strane nadležnih tijela, od onih koje su utvrđene u ovoj Direktivi."

8. U članku 2. („Područje primjene") stavku 1. navodi se:

„Ova se Direktiva primjenjuje na obradu osobnih podataka od strane nadležnih tijela u svrhe utvrđene u članku 1. stavku 1."

9. U članku 3. („Definicije") utvrđuje se:

„Za potrebe ove Direktive:

[…]

2. ‚obrada' znači svaki postupak ili skup postupaka koji se obavljaju na osobnim podacima ili skupovima osobnih podataka, bilo automatiziranim bilo neautomatiziranim sredstvima kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje;

[…]

7. ‚nadležno tijelo' znači:

(a) svako tijelo javne vlasti nadležno za sprečavanje, istragu, otkrivanje ili progon kaznenih djela ili izvršavanje kaznenih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje; ili

[…]."

10. Člankom 4. („Načela obrade osobnih podataka") stavkom 1. propisuje se:

„Države članice osiguravaju da su osobni podaci:

(a) obrađivani zakonito i pošteno;

(b) prikupljeni u posebne, izričite i zakonite svrhe te da ih se ne obrađuje na način koji nije u skladu s tim svrhama;

(c) primjereni i relevantni te da nisu pretjerani u odnosu na svrhe u koje se obrađuju;

[…]

(e) čuvani u obliku koji omogućuje identifikaciju ispitanikâ samo onoliko dugo koliko je potrebno u svrhe radi kojih se osobni podaci obrađuju;

(f) obrađivani na način kojim se osigurava odgovarajuća sigurnost osobnih podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih tehničkih ili organizacijskih mjera.”

11. U članku 8. („Zakonitost obrade”) ističe se:

„1. Države članice osiguravaju da je obrada zakonita samo ako je nužna i samo u onoj mjeri u kojoj je nužna kako bi nadležno tijelo obavilo zadaću u svrhe navedene u članku 1. stavku 1. te da se temelji na pravu Unije ili pravu države članice.

2. Pravom države članice kojim se uređuje obrada unutar područja primjene ove Direktive navode se barem ciljevi obrade, osobni podaci za obradu i svrhe obrade.”

12. Člankom 13. („Informacije koje se stavljaju na raspolaganje ili daju ispitaniku”) propisuje se:

„1. Države članice osiguravaju da voditelj obrade ispitaniku stavlja na raspolaganje barem sljedeće informacije:

[…]

(d) pravo na podnošenje pritužbe nadzornom tijelu i kontaktne podatke nadzornog tijela;

[…]

3. Države članice mogu donijeti zakonodavne mjere za odgađanje, ograničavanje ili uskraćivanje pružanja informacija ispitaniku na temelju stavka 2. u onoj mjeri i u onom trajanju u kojem takva mjera predstavlja potrebnu i proporcionalnu mjeru u demokratskom društvu uz dužno poštovanje temeljnih prava i legitimnih interesa dotičnog pojedinca, kako bi se:

(a) izbjeglo ometanje službenih ili pravnih ispitivanja, istraga ili postupaka;

(b) izbjeglo dovođenje u pitanje sprečavanja, otkrivanja, istrage ili progona kaznenih djela ili izvršavanja kaznenih sankcija;

(c) zaštitila javna sigurnost;

(d) zaštitila nacionalna sigurnost;

(e) zaštitila prava i slobode drugih.

[…]”

13. U skladu s člankom 15. („Ograničenja prava pristupa”) stavkom 1.:

„Države članice mogu donijeti zakonodavne mjere kojima se ispitaniku u cijelosti ili djelomično može ograničiti pravo pristupa u onoj mjeri i u onom trajanju u kojem takvo djelomično ili potpuno ograničavanje čini neophodnu i proporcionalnu mjeru u demokratskom društvu uz dužno poštovanje temeljnih prava i legitimnih interesa dotičnog pojedinca kako bi se:

(a) izbjeglo ometanje službenih ili pravnih ispitivanja, istraga ili postupaka;

(b) izbjeglo dovođenje u pitanje sprečavanja, otkrivanja, istrage ili progona kaznenih djela ili izvršavanja kaznenih sankcija;

(c) zaštitila javna sigurnost;

(d) zaštitila nacionalna sigurnost;

(e) zaštitila prava i slobode drugih.”

14. Na temelju članka 27. („Procjena učinka na zaštitu podataka”):

„1. Ako je vjerojatno da će neka vrsta obrade, osobito putem novih tehnologija i uzimajući u obzir prirodu, opseg, kontekst i svrhe te obrade, prouzročiti visoki rizik za prava i slobode pojedinaca, države članice osiguravaju da voditelj obrade prije obrade provede procjenu učinka predviđenih postupaka obrade na zaštitu osobnih podataka.

2. Procjena iz stavka 1. mora sadržavati barem općenit opis predviđenih postupaka obrade, procjenu rizika za prava i slobode ispitanika, predviđene mjere za rizike, zaštitne i sigurnosne mjere i mehanizme kako bi se osigurala zaštita osobnih podataka i dokazala usklađenost s ovom Direktivom, uzimajući u obzir prava i legitimne interese ispitanika i drugih uključenih osoba.”

15. Članak 28. („Prethodno savjetovanje s nadzornim tijelom”) glasi:

„1. Države članice osiguravaju da se voditelj obrade ili izvršitelj obrade savjetuje s nadzornim tijelom prije obrade osobnih podataka koji će biti uključeni u novi sustav pohrane koji se treba uspostaviti, ako:

(a) procjena učinka na zaštitu podataka kako je predviđeno člankom 27. upućuje na to da bi obrada mogla rezultirati visokim rizikom ako voditelj obrade ne poduzme mjere kako bi umanjio rizik; ili

(b) vrsta obrade, posebno ako se upotrebljavaju nove tehnologije, mehanizmi ili postupci, predstavlja visok rizik za prava i slobode ispitanikâ.

[…].”

16. Člankom 54. („Pravo na učinkoviti sudski pravni lijek protiv voditelja obrade ili izvršitelja obrade”) utvrđuje se:

„Ne dovodeći u pitanje nijedan dostupan upravni ili izvansudski pravni lijek, uključujući pravo na podnošenje pritužbe nadzornom tijelu u skladu s člankom 52., države članice ispitaniku

osiguravaju pravo na učinkovit sudski pravni lijek ako on smatra da su mu prekršena njegova prava utvrđena odredbama donesenima na temelju ove Direktive uslijed obrade njegovih osobnih podataka koja nije u skladu s tim odredbama."

