Kohtulahendite kogumik

KOHTUJURISTI ETTEPANEK
MANUEL CAMPOS SÁNCHEZ-BORDONA
esitatud 20. aprillil 2023 [1]

Kohtuasi C-548/21

C. G.

versus

Bezirkshauptmannschaft Landeck

(eelotsusetaotlus, mille on esitanud Landesverwaltungsgericht Tirol (Tirooli liidumaa halduskohus, Austria))

Eelotsusemenetlus – Telekommunikatsioon – Isikuandmete kaitse – Direktiiv (EL) 2016/680 – Kriminaalmenetlus – Ametiasutuste katse tutvuda mobiiltelefonis salvestatud andmetega ilma kohtu loata või sõltumatu haldusasutuse loata

1. Eelotsusetaotlus käsitleb sisuliselt tingimusi, millele peavad vastama politseiasutused selleks, et tutvuda selle isiku mobiiltelefonis salvestatud andmetega, kelle suhtes on algatatud kriminaalmenetlus.

2. Nagu ma selgitan, on eelotsusetaotluse vastuvõetavuse osas märkimisväärseid puudusi. Kui Euroopa Kohus otsustab siiski küsimust sisuliselt arutada, tuleb tal teha otsus direktiivi 2002/58/EÜ [2] ja direktiivi (EL) 2016/680 [3] vastavate kohaldamisalade kohta.

[1] Algkeel: hispaania.

[2] Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT 2002, L 201, lk 37; ELT eriväljaanne 13/29, lk 514).

[3] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK (ELT 2016, L 119, lk 89).

I. Õiguslik raamistik

A. Liidu õigus

1. Määrus (EL) 2016/679[4]

3. Artikli 2 („Sisuline kohaldamisala“) lõikes 2 on sätestatud:

„Käesolevat määrust ei kohaldata, kui:

[…]

d) isikuandmeid töötlevad pädevad asutused süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise ja kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil.“

2. Direktiiv 2016/680

4. Põhjenduses 2 on kinnitatud:

„Isikuandmete töötlemisele kohaldatavad füüsiliste isikute kaitse põhimõtted ja normid peaks […] austama nende põhiõigusi ja -vabadusi, eelkõige õigust isikuandmete kaitsele. Käesoleva direktiivi eesmärk on aidata kaasa vabadusel, turvalisusel ja õigusel rajaneva ala lõplikule väljakujundamisele.“

5. Põhjenduses 46 on märgitud:

„Andmesubjekti õiguste piiramine peaks olema kooskõlas harta ning Euroopa inimõiguste konventsiooniga, nagu neid tõlgendavad Euroopa Kohus ja Euroopa Inimõiguste Kohus[5] oma praktikas, ning eelkõige tuleb seejuures austada nende õiguste ja vabaduste põhiolemust.“

6. Põhjenduses 49 on märgitud:

„Kui isikuandmeid töödeldakse kriminaaluurimise ja kriminaalkohtumenetluse käigus, peaks liikmesriikidel olema võimalik ette näha, et teabe saamise, isikuandmetega tutvumise ja nende parandamise, kustutamise ja nende töötlemise piiramise õigust teostatakse vastavalt kohtumenetlust käsitlevatele liikmesriigi õigusnormidele.“

7. Artiklis 1 („Reguleerimisese ja eesmärgid“) on sätestatud:

„1. Käesolevas direktiivis sätestatakse õigusnormid, mis käsitlevad füüsiliste isikute kaitset isikuandmete töötlemisel pädevate asutuste poolt süütegude tõkestamiseks, uurimiseks, avastamiseks, nende eest vastutusele võtmiseks või kriminaalkaristuste täitmisele pööramiseks, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmiseks ja nende ennetamiseks.

[4] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT 2016, L 119, lk 1). Edaspidi „isikuandmete kaitse üldmäärus“.

[5] Edaspidi „EIK“.

2. Kooskõlas käesoleva direktiiviga liikmesriigid:

a) kaitsevad füüsiliste isikute põhiõigusi ja -vabadusi, eriti nende õigust isikuandmete kaitsele, ning

[…]

3. Käesolev direktiiv ei takista liikmesriike kehtestamast isikuandmete töötlemisel pädevate asutuste poolt andmesubjekti õiguste ja vabaduste kaitseks rangemaid kaitsemeetmeid kui käesolevas direktiivis.“

8. Artikli 2 „Kohaldamisala“ lõikes 1 on sätestatud:

„Käesolevat direktiivi kohaldatakse isikuandmete töötlemisele pädevate asutuste poolt artikli 1 lõikes 1 sätestatud eesmärkidel.“

9. Artiklis 3 („Mõisted“) on sätestatud:

„Käesolevas direktiivis kasutatakse järgmisi mõisteid:

[…]

2) „isikuandmete töötlemine“ – isikuandmete või nende kogumitega tehtav automatiseeritud või automatiseerimata toiming või toimingute kogum, nagu kogumine, dokumenteerimine, korrastamine, struktureerimine, säilitamine, kohandamine ja muutmine, päringute tegemine, lugemine, kasutamine, edastamise, levitamise või muul moel kättesaadavaks tegemise teel avalikustamine, ühitamine või ühendamine, piiramine, kustutamine või hävitamine;

[…]

7) „pädev asutus“ –

   a) avaliku sektori asutus, kes on pädev süütegusid tõkestama, uurima, avastama või nende eest vastutusele võtma või kriminaalkaristusi täitmisele pöörama, sealhulgas kaitsma avalikku julgeolekut ähvardavate ohtude eest ja neid ohte ennetama, või

[…]“.

10. Artiklis 4 („Isikuandmete töötlemise põhimõtted“) on lõikes 1 ette nähtud:

„Liikmesriigid näevad ette järgmist:

a) isikuandmeid töödeldakse seaduslikult ja õiglaselt;

b) isikuandmeid kogutakse täpselt ja selgelt kindlaksmääratud ning õiguspärastel eesmärkidel ning neid ei töödelda viisil, mis on nende eesmärkidega vastuolus;

c) isikuandmed on piisavad ja asjakohased ega ole liiased nende töötlemise eesmärkide suhtes;

[…]

e) isikuandmeid säilitatakse kujul, mis võimaldab andmesubjekte tuvastada üksnes seni, kuni see on vajalik selle eesmärgi täitmiseks, milleks isikuandmeid töödeldakse;

f) isikuandmeid töödeldakse viisil, mis tagab isikuandmete asjakohase turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kadumise, hävimise või kahjustumise eest, kasutades asjakohaseid tehnilisi või korralduslikke meetmeid.“

11. Artiklis 8 („Isikuandmete töötlemise seaduslikkus“) on märgitud:

„1. Liikmesriigid näevad ette, et isikuandmete töötlemine on seaduslik ainult sel juhul ja niivõrd, kui see on vajalik pädeva asutuse poolt artikli 1 lõikes 1 sätestatud eesmärkide kohase ülesande täitmiseks ning see põhineb liidu või liikmesriigi õigusel.

