CONCLUSIE VAN ADVOCAAT-GENERAAL
M. CAMPOS SÁNCHEZ-BORDONA
van 20 april 2023[1]

Zaak C-548/21

C. G.
tegen
Bezirkshauptmannschaft Landeck

[verzoek van het Landesverwaltungsgericht Tirol (bestuursrechter in eerste aanleg van de deelstaat Tirol, Oostenrijk) om een prejudiciële beslissing]

„Prejudiciële verwijzing – Telecommunicatie – Bescherming van persoonsgegevens – Richtlijn (EU) 2016/680 – Strafprocedure – Poging van overheidsinstanties om zonder toestemming van een rechterlijke instantie of onafhankelijk bestuursorgaan toegang te krijgen tot op een mobiele telefoon opgeslagen gegevens”

1. Dit verzoek om een prejudiciële beslissing betreft, kort samengevat, de voorwaarden waaraan politiediensten moeten voldoen om toegang te krijgen tot gegevens die zijn opgeslagen op de mobiele telefoon van de persoon tegen wie een strafrechtelijk onderzoek loopt.

2. Zoals ik zal trachten toe te lichten, vertoont de prejudiciële verwijzing aanmerkelijke tekortkomingen in verband met de ontvankelijkheid ervan. Mocht het Hof desondanks besluiten de zaak ten gronde te onderzoeken, dan zal het zich moeten uitspreken over de respectieve werkingssferen van richtlijn 2002/58/EG[2] en richtlijn (EU) 2016/680[3].

[1] Oorspronkelijke taal: Spaans.

[2] Richtlijn van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PB 2002, L 201, blz. 37).

[3] Richtlijn van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van kaderbesluit 2008/977/JBZ van de Raad (PB 2016, L 119, blz. 89).

I. Toepasselijke bepalingen

A. Unierecht

1. Verordening 2016/679

3. In artikel 2 („Materieel toepassingsgebied") van verordening (EU) 2016/679[4] wordt in lid 2 bepaald:

„Deze verordening is niet van toepassing op de verwerking van persoonsgegevens:

[…]

d) door de bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid."

2. Richtlijn 2016/680

4. In overweging 2 wordt verklaard:

„De beginselen en regels betreffende de bescherming van natuurlijke personen bij de verwerking van hun persoonsgegevens dienen, ongeacht hun nationaliteit of verblijfplaats, in overeenstemming te zijn met hun grondrechten en fundamentele vrijheden, met name met hun recht op bescherming van persoonsgegevens. Deze richtlijn is bedoeld om bij te dragen aan de totstandkoming van een ruimte van vrijheid, veiligheid en recht."

5. Overweging 46 luidt:

„Elke beperking van de rechten van de betrokkene dient in overeenstemming te zijn met het Handvest [van de grondrechten van de Europese Unie] en met het [Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM)], zoals uitgelegd in de rechtspraak van respectievelijk het Hof […] en het Europees Hof voor de Rechten van de Mens[5], en met name de wezenlijke inhoud van die rechten en vrijheden te eerbiedigen."

6. In overweging 49 staat te lezen:

„Indien de persoonsgegevens in het kader van een strafrechtelijk onderzoek en een strafrechtelijke procedure worden verwerkt, moeten de lidstaten erin kunnen voorzien dat het recht op informatie, inzage en op rectificatie of wissing van persoonsgegevens en op verwerkingsbeperking overeenkomstig het nationaal procesrecht wordt uitgeoefend."

[4] Verordening van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PB 2016, L 119, blz. 1; hierna: „AVG").

[5] Hierna: „EHRM".

7. In artikel 1 („Onderwerp en doelstellingen”) wordt bepaald:

„1. Bij deze richtlijn worden de regels vastgesteld betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

2. Overeenkomstig deze richtlijn hebben de lidstaten de verplichting:

a) de grondrechten en de fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens te beschermen; […]

[…]

3. Deze richtlijn belet de lidstaten niet uitgebreidere waarborgen te bieden dan die waarin deze richtlijn voorziet voor de bescherming van de rechten en vrijheden van de betrokkene in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten.”

8. Artikel 2 („Toepassingsgebied”), lid 1, schrijft voor:

„Deze richtlijn is van toepassing op de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de doeleinden van artikel 1, lid 1.”

9. In artikel 3 („Definities”) kan worden gelezen:

„Voor de toepassing van deze richtlijn wordt verstaan onder:

[…]

2) ‚verwerking’: een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, bekendmaking door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;

[…]

7) ‚bevoegde autoriteit’:

a) iedere overheidsinstantie die bevoegd is voor de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid; […]

[…]

[…]”

10. Artikel 4 („Beginselen inzake verwerking van persoonsgegevens”), lid 1, kent de volgende bewoordingen:

„De lidstaten schrijven voor dat persoonsgegevens:

a) rechtmatig en eerlijk worden verwerkt;

b) voor welbepaalde, uitdrukkelijk omschreven en legitieme doeleinden worden verzameld en niet op een met die doeleinden onverenigbare wijze worden verwerkt;

c) toereikend, ter zake dienend en niet bovenmatig in verhouding tot de doeleinden waarvoor zij worden verwerkt, zijn;

[…]

e) worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt;

f) met gebruikmaking van passende technische of organisatorische middelen op een dusdanige manier worden verwerkt dat de beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.”

11. Artikel 8 („Rechtmatigheid van de verwerking”) luidt als volgt:

„1. De lidstaten zorgen ervoor dat verwerking alleen rechtmatig is indien en voor zover die verwerking noodzakelijk is voor de uitvoering door een bevoegde autoriteit van een taak voor de in artikel 1, lid 1, bedoelde doeleinden, en dat die verwerking gebaseerd is op het Unierecht of het lidstatelijke recht.

2. In het lidstatelijke recht dat verwerking binnen het toepassingsgebied van deze richtlijn regelt, worden ten minste de verwerkingsdoeleinden, de te verwerken persoonsgegevens en de doeleinden van de verwerking gespecificeerd.”