B. Nacionalno pravo

17. Člankom 18. Strafprozessordnunga[6] kriminalističkoj se policiji dodjeljuju zadaće kaznenog sudovanja (stavak 1.). Za istrage kriminalističke policije odgovorna su sigurnosna tijela (stavak 2.). Tijela službe za javnu sigurnost obavljaju izvršnu funkciju kriminalističke policije, odnosno istražuju i provode progon kaznenih djela (stavak 3.).

18. U skladu s člankom 99. ZKP-a, kriminalistička policija istragu provodi po prijavi ili po službenoj dužnosti, pri čemu slijedi naloge državnog odvjetništva i sudova (stavak 1.). Ako je za određenu istražnu mjeru potreban nalog državnog odvjetništva, u slučaju da postoji neposredna opasnost kriminalistička policija može izvršiti odgovarajuću ovlast i ako takav nalog ne postoji. U tom slučaju bez odgađanja mora zatražiti odobrenje (stavak 2.).

19. U skladu s člankom 111. stavkom 2. ZKP-a, kad treba prikupiti podatke pohranjene na nosačima podataka, svaka je osoba obvezna dopustiti da se navedenim podacima pristupi te, nakon što se to od nje zatraži, uručiti elektronički nosač podataka u formatu koji se načelno koristi ili omogućiti njegovu izradu. Treba usto dopustiti da se izradi sigurnosni primjerak podataka pohranjenih na nosačima podataka.

II. Činjenice, spor i prethodna pitanja

20. C. G. njemački je državljanin koji radi i boravi u Austriji.

21. Službenici Zollamta Innsbruck (Carinska uprava u Innsbrucku, Austrija) zaplijenili su 23. veljače 2021. u okviru nadzora narkotika paket naslovljen na C. G.-a koji je sadržavao 85 grama kanabisa.

22. Dva policijska službenika ispitala su 6. ožujka 2021. C. G.-a o pošiljatelju paketa te su pretražila njegov stan. Tijekom pretrage oduzeli su mu mobilni telefon (u kojem su bile SIM i SD kartica) te su mu uručili zapisnik o oduzimanju.

23. Nakon što je od njega zatraženo da dopusti pristup podacima o vezama s njegova mobilnog telefona, C. G. je to odbio, a nije htio otkriti ni lozinku za otključavanje telefona.

24. Bezirkspolizeikommand Landeck (Zapovjedništvo okružne policijske postaje u Landecku, Austrija) nije uspjelo otključati mobilni telefon. Mobilni telefon dostavljen je Bundeskriminalamtu (Savezni ured kriminalističke policije, Austrija) u Beču, gdje ga se ponovno bezuspješno pokušalo otključati i očitati pohranjene podatke.

25. U trenutku kad ih je policija poduzela, za mjere nije postojao ni nalog državnog odvjetništva ni nalog suda.

[6] Zakon o kaznenom postupku. U daljnjem tekstu: ZKP. BGBl br. 631/1975, u verziji primjenjivoj u vrijeme nastanka činjenica (BGBl I br. 24/2020).

26. C. G. je 31. ožujka 2021. podnio žalbu Landesverwaltungsgerichtu Tirol (Zemaljski upravni sud u Tirolu, Austrija) protiv prisilne mjere koja mu je izrečena te je osporavao to što mu je mobilni telefon oduzet. Mobilni telefon vraćen mu je 20. travnja 2021.

27. C. G. nije obaviješten o pokušajima analize sadržaja mobilnog telefona; za njih je saznao tek kad je policijski službenik koji mu je oduzeo mobilni telefon i zatim pokrenuo digitalnu obradu ispitan kao svjedok pod prisegom. Ti pokušaji nisu navedeni ni u spisu kriminalističke policije.

28. U tim je okolnostima Landesverwaltungsgericht Tirol (Zemaljski upravni sud u Tirolu) Sudu uputio sljedeća prethodna pitanja:

„1. Treba li članak 15. stavak 1. (eventualno u vezi s člankom 5.) Direktive 2002/58, kako je izmijenjena Direktivom 2009/136/EZ, u vezi s člancima 7. i 8. Povelje […] tumačiti na način da pristup tijela javne vlasti podacima pohranjenima na mobilnim telefonima čini tako ozbiljno zadiranje u temeljna prava zajamčena navedenim člancima Povelje da se taj pristup u području sprečavanja, istrage, otkrivanja i progona kaznenih djela mora ograničiti na borbu protiv teških kaznenih djela?

2. Treba li članak 15. stavak 1. Direktive 2002/58, kako je izmijenjena Direktivom 2009/136/EZ, u vezi s člancima 7., 8., 11. kao i člankom 52. stavkom 1. Povelje […] tumačiti na način da mu se protivi nacionalna odredba poput članka 18. u vezi s člankom 99. stavkom 1. [ZKP-a], prema kojoj sigurnosna tijela u okviru kaznene istrage bez odobrenja suda ili neovisnog upravnog tijela sama sebi pribavljaju sveobuhvatan i nekontroliran pristup svim digitalnim podacima pohranjenima na mobilnom telefonu?

3. Treba li članak 47. Povelje […], eventualno u vezi s njezinim člancima 41. i 52., uzimajući u obzir načelâ jednakosti oružja i djelotvorne sudske zaštite, razumjeti na način da mu se protivi odredba države članice kojom se poput članka 18. u vezi s člankom 99. stavkom 1. [ZKP-a] omogućava digitalna obrada mobilnog telefona, a da se osoba čiji se podaci obrađuju o tome prethodno ili barem nakon određivanja mjere ne obavijesti?”

III. Postupak pred Sudom

29. Tajništvo Suda zahtjev za prethodnu odluku zaprimilo je 6. rujna 2021.

30. Sud je 20. listopada 2021. od suda koji je uputio zahtjev zatražio da se očituje o tome bi li za rješavanje predmeta mogla biti relevantna Direktiva 2016/680.

31. Sud koji je uputio zahtjev odgovorio je 11. studenoga 2021. da Direktivu 2016/680 treba primijeniti na glavni postupak.

32. Pisana očitovanja podnijele su njemačka, austrijska, ciparska, danska, estonska, francuska, mađarska, irska, nizozemska, norveška, poljska i švedska vlada te Europska komisija.