2. Käesoleva direktiivi kohaldamisalasse kuuluvat isikuandmete töötlemist reguleerivas liikmesriigi õiguses täpsustatakse vähemalt isikuandmete töötlemise üldised eesmärgid, töödeldavad isikuandmed ja nende töötlemise konkreetsed eesmärgid.“

12. Artikkel 13 („Andmesubjektile kättesaadavaks tehtud või antud teave“) näeb ette:

„1. Liikmesriigid näevad ette, et vastutav töötleja teeb andmesubjektile kättesaadavaks vähemalt järgmise teabe:

[…]

d) õigus esitada kaebus järelevalveasutusele ning järelevalveasutuse kontaktandmed;

[…]

3. Liikmesriigid võivad asjaomase füüsilise isiku põhiõigusi ja õigustatud huve nõuetekohaselt arvestades võtta seadusandlikke meetmeid, millega nähakse ette andmesubjektile lõike 2 kohaselt esitatava teabe hilisem või piiratud esitamine või esitamata jätmine sellises ulatuses ja seni, kuni selline meede on demokraatlikus ühiskonnas vajalik ja proportsionaalne:

a) ametlike või õiguslike päringute, uurimiste või menetluste takistamise vältimiseks;

b) süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise kahjustamise vältimiseks;

c) avaliku julgeoleku kaitseks;

d) riigi julgeoleku kaitseks;

e) teiste isikute õiguste ja vabaduste kaitseks.

[…]“.

13. Artikli 15 („Isikuandmetega tutvumise õiguse piiramine“) lõikes 1 on sätestatud:

„Liikmesriigid võivad asjaomase füüsilise isiku põhiõigusi ja õigustatud huve nõuetekohaselt arvestades võtta seadusandlikke meetmeid, millega nähakse ette andmesubjekti isikuandmetega tutvumise õiguse täielik või osaline piiramine sellises ulatuses ja seni, kuni selline piiramine on demokraatlikus ühiskonnas vajalik ja proportsionaalne meede

a) ametlike või õiguslike päringute, uurimiste või menetluste takistamise vältimiseks;

b) süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise kahjustamise vältimiseks;

c) avaliku julgeoleku kaitseks;

d) riigi julgeoleku kaitseks;

e) teiste isikute õiguste ja vabaduste kaitseks.“

14. Artiklis 27 („Andmekaitsealane mõjuhinnang“) on sätestatud:

„1. Kui teatavat tüüpi isikuandmete töötlemise, eelkõige uut tehnoloogiat kasutava isikuandmete töötlemise tulemusena ning töötlemise laadi, ulatust, konteksti ja eesmärke arvesse võttes tekib füüsiliste isikute õigustele ja vabadustele tõenäoliselt suur oht, näevad liikmesriigid ette, et vastutav töötleja hindab enne isikuandmete töötlemist kavandatavate isikuandmete töötlemise toimingute mõju isikuandmete kaitsele.

2. Lõikes 1 osutatud hindamine sisaldab vähemalt kavandatud isikuandmete töötlemise toimingute üldkirjeldust, ohuhinnangut seoses andmesubjektide õiguste ja vabadustega, kõnealuste ohtude käsitlemiseks kavandatud meetmeid, kaitsemeetmeid, turvameetmeid ja mehhanisme, mis tagavad isikuandmete kaitse ja tõendavad kooskõla käesoleva direktiiviga, võttes arvesse andmesubjektide ja teiste asjaomaste isikute õigusi ja õigustatud huve.“

15. Artikkel 28 („Eelnev konsulteerimine järelevalveasutusega“) sätestab:

„1. Liikmesriigid näevad ette, et vastutav töötleja või volitatud töötleja konsulteerib järelevalveasutusega enne, kui ta hakkab töötlema isikuandmeid, mis kantakse uude loodavasse andmete kogumisse, kui:

a) artiklis 27 sätestatud andmekaitsealasest mõjuhinnangust nähtub, et isikuandmete töötlemise tulemusena tekiks vastutava töötleja poolt ohu leevendamiseks võetavate meetmete puudumise korral suur oht, või

b) isikuandmete töötlemise laadiga, eelkõige kui kasutatakse uusi tehnoloogiaid, mehhanisme või menetlusi, kaasneb suur oht andmesubjekti õigustele ja vabadustele.

[…]“.

16. Artiklis 54 („Õigus tõhusale õiguskaitsevahendile vastutava töötleja või volitatud töötleja vastu“) on ette nähtud:

„Ilma et see piiraks kättesaadavate halduslike kaitsevahendite või kohtuväliste heastamisvahendite kasutamist, sealhulgas artikli 52 kohast õigust esitada kaebus järelevalveasutusele, näevad liikmesriigid ette, et andmesubjektil, kes leiab, et käesoleva direktiivi sätteid rikkuva isikuandmete töötlemise tulemusena on rikutud kõnealustest sätetest talle tulenevaid õigusi, on õigus kasutada tõhusat õiguskaitsevahendit.“

B. Liikmesriigi õigus

17. Austria kriminaalmenetluse seadustiku (Strafprozessordnung)[6] §-s 18 on kriminaalpolitseile määratud ülesanded kriminaalõigusemõistmise teenistuses (lõige 1). Kriminaalpolitsei juurdluse eest vastutavad julgeolekuasutused (lõige 2). Avaliku julgeoleku teenistuse organid tagavad kriminaalpolitsei täitevteenistuse, mis seisneb süütegude uurimises ja nende eest vastutusele võtmises (lõige 3).

18. StPO § 99 kohaselt viib kriminaalpolitsei uurimisi läbi omal algatusel või kaebuse alusel ning peab seejuures täitma prokuratuuri ja kohtute korraldusi (lõige 1). Kui uurimismeetme võtmiseks on vaja prokuratuuri korraldust, võib kriminaalpolitsei vahetu ohu korral kasutada vastavat õigust ka ilma sellise korralduseta. Sellisel juhul peab ta viivitamatult luba taotlema (lõige 2).

19. StPO § 111 lõikes 2 on sätestatud, et kui andmekandjatele salvestatud teavet tuleb koguda, on iga isik kohustatud võimaldama juurdepääsu sellele teabele ning nõudmisel andma üle või võimaldama teha elektroonilise andmekandja üldkasutatavas failivormingus. Lisaks peab ta võimaldama teha andmekandjatele salvestatud andmetest varukoopiat.

II. Faktilised asjaolud, kohtuvaidlus ja eelotsuse küsimused

20. C. G. on Saksa kodanik, kes töötab ja elab Austrias.

21. Innsbrucki (Austria) tolliameti ametnikud vaatasid 23. veebruaril 2021 narkootiliste ainete kontrolli käigus läbi C. G-le saadetud paki, mis sisaldas 85 grammi kanepit.

22. Kaks politseinikku esitasid 6. märtsil 2021 C. G-le küsimusi paki saatja kohta ja otsisid läbi tema elukoha. Läbiotsimise käigus konfiskeerisid nad tema mobiiltelefoni (milles olid SIM-kaart ja SD-kaart) ning andsid talle konfiskeerimisprotokolli.

23. Kui C. G-lt nõuti, et ta võimaldaks juurdepääsu mobiiltelefoni ühendusandmetele, siis ta keeldus, samuti keeldus ta avaldamast telefoni sisselogimise turvakoodi.

24. Landecki (Austria) politseiametil ei õnnestunud mobiiltelefoni lukustust avada. See saadeti Viini (Austria) föderaalsesse kriminaalpolitseiametisse (Bundeskriminalamt), kus püüti telefoni lukustust uuesti avada ja selles salvestatud andmeid vaadata, kuid see ei õnnestunud.

[6] Kriminaalmenetluse seadustik. Edaspidi „StPO“. *BGBl* nr 631/1975, versioonis, mida kohaldati asjaolude asetleidmise ajal (*BGBl I* nr 243/2021).