12. Artikel 13 („Aan de betrokkene ter beschikking gestelde of verstrekte informatie”) schrijft voor:

„1. De lidstaten voorzien erin dat de verwerkingsverantwoordelijke de betrokkene ten minste de volgende informatie ter beschikking stelt:

[…]

d) het bestaan van het recht klacht in te dienen bij de toezichthoudende autoriteit, en de contactgegevens van de toezichthoudende autoriteit;

[…]

3. De lidstaten kunnen wettelijke maatregelen treffen om de verstrekking van de in lid 2 bedoelde informatie aan de betrokkene uit te stellen, te beperken of achterwege te laten, voor zover en zolang een dergelijke maatregel in een democratische samenleving, met inachtneming van de grondrechten en de legitieme belangen van de natuurlijke persoon in kwestie, een noodzakelijke en evenredige maatregel is om:

a) belemmering van officiële of gerechtelijke onderzoeken of procedures te voorkomen;

b) nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen te voorkomen;

c) de openbare veiligheid te beschermen;

d) de nationale veiligheid te beschermen;

e) de rechten en vrijheden van anderen te beschermen.

[…]"

13. Artikel 15 („Beperkingen van het inzagerecht"), lid 1, is als volgt verwoord:

„De lidstaten kunnen wettelijke maatregelen treffen om het inzagerecht van de betrokkene geheel of gedeeltelijk te beperken, voor zover en zolang die volledige of gedeeltelijke beperking in een democratische samenleving, met inachtneming van de grondrechten en legitieme belangen van de natuurlijke persoon in kwestie, een noodzakelijke en evenredige maatregel is om:

a) belemmering van officiële of gerechtelijke onderzoeken of procedures te voorkomen;

b) nadelige gevolgen voor de voorkoming, de opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen te voorkomen;

c) de openbare veiligheid te beschermen;

d) de nationale veiligheid te beschermen;

e) de rechten en vrijheden van anderen te beschermen."

14. Artikel 27 („Gegevensbeschermingseffectbeoordeling") luidt:

„1. Wanneer een soort verwerking, in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de reikwijdte, de context of de doeleinden daarvan, waarschijnlijk een hoog risico voor de rechten en vrijheden van natuurlijke personen oplevert, voorzien de lidstaten erin dat de verwerkingsverantwoordelijke vóór de verwerking een beoordeling verricht van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens.

2. De in lid 1 bedoelde beoordeling bevat ten minste een algemene beschrijving van de beoogde verwerkingen, een beoordeling van de risico's voor de rechten en vrijheden van de betrokkenen, de beoogde maatregelen ter beperking van de risico's, de voorzorgsmaatregelen, de beveiligingsmaatregelen en de mechanismen die zijn ingesteld om de persoonsgegevens te

beschermen en aan te tonen dat aan deze richtlijn is voldaan, met inachtneming van de rechten en legitieme belangen van de betrokkenen en andere betrokken personen."

15. Artikel 28 („Voorafgaande raadpleging van de toezichthoudende autoriteit") schrijft voor:

„1. De lidstaten voorzien erin dat de verwerkingsverantwoordelijke of de verwerker de toezichthoudende autoriteit raadpleegt voordat de verwerking van persoonsgegevens in een nieuw bestand zal worden opgenomen, wanneer:

a) uit een gegevensbeschermingseffectbeoordeling als bedoeld in artikel 27 blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken; of

b) de aard van de verwerking, in het bijzonder wanneer wordt gebruikgemaakt van nieuwe technologieën, mechanismen of procedures, een hoog risico voor de rechten en vrijheden van betrokkenen met zich meebrengt.

[…]"

16. In artikel 54 („Recht om een doeltreffende voorziening in rechte in te stellen tegen een verwerkingsverantwoordelijke of een verwerker") wordt bepaald:

„Onverminderd andere mogelijkheden van administratief of buitengerechtelijk beroep, waaronder het recht op grond van artikel 52 klacht in te dienen bij een toezichthoudende autoriteit, schrijven de lidstaten voor dat iedere betrokkene het recht heeft een doeltreffende voorziening in rechte in te stellen, indien hij van mening is dat een inbreuk is gepleegd op zijn rechten uit hoofde van krachtens deze richtlijn vastgestelde bepalingen als gevolg van een verwerking van zijn persoonsgegevens die niet aan die bepalingen voldoet."

B. Nationaal recht

17. § 18 van de Strafprozessordnung[6] kent de recherche taken toe ten dienste van de strafrechtspleging (lid 1). Door de recherche uitgevoerde onderzoeken vallen onder de verantwoordelijkheid van de veiligheidsautoriteiten (lid 2). De organen van de openbare veiligheidsdienst verrichten de uitvoerende recherchedienst, die bestaat uit het onderzoeken en vervolgen van strafbare feiten (lid 3).

18. Volgens § 99 StPO opent de recherche ambtshalve of op basis van een aangifte onderzoeken en moet zij de bevelen van het openbaar ministerie en rechterlijke instanties opvolgen (lid 1). Wanneer een onderzoeksmaatregel een bevel van het openbaar ministerie vereist, kan de recherche bij een rechtstreeks dreigend gevaar de overeenkomstige bevoegdheid ook zonder een dergelijk bevel uitoefenen. In dat geval moet onmiddellijk een verzoek om toestemming worden ingediend (lid 2).

[6] Wetboek van strafvordering (BGBl nr. 631/1975), in de ten tijde van de feiten van het hoofdgeding toepasselijke versie (BGBl I nr. 24/2020) (hierna: „StPO").

19. Volgens § 111, lid 2, StPO is, wanneer op een gegevensdrager opgeslagen informatie moet worden verzameld, eenieder verplicht om toegang tot die informatie te verlenen en deze op verzoek te verstrekken in een algemeen gebruikt bestandsformaat op een elektronische gegevensdrager, of om het aanmaken daarvan toe te staan. Bovendien moet eenieder toestaan dat er een back-up wordt gemaakt van de op de gegevensdrager opgeslagen informatie.

II. Feiten, hoofdgeding en prejudiciële vragen

20. C. G. heeft de Duitse nationaliteit en werkt en verblijft in Oostenrijk.

21. Op 23 februari 2021 hebben ambtenaren van het douanekantoor Innsbruck (Oostenrijk) bij een drugscontrole een aan verzoeker geadresseerd pakket met daarin 85 gram cannabis in beslag genomen.

22. Op 6 maart 2021 verhoorden twee politieagenten C. G. over de afzender van het drugspakket en doorzochten zij zijn woning. Tijdens die doorzoeking werd zijn mobiele telefoon (met inbegrip van een simkaart en een SD-kaart) in beslag genomen en werd hem het proces-verbaal van de inbeslagneming overhandigd.

23. Toen C. G. werd verzocht toegang tot de verkeersgegevens van zijn mobiele telefoon te verlenen, weigerde hij dit, en ook de toegangscode weigerde hij mee te delen.