33. Na raspravi održanoj 16. siječnja 2023. sudjelovale su sve stranke koje su podnijele očitovanja, osim njemačke, mađarske i poljske vlade, kao i finska vlada. Sud je od navedenih stranaka zatražio da se u svojim argumentima usmjere na Direktivu 2016/680 i da usmeno odgovore na određena pitanja o njoj.

IV. Analiza

A. Nedopuštenost

34. Sud koji je uputio zahtjev prvotno je u svojim pitanjima tražio samo tumačenje Direktive 2002/58. Međutim, gotovo sve stranke koje sudjeluju u postupku slažu se da se ta direktiva ne primjenjuje na ovaj predmet, pa prema tome ni njezino tumačenje nije potrebno za rješavanje spora.

35. U skladu s člankom 3. Direktive 2002/58, ona se primjenjuje na „[…] obradu osobnih podataka vezanih uz pružanje javno dostupnih usluga elektroničkih komunikacija na javno dostupnim komunikacijskim mrežama u [Uniji], uključujući javne komunikacijske mreže koje podržavaju prikupljanje podataka i naprava za identifikaciju”.

36. Sud je odlučio da, „kada države članice izravno provode mjere koje odstupaju od povjerljivosti elektroničkih komunikacija, a da ne određuju obveze obrade pružateljima usluga takvih komunikacija, zaštita podataka dotičnih osoba nije obuhvaćena Direktivom 2002/58, nego samo nacionalnim pravom, podložno primjeni [Direktive 2016/680]” [7].

37. U predmetu o kojem je ovdje riječ podacima su pokušala pristupiti izravno policijska tijela u okviru kaznene istrage. Pružatelji elektroničkih komunikacijskih usluga nisu u tome sudjelovali niti je od njih zatraženo da ustupe osobne podatke. Stoga se ne primjenjuje Direktiva 2002/58.

38. Propis prava Unije kojim je uređena ova situacija jest Direktiva 2016/680, na temelju čijeg članka 2. stavka 1. se ta direktiva primjenjuje na obradu osobnih podataka od strane nadležnih tijela u „svrhe […] istrage […] kaznenih djela”.

39. To je dovoljno da se zauzme stajalište da je zahtjev za prethodnu odluku, onako kako ga je sastavio nacionalni sud, nedopušten jer se traži tumačenje propisa prava Unije koji se ne primjenjuje na slučaj.

40. Međutim, točno je da se člankom 267. UFEU-a Sudu omogućuje da preoblikuje prethodna pitanja koja mu se upute ili da navede druga pravna pravila prava Unije koja bi mogla biti relevantna kako bi nacionalnom sudu pružio koristan odgovor [8].

41. Sud je od suda koji je uputio zahtjev zatražio da se očituje o eventualnoj primjeni Direktive 2016/680. Time mu je dao priliku da sam dopuni ili preoblikuje svoja pitanja. Umjesto da je to učinio, sud koji je uputio zahtjev samo je istaknuo da „u ovom predmetu treba u svakom slučaju poštovati odredbe Direktive 2016/680”, ali nije naveo u pogledu kojih odredbi te direktive ima dvojbe niti je obrazložio razmatranja u pogledu merituma [9].

[7] Presuda od 6. listopada 2020., La Quadrature du Net i dr. (C-511/18, C-512/18 i C-520/18, EU:C:2020:791, t. 103.; u daljnjem tekstu: presuda La Quadrature du Net)

[8] Vidjeti među ostalim presudu od 28. travnja 2016., Oniors Bio (C-233/15, EU:C:2016:305, t. 30.).

[9] Sud je smatrao da je potrebno pozvati strane da navedu „koje su, prema njihovu mišljenju, relevantne odredbe Direktive 2016/680 s obzirom na koje bi Sud, po potrebi, trebao preoblikovati tri prethodna pitanja koja mu je uputio sud koji je uputio zahtjev (četvrto od pitanja postavljenih na raspravi na koja se očekivao usmeni odgovor).

42. Sud je u više navrata utvrdio da „je nužno, kako je to određeno u članku 94. točki (c) Poslovnika, da zahtjev za prethodnu odluku sadržava prikaz razloga koji su naveli sud koji je uputio zahtjev da se zapita o tumačenju ili valjanosti određenih odredaba prava Unije kao i pojašnjenje veze koja po mišljenju tog suda postoji između tih odredaba i nacionalnog zakonodavstva primjenjivog u glavnom postupku”[10].

43. Međutim, s obzirom na navedeno, jasno je da se u ovom zahtjevu za prethodnu odluku ne poštuju zahtjevi iz članka 94. Poslovnika Suda. Iako Sud pokazuje određenu fleksibilnost u tom pogledu, suradnja sa sudom koji je uputio zahtjev mora biti uzajamna: ako se pokaže da sud koji je uputio zahtjev neopravdano ne želi surađivati i navesti dvojbe koje ima u pogledu tumačenja prava Unije koje smatra primjenjivim (u ovom je slučaju to Direktiva 2016/680), čini mi se da je logično proglasiti zahtjev za prethodnu odluku nedopuštenim[11].

44. Tomu treba pridodati da navedeni sud:

– Nije naveo koja je priroda obrade koju su policijska tijela pokušala izvršiti ni osobnih podataka koje su konkretno tražili. Čini se da najprije navodi da je riječ samo o podacima o vezi (odnosno o prometu i lokaciji), ali potom ne isključuje mogućnost da je otključavanje telefona omogućilo pristup „svim digitalnim podacima pohranjenima na mobilnom telefonu”[12] pa čak i sadržaju elektroničkih komunikacija i poruka koje su razmijenjene pomoću njega[13].

– Upućuje na oduzimanje telefona i na pristup, ili pokušaj pristupa, podacima koji su na njemu pohranjeni, kao i na njihovo naknadno „korištenje” (*Auswertung*), odnosno obradu i čitanje. Napominje da čitanje „znači potpuno nekontrolirani pristup cjelokupnoj digitalnoj komunikaciji osobe čiji se podaci obrađuju”, što omogućuje da se „rekonstruir[a] vrlo detaljnu i dubinsku sliku gotovo svih područja privatnog života”.

45. U tim okolnostima, Sud ne bi trebao *preoblikovati* pitanja suda koji je uputio zahtjev, nego zapravo *nanovo sastaviti* zahtjev za prethodnu odluku, koji se usto dijelom temelji na hipotetskim razmatranjima, a ne na utvrđenim činjenicama. I to, da ponovim, nakon što se sudu koji je uputio zahtjev ponudila mogućnost da sam dopuni ili preoblikuje svoja pitanja.