25. Nende meetmete jaoks ei olnud sel ajal, kui politsei need võttis, prokuratuuri korraldust ega kohtuotsust.

26. C. G. esitas 31. märtsil 2021 Landesverwaltungsgericht Tirolile (Tirooli liidumaa halduskohus, Austria) kaebuse tema suhtes rakendatud sunnimeetme peale, vaidlustades oma mobiiltelefoni konfiskeerimise. Telefon tagastati talle 20. aprillil 2021.

27. C. G-d ei teavitatud mobiiltelefoni sisu analüüsimise katsetest; ta sai sellest teada seetõttu, et politseiametnik, kes telefoni konfiskeeris ja alustas seejärel digitaalset analüüsi, kuulati üle tunnistajana, kellel oli kohustus rääkida tõtt. Neid katseid ei dokumenteeritud ka kriminaalpolitsei toimikus.

28. Nendel asjaoludel esitas Landesverwaltungsgericht Tirol (Tirooli liidumaa halduskohus) Euroopa Kohtule järgmised eelotsuse küsimused:

„1. Kas direktiivi 2002/58, mida on muudetud direktiiviga 2009/136/EÜ, artikli 15 lõiget 1 (vajaduse korral koostoimes artikliga 5) tuleb […] harta artikleid 7 ja 8 arvesse võttes tõlgendada nii, et avaliku võimu juurdepääs mobiiltelefonis säilitatavatele andmetele kujutab endast harta viidatud artiklitega tagatud põhiõiguste riivet, mis on nii raske, et sellist juurdepääsu tuleks süütegude ennetamisel, uurimisel, avastamisel ja menetlemisel piirata võitlusega raske kuritegevuse vastu?

2. Kas direktiivi 2002/58, mida on muudetud direktiiviga 2009/136, artikli 15 lõiget 1 tuleb harta artikleid 7, 8 ja 11 ning artikli 52 lõiget 1 arvesse võttes tõlgendada nii, et sellega on vastuolus sellised riigisisesed õigusnormid nagu [StPO] § 18 koostoimes § 99 lõikega 1, mille kohaselt on julgeolekuasutustel kriminaaluurimise käigus ilma kohtu või sõltumatu haldusasutuse loata õigus ise saada täielik ja kontrollimatu juurdepääs kõigile mobiiltelefonis säilitatavatele digitaalsetele andmetele?

3. Kas harta artiklit 47, vajaduse korral koostoimes artiklitega 41 ja 52, tuleb poolte võrdsuse ja tõhusa õiguskaitsevahendi seisukohast mõista nii, et sellega on vastuolus selline liikmesriigi õigusnorm nagu [StPO] § 18 koostoimes § 99 lõikega 1, mis võimaldab mobiiltelefoni andmete digitaalset analüüsimist ilma, et asjaomast isikut teavitataks sellest enne või vähemalt pärast meetme võtmist?“

III. Menetlus Euroopa Kohtus

29. Eelotsusetaotlus registreeriti Euroopa Kohtus 6. septembril 2021.

30. Euroopa Kohus palus 20. oktoobril 2021 eelotsusetaotluse esitanud kohtul selgitada, kas direktiiv 2016/680 võib olla käesoleval juhul asjakohane.

31. Eelotsusetaotluse esitanud kohus vastas 11. novembril 2021, et põhikohtuasjas tuleb direktiivi 2016/680 kohaldada.

32. Kirjalikud seisukohad on esitanud Saksamaa, Austria, Küprose, Taani, Eesti, Prantsuse, Ungari, Iiri, Madalmaade, Norra, Poola ja Rootsi valitsus ning Euroopa Komisjon.

33. 16. jaanuaril 2023 toimunud kohtuistungil osalesid need, kes olid esitanud kirjalikud seisukohad, välja arvatud Saksamaa, Ungari ja Poola valitsus, ning lisaks Soome valitsus. Euroopa Kohus palus neil kõigil keskenduda oma argumentides direktiivile 2016/680 ja vastata suuliselt teatud küsimustele selle direktiivi kohta.

IV. Analüüs

A. Vastuvõetamatus

34. Eelotsusetaotluse esitanud kohus esitas alguses oma küsimused ainult direktiivi 2002/58 tõlgendamise kohta. Peaaegu kõik menetlusse astujad on siiski ühel meelel selles, et see direktiiv ei ole selles kohtuasjas kohaldatav ja et selle tõlgendamine ei ole järelikult kohtuvaidluse lahendamiseks vajalik.

35. Direktiivi 2002/58 artikli 3 kohaselt reguleerib see direktiiv „isikuandmete töötlemis[t], mis toimub seoses üldkasutatavate elektrooniliste sideteenuste osutamisega [liidu] üldkasutatavates sidevõrkudes, sealhulgas andmete kogumist ja tuvastusseadmeid toetavates üldkasutatavates sidevõrkudes“.

36. Euroopa Kohus on tuvastanud, et „kui liikmesriigid rakendavad elektroonilise side konfidentsiaalsusest kõrvale kalduvaid meetmeid otse, panemata sellise side teenuste osutajatele töötlemiskohustust, ei reguleeri asjaomaste isikuandmete kaitset mitte direktiiv 2002/58, vaid üksnes liikmesriigi õigus, kui [direktiivi 2016/680] kohaldamisest ei tulene teisiti“ [7].

37. Käesolevas asjas püüdis politsei andmeid kätte saada otseselt kriminaaluurimise raames. Elektroonilise side teenuste osutajad, kellel ei palutud isikuandmeid edastada, sellesse ei sekkunud. Direktiiv 2002/58 siin seega kohaldatav ei ole.

38. Seda olukorda reguleeriv liidu õigusnorm on direktiiv 2016/680, mille artikli 2 lõike 1 kohaselt kohaldatakse seda direktiivi isikuandmete töötlemise suhtes pädevate asutuste poolt „süütegude […] uurimiseks“.

39. Sellest piisab, et järeldada, et eelotsusetaotlus, nagu eelotsusetaotluse esitanud kohus on selle sõnastanud, on vastuvõetamatu, kuna liidu õigusnorm, mille tõlgendamist ta taotles, ei ole käesolevas asjas kohaldatav.

40. On siiski tõsi, et ELTL artikliga 267 on Euroopa Kohtul lubatud talle esitatud küsimused ümber sõnastada või märkida, et on muid liidu õigusnorme, mis võivad olla asjakohased, et anda liikmesriigi kohtule tarvilik vastus. [8]

[7] Euroopa Kohtu 6. oktoobri 2020. aasta kohtuotsus La Quadrature du Net jt (C-511/18, C-512/18 ja C-520/18, EU:C:2020:791; edaspidi „kohtuotsus La Quadrature du Net“, punkt 103).

[8] Muu hulgas 28. aprilli 2016. aasta kohtuotsus Oniors Bio (C-233/15, EU:C:2016:305, punkt 30).

41. Euroopa Kohus palus eelotsusetaotluse esitanud kohtul avaldada seisukoht direktiivi 2016/680 võimaliku mõju suhtes. Seega andis ta sellele kohtule võimaluse ise oma küsimusi täiendada või ümber sõnastada. Selle asemel teatas eelotsusetaotluse esitanud kohus üksnes, et „käesolevas asjas tuleb igal juhul järgida direktiivi 2016/680 sätteid“, nimetamata siiski, milliste selle sätete suhtes tal on kahtlusi, ja arendamata pikemalt muid sisulisi kaalutlusi.[9]

42. Euroopa Kohus on korduvalt otsustanud, et „nagu on ette nähtud kodukorra artikli 94 punktis c – on tingimata vajalik, et eelotsusetaotlus sisaldaks selgitust selle kohta, millistel põhjustel liikmesriigi kohus tõstatas liidu õigusnormide tõlgendamise või kehtivuse küsimuse ning millist seost ta nende õigusnormide ja põhikohtuasjas kohaldatavate riigisiseste õigusnormide vahel näeb“[10].