24. Het Bezirkspolizeikommando Landeck (regionale politie Landeck, Oostenrijk) slaagde er niet in de mobiele telefoon te ontgrendelen. De mobiele telefoon werd aan het Bundeskriminalamt (federale recherche, Oostenrijk) in Wenen gezonden, waar nogmaals zonder succes werd geprobeerd de telefoon te ontgrendelen en de daarop opgeslagen gegevens uit te lezen.

25. Op het moment dat de maatregelen door de politie werden genomen, was daarvoor geen bevel van het openbaar ministerie of rechterlijke beschikking uitgevaardigd.

26. Op 31 maart 2021 heeft C. G. bij het Landesverwaltungsgericht Tirol (bestuursrechter in eerste aanleg van de deelstaat Tirol, Oostenrijk) beroep ingesteld tegen de aan hem opgelegde dwangmaatregelen, waarbij hij de inbeslagneming betwistte. De mobiele telefoon werd hem op 20 april 2021 terugbezorgd.

27. C. G. werd op geen enkel tijdstip geïnformeerd dat de politie had geprobeerd de mobiele telefoon te analyseren of uit te lezen, wat pas aan het licht kwam toen de politieagent die de telefoon in beslag had genomen en daarna met de digitale analyse was begonnen, als getuige onder ede werd verhoord. Ook in het strafdossier zijn die pogingen niet gedocumenteerd.

28. Tegen deze achtergrond heeft het Landesverwaltungsgericht Tirol het Hof de volgende prejudiciële vragen voorgelegd:

„1) Moet artikel 15, lid 1 (eventueel gelezen in samenhang met artikel 5), van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136/EG, in het licht van de artikelen 7 en 8 van het [Handvest], aldus worden uitgelegd dat de toegang van overheidsinstanties tot de op mobiele telefoons opgeslagen gegevens op dermate ernstige wijze inbreuk maakt op de door die

artikelen van het Handvest gewaarborgde grondrechten dat die toegang op het gebied van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten moet worden beperkt tot de bestrijding van zware criminaliteit?

2) Moet artikel 15, lid 1, van richtlijn 2002/58, zoals gewijzigd bij richtlijn 2009/136, in het licht van de artikelen 7, 8 en 11 alsook artikel 52, lid 1, van het [Handvest], aldus worden uitgelegd dat het zich verzet tegen een nationale regeling als § 18 juncto § 99, lid 1, [StPO], op grond waarvan veiligheidsdiensten zichzelf in het kader van een strafrechtelijk onderzoek zonder toestemming van een rechterlijke instantie of onafhankelijk bestuursorgaan volledige en ongecontroleerde toegang kunnen verschaffen tot alle op een mobiele telefoon opgeslagen digitale gegevens?

3) Moet artikel 47 van het [Handvest], eventueel gelezen in samenhang met de artikelen 41 en 52 van het Handvest, vanuit het oogpunt van het beginsel van wapengelijkheid (equality of arms) en een doeltreffende voorziening in rechte aldus worden uitgelegd dat het zich verzet tegen een regeling van een lidstaat die, zoals § 18 juncto § 99, lid 1, StPO, toestaat dat een mobiele telefoon digitaal wordt uitgelezen zonder dat de betrokkene daarvan vooraf of op zijn minst na de toepassing van de maatregel in kennis wordt gesteld?”

III. Procedure bij het Hof

29. Het verzoek om een prejudiciële beslissing is op 6 september 2021 ingekomen ter griffie van het Hof.

30. Op 20 oktober 2021 heeft het Hof de verwijzende rechter verzocht te kennen te geven of richtlijn 2016/680 relevant zou kunnen zijn voor de zaak.

31. Op 11 november 2021 heeft de verwijzende rechter geantwoord dat richtlijn 2016/680 in het hoofdgeding moet worden toegepast.

32. De Cypriotische, de Deense, de Duitse, de Estse, de Franse, de Hongaarse, de Ierse, de Nederlandse, de Noorse, de Oostenrijkse, de Poolse en de Zweedse regering en de Europese Commissie hebben schriftelijke opmerkingen ingediend.

33. Ter terechtzitting van 16 januari 2023 zijn, met uitzondering van de Duitse, de Hongaarse en de Poolse regering, degenen die schriftelijke opmerkingen hadden ingediend, alsook de Finse regering verschenen. Al deze interveniënten werden door het Hof verzocht hun argumentatie toe te spitsen op richtlijn 2016/680 en mondeling te antwoorden op bepaalde vragen met betrekking tot deze richtlijn.

IV. Beoordeling

A. Niet-ontvankelijkheid

34. De verwijzende rechter heeft met zijn vragen aanvankelijk alleen verzocht om uitlegging van richtlijn 2002/58. Bijna alle in de procedure interveniërende partijen zijn het er echter over eens dat die richtlijn niet van toepassing is op de onderhavige zaak en een uitlegging ervan derhalve niet noodzakelijk is voor de beslechting van het hoofdgeding.

35. Volgens artikel 3 ervan geldt richtlijn 2002/58 voor „de verwerking van persoonsgegevens in verband met de levering van openbare elektronischecommunicatiediensten over openbare communicatienetwerken in de [Unie], met inbegrip van openbare communicatienetwerken die systemen voor gegevensverzameling en identificatie ondersteunen".

36. Het Hof heeft verklaard dat „[w]anneer de lidstaten […] rechtstreeks maatregelen toepassen die inbreuk maken op het beginsel van de vertrouwelijkheid van elektronische communicatie, zonder dat zij verwerkingsverplichtingen opleggen aan aanbieders van elektronischecommunicatiediensten, […] de bescherming van de gegevens van de betrokken personen niet [wordt] beheerst door richtlijn 2002/58, maar uitsluitend door nationaal recht, behoudens de toepassing van richtlijn [2016/680]".[7]

37. In de onderhavige zaak hebben politiediensten in het kader van een strafrechtelijk onderzoek rechtstreeks geprobeerd om toegang tot gegevens te krijgen. Er was geen sprake van tussenkomst van aanbieders van elektronischecommunicatiediensten of van een aan hen gericht verzoek om persoonsgegevens te verstrekken. Richtlijn 2002/58 is derhalve niet van toepassing.

38. De Unierechtelijke regeling die op deze situatie van toepassing is, is richtlijn 2016/680, waarvan artikel 2, lid 1, voorschrijft dat de richtlijn van toepassing is op de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op het onderzoek van strafbare feiten.