46. Stoga zagovaram da se zahtjev za prethodnu odluku proglasi nedopuštenim, kao što su to zatražile različite države članice intervenijenti.

47. Zahtjev za prethodnu odluku nedopuštenim bi trebalo proglasiti i zbog činjenice, koja je istaknuta na raspravi, da se pred sudom koji je uputio zahtjev ne vodi pravi spor u kojem je nužno tumačenje pravnih pravila prava Unije.

48. Naime, austrijska vlada (o kojoj ovise policijska tijela koja su sudjelovala u istrazi) priznaje da je postupanje tih tijela bilo nezakonito i da su njime povrijeđena prava dotičnog pojedinca. Budući da je žalitelj, u skladu s tvrdnjama iz odluke kojom se upućuje zahtjev za prethodnu odluku, pred upravnim sudom opravdano pobijao policijske mjere za koje tužena uprava smatra da su nezakonite, spor koji se vodio pred sudom koji je uputio zahtjev više ne postoji.

[10] Presuda od 6. listopada 2021., Consorzio Italian Management i Catania Multiservizi (C-561/19, EU:C:2021:799, t. 69.)

[11] Slažem se s ocjenom francuske vlade (točke 36. do 41. njezinih pisanih očitovanja).

[12] Tako se ističe u drugom prethodnom pitanju.

[13] Sud koji je uputio zahtjev tvrdi da je „u pogledu podataka o vezi moguće rekonstruirati gotovo sve kontakte prema učestalosti, vremenu i trajanju komunikacije, u pogledu komunikacije vođene SMS-om i drugim oblicima slanja poruka može se rekonstruirati i sadržaj; ujedno se obradom pohranjenih fotografija i podataka o povijesti pregledavanja dobiva vrlo intiman uvid u privatni život dotične osobe)”.

49. U svakom slučaju, za slučaj da se Sud ne slaže s mojim mišljenjem, u nastavku ću se podredno osvrnuti na probleme u pogledu merituma na kojima se temelje prethodna pitanja.

50. Međutim, smatram da je najprije potrebno isključiti mogućnost postojanja drugog razloga za nedopuštenost na koji su se pozvale neke stranke koje sudjeluju u ovom postupku [14]. Prema njihovu mišljenju, s obzirom na to da se Direktiva 2016/680 odnosi na zaštitu pojedinaca u vezi s *obradom* njihovih podataka, ona se ne primjenjuje u slučaju kao što je ovaj, u kojem nije došlo do obrade, nego do *pokušaja pristupa* podacima koje se naposljetku nije uspjelo prikupiti.

51. Komisija pak smatra da zbog korisnog učinka Direktive 2016/680 prednost ima tumačenje njezina predmeta koje nije ograničeno na obradu podataka u užem smislu, nego obuhvaća i pitanja koja su izravno povezana s obradom. Jedno od takvih pitanja bio bi i pokušaj pristupa podacima koji se nastoje obraditi [15].

52. Prema mojem mišljenju, nije potrebno proširivati granice područja primjene Direktive 2016/680 [16] jer njezina je primjena u ovom slučaju opravdana ne zato što je mobilni telefon oduzet [17], nego zbog naknadnog postupanja policijskih tijela u svrhu dobivanja određenih ispitanikovih osobnih podataka iz mobilnog telefona, radi čega ga se pokušalo otključati i omogućiti pristup njegovu sadržaju.

53. Među postupcima koji se u članku 3. točki 2. Direktive 2016/680 definiraju kao „obrada" nalazi se „stavljanj[e] [osobnih podataka] na raspolaganje na drugi način", do kojeg dolazi tijekom kaznene istrage. Smatram da policijsko tijelo, kad oduzme telefon na kojem su ti podaci pohranjeni i rukuje njime kako bi došao do njih, započinje „postupak" obrade, neovisno o tome je li ona neuspješna zbog tehničkih razloga u pogledu kriptografske sigurnosti.

54. Neuspješan pokušaj pristupa osobnim podacima pohranjenima na mobilnom telefonu tijekom kaznene istrage uređuje se Direktivom 2016/680 zbog sličnih razloga zbog kojih je Sud utvrdio da se Direktiva 2002/58 primjenjuje na (također neuspješni) *pokušaj* dobivanja sudskog odobrenja za pristup određenim podacima o osobi protiv koje se vodila istraga, koje je posjedovao pružatelj elektroničkih komunikacijskih usluga [18].

55. U tim okolnostima, da sud koji je uputio zahtjev mora odlučivati o nezakonitosti policijskog postupanja (koju je austrijska vlada, kao što sam to već istaknuo, priznala), njegova bi ocjena, i u slučaju da je mjera bila uspješna i u slučaju da je njezino izvršenje tek započelo bez uspjeha, mogla ovisiti o zakonitosti svrhe koja se željela postići tim postupanjem.

[14] Mislim konkretno na austrijsku, francusku, nizozemsku i norvešku vladu.

[15] Prema Komisijinu mišljenju, „nije važno jesu li pokušaji bili uspješni ili bezuspješni. Pojava tehničkih poteškoća zbog kojih su pokušaji pristupa bezuspješni okolnost je koju nije moguće predvidjeti i koja ne utječe na rizike u pogledu zaštite osobnih podataka".

[16] Osobito mi se nepotrebnom čini primjena članaka 27. i 28. Direktive 2016/680, što je predložila Komisija u svojim pisanim očitovanjima. „Procjena učinka na zaštitu podataka" utvrđena člankom 27. odnosi se općenito na „nek[u] vrst[u] obrade", a ne na konkretne ili posebne obrade. To proizlazi iz uvodne izjave 58. Direktive 2016/680: „[p]rocjenama učinka trebali bi se obuhvatiti relevantni sustavi i procesi postupaka obrade, ali *ne i pojedinačni slučajevi*" (moje isticanje). Komisija je na raspravi pojasnila zašto je uputila na obje odredbe: navela ih je samo kako bi istaknula da se u Direktivi 2016/680 također predviđaju situacije koje prethode obradi podataka u pravom smislu.

[17] Direktivom 2016/680 ne uređuje se oduzimanje telefona kao načina prikupljanja dokaza u okviru kaznene istrage.