43. Eespool esitatu tõttu on aga kodukorra artikli 94 nõuete rikkumine käesolevas eelotsusetaotluses selge. Kuigi Euroopa Kohus näitab siinkohal üles teatavat paindlikkust, peab koostöö eelotsusetaotluse esitanud kohtuga olema vastastikune: kui viimati nimetatu põhjendamatult ei tee koostööd, et väljendada oma kahtlusi liidu õiguse tõlgendamise suhtes, mida ta peab kohaldatavaks (käesoleval juhul direktiiv 2016/680), näib mulle loogiline jätta eelotsusetaotlus vastuvõetamatuse tõttu läbi vaatamata.[11]

44. Eespool öeldule lisandub, et see kohus:

– ei ole täpsustanud, mis laadi töötlemist politsei püüdis läbi viia või milliseid isikuandmeid konkreetselt otsiti. Esiteks näib ta osutavat sellele, et piirduti ainult ühendusandmetega (st liiklus- ja asukohaandmetega), kuid seejärel ei välista ta võimalust, et telefoni lukustusest avamine oleks andnud juurdepääsu „kõigile mobiiltelefonis säilitatavatele digitaalsetele andmetele“,[12] sealhulgas telefoni teel toimunud side ja elektrooniliste sõnumite vahetuse sisule[13];

– viitab nii telefoni konfiskeerimisele ja selles salvestatud andmetega tutvumisele või tutvumise katsele kui ka nende andmete hilisemale „kasutamisele“ (*Auswertung*), see tähendab analüüsimisele ja lugemisele. Ta lisab, et see viimane tähendab „siiski täiesti kontrollimatut juurdepääsu asjaomase isiku kogu digitaalsele sidele“, mis võimaldab „rekonstrueerida väga üksikasjaliku ja põhjaliku ülevaate pea kõikidest eraelu valdkondadest“.

45. Nendes tingimustes viiks Euroopa Kohus eelotsusetaotluse esitanud kohtu küsimuste ümbersõnastamise asemel läbi pigem eelotsusetaotluse tõelise rekonstrueerimise, mis põhineb pealegi osaliselt hüpoteetilistel kaalutlustel, mitte tuvastatud faktidel. Kõike seda pärast seda – ma rõhutan –, kui ta on varem andnud kohtule võimaluse oma küsimusi ise täiendada või ümber sõnastada.

46. Teen seega ettepaneku tunnistada eelotsusetaotlus vastuvõetamatuks, nagu seda taotlesid mitu menetlusse astunud riiki.

[9] Euroopa Kohus pidas vajalikuks paluda pooltel teatada, „millised on nende arvates direktiivi 2016/680 asjakohased sätted, millest lähtudes peaks Euroopa Kohus vajaduse korral eelotsusetaotluse esitanud kohtu kolm eelotsuse küsimust ümber sõnastama“ (kohtuistungil suuliselt vastamiseks esitatud neljas küsimus).

[10] 6. oktoobri 2021. aasta kohtuotsus Consorzio Italian Management ja Catania Multiservizi (C-561/19, EU:C:2021:799, punkt 69).

[11] Nõustun selles hinnangus Prantsuse valitsusega (tema kirjalike seisukohtade punktid 36–41).

[12] Nii tuleneb teisest eelotsuse küsimusest.

[13] Eelotsusetaotluse esitanud kohus kinnitab, et „võrguliiklusandmete põhjal saab taastada praktiliselt kõigi kontaktide side sageduse, aja ja kestuse ning tekstisõnumite ja teiste sõnumirakenduste põhjal ka side sisu, kusjuures säilitatud fotode ja brauseri ajaloo hindamine annab väga intiimse ülevaate asjaomase isiku eraelust“.

47. Samamoodi peaks vastuvõetamatuks tunnistamiseni viima ka asjaolu, mida rõhutati kohtuistungil, et asja menetlevas kohtus ei ole enam tõelist vaidlust, mis nõuaks liidu õigusnormide tõlgendamist.

48. Austria valitsus (kellest sõltuvad uurimisse kaasatud politseiasutused) tunnistab nimelt, et nende ametivõimude teguviis oli ebaseaduslik ja riivas asjaomase isiku õigusi. Arvestades, et eelotsusetaotluse kohaselt oli kaebaja nõue halduskohtule esitatud just nimelt nende politseimeetmete vastu, mida vastustajaks olev ametiasutus pidas õigusvastaseks, on eelotsusetaotluse esitanud kohtule lahendamiseks esitatud vaidlus ära langenud.

49. Igal juhul, juhuks kui Euroopa Kohus minu arvamusega ei nõustu, käsitlen teise võimalusena eelotsuse küsimuste aluseks olevaid sisulisi probleeme.

50. Enne näib mulle siiski vajalik välistada veel teine vastuvõetamatuse alus, millele on viidanud mõned menetlusse astujatest.[14] Nad leiavad, et kuna direktiivi 2016/680 eesmärk on kaitsta füüsilisi isikuid nende andmete *töötlemisel*, ei reguleeri see selliseid juhtumeid nagu põhikohtuasjas, kus ei toimunud töötlemist, vaid lihtsalt *püüti andmeid kätte saada*, mida lõpuks ei saadud.

51. Komisjoni arvates tuleks vastupidi direktiivi 2016/680 soovitava toime huvides eelistada selle eesmärgi sellist tõlgendust, mis ei piirdu ainult andmetöötlusega kitsas tähenduses, vaid hõlmab ka sellega otseselt seotud küsimusi. Üks neist on tema sõnul katse saada kätte neid andmeid, mida tahetakse töödelda.[15]

52. Leian, et ilma et oleks vaja direktiivi 2016/680 kohaldamisala piire nihutada[16], on direktiivi kohaldamine sel juhul põhjendatud mitte seetõttu, et mobiiltelefon konfiskeeriti,[17] vaid sellele järgnenud politsei teguviisi tõttu, mille eesmärk oli saada telefonist asjaomase isiku teatavaid isikuandmeid, milleks nad püüdsid telefoni lukustust avada ja pääseda ligi selle sisule.

53. Toimingute hulgas, mis on direktiivi 2016/680 artikli 3 punktis 2 määratletud „töötlemisena“, on isikuandmete „muul moel kättesaadavaks tegemine“ kriminaaluurimise raames. Leian, et kui politsei konfiskeerib telefoni, kus neid andmeid säilitatakse, ja manipuleerib seda selleks, et sealt andmeid kätte saada, algatab ta andmetöötluse „toimingu“, isegi kui see ei õnnestu tehnilistel põhjustel, mis on seotud krüptograafilise andmeturbega.

54. Luhtunud katset kriminaaluurimise raames isikuandmeid mobiiltelefonist kätte saada reguleerib direktiiv 2016/680 analoogsetel põhjustel nendega, mille tõttu on Euroopa Kohus tunnistanud direktiivi 2002/58 kohaldatavaks (samuti luhtunud) *katsele* saada kohtu luba juurdepääsuks elektroonilise side teenuste osutajate säilitatavatele uurimisaluse isiku isikuandmetele, mis on elektroonilise side operaatori valduses.[18]

[14] Pean silmas konkreetselt Austria, Prantsuse, Madalmaade ja Norra valitsust.