39. Een en ander zou volstaan om te concluderen tot niet-ontvankelijkheid van de door de verwijzende rechter gedane prejudiciële verwijzing, aangezien de Unierechtelijke regeling waarvan hij de uitlegging verlangt niet op de zaak van toepassing is.

40. Artikel 267 VWEU biedt het Hof evenwel de mogelijkheid om, teneinde de nationale rechter van een dienstig antwoord te voorzien, de voorgelegde vragen te herformuleren of te wijzen op andere regels van Unierecht die mogelijk relevant zijn.[8]

41. Het Hof heeft de verwijzende rechter verzocht zich uit te spreken over de eventuele toepasselijkheid van richtlijn 2016/680. De verwijzende rechter is derhalve de gelegenheid geboden om zijn vragen zelf aan te vullen of te herformuleren. In plaats van dat te doen, heeft de verwijzende rechter slechts meegedeeld dat „in casu richtlijn 2016/680 hoe dan ook moet worden geëerbiedigd", zonder echter toe te lichten over welke bepalingen van deze richtlijn hij twijfels heeft of zijn antwoord uit te strekken tot andere overwegingen ten gronde[9].

42. Het Hof heeft bij herhaling verklaard dat „het onontbeerlijk [is] dat, zoals is bepaald in artikel 94, onder c), van het Reglement voor de procesvoering, de verwijzingsbeslissing een uiteenzetting bevat van de redenen die de verwijzende rechter ertoe hebben gebracht om zich over de uitlegging of de geldigheid van een aantal Unierechtelijke bepalingen vragen te stellen alsook het verband tussen die bepalingen en de op het hoofdgeding toepasselijke nationale wettelijke regeling".[10]

7 Arrest van 6 oktober 2020, La Quadrature du Net e.a. (C-511/18, C-512/18 en C-520/18, EU:C:2020:791; hierna: „arrest La Quadrature du Net", punt 103).

8 Zie onder meer arrest van 28 april 2016, Oniors Bio (C-233/15, EU:C:2016:305, punt 30).

9 Het Hof heeft zich gedwongen gezien zich tot partijen te wenden met het verzoek om aan te geven „welke bepalingen in [hun] opvatting de relevante bepalingen van richtlijn 2016/680 zijn in het licht waarvan het Hof, in voorkomend geval, de drie prejudiciële vragen van de verwijzende rechter dient te herformuleren" (vierde bij de mondelinge behandeling gestelde vraag).

10 Arrest van 6 oktober 2021, Consorzio Italian Management en Catania Multiservizi (C-561/19, EU:C:2021:799, punt 69).

43. Uit het bovenstaande blijkt duidelijk dat de voorwaarden van artikel 94 van het Reglement voor de procesvoering in deze verwijzing niet zijn vervuld. Hoewel het Hof in dit opzicht een zekere flexibiliteit tentoonspreidt, moet de samenwerking met de verwijzende rechter wederkerig zijn: als de verwijzende rechter – zonder rechtvaardiging – niet meewerkt door zijn twijfels over de uitlegging van het Unierecht dat hij van toepassing acht (in casu richtlijn 2016/680) niet uiteen te zetten, lijkt het mij logisch om het verzoek om een prejudiciële beslissing niet-ontvankelijk te verklaren. [11]

44. Daar komt bij dat de verwijzende rechter:

– de aard van de door de politiediensten gedane poging tot verwerking of van de specifiek gezochte persoonsgegevens niet nader heeft gespecificeerd. In eerste instantie lijkt hij aan te geven dat het enkel gaat om verbindingsgegevens (dat wil zeggen verkeers- en locatiegegevens), maar vervolgens sluit hij niet uit dat met het ontgrendelen van de telefoon toegang wordt verschaft tot „alle […] opgeslagen digitale gegevens" [12] en zelfs tot de inhoud van via die telefoon uitgewisselde communicatie en elektronische berichten [13];

– zowel de inbeslagneming van de telefoon als (de poging tot) het verkrijgen van toegang tot de op die telefoon opgeslagen gegevens en het daaropvolgende „uitlezen" (*Auswertung*) ervan, dat wil zeggen het analyseren en lezen ervan, aan de orde stelt. Dat uitlezen, voegt hij eraan toe, „betekent […] de compleet ongecontroleerde toegang tot de volledige digitale communicatie van de betrokkene", waardoor „een zeer gedetailleerd en diepgaand beeld van bijna alle gebieden van de persoonlijke levenssfeer [kan] worden gereconstrueerd".

45. In deze omstandigheden zou het Hof, in plaats van de vragen van de verwijzende rechter te *herformuleren*, de prejudiciële verwijzing – die bovendien deels op hypothetische overwegingen veeleer dan op aangetoonde feiten is gebaseerd – *geheel opnieuw formuleren*. En dit alles – het zij nogmaals gezegd – nadat de verwijzende rechter de mogelijkheid was geboden om zijn vragen zelf aan te vullen of te herformuleren.

46. Ik stel daarom voor om de prejudiciële verwijzing niet-ontvankelijk te verklaren, zoals door diverse van de interveniërende lidstaten is bepleit.

47. Ook de ter terechtzitting genoemde omstandigheid dat er voor de verwijzende rechter geen daadwerkelijk geschil meer bestaat dat een uitlegging van een Unierechtelijke regeling vereist, leidt tot de conclusie dat de prejudiciële verwijzing niet-ontvankelijk is.

48. De Oostenrijkse regering (waar de bij het onderzoek betrokken politiediensten onder ressorteren) erkent dat het optreden van die diensten onrechtmatig was en inbreuk heeft gemaakt op de rechten van de betrokkene. Aangezien de door verzoeker bij de bestuursrechter ingestelde vordering volgens de verwijzingsbeslissing juist gericht was tegen de politiemaatregelen die de verwerende overheidsinstantie onrechtmatig acht, is er van het aan de verwijzende rechter voorgelegde geschil geen sprake meer.

[11] Ik ben het op dit punt eens met de Franse regering (punten 36-41 van haar schriftelijke opmerkingen).

[12] Zie de tweede prejudiciële vraag.

[13] Zo verklaart de verwijzende rechter dat „wat de verkeersgegevens betreft, […] bijna alle contacten [kunnen] worden gereconstrueerd qua frequentie, tijdstip en duur van de communicatie, en wat de communicatie via sms en andere messengerdiensten betreft […] tevens de inhoud ervan [kan] worden gereconstrueerd[, alsmede dat] ook de analyse van opgeslagen foto's en de browsergeschiedenis […] een zeer intiem inzicht in het privéleven van de betrokkene [geeft]".