[18] Presuda od 2. listopada 2018., Ministerio Fiscal (C-207/16, EU:C:2018:788)

B. Meritum

1. Prvo prethodno pitanje

56. Sud koji je uputio zahtjev želi znati čini li, u skladu s člankom 15. stavkom 1. (eventualno u vezi s člankom 5.) Direktive 2002/58, u vezi s člancima 7. i 8. Povelje, „pristup tijela javne vlasti podacima pohranjenima na mobilnim telefonima […] tako ozbiljno zadiranje u temeljna prava zajamčena navedenim člancima Povelje da se taj pristup u području sprečavanja, istrage, otkrivanja i progona kaznenih djela mora ograničiti na borbu protiv teških kaznenih djela".

57. Ako bi zahtjev za prethodnu odluku bio dopušten, prvo pitanje trebalo bi preoblikovati zbog neprimjenjivosti Direktive 2002/58 tako da bi Sud u svojem odgovoru mogao tumačiti Direktivu 2016/680.

58. U odgovoru bi trebalo redom razjasniti može li se u slučajevima kao što je ovaj govoriti o zadiranju u prava i, ako može, je li na temelju Direktive 2016/680 pristup podacima moguć samo u slučaju borbe protiv teških kaznenih djela.

59. Postupci obrade podataka po definiciju mogu narušiti pravo na poštovanje privatnog života (članak 7. Povelje) i pravo na zaštitu osobnih podataka (članak 8. Povelje). Tijela javne vlasti stoga moraju poštovati uvjete predviđene u članku 52. stavku 1. Povelje kako bi opravdala svoje zadiranje u ostvarivanje tih temeljnih prava.

60. Zadiranje u prava zajamčena člancima 7. i 8. Povelje tim je veće ako se njime: (a) nastoji pristupiti osjetljivim podacima koji su načelno pohranjeni na mobilnim telefonima, a čije bi otkrivanje moglo razotkriti određene dijelove života njihovih nositelja za koje treće osobe ne bi trebale znati; te (b) omogućava pristup sadržaju komunikacija.

61. Međutim, s općenitog stajališta i s obzirom na njezin sadržaj, Direktivu 2016/680 ne može se tumačiti na način da je obrada podataka na koju se Direktiva odnosi ograničena samo na slučajeve borbe protiv teških kaznenih djela.

62. Direktiva 2016/680 odnosi se na bilo kakav postupak obrade [19] osobnih podataka koji provode tijela nadležna za sprečavanje, istragu, otkrivanje ili progon *svih vrsta* kaznenih djela.

63. Iz načela koja se u Direktivi 2016/680 utvrđuju u pogledu obrade osobnih podataka u tu svrhu (članak 4.) ili uvjeta za zakonitost obrade (članak 8.) ne proizlazi da je obrada podataka načelno moguća jedino u slučaju teških kaznenih djela.

64. Ograničavanje na slučajeve borbe protiv teških kaznenih djela ne bi se moglo opravdati ni jednostavnim proširivanjem sudske prakse Suda u pogledu Direktive 2002/58 [20] na slučajeve kao što je ovaj.

[19] U članku 3. točki 2. Direktive 2016/680 navodi se jako širok popis tih „postupaka". Vidjeti njihov prijepis u točki 9. ovog mišljenja.

[20] Presuda La Quadrature du Net te presude od 21. prosinca 2016., Tele2 Sverige i Watson i dr. (C-203/15 i C-698/15, EU:C:2016:970; u daljnjem tekstu: presuda Tele2 Sverige i Watson); od 2. listopada 2018., Ministerio Fiscal (C-207/16, EU:C:2018:788); od 6. listopada 2020., Privacy International (C-623/17, EU:C:2020:790) i od 2. ožujka 2021., Prokuratuur (Uvjeti pristupa podacima o elektroničkim komunikacijama) (C-746/18, EU:C:2021:152; u daljnjem tekstu: presuda Prokuratuur)

65. Smatram da to nije moguće jer se, ne dovodeći u pitanje ono što navodim u nastavku, ta sudska praksa odnosi na opće i neselektivno zadržavanje osobnih podataka generičke i nedefinirane skupine, koje sustavno obavljaju pružatelji elektroničkih komunikacijskih usluga. Opseg zadiranja koje takvo zadržavanje pretpostavlja za društvo u cjelini razlog je zašto je Sud bio osobito strog prilikom njegove zabrane i predviđanja odstupanja od te zabrane.

66. To nije slučaj kad se pristup koji se želi dobiti ne odnosi na skupinu ili velike grupe stanovnika (odnosno na osobne podatke generičke i nedefinirane skupine), nego na podatke pohranjene na jednom mobilnom telefonu, i to u okviru također pojedinačnog postupka kaznene istrage, koji je posebno uređen Direktivom 2016/680.

67. Cilj Direktive 2016/680 upravo je obrada podataka koju izvršavaju tijela nadležna za sprečavanje, istragu, otkrivanje ili progon kaznenih djela. I to svih vrsta kaznenih djela, a ne samo teških.

68. Osim toga, kao što su to naglasili neki intervenijenti u prethodnom postupku, s obzirom na to da se u Direktivi 2016/680 ne navodi ništa u pogledu težine kaznenih djela, ta se direktiva može neujednačeno primjenjivati u državama članicama jer se u različitim nacionalnim pravima ocjene u pogledu težine određenog kažnjivog postupanja znatno razlikuju [21].

69. Na temelju Direktive 2016/680, ukratko, zakonitost obrade osobnih podataka koja se njome uređuje nije uvjetovana time da se obrada obavlja radi borbe protiv teških kaznenih djela.

70. To nije u suprotnosti s time da se, u skladu s načelom proporcionalnosti i u svakom slučaju zasebno, obrada podataka koju nadležna tijela nastoje obaviti u skladu s Direktivom 2016/680 mora prilagoditi s obzirom na: (a) prirodu kaznenih djela protiv kojih se provodi progon i (b) vrstu osobnih podataka koji se nastoje obraditi.

71. U tom se smislu slažem s nekim od tvrdnji njemačke vlade o ograničenju pristupa podacima s oduzetih telefona ako je na temelju njih, s obzirom na digitalni sadržaj telefona, moguće utvrditi potpuni profil ličnosti njihovih vlasnika. Prema mišljenju njemačke vlade, taj pristup treba biti ograničen na podatke koji su nužni kao dokaz u konkretnom slučaju i možda nije prikladan kad je riječ o slučajevima kao što su „lakše kazneno djelo koje se istražuje ili mala dokazna vrijednost podataka koji se nastoje prikupiti” [22].