[15] Komisjoni arvates „ei ole oluline, kas katsed õnnestuvad või mitte. Tehniliste raskuste ilmnemine, mis takistab juurdepääsukatsete õnnestumist, on asjaolu, mida ei ole võimalik ette teada ja mis ei mõjuta ohte isikuandmete kaitsele“.

[16] Mulle näib eriti asjatu tugineda direktiivi 2016/680 artiklitele 27 ja 28, mille pakkus välja komisjon oma kirjalikes seisukohtades. Artiklis 27 ette nähtud „andmekaitsealane mõjuhinnang“ puudutab üldiselt „teatavat tüüpi töötlemist“, mitte konkreetset või erilist töötlemist. Näiteks nähtub direktiivi 2016/680 põhjendusest 58: „[m]õjuhinnangud peaksid hõlmama isikuandmete töötlemise toimingute asjaomaseid süsteeme ja menetlusi, *kuid mitte üksikjuhtumeid*“ (kohtujuristi kursiiv). Kohtuistungil täpsustas komisjon nendele kahele sättele tuginemist, mida ta osundas ainult selleks, et rõhutada, kuidas direktiiv 2016/680 käsitleb ka olukordi, mis eelnevad otseses mõttes andmete töötlemisele.

[17] Direktiiv 2016/680 ei reguleeri telefoni kui tõendi äravõtmist kriminaaluurimise raames.

[18] 2. oktoobri 2018. aasta kohtuotsus Ministerio Fiscal (C-207/16, EU:C:2018:788).

55. Selles kontekstis, kui eelotsusetaotluse esitanud kohus peaks tegema otsuse politseitegevuse õigusvastasuse kohta (mida Austria valitsus tunnistab, nagu ma juba märkisin), võib tema hinnang sõltuda sellega taotletava eesmärgi õiguspärasusest nii juhul, kui meede õnnestus, kui ka juhul, kui seda ainult hakati rakendama, kuid edutult.

B. Sisulised küsimused

1. Esimene eelotsuse küsimus

56. Asja menetlev kohus soovib teada, kas direktiivi 2002/58 artikli 15 lõige 1 (vajaduse korral koostoimes artikliga 5) tähendab harta artikleid 7 ja 8 arvesse võttes, et „avalike võimuorganite juurdepääs mobiiltelefonis säilitatavatele andmetele kujutab endast harta viidatud artiklitega tagatud põhiõiguste riivet, mis on nii raske, et sellist juurdepääsu tuleks süütegude ennetamisel, uurimisel, avastamisel ja menetlemisel piirata võitlusega raske kuritegevuse vastu“.

57. Kui eelotsusetaotlus oleks vastuvõetav, nõuab direktiivi 2002/58 kohaldamata jätmine esimese küsimuse ümbersõnastamist nii, et Euroopa Kohtu vastus tõlgendaks direktiivi 2016/680.

58. See vastus peaks järgemööda selgitama, kas niisugustel juhtudel, nagu on kõne all käesolevas asjas, saab rääkida riivest, ning kui on tegemist riivega, siis kas direktiiv 2016/680 nõuab, et andmetega võib tutvuda ainult raske kuritegevuse vastu võitlemise juhtudel.

59. Andmetöötlustoimingud võivad juba oma määratluse poolest kahjustada õigust eraelu puutumatusele (harta artikkel 7) ja isikuandmete kaitsele (harta artikkel 8). Ametiasutused peavad seega järgima harta artikli 52 lõikes 1 ette nähtud tingimusi, et põhjendada sekkumist nende põhiõiguste teostamisse.

60. Harta artiklitega 7 ja 8 kaitstud õiguste riive on seda suurem, kui sellega: a) tahetakse kätte saada selliseid tundlikku laadi andmeid nagu need, mis on tavaliselt mobiiltelefonides salvestatud ja mille teada saamine võib avaldada andmesubjektide elu niisuguseid tahke, mis peavad jääma kolmandate isikute eest varjatuks, ja b) võimaldatakse juurdepääs side sisule.

61. Kuid üldiselt ja võttes arvesse direktiivi 2016/680 sisu, ei saa seda direktiivi tõlgendada nii, et selles silmas peetud andmetöötlused on ette nähtud ainult raske kuritegevuse vastu võitlemise juhtudel.

62. Direktiiv 2016/680 käsitleb igasugust isikuandmete töötlemise toimingut,[19] mida pädevad asutused teevad igat tüüpi süütegude tõkestamiseks, uurimiseks, avastamiseks ja nende eest vastutusele võtmiseks.

63. Direktiiviga 2016/680 kehtestatud põhimõtetest isikuandmete töötlemise kohta sellel eesmärgil (artikkel 4) või selle töötlemise seaduslikkuse tingimustest (artikkel 8) ei nähtu, et üldjuhul on andmete töötlemine võimalik üksnes raskete kuritegude korral.

[19] Direktiivi 2016/680 artikli 3 punktis 2 osutatud „toimingute“ tüübistik on väga lai. Vt käesoleva ettepaneku punktis 9 ära toodud tekst.

64. Ainult raske kuritegevuse vastu võitlemise juhtudega piiritlemine ei saaks põhineda ka direktiivi 2002/58 käsitleva Euroopa Kohtu praktika[20] laiendamisel sellistele juhtudele nagu käesolevas asjas.

65. Minu arvates ei saa see nii olla, sest – ilma et see piiraks seda, mida ma järgmiseks selgitan – see kohtupraktika puudutab üldise ja määratlemata rühma isikuandmete üldiselt ja vahet tegemata säilitamist, mida teevad süstemaatiliselt elektroonilise side teenuste osutajad. Selle riive ulatus, mida andmete säilitamine endast kujutab ühiskonnale tervikuna, seletab, miks on Euroopa Kohus selle keelamisel ja sellest keelust erandeid ette nähes eriti range.

66. See ei ole aga nii juhul, kui taotletav juurdepääs ei puuduta kogu elanikkonda või selle suuri rühmi (st üldise ja määratlemata rühma isikuandmed), vaid konkreetses mobiiltelefonis säilitatavat teavet samuti üksiku kriminaaluurimise menetluse raames, mille puhul kehtib konkreetselt direktiiv 2016/680.

67. Direktiivi 2016/680 ainus eesmärk on andmete töötlemine pädevate asutuste poolt süütegude ennetamiseks, avastamiseks, uurimiseks ja nende eest vastutusele võtmiseks. See kehtib igat laadi süütegude, mitte ainult raskete kuritegude korral.

68. Lisaks, nagu rõhutasid mõned eelotsusemenetluses menetlusse astujad, kuna direktiivis 2016/680 viited süütegude raskusastmele puuduvad, ei pruugita liikmesriikides seda direktiivi kohaldada ühetaoliselt, sest hinnangud karistatava tegevuse suurema või väiksema raskusastme kohta on liikmesriikide õiguses oluliselt erinevad.[21]

69. Direktiiv 2016/680 ei kehtesta seega õiguspärasuse tingimusena nõuet, et selles direktiivis ette nähtud isikuandmete töötlemine peab olema võimalik ainult võitlemiseks raske kuritegevusega.

70. See ei mõjuta asjaolu, et vastavalt proportsionaalsuse põhimõttele ja iga juhtumi puhul tuleb andmete töötlemist, mida pädevad asutused kavatsevad direktiivi 2016/680 alusel läbi viia, kohandada olenevalt: a) karistatavate süütegude laadist ja b) nende isikuandmete olemusest, mida töödeldakse.