49. Hoe dan ook zal ik mij, voor het geval het Hof mijn standpunt niet zou delen, subsidiair buigen over de wezenlijke problemen die ten grondslag liggen aan de prejudiciële vragen.

50. Alvorens dat te doen, acht ik het echter noodzakelijk om een andere, door enkele interveniënten in de procedure opgeworpen grond voor niet-ontvankelijkheid [14] uit te sluiten. In hun optiek is richtlijn 2016/680, die de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens regelt, niet van toepassing op gevallen als het onderhavige, waarin er geen sprake van *verwerking* zou zijn, doch louter van een *poging om zich toegang te verschaffen* tot gegevens die uiteindelijk niet konden worden verkregen.

51. Volgens de Commissie daarentegen verlangt het nuttig effect van richtlijn 2016/680 dat het Hof opteert voor een uitlegging van het voorwerp van die richtlijn die zich niet beperkt tot de verwerking van gegevens in strikte zin, maar zich ook uitstrekt tot kwesties die daar rechtstreeks mee verband houden. Een van die kwesties is de poging om zich toegang te verschaffen tot gegevens waarvan de verwerking werd beoogd. [15]

52. In mijn ogen is de toepasselijkheid van richtlijn 2016/680 op de aan de orde zijnde situatie, zonder dat de grenzen van de werkingssfeer ervan hoeven te worden opgerekt [16], niet zozeer gerechtvaardigd omdat de mobiele telefoon in beslag is genomen [17], als wel vanwege de daaropvolgende maatregelen die de politiediensten hebben genomen om bepaalde persoonsgegevens van de betrokkene te verkrijgen, met welk doel zij hebben getracht de telefoon te ontgrendelen en zich toegang tot de inhoud ervan te verschaffen.

53. Een van de in artikel 3, punt 2, van richtlijn 2016/680 als „verwerking" gedefinieerde bewerkingen is het „op andere wijze ter beschikking stellen" van persoonsgegevens in het kader van een strafrechtelijk onderzoek. Ik ben van mening dat wanneer de politiedienst een telefoon waarop persoonsgegevens worden bewaard in beslag neemt en de telefoon manipuleert om die gegevens daaraan te onttrekken, hij een „verwerking" initieert, ook als die poging mislukt om technische redenen die verband houden met de cryptografische beveiliging van de telefoon.

54. Een mislukte poging om zich in het kader van een strafrechtelijk onderzoek toegang te verschaffen tot persoonsgegevens die op een mobiele telefoon worden bewaard, valt onder richtlijn 2016/680, om soortgelijke redenen als die welke het Hof ertoe hebben gebracht om richtlijn 2002/58 van toepassing te verklaren op de (eveneens mislukte) *poging* om rechterlijke toestemming te verkrijgen voor het verkrijgen van toegang tot bepaalde gegevens van een onderzochte persoon die in bezit van een aanbieder van elektronischecommunicatiediensten waren [18].

[14] Concreet gaat het om de Franse, de Nederlandse, de Noorse en de Oostenrijkse regering.

[15] Volgens de Commissie „is het niet relevant of de pogingen zijn bekroond met succes of niet. Dat zich technische moeilijkheden voordoen die het welslagen van de pogingen tot het verkrijgen van toegang belemmeren, is een omstandigheid die vooraf niet bekend kan zijn en die niet afdoet aan de risico's voor de bescherming van persoonsgegevens."

[16] Met name het inroepen van de artikelen 27 en 28 van richtlijn 2016/680, zoals de Commissie heeft voorgesteld in haar schriftelijke opmerkingen, lijkt mij niet nodig. De door artikel 27 ingevoerde „gegevensbeschermingseffectbeoordeling" heeft in algemene zin betrekking op „een soort verwerking", en niet op specifieke of individuele verwerkingen. Dit kan worden opgemaakt uit overweging 58 van richtlijn 2016/680: „Effectbeoordelingen dienen relevante systemen en procedures van verwerkingsactiviteiten te bestrijken, maar *geen individuele gevallen*" (cursivering van mij). Ter terechtzitting heeft de Commissie haar beroep op beide bepalingen genuanceerd; zij zou die slechts zou hebben aangehaald om te benadrukken dat richtlijn 2016/680 ook ziet op situaties die voorafgaan aan de eigenlijke verwerking van gegevens.

[17] Richtlijn 2016/680 regelt niet de inbeslagneming van telefoons als bewijsmiddel in het kader van een strafrechtelijk onderzoek.

[18] Arrest van 2 oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788).

55. Indien de verwijzende rechter zich zou moeten uitspreken over de onrechtmatigheid van het politieoptreden (die, zoals ik reeds heb uiteengezet, door de Oostenrijkse regering is erkend), zou zijn beoordeling in die context kunnen afhangen van de rechtmatigheid van het daarmee nagestreefde doel, ongeacht of de maatregel met succes is uitgevoerd of enkel – zonder resultaat – is geïnitieerd.

B. Ten gronde

1. Eerste prejudiciële vraag

56. De verwijzende rechter wenst te vernemen of ingevolge artikel 15, lid 1 (eventueel gelezen in samenhang met artikel 5), van richtlijn 2002/58 en in het licht van de artikelen 7 en 8 van het Handvest „de toegang van overheidsinstanties tot de op mobiele telefoons opgeslagen gegevens op dermate ernstige wijze inbreuk maakt op de door die artikelen van het Handvest gewaarborgde grondrechten dat die toegang op het gebied van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten moet worden beperkt tot de bestrijding van zware criminaliteit".

57. Indien het verzoek ontvankelijk zou worden verklaard, zou de niet-toepasselijkheid van richtlijn 2002/58 vereisen dat de eerste vraag wordt geherformuleerd, zodat het Hof in zijn antwoord een uitlegging van richtlijn 2016/680 kan geven.

58. Dat antwoord zou achtereenvolgens moeten verduidelijken of er in gevallen als het onderhavige kan worden gesproken van inmenging, en zo ja of richtlijn 2016/680 vereist dat de toegang tot gegevens wordt beperkt tot gevallen waarin het doel van die toegang de bestrijding van ernstige criminaliteit is.

59. Gegevensverwerkingen kunnen per definitie afbreuk doen aan het recht op eerbiediging van het privéleven (artikel 7 van het Handvest) en het recht op bescherming van persoonsgegevens (artikel 8 van het Handvest). Bijgevolg moeten overheidsinstanties voldoen aan de voorwaarden van artikel 52, lid 1, van het Handvest om hun inmenging in de uitoefening van deze grondrechten te rechtvaardigen.