72. U *teoriji*, Direktiva 2016/680 stoga ne podrazumijeva sustavnu nezakonitost pristupa osobnim podacima koji su pohranjeni na mobilnom telefonu u svrhu olakšavanja istrage povodom postupanja koja se mogu kvalificirati kao opće ili uobičajeno kazneno djelo. Ako je u *konkretnom* slučaju taj pristup potreban, odgovarajuće ga tijelo mora ocijeniti u svakom pojedinačnom slučaju, uzimajući u obzir njegovu nužnost i kriterij proporcionalnosti na koji sam prethodno uputio.

73. Prema mojem mišljenju, to se zaključuje iz odredbi Direktive 2016/680 kojima se utvrđuju uvjeti valjanosti obrade osobnih podataka u okviru borbe protiv teških kaznenih djela:

– Članka 4. stavka 1. točke (a); na temelju kojeg podaci trebaju biti „obrađivani zakonito”.

[21] Francuska vlada navodi primjer kaznenih djela u području posjedovanja i trgovanja drogom, koja se smatraju različito teškima u austrijskim i francuskim kaznenim pravnim pravilima. Švedska vlada iznosi slično stajalište.

[22] Pisana očitovanja njemačke vlade, t. 20.

– Članka 8. stavka 1., u kojem se ističe da obrada treba biti *nužna* i da se treba temeljiti na pravu Unije ili pravu države članice.

2. Drugo prethodno pitanje

74. Svojim drugim pitanjem sud koji je uputio zahtjev želi saznati protivi li se članku 15. stavku 1. Direktive 2002/58, u vezi s člancima 7., 8., 11. kao i člankom 52. stavkom 1. Povelje, „nacionalna odredba poput članka 18. u vezi s člankom 99. stavkom 1. [ZKP-a], prema kojoj sigurnosna tijela u okviru kaznene istrage bez odobrenja suda ili neovisnog upravnog tijela sama sebi pribavljaju sveobuhvatan i nekontroliran pristup svim digitalnim podacima pohranjenima na mobilnom telefonu".

75. Pitanje je sročeno višeznačno. Sud koji je uputio zahtjev:

– Priznaje da se člankom 110. stavkom 2. ZKP-a propisuje da je za oduzimanje imovine načelno potrebno odobrenje državnog odvjetništva. Policijsko tijelo može oduzeti imovinu bez takvog odobrenja samo u iznimnim slučajevima predviđenima u stavku 3. istog članka (o kojima ovdje, čini se, nije riječ).

– Međutim, dodaje da obrada informacija pohranjenih na mobilnim telefonima „nije jednoznačno uređena [ZKP-om]" i da bi im sigurnosna tijela mogla pristupati na vlastitu inicijativu bez prethodnog odobrenja.

76. Austrijska vlada iznosi verziju nacionalnih propisa koja se ne podudara s verzijom iz odluke kojom se upućuje zahtjev za prethodnu odluku. Konkretno, tvrdi da su u skladu s nacionalnim pravom i oduzimanje telefona (osim u hitnim slučajevima) i obrada podataka koji su u njemu pohranjeni mogući samo uz odobrenje državnog odvjetništva [23]. Ako ne postoji nalog državnog odvjetništva, policijsko korištenje podacima koji su pohranjeni na tom telefonu je nezakonito.

77. Na sudu koji je uputio zahtjev jest da utvrdi sadržaj nacionalnih propisa. U okviru postupka predviđenog člankom 267. UFEU-a Sud nije nadležan za tumačenje nacionalnog prava, nego je isključivo na sudu koji je uputio zahtjev da definira točan opseg nacionalnih zakona i drugih propisa [24].

78. Ne želim se upuštati u raspravu o tumačenju austrijskog prava, ali mi je samo iz odredbi koje navodi sud koji je uputio zahtjev (članak 18. ZKP-a u vezi s njegovim člankom 99. stavkom 1.) teško doći do zaključka koji je on izveo. Međutim, ponavljam da o tom pitanju može odlučivati samo sud koji je uputio zahtjev.

79. U svakom slučaju, sud koji je uputio zahtjev smatra da se na slučaj kao što je ovaj može primijeniti sudska praksa iz presude Prokuratuur [25] u pogledu prethodnog nadzora koji sud ili neovisno tijelo obavlja nad pristupom zadržanim podacima.

[23] Točka 19. pisanih očitovanja austrijske vlade. Upućuje se na odluku Oberster Gerichtshofa (Vrhovni sud, Austrija) od 13. listopada 2020. (predmet br. 11 Os 56/20z) u kojoj se obrada podataka s mobilnog telefona koju je izvršila kriminalistička policija, a koju nije odobrilo državno odvjetništvo, proglašava nezakonitom jer se njome povređuju subjektivna prava dotičnog pojedinca.

[24] Vidjeti među ostalim presudu od 28. travnja 2022., SeGEC i dr. (C-277/21, EU:C:2022:318, t. 21.).

[25] Presuda Prokuratuur, t. 51.: „bitno je da se prije pristupa nadležnih nacionalnih tijela zadržanim podacima provede nadzor suda ili neovisnog upravnog tijela i da odluka tog suda ili tijela bude donesena nakon obrazloženog zahtjeva tih tijela podnesenog osobito u okviru postupaka sprečavanja, otkrivanja ili progona kaznenih djela".

80. S druge strane, nizozemska vlada smatra da tu sudsku praksu treba tumačiti u kontekstu nacionalnog propisa kojim se nadležnim tijelima omogućavao *opći* pristup *svim* zadržanim podacima o prometu i lokaciji. To bi objasnilo zahtjev za prethodno odobrenje suda koje se pak ne bi moglo opravdati u slučaju pristupa podacima s jednog mobilnog telefona.

81. Norveška vlada u istom smislu tvrdi da se među mnogim jamstvima koja su utvrđena u Direktivi 2016/680 [26] ne navodi izričito zahtjev za prethodno odobrenje koje izdaje pravosudno tijelo ili neovisno upravno tijelo.

82. Komisija, koja polazi od pretpostavke da odredbe Direktive 2016/680 treba tumačiti u vezi s Poveljom, tvrdi da obveza koja se državama članicama propisuje u članku 8. stavku 1. te direktive (uvjeti za zakonitu obradu) znači da je nužno poštovati temeljna prava zajamčena člancima 7. i 8. Povelje.

83. Slažem se s Komisijom u pogledu toga da su nacionalni zakonodavci, u skladu s tim odredbama Povelje, obvezni utvrditi nužna pravila kako bi se zajamčilo da je pristup podacima u svakom slučaju opravdan i ograničen samo na ono što je strogo nužno i proporcionalno.