71. Nõustun selles osas Saksamaa valitsuse kinnitusega konfiskeeritud telefonide andmetele juurdepääsu piiramise kohta, kui nende digitaalse sisu põhjal saab kindlaks määrata andmesubjekti täieliku isikuprofiili. Saksamaa valitsuse arvates peaks see juurdepääs piirduma ainult andmetega, mis on konkreetsel juhul vajalikud tõenditena, ning juurdepääs ei pruugi olla asjakohane, kui esinevad sellised tegurid nagu „uurimise esemeks oleva süüteo väike raskusaste või saadavate andmete nõrk tõendusjõud“.[22]

72. *Abstraktselt* ei tähenda direktiiv 2016/680 seega, et juurdepääs mobiiltelefonis salvestatud isikuandmetele selleks, et hõlbustada niisuguse tegevuse uurimist, mis võib kuuluda üldise või levinud kuritegevuse hulka, oleks süstemaatiliselt ebaseaduslik. Seda, kas selline juurdepääs on *konkreetselt* vajalik, peab asjaomane ametiasutus igal juhul hindama, lähtudes selle juurdepääsu vajalikkuse ja proportsionaalsuse kriteeriumist, millele ma äsja viitasin.

[20] Kohtuotsus La Quadrature du Net ja 21. detsembri 2016. aasta kohtuotsus Tele2 Sverige ja Watson jt (C-203/15 ja C-698/15, EU:C:2016:970; edaspidi „kohtuotsus Tele2 Sverige ja Watson“); 2. oktoobri 2018. aasta kohtuotsus Ministerio Fiscal (C-207/16, EU:C:2018:788); 6. oktoobri 2020. aasta kohtuotsus Privacy International (C-623/17, EU:C:2020:790) ja 2. märtsi 2021. aasta kohtuotsus Prokuratuur (tingimused elektroonilise side andmetele juurdepääsuks) (C-746/18, EU:C:2021:152; edaspidi „kohtuotsus Prokuratuur“).

[21] Prantsuse valitsus toob näiteks narkootiliste ainete valdamise ja kaubitsemisega seotud süüteod, mille raskusastmed on Austria ja Prantsusmaa kriminaalõigusnormides erinevad. Sama seisukohta avaldab ka Rootsi valitsus.

[22] Saksamaa valitsuse kirjalikud seisukohad, punkt 20.

73. See tuleneb minu arvates direktiivi 2016/680 sätetest, millega määratakse kindlaks isikuandmete töötlemise kehtivuse tingimused kuritegevuse vastu võitlemisel:

– artikli 4 lõike 1 punkt a, mille kohaselt on vajalik, et „isikuandmeid töödeldakse seaduslikult“;

– artikli 8 lõige 1, milles rõhutatakse, et töötlemine peab osutuma *vajalikuks* ja põhinema liidu või liikmesriigi õigusel.

2. Teine eelotsuse küsimus

74. Teise eelotsuse küsimusega soovib eelotsusetaotluse esitanud kohus teada, kas direktiivi 2002/58 artikli 15 lõikega 1 koostoimes harta artiklitega 7, 8 ja 11 ning artikli 52 lõikega 1 „on vastuolus sellised riigisisesed õigusnormid nagu [StPO] § 18 koostoimes § 99 lõikega 1, mille kohaselt on julgeolekuasutustel kriminaaluurimise käigus ilma kohtu või sõltumatu haldusasutuse loata õigus ise saada täielik ja kontrollimatu juurdepääs kõigile mobiiltelefonis säilitatavatele digitaalsetele andmetele“.

75. Küsimuse sõnastus on teataval määral mitmeti mõistetav. Eelotsusetaotluse esitanud kohus:

– tunnistab, et StPO § 110 lõige 2 näeb ette, et vara konfiskeerimiseks on põhimõtteliselt vaja prokuratuuri luba. Politseiasutus võib vara ilma sellise loata konfiskeerida üksnes sama paragrahvi lõikes 3 nimetatud erandjuhtudel (mida käesoleval juhul ei näi esinevat);

– lisab siiski, et mobiiltelefonides salvestatud teabe analüüsimist „ei ole [StPOs] ühemõtteliselt reguleeritud“ ja et nende andmetega võivad julgeolekuasutused tutvuda omal algatusel, ilma eelneva loata.

76. Austria valitsus esitab riigisiseste õigusnormide versiooni, mis ei ole eelotsusetaotluses esitatuga kooskõlas. Ta kinnitab konkreetselt, et riigisisese õiguse kohaselt on nii telefoni konfiskeerimine (välja arvatud kiireloomulistel juhtudel) kui ka selles salvestatud andmete analüüsimine võimalik ainult prokuratuuri loal.[23] Ilma prokuratuuri korralduseta on telefonis säilitatavate andmete kasutamine politsei poolt õigusvastane.

77. Eelotsusetaotluse esitanud kohus peab kontrollima riigisiseste õigusnormide sõnastust. ELTL artiklis 267 ette nähtud menetluses puudub Euroopa Kohtul pädevus tõlgendada riigisisest õigust ning üksnes liikmesriigi kohus on pädev määrama kindlaks riigisiseste õigus- ja haldusnormide täpse ulatuse.[24]

78. Ma ei soovi küll sekkuda Austria õiguse tõlgendamise poleemikasse, kuid mulle näib raske tuletada ainult eelotsusetaotluse esitanud kohtu osutatud sätetest (StPO § 18 koostoimes sama seaduse § 99 lõikega 1) niisugust tagajärge, nagu see kohus ise järeldab. Kordan aga, et see on küsimus, mille saab lahendada ainult see kohus.

[23] Austria valitsuse seisukohtade punkt 19. Ta viitab Oberster Gerichtshofi (Austria kõrgeim kohus) 13. oktoobri 2020. aasta kohtuotsusele (kohtuasi 11 Os 56/20z), milles kvalifitseeritakse mobiiltelefoni andmete analüüsimine kriminaalpolitsei poolt ilma prokuratuuri loata õigusvastaseks, kuna see rikub andmesubjekti subjektiivseid õigusi.

[24] Vt muu hulgas 28. aprill 2022. aasta kohtuotsus SeGEC jt (C-277/21, EU:C:2022:318, punkt 21).

79. Igal juhul leiab eelotsusetaotluse esitanud kohus, et kohtuotsuse Prokuratuur[25] seisukoht selles, kuidas kohus või sõltumatu asutus säilitatavatele andmetele juurdepääsu eelnevalt kontrollib, on sellisele juhtumile nagu käesolev ülekantav.

80. Madalmaade valitsuse arvates tuleb seda kohtupraktikat mõista vastupidi niisuguste riigisiseste õigusnormide kontekstis, mis võimaldavad pädevate asutuste *üldist* juurdepääsu *kõikidele* säilitatavatele liiklusandmetele ja asukohaandmetele. See seletab tema sõnul eelneva kohtuliku loa nõuet, mis ei pruugi siiski olla põhjendatud üheainsa mobiiltelefoni andmetele juurdepääsu korral.

81. Sama mõttekäiku järgides väidab Norra valitsus, et direktiivis 2016/680[26] ette nähtud mitme tagatise hulgas ei ole sõnaselgelt nõuet, et on vaja eelnevat luba kohtult või sõltumatult haldusasutuselt.