60. De inmenging in de door de artikelen 7 en 8 van het Handvest beschermde rechten zal des te groter zijn wanneer met die inmenging a) wordt beoogd toegang te verkrijgen tot gegevens van gevoelige aard die gewoonlijk op mobiele telefoons worden vastgelegd en waarvan de kennis facetten van het leven van de bezitters ervan kan onthullen die moeten worden beschermd tegen kennisneming door derden, en b) toegang tot de inhoud van communicatie mogelijk wordt gemaakt.

61. Vanuit een algemeen perspectief kan richtlijn 2016/680, gelet op de inhoud ervan, echter niet aldus worden uitgelegd dat de daaronder vallende gegevensverwerkingen zijn beperkt tot uitsluitend gevallen waarin het doel van die toegang de bestrijding van ernstige criminaliteit is.

62. Richtlijn 2016/680 ziet op elke, door de bevoegde autoriteiten gedane verwerking [19] van persoonsgegevens met het oog op het voorkomen, onderzoeken, opsporen of vervolgen van *alle soorten* strafbare feiten.

63. Uit de door richtlijn 2016/680 vastgestelde beginselen inzake de verwerking van persoonsgegevens voor die doelen (artikel 4) en uit de voorwaarden voor de rechtmatigheid van de verwerking (artikel 8) volgt niet dat gegevens in de regel alleen kunnen worden verwerkt in gevallen van ernstige criminaliteit.

64. Een dergelijke beperking tot gevallen waarin het doel de bestrijding van ernstige criminaliteit is, kan ook niet worden gebaseerd op de stelling dat de rechtspraak van het Hof betreffende richtlijn 2002/58 [20] zonder meer kan worden geëxtrapoleerd naar situaties als die in casu.

65. Deze extrapolatie gaat mijns inziens niet op omdat, onverminderd hetgeen ik hierna zal uiteenzetten, die rechtspraak betrekking heeft op het systematisch op algemene en willekeurige basis bewaren van persoonsgegevens van een generieke en onbepaalde groep door aanbieders van elektronischecommunicatiediensten. De omvang van de inmenging die dat type bewaring met zich meebrengt voor de samenleving als geheel, verklaart waarom het Hof zich bijzonder streng heeft getoond bij het verbieden ervan en het vaststellen van uitzonderingen op dat verbod.

66. Anders ligt het wanneer de beoogde toegang geen betrekking heeft op de hele bevolking of grote groepen ervan (dat wil zeggen persoonsgegevens van een generieke en onbepaalde groep), maar op informatie die op één enkele mobiele telefoon is opgeslagen in het kader van één enkel strafrechtelijk onderzoek, waarop specifiek richtlijn 2016/680 betrekking heeft.

67. Richtlijn 2016/680 ziet namelijk juist op de verwerking van gegevens door de autoriteiten die bevoegd zijn voor het voorkomen, onderzoeken, opsporen of vervolgen van strafbare feiten; het gaat hier om alle soorten strafbare feiten, niet alleen om ernstige strafbare feiten.

68. Bovendien zou het, zoals enkele interveniënten in de prejudiciële procedure hebben opgemerkt, in de lidstaten onmogelijk zijn om richtlijn 2016/680 uniform toe te passen doordat die richtlijn geen aanwijzingen bevat inzake de ernst van de strafbare feiten. De ernst die aan een strafbare gedraging wordt toegekend, kan immers aanmerkelijk verschillen tussen de lidstaten. [21]

69. Richtlijn 2016/680 stelt derhalve niet als rechtmatigheidsvoorwaarde dat de in die richtlijn geregelde verwerking van persoonsgegevens alleen kan worden verricht met het oog op de bestrijding van ernstige criminaliteit.

70. Het voorgaande neemt niet weg dat de verwerking van gegevens die de bevoegde autoriteiten overeenkomstig richtlijn 2016/680 willen uitvoeren, op grond van het evenredigheidsbeginsel en per individueel geval in verhouding moet staan tot a) de aard van de vervolgde strafbare feiten en b) de soort verwerkte persoonsgegevens.

[19] Wat „bewerkingen” kunnen inhouden is in artikel 3, punt 2, van richtlijn 2016/680 zeer ruim opgevat. Zie de weergave ervan in punt 9 van deze conclusie.

[20] Arrest La Quadrature du Net, alsmede arresten van 21 december 2016, Tele2 Sverige en Watson e.a. (C-203/15 en C-698/15, EU:C:2016:970; hierna: „arrest Tele2 Sverige en Watson”); 2 oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788); 6 oktober 2020, Privacy International (C-623/17, EU:C:2020:790), en 2 maart 2021, Prokuratuur (Voorwaarden voor toegang tot elektronischecommunicatiegegevens) (C-746/18, EU:C:2021:152; hierna: „arrest Prokuratuur”).

[21] De Franse regering noemt als voorbeeld de strafbare feiten van het bezit van en de handel in drugs, waarvan de ernst in het Oostenrijkse strafrecht anders wordt gekwalificeerd dan in het Franse. In diezelfde zin heeft ook de Zweedse regering zich uitgesproken.

71. In die zin ben ik het eens met een aantal argumenten van de Duitse regering inzake de beperking van de toegang tot de gegevens van in beslag genomen telefoons, voor zover daarmee een volledig profiel van de persoonlijkheid van de bezitters ervan kan worden vastgesteld aan de hand van de digitale inhoud van de telefoon. Volgens de Duitse regering moet de toegang worden beperkt tot gegevens die in een specifiek geval noodzakelijk zijn als bewijsmiddel, en is het mogelijk niet passend om toegang te verlenen in het licht van factoren als „de minder ernstige aard van het onderzochte strafbare feit of de zwakke bewijskracht van de gegevens die men beoogt te verkrijgen” [22].

72. In abstracto is volgens richtlijn 2016/680 de toegang tot op een mobiele telefoon opgeslagen persoonsgegevens met het oog op het onderzoek van gedragingen die kunnen worden gekwalificeerd als algemene of gewone criminaliteit, dus niet per se onrechtmatig. Of die toegang in concreto is toegestaan, zal de bevoegde autoriteit per geval moeten beoordelen, rekening houdend met de noodzaak om toegang te krijgen en het evenredigheidscriterium waarnaar ik hierboven heb verwezen.