84. Međutim, nema razloga da se takva nacionalna pravila konkretno odnose na pristup osobnim podacima koji su, kao što je to ovdje slučaj, pohranjeni na mobilnom telefonu, nego to mogu biti pravila koja su u nacionalnom pravu općenito utvrđena u području prikupljanja dokaza.

85. U tom sam pogledu već naveo točku 103. presude La Quadrature du Net u kojoj je riječ o mjerama koje provode države članice i koje odstupaju od povjerljivosti elektroničkih komunikacija, a da ne određuju obveze obrade pružateljima usluga takvih komunikacija [27].

86. Stoga nema potrebe da se iz Direktive 2016/680 izvode *posebna* postupovna pravila u pogledu jamstva zakonitosti pristupa podacima pohranjenim na mobilnom telefonu [28], nego se primjenjuju nacionalna pravna pravila kojima se uređuje izvršavanje ovlasti pretrage i oduzimanja u okviru kaznenih istraga [29].

87. Osim toga, upućivanje na odredbe nacionalnog prava kako bi se osigurala zakonitost pristupa na temelju Direktive 2016/680 u skladu je sa sudskom praksom ESLJP-a. ESLJP je upravo u jednom slučaju koji se odnosio na Republiku Austriju u pogledu članka 8. EKLJP-a (pravo na poštovanje privatnog i obiteljskog života, doma i komuniciranja) utvrdio da se austrijsko zakonodavstvo o oduzimanju imovine i konkretno dokumenata primjenjuje na pretragu i prikupljanje podataka pohranjenih na računalnim nosačima [30].

[26] Osim jamstava utvrđenih u člancima 4. i 8., riječ je o jamstvima iz poglavlja III. („Prava ispitanika”), IV. („Voditelj obrade i izvršitelj obrade”), VI. („Neovisna nadzorna tijela”) i VIII. („Sudski pravni lijekovi, odgovornost i sankcije”).

[27] Vidjeti točku 36. ovog mišljenja.

[28] O težini takvog poduhvata svjedoče točke 34. do 39. Komisijinih pisanih očitovanja u kojima nastoji dati svoj doprinos definiranju jasnih i preciznih pravila za utvrđivanje ograničenja i prikladnih jamstava u pogledu pristupa podacima s mobilnog telefona.

[29] Ta pravna pravila, kao što na to podsjećaju primjerice danska i irska vlada, nisu obuhvaćena područjem primjene prava Unije, ali mogu poslužiti za ispunjavanje određenog zahtjeva koji proizlazi iz navedenog prava.

[30] Vidjeti presudu ESLJP-a od 16. listopada 2007., Wieser i Bicos Beteiligungen protiv Austrije (CE:ECHR:2007:1016JUD007433601, t. 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. Ako policijska tijela, kao što to tvrdi austrijska vlada uz pozivanje na sudsku praksu Oberster Gerichtshofa (Vrhovni sud), nisu ovlaštena pristupiti podacima pohranjenima na nekom mobilnom telefonu bez odobrenja državnog odvjetništva, drugo prethodno pitanje postaje velikim dijelom besmisleno.

89. U svakom slučaju, u odgovoru na to pitanje ne može se zanemariti to da je na temelju pristupa osobnim podacima s oduzetog telefona moguće „rekonstruirati vrlo detaljnu i dubinsku sliku gotovo svih područja privatnog života" ispitanika [31]. Ako je to slučaj, policijska tijela ne bi mogla postupati bez prethodnog odobrenja na koje se upućuje u presudi Prokuratuur.

90. Na prvi se pogled čini da ta tvrdnja nije u skladu s neprimjenom Direktive 2002/58 (koja se tumači u presudi Prokuratuur) u ovom slučaju, za što sam se prethodno zalagao. Međutim, smatram da *ratio* te presude dovodi do istog rješenja.

91. Iako se podacima (metapodacima) u sporu koji je doveo do presude Prokuratuur pristupilo tako što su oni prikupljeni od pružatelja elektroničkih komunikacijskih usluga, i u tom je slučaju, kao ovdje, bila riječ o pojedinačnoj kaznenoj istrazi, koja se vodila protiv određene osobe. Nastojali su se prikupiti „poda[ci] u vezi s više telefonskih brojeva […] i […] različitim IMEI kodovima" [32].

92. U presudi Prokuratuur mogu se, prema mojem mišljenju, razlikovati dvije razine: (a) razina na kojoj se dovode u pitanje opći propisi države članice o općem i neselektivnom zadržavanju te naknadnom pristupu podacima koje posjeduju pružatelji usluga; te (b) razina prethodnog nadzora nad pristupom tim metapodacima u konkretnom slučaju ako je na temelju njih moguće rekonstruirati detaljan profil privatnog života dotične osobe.

93. Okolnost da u predmetu o kojem je ovdje riječ podatke koji otkrivaju privatni život ne posjeduju pružatelji usluga i da se oni prikupljaju (ili nastoje prikupiti) s jednog oduzetog telefona čini mi se manje važnom u odnosu na *ratio* zahtjeva prethodnog nadzora na koji se upućuje u presudi Prokuratuur.

94. Taj se prethodni nadzor naposljetku temelji na zaštiti koja je zajamčena člancima 7. i 8. Povelje. Tijelo koje ga provodi mora „mo[ći] osigurati pravednu ravnotežu između, s jedne strane, interesa povezanih s potrebama istrage u okviru borbe protiv kriminaliteta i, s druge strane, temeljnih prava na poštovanje privatnog života i zaštite osobnih podataka osoba čiji su podaci obuhvaćeni pristupom" [33].

3. Treće prethodno pitanje

95. Trećim prethodnim pitanjem sud koji je uputio zahtjev želi saznati protivi li se članku 47. Povelje (eventualno u vezi s njezinim člancima 41. i 52.) zakonodavstvo kao što je austrijsko [34] kojim se „omogućava digitalna obrada mobilnog telefona, a da se osoba čiji se podaci obrađuju o tome prethodno ili barem nakon određivanja mjere ne obavijesti".

[31] Vidjeti tvrdnje suda koji je uputio zahtjev koje se navode u točki 44. ovog mišljenja.

[32] Presuda Prokuratuur, t. 17.

[33] Presuda Prokuratuur, t. 52.

[34] Ponovno se upućuje na članak 18. ZKP-a u vezi s njegovim člankom 99.