82. Komisjon lähtub seisukohast, et direktiivi 2016/680 sätteid tuleb tõlgendada hartast lähtudes, ja väidab, et selle direktiivi artikli 8 lõikega 1 liikmesriikidele pandud kohustus (andmete töötlemise seaduslikkuse tingimused) hõlmab vajadust austada harta artiklitega 7 ja 8 tagatud põhiõigusi.

83. Jagan komisjoni arvamust, et neid harta sätteid järgides on liikmesriikide seadusandjad kohustatud kehtestama vajalikud eeskirjad, et tagada, et andmetele juurdepääs oleks iga juhtumi puhul põhjendatud ja piirduks ainult sellega, mis on rangelt vajalik ja proportsionaalne.

84. Niisugused riigisisesed õigusnormid ei pea siiski tingimata olema konkreetselt seotud juurdepääsuga isikuandmetele, mis on mobiiltelefonis, nagu käesoleval juhul, vaid võivad olla normid, mis on riigisiseses õiguses ette nähtud tõendite kogumise valdkonnas üldiselt.

85. Sellega seoses esitasin juba kohtuotsuse La Quadrature du Net punkti 103 osas, mis puudutab liikmesriikide meetmeid elektroonilise side konfidentsiaalsuse kohta, kehtestamata selliste sideteenuste osutajatele andmete töötlemise kohustusi.[27]

86. Ilma et direktiivist 2016/680 oleks seega vaja tuletada *konkreetseid* menetluseeskirju, mis tagavad mobiiltelefonis säilitatavale teabele juurdepääsu õiguspärasuse[28], kohaldatakse riigisiseseid eeskirju, mis reguleerivad läbiotsimis- ja konfiskeerimisvolituste teostamist kriminaaluurimise raames[29].

87. Viide riigisisestele õigusnormidele, et tagada direktiivi 2016/680 alusel juurdepääsu õiguspärasus, on pealegi kooskõlas Euroopa Inimõiguste Kohtu praktikaga. Just nimelt olukorras, mis puudutab Austria Vabariiki seoses EIÕK artikliga 8 (õigus era- ja perekonnaelu austamisele

[25] Kohtuotsus Prokuratuur, punkt 51: „On esmatähtis, et riigi pädevate asutuste juurdepääs säilitatud andmetele oleks allutatud kohtu või sõltumatu haldusasutuse teostatavale eelnevale kontrollile ja et see kohus või haldusasutus teeks oma otsuse juurdepääsu taotleva asutuse põhjendatud taotluse alusel, mis on ennekõike esitatud kuriteo ennetamise, avastamise või kohtus menetlemise raames.“

[26] Lisaks artiklites 4 ja 8 sätestatud tagatistele III peatüki („Andmesubjekti õigused“), IV peatüki („Vastutav töötleja ja volitatud töötleja“), VI peatüki („Sõltumatud järelevalveasutused“) ja VIII peatüki („Õiguskaitsevahendid, vastutus ja karistused“) tagatised.

[27] Vt käesoleva ettepaneku punkt 36.

[28] Tegu on ülesandega, mille keerukusest annavad tunnistust pingutused, mida komisjon tegi oma seisukohtade punktides 34–39, et aidata määratleda selgeid ja täpseid eeskirju mobiiltelefoni andmetele juurdepääsu suhtes kehtivate piirangute ja tagatiste kehtestamiseks.

[29] Eeskirjad, mis – nagu meenutavad näiteks Taani ja Iiri valitsus – ei kuulu liidu õiguse kohaldamisalasse, kuid mida võib kasutada sellest õigusest tuleneva nõude täitmiseks.

ning kodu ja kirjavahetuse puutumatusele), tuvastas EIK, et esemete ja eelkõige dokumentide konfiskeerimist käsitlevad Austria õigusnormid on kohaldatavad andmekandjatele salvestatud andmete läbiotsimisele ja konfiskeerimisele. [30]

88. Kui politseil ei ole õigust konkreetses mobiiltelefonis salvestatud andmetega tutvuda ilma prokuratuuri loata, nagu väidab Austria valitsus Oberster Gerichtshofi (Austria kõrgeim kohus) kohtupraktikale viidates, kaotab teine eelotsuse küsimus suure osa oma mõttest.

89. Igal juhul ei välista vastus sellele küsimusele seda, et juurdepääs konfiskeeritud telefonis sisalduvatele isikuandmetele viiks selleni, et on võimalik „rekonstrueerida väga üksikasjaliku ja põhjaliku ülevaate pea kõikidest [asjaomase isiku] eraelu valdkondadest“. [31] Kui see oleks nii, siis ei saaks politsei vabaneda kohtuotsuses Prokuratuur nimetatud eelneva loa taotlemise kohustusest.

90. Esmapilgul näib, et see kinnitus ei ole kooskõlas direktiivi 2002/58 (mida tõlgendatakse kohtuotsuses Prokuratuur) käesolevas asjas kohaldamata jätmisega, nagu ma eespool soovitasin. Leian siiski, et selle kohtuotsuse mõte toetab sama lahendust.

91. Kuigi kohtuasjas, milles tehti kohtuotsus Prokuratuur, toimus andmetega tutvumine elektroonilise side teenuste osutajatelt (metaandmete) saamise teel, oli seal nagu käesolevas asjas tegemist konkreetse isiku suhtes algatatud individuaalse kriminaaluurimisega. Tegemist oli andmete kogumisega „[…] mitme telefoninumbri ja tema erinevate rahvusvahelise mobiilside terminalseadme tunnuste kohta“. [32]

92. Kohtuotsuses Prokuratuur saab minu arvates eristada kahte tasandit: a) seda, milles seatakse kahtluse alla liikmesriigi üldnormid, mis käsitlevad teenuseosutajate valduses olevate andmete üldist ja vahet tegemata säilitamist ning nendega edaspidi tutvumist, ja b) nende metaandmetega konkreetsel juhul tutvumise eelneva kontrolli tasandit, kui need andmed võimaldavad saada isiku eraelust täpse pildi.

93. Asjaolu, et käesolevas asjas ei ole eraelu kajastavad andmed teenuseosutajate valduses ja et need saadakse (või püütakse saada) ühest konfiskeeritud telefonist, on minu arvates teisejärguline, võrreldes eelneva kontrolli nõude mõttega, millele apelleeritakse kohtuotsuses Prokuratuur.

94. Selle eelneva kontrolli aluseks on lõppastmes harta artiklitega 7 ja 8 tagatud kaitse. Seda kontrolli teostav asutus peab suutma „tagada õiglase tasakaalu ühelt poolt kuritegevusevastase võitluse raames uurimise vajadustega seotud huvide ning teiselt poolt isikute, kelle andmetele juurdepääsu taotletakse, põhiõiguste vahel eraelu puutumatusele ja isikuandmete kaitsele“ [33].

[30] EIK 16. oktoobri 2007. aasta kohtuotsus Wieser ja Bicos Beteiligungen *vs*. Austria (CE:ECHR:2007:1016JUD007433601), punkt 54: „Austria kriminaalmenetluse seadustikus ei ole konkreetseid sätteid elektrooniliste andmete läbiotsimiseks ja konfiskeerimiseks. Kuid see sisaldab täpseid sätteid esemete konfiskeerimiseks ja lisaks erinorme dokumentide konfiskeerimiseks. Riigisiseste kohtute praktikast tuleneb, et neid sätteid kohaldatakse samuti elektrooniliste andmete läbiotsimiseks ja konfiskeerimiseks.“

[31] Vt eelotsusetaotluse esitanud kohtu seisukohad, mis on esitatud käesoleva ettepaneku punktis 44.