73. Dit kan mijns inziens worden afgeleid uit de bepalingen van richtlijn 2016/680 die zien op de voorwaarden voor de geldigheid van de verwerking van persoonsgegevens in het kader van de bestrijding van criminaliteit:

– artikel 4, lid 1, onder a), krachtens hetwelk de gegevens „rechtmatig […] worden verwerkt”;

– artikel 8, lid 1, waarin wordt bepaald dat de verwerking *noodzakelijk* moet zijn en moet zijn gebaseerd op het Unierecht of het lidstatelijke recht.

2. Tweede prejudiciële vraag

74. Met zijn tweede vraag wenst de verwijzende rechter te vernemen of artikel 15, lid 1, van richtlijn 2002/58, gelezen in samenhang met de artikelen 7, 8 en 11 alsook artikel 52, lid 1, van het Handvest, „zich verzet tegen een nationale regeling als § 18 juncto § 99, lid 1, [StPO], op grond waarvan veiligheidsdiensten zichzelf in het kader van een strafrechtelijk onderzoek zonder toestemming van een rechterlijke instantie of onafhankelijk bestuursorgaan volledige en ongecontroleerde toegang kunnen verschaffen tot alle op een mobiele telefoon opgeslagen digitale gegevens”.

75. De formulering van de vraag draagt een zekere ambiguïteit in zich. De verwijzende rechter:

– erkent dat § 110, lid 2, StPO bepaalt dat voor inbeslagnemingen van voorwerpen in beginsel de toestemming van het openbaar ministerie is vereist. Alleen in de in § 110, lid 3, vermelde buitengewone gevallen (waarvan er in casu geen enkel aan de orde lijkt te zijn) kunnen politiediensten voorwerpen zonder die toestemming in beslag nemen;

– voegt daar echter aan toe dat het analyseren van op mobiele telefoons opgeslagen gegevens „[in de StPO] niet eensluidend is geregeld” en dat veiligheidsdiensten een dergelijke analyse op eigen initiatief zouden kunnen verrichten zonder voorafgaande toestemming.

[22] Schriftelijke opmerkingen van de Duitse regering, punt 20.

76. De Oostenrijkse regering hanteert een uitlegging van de nationale regeling die zich niet verdraagt met die welke in de verwijzingsbeslissing wordt uiteengezet. In het bijzonder stelt de Oostenrijkse regering dat zowel de inbeslagneming van de telefoon (behalve in noodgevallen) als het analyseren van de daarop opgeslagen gegevens naar nationaal recht slechts mogelijk is met toestemming van het openbaar ministerie.[23] Zonder bevel van het openbaar ministerie is het uitlezen door de politie van de op die telefoon bewaarde gegevens onrechtmatig.

77. Het is de taak van de verwijzende rechter om de bepalingen van de nationale regeling uit te leggen. In het kader van de procedure van artikel 267 VWEU is het Hof niet bevoegd om dat te doen, maar staat het uitsluitend aan de verwijzende rechter om de juiste strekking van de nationale wettelijke en bestuursrechtelijke bepalingen vast te stellen.[24]

78. Zonder mij te willen mengen in het debat over de uitlegging van het Oostenrijkse recht, schijnt het mij toe dat de gevolgtrekking van de verwijzende rechter moeilijk kan worden gemaakt op basis van alleen de door hem genoemde bepalingen (§ 18 StPO juncto § 99, lid 1, van die wet). Dat is echter, zoals is aangegeven, uitsluitend een zaak van die rechter.

79. Hoe het ook zij, de verwijzende rechter is van oordeel dat de rechtspraak van het arrest Prokuratuur[25], die ziet op de voorafgaande toetsing van de toegang tot bewaarde gegevens door een rechter of een onafhankelijke entiteit, kan worden toegepast op een situatie als die welke in casu aan de orde is.

80. Volgens de Nederlandse regering moet die rechtspraak daarentegen worden begrepen in de context van een nationale regeling die de bevoegde autoriteiten *algemene* toegang tot *alle* bewaarde verkeers- en locatiegegevens verleende. Dit zou een verklaring vormen voor de voorwaarde van voorafgaande rechterlijke toestemming, die in het geval van toegang tot gegevens op één enkele mobiele telefoon echter mogelijkerwijs niet gerechtvaardigd is.

81. In diezelfde zin betoogt de Noorse regering dat onder de vele waarborgen waarin richtlijn 2016/680 voorziet[26], die van de noodzaak van voorafgaande toestemming van een rechterlijke instantie of onafhankelijk bestuursorgaan niet uitdrukkelijk wordt vermeld.

82. De Commissie gaat ervan uit dat de bepalingen van richtlijn 2016/680 moeten worden uitgelegd in het licht van het Handvest en betoogt dat de in artikel 8, lid 1, van die richtlijn aan de lidstaten opgelegde verplichting (voorwaarden voor de rechtmatigheid van de verwerking) met zich meebrengt dat de door de artikelen 7 en 8 van het Handvest gewaarborgde grondrechten moeten worden geëerbiedigd.

[23] Punt 19 van de schriftelijke opmerkingen van de Oostenrijkse regering. Daarin verwijst zij naar de uitspraak van het Oberste Gerichtshof (hoogste federale rechter in civiele en strafzaken, Oostenrijk) van 13 oktober 2020 (zaak 11 Os 56/20z), waarin het zonder toestemming van het openbaar ministerie analyseren van de gegevens op een mobiele telefoon door de recherche wordt aangemerkt als onrechtmatig daar er sprake is van een schending van de subjectieve rechten van de betrokkene.

[24] Zie onder meer arrest van 28 april 2022, SeGEC e.a. (C-277/21, EU:C:2022:318, punt 21).

[25] Arrest Prokuratuur, punt 51: „[H]et [is] van wezenlijk belang dat de toegang van de bevoegde nationale instanties tot de bewaarde gegevens wordt onderworpen aan voorafgaande toetsing door een rechterlijke instantie of door een onafhankelijke bestuurlijke entiteit, en dat deze rechterlijke instantie of deze entiteit haar beslissing geeft op een met redenen omkleed verzoek van deze instanties dat met name wordt ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten."

[26] Naast de waarborgen van de artikelen 4 en 8 zijn er ook nog de waarborgen die zijn vervat in de hoofdstukken III („Rechten van de betrokkene"), IV („Verwerkingsverantwoordelijke en verwerker"), VI („Onafhankelijke toezichthoudende autoriteiten") en VIII („Beroep, aansprakelijkheid en straffen").