96. Smatram da bi tako sročeno pitanje moglo biti nevažno za rješavanje spora jer je ispitanik mogao ostvariti pravo zajamčeno člankom 47. Povelje tako da od suda koji je uputio zahtjev zatraži da se policijsko postupanje s oduzetim telefonom, uključujući naknadni (bezuspješni) pokušaj korištenja podataka koji su u njemu pohranjeni, proglasi ništavim.

97. Kad je riječ o tim dvama trenucima tijekom policijskog postupanja, treba razlikovati:

– Kad je riječ o samom oduzimanju telefona, informacije koje se navode u spisu pokazuju da je ispitanik znao za oduzimanje i da je policijskim tijelima odbio otkriti lozinku za otključavanje kad su mu ga oduzela.

– Kad je riječ o pokušaju obrade podataka, čini se da sve upućuje na to da voditelj obrade o tome nije obavijestio ispitanika, iako austrijska vlada tvrdi da je ispitanik bio upoznat s izvješćem u kojem se navodi kako je kriminalistička policija postupila s telefonom [35].

98. Stoga u pogledu korištenja podacima i upoznatosti ispitanika s njim i dalje postoje određene nejasnoće koje je, kao što sam to već istaknuo, trebao razjasniti sud koji je uputio zahtjev u svojoj odluci kojom se upućuje zahtjev za prethodnu odluku, a zbog tih nejasnoća nije moguće pružiti koristan odgovor na treće prethodno pitanje.

99. U svakom slučaju, iznijet ću svoje mišljenje o tom pitanju za slučaj da Sud ne ocijeni da je ono nedopušteno. U tom slučaju, budući da Direktiva 2002/58 nije primjenjiva, pitanje bi trebalo preoblikovati s obzirom na Direktivu 2016/680, čiji članci 13., 15. i 54. pružaju smjernice za odgovor na njega.

100. U skladu s Direktivom 2016/680, ispitaniku na raspolaganje treba staviti informacije o obradi njegovih podataka koje su potrebne, među ostalim, za: (a) podnošenje pritužbe nadzornom tijelu (članak 13. stavak 1. točka (d)) te (b) ostvarivanje prava na djelotvornu sudsku zaštitu zbog povrede prava koja su mu zajamčena Direktivom 2016/680, ne dovodeći u pitanje dostupne upravne ili izvansudske pravne lijekove (članak 54.).

101. Ne treba, međutim, zaboraviti da se i člankom 13. stavkom 3. i člankom 15. stavkom 1. Direktive 2016/680 državama članicama dopušta da donesu zakonodavne mjere:

– za odgađanje, ograničavanje ili uskraćivanje pružanja informacija ispitaniku na temelju članka 13. stavka 2.;

– kojima se ispitaniku u cijelosti ili djelomično ograničava pravo na pristup obrađenim podacima u onoj mjeri i u onom trajanju u kojem takvo ograničavanje čini neophodnu i proporcionalnu mjeru kako bi se, među ostalim, izbjeglo ometanje službenih ili pravnih istraga ili postupaka ili izbjeglo dovođenje u pitanje istrage kaznenih djela [36].

102. U svakom slučaju, zakonitost obrade podataka ne ovisi o tome jesu li nadležna tijela ispunila (naknadne) obveze koje im se propisuju člankom 13. Direktive 2016/680, nego o zakonitosti svrhe kojom je obrada opravdana, odnosno o tome jesu li ta upravna tijela bila ovlaštena pokrenuti obradu osobnih podataka.

[35] Točka 37. njezinih pisanih očitovanja

[36] Vidjeti u tom smislu presudu Tele2 Sverige i Watson, t. 121. Sudska praksa u pogledu Direktive 2002/58 iz te presude može se primijeniti na Direktivu 2016/680 u kontekstu jamstva sudske zaštite prava koja imaju nositelji podataka koji se obrađuju.

103. S tog je gledišta pitanje je li ispitanik bio obaviješten o pokušajima pristupa podacima pohranjenima na telefonu koji mu je oduzet nešto što samo po sebi nema veze sa zakonitošću policijskog postupanja zbog materijalnih razloga. Postupanje voditelja obrade koje je eventualno protivno obvezama koje on ima na temelju članka 13. Direktive 2016/680 moglo bi imati druge posljedice, ali ponavljam da ono samo po sebi ne utječe na zakonitost ili nezakonitost te obrade.

104. Na sudu koji je uputio zahtjev jest da utvrdi može li dotični pojedinac na temelju nacionalnih propisa učinkovito ostvariti svoja prava.

V. Zaključak

105. S obzirom na prethodno navedeno, predlažem Sudu da zahtjev za prethodnu odluku koji je uputio Landesverwaltungsgericht Tirol (Zemaljski upravni sud u Tirolu, Austrija) proglasi nedopuštenim.

Podredno, predlažem da se na pitanja koja taj zahtjev sadržava odgovori na sljedeći način:

„1. Članak 4. stavak 1. točku (a) i članak 8. stavak 1. Direktive (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP, u vezi s člancima 7., 8. i 52. Povelje Europske unije o temeljnim pravima,

treba tumačiti na način da

pristup osobnim podacima pohranjenima na mobilnom telefonu koji imaju tijela javne vlasti u okviru kaznene istrage kako bi te podatke obradila nije ograničen na slučajeve borbe protiv teških kaznenih djela.

Navedeni pristup mora biti opravdan u svakom pojedinačnom slučaju i ograničen samo na ono što je strogo nužno i proporcionalno, ovisno o prirodi kaznenih djela protiv kojih se provodi progon i osobnih podataka kojima se želi pristupiti.

Policijska tijela ne mogu u okviru kaznene istrage samostalno i bez prethodnog odobrenja suda pribaviti sveobuhvatan i nekontroliran pristup svim podacima pohranjenima na mobilnom telefonu ako je na temelju njih moguće dobiti preciznu sliku o privatnom životu dotične osobe.

2. Članke 13., 15. i 54. Direktive 2016/680, u vezi s člancima 47. i 52. Povelje,

treba tumačiti na način da

ne dovodeći u pitanje ograničenja dopuštena člankom 15. stavkom 1. Direktive 2016/680 ni druge dostupne upravne ili izvansudske pravne lijekove, vlasnika mobilnog telefona treba obavijestiti o obradi osobnih podataka pohranjenih na tom telefonu koju su izvršila odgovarajuća tijela, i to u trenutku i na način koji je prikladan kako bi se osiguralo djelotvorno ostvarivanje prava na podnošenje pravnog lijeka protiv eventualne povrede prava zajamčenih Direktivom 2016/680”.