[32] Kohtuotsus Prokuratuur (punkt 17).

[33] Kohtuotsus Prokuratuur (punkt 52).

3. Kolmas eelotsuse küsimus

95. Kolmanda eelotsuse küsimusega soovib eelotsusetaotluse esitanud kohus teada, kas harta artikliga 47 (vajaduse korral koostoimes artiklitega 41 ja 52) on vastuolus sellised õigusnormid nagu Austria õigusnorm [34], mis „võimaldab mobiiltelefoni andmete digitaalset analüüsimist ilma, et asjaomast isikut teavitataks sellest enne või vähemalt pärast meetme võtmist".

96. Ma leian, et selliselt sõnastatud küsimus ei pruugi olla vaidluse lahendamiseks vajalik, sest asjaomane isik sai kasutada harta artiklis 47 sätestatud õigust, paludes eelotsusetaotluse esitanud kohtul tunnistada tühiseks konfiskeeritud telefoni suhtes võetud politseimeede, mis hõlmas telefonis säilitatavate andmete edasist (ja luhtunud) kasutamist.

97. Nende kahe politsei tegevuse hetke puhul tuleb eristada:

– telefoni enda konfiskeerimist, mille kohta nähtub toimiku materjalidest, et asjaomane isik sai sellest teada ning keeldus andmast politseile telefoni lukustusest avamise koodi, kui temalt telefon ära võeti;

– andmete analüüsimise katset, mille kohta näib kõik viitavat sellele, et vastutav töötleja ei teavitanud andmesubjekti sellest toimingust, kuigi Austria valitsus kinnitab, et viimane oli teadlik aruandest, milles on märgitud politsei meede telefoni suhtes. [35]

98. Seega valitseb andmete kasutamise ja asjaomase isiku sellest teadlikkuse suhtes teatud ebakindlus, mida oleks eelotsusetaotluse esitanud kohus pidanud eelotsusetaotluses selgitama, nagu ma juba märkisin, ning mis takistab kolmandale eelotsuse küsimusele tarviliku vastuse andmist.

99. Juhuks kui Euroopa Kohus ei peaks seda küsimust vastuvõetamatuks tunnistama, esitan igaks juhuks selle kohta seisukoha. Sel juhul ja võttes arvesse, et direktiiv 2002/58 ei ole kohaldatav, tuleks see küsimus ümber sõnastada, lähtudes direktiivist 2016/680, mille artiklid 13, 15 ja 54 annavad juhatust sellele vastamiseks.

100. Direktiivi 2016/680 kohaselt tuleb andmesubjektile esitada tema andmete töötlemist käsitlev teave, mis on vajalik muu hulgas selleks, et: a) esitada kaebus järelevalveasutusele (artikli 13 lõike 1 punkt d) ja b) saada tõhus kohtulik kaitse direktiiviga 2016/680 tagatud õiguste rikkumise eest, ilma et see piiraks kättesaadavate halduslike kaitsevahendite või kohtuväliste heastamisvahendite kasutamist (artikkel 54).

101. Siiski ei tohi unustada, et nii direktiivi 2016/680 artikli 13 lõige 3 kui ka artikli 15 lõige 1 lubavad liikmesriikidel võtta seadusandlikke meetmeid, millega:

– nähakse artikli 13 lõike 2 alusel ette andmesubjektile teabe hilisem või piiratud esitamine või esitamata jätmine;

– piiratakse osaliselt või täielikult andmesubjekti õigust tutvuda töödeldud andmetega tingimusel, et selline piirang on vajalik ja proportsionaalne meede muu hulgas selleks, et

[34] Ta viitab taas StPO §-le 18 koostoimes selle §-ga 99.

[35] Tema kirjalike seisukohtade punkt 37.

vältida ametlike või kohtulike uurimiste või menetluste takistamist või süütegude uurimise kahjustamist.[36]

102. Igal juhul ei sõltu andmetöötluse õiguspärasus mitte sellest, kas pädevad asutused täidavad (hilisemaid) kohustusi, mis on neile kehtestatud direktiivi 2016/680 artikliga 13, vaid selle töötlemise aluseks olnud eesmärgi õiguspärasusest; see tähendab sellest, kas haldusasutustel oli õigus isikuandmeid töödelda.

103. Seda silmas pidades ei ole asjaolu, et andmesubjektile teatati katsetest temalt konfiskeeritud telefonis salvestatud andmetega tutvuda, sisulistel põhjustel iseenesest mingil määral seotud politseimeetme õiguspärasusega. Vastutava töötleja tegevusel, mis võib olla vastuolus direktiivi 2016/680 artiklist 13 tulenevate kohustustega, võib olla muid tagajärgi, kuid ma kordan, et see ei mõjuta iseenesest selle töötlemise õiguspärasust või õigusvastasust.

104. Eelotsusetaotluse esitanud kohtu ülesanne on kindlaks teha, kas liikmesriigi õigusnormid võimaldavad puudutatud isikul neid õigusi tõhusalt kasutada.

V. Ettepanek

105. Eeltoodut arvestades teen Euroopa Kohtule ettepaneku tunnistada Landesverwaltungsgericht Tiroli (Tirooli liidumaa halduskohus, Austria) esitatud eelotsusetaotlus vastuvõetamatuks.

Teise võimalusena teen ettepaneku vastata sellele taotlusele järgmiselt:

1. Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiivi (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK, artikli 4 lõike 1 punkti a ja artikli 8 lõiget 1 koostoimes Euroopa Liidu põhiõiguste harta artiklitega 7, 8 ja 52

   tuleb tõlgendada nii, et

   kriminaaluurimise raames ei piirdu avalike võimuorganite juurdepääs mobiiltelefonis salvestatud isikuandmetele nende töötlemiseks ainult raske kuritegevuse vastu võitlemise juhtudega.

   Selline juurdepääs peab olema iga juhtumi puhul eraldi põhjendatud ning piirduma ainult sellega, mis on rangelt vajalik ja proportsionaalne, olenevalt karistatavate süütegude laadist ja taotletud isikuandmetest.

   Politsei ei saa iseenesest ja ilma kohtu eelneva loata kriminaalmenetluse raames saada täielikku ja kontrollimatut juurdepääsu kõigile mobiiltelefonis salvestatud andmetele, kui need võimaldavad saada isiku eraelust täpse pildi.

2. Direktiivi 2016/680 artikleid 13, 15 ja 54 koostoimes harta artiklitega 47 ja 52

[36] Vt selle kohta kohtuotsus Tele2 Sverige ja Watson (punkt 121). Selle direktiivi 2002/58 käsitlev doktriin on ülekantav direktiivile 2016/680 seoses töödeldavate andmete subjektide õiguste kohtuliku kaitse tagamisega.

tuleb tõlgendada nii, et

kui direktiivi 2016/680 artikli 15 lõikega 1 lubatud piirangutest või muudest kättesaadavatest halduslikest kaitsevahenditest või kohtuvälistest heastamisvahenditest ei tulene teisiti, tuleb mobiiltelefoni omanikku teavitada sellest, kuidas asjaomased asutused sellesse salvestatud isikuandmeid töötlevad, sel ajal ja viisil, mis on vajalik selleks, et tagada talle kohtuliku kaitse õiguse tõhus kasutamine, kui esineb direktiiviga 2016/680 antud õiguste võimalik rikkumine.