83. Ik ben het eens met de Commissie dat de nationale wetgever die bepalingen van het Handvest in acht moet nemen en de voorschriften moet vaststellen die nodig zijn om te waarborgen dat de toegang tot gegevens in elk afzonderlijk geval gerechtvaardigd is en beperkt blijft tot wat strikt noodzakelijk en evenredig is.

84. Die nationale voorschriften hoeven echter niet specifiek te zijn voor de toegang tot persoonsgegevens die, zoals in casu het geval is, zijn opgeslagen op een mobiele telefoon, maar kunnen die zijn waarin het nationale recht in algemene zin voorziet ter zake van het verkrijgen van bewijs.

85. In dit verband heb ik reeds melding gemaakt van punt 103 van het arrest La Quadrature du Net met betrekking tot maatregelen van de lidstaten die afbreuk doen aan de vertrouwelijkheid van elektronische communicatie zonder dat verwerkingsverplichtingen worden opgelegd aan aanbieders van elektronischecommunicatiediensten. [27]

86. Het is dus niet nodig om uit richtlijn 2016/680 *specifieke* procedurele regels af te leiden waarmee de rechtmatigheid van de toegang tot op een mobiele telefoon opgeslagen gegevens wordt gewaarborgd. [28] Van toepassing zijn de nationale regels voor het verrichten van doorzoekingen en inbeslagnemingen in strafrechtelijke onderzoeken. [29]

87. Dat naar nationaalrechtelijke bepalingen wordt verwezen om de rechtmatigheid van de toegang overeenkomstig richtlijn 2016/680 te waarborgen, strookt bovendien met de rechtspraak van het EHRM. Juist in een zaak waarbij de Republiek Oostenrijk betrokken was en die betrekking had op artikel 8 EVRM (recht op eerbiediging van het privéleven, het familie- en gezinsleven, de woning en de communicatie) heeft het EHRM geoordeeld dat de Oostenrijkse wetgeving inzake de inbeslagneming van voorwerpen – en in het bijzonder van documenten – ook van toepassing is op de doorzoeking en inbeslagneming van gegevens die worden bewaard op informatiedragers. [30]

88. Indien – zoals de Oostenrijkse regering onder aanhaling van de rechtspraak van het Oberste Gerichtshof betoogt – de politiediensten zonder toestemming van het openbaar ministerie zich geen toegang kunnen verschaffen tot gegevens die op een bepaalde mobiele telefoon worden bewaard, verliest de tweede prejudiciële vraag goeddeels haar zin.

89. Hoe dan ook kan bij de beantwoording van die vraag niet worden uitgesloten dat de toegang tot persoonsgegevens op de in beslag genomen telefoon zal leiden tot de reconstructie van „een zeer gedetailleerd en diepgaand beeld van bijna alle gebieden van de persoonlijke levenssfeer" van de betrokkene [31]. Als dit het geval is, moeten de politiediensten beschikken over de in het arrest Prokuratuur genoemde voorafgaande toestemming.

[27] Zie punt 36 van deze conclusie.

[28] Een goed voorbeeld van de moeilijkheden van een dergelijke aanpak zijn de inspanningen van de Commissie in de punten 34-39 van haar schriftelijke opmerkingen om bij te dragen aan het vaststellen van duidelijke en nauwkeurige regels voor het afbakenen van de grenzen en het bieden van passende waarborgen waar het gaat om de toegang tot gegevens op een mobiele telefoon.

[29] Deze regels vallen, zoals onder meer de Deense en de Ierse regering opmerken, buiten de werkingssfeer van het Unierecht maar kunnen dienen om te voldoen aan een vereiste dat voortvloeit uit dat recht.

[30] Arrest van het EHRM van 16 oktober 2007, Wieser en Bicos Beteiligungen tegen Oostenrijk (CE:ECHR:2007:1016JUD007433601, § 54): „[T]he 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."

[31] Zie de opmerkingen van de verwijzende rechter die zijn weergegeven in punt 44 van deze conclusie.

90. Op het eerste gezicht zou het kunnen lijken dat deze vaststelling niet valt te rijmen met het feit dat, zoals ik hierboven heb verdedigd, richtlijn 2002/58 (die wordt uitgelegd in het arrest Prokuratuur) niet toepasselijk is op de aan de orde zijnde situatie. Ik ben evenwel van mening dat de ratio van dat arrest steun biedt voor dezelfde oplossing.

91. In het geding dat heeft geleid tot het arrest Prokuratuur ging het, ofschoon de toegang werd verkregen door het opvragen van (meta)gegevens van aanbieders van elektronischecommunicatiediensten, om één enkel strafrechtelijk onderzoek dat gericht was tegen een specifieke persoon. Het doel was om „gegevens betreffende meerdere telefoonnummers en verschillende [International Mobile Equipment Identity (internationaal identificatienummer voor mobiele apparaten)]-codes” [32] te verzamelen.

92. In het arrest Prokuratuur kunnen mijns inziens twee dimensies worden onderscheiden: a) de vraag of de algemene regeling van een lidstaat inzake de algemene en ongedifferentieerde bewaring van gegevens die in het bezit zijn van dienstenaanbieders en de latere toegang tot die gegevens zich verdraagt met het Unierecht, en b) de vraag of er in een individueel geval een voorafgaande toetsing van de toegang tot dergelijke metagegevens moet plaatsvinden wanneer deze het mogelijk maken om een nauwkeurig beeld van de persoonlijke levenssfeer van een persoon op te stellen.

93. De omstandigheid dat in casu de gegevens die een beeld van de persoonlijke levenssfeer geven niet in het bezit van de dienstenaanbieders zijn en worden verkregen (of daar althans een poging toe wordt gedaan) via één enkele in beslag genomen telefoon, lijkt mij van secundair belang vergeleken met de in het arrest Prokuratuur voorgestane ratio die ten grondslag ligt aan het vereiste van voorafgaande toetsing.

94. Deze voorafgaande toetsing vindt uiteindelijk haar grond in de bescherming die wordt gewaarborgd door de artikelen 7 en 8 van het Handvest. De instantie die de toetsing uitvoert, moet in staat zijn om „een juist evenwicht te verzekeren tussen, enerzijds, de belangen die verband houden met de behoeften van het onderzoek in het kader van de bestrijding van criminaliteit, en, anderzijds, de fundamentele rechten op eerbiediging van de persoonlijke levenssfeer en op bescherming van de persoonsgegevens van de personen op wier gegevens de toegang betrekking heeft” [33].

3. Derde prejudiciële vraag

95. Met zijn derde vraag wenst de verwijzende rechter te vernemen of artikel 47 van het Handvest (eventueel gelezen in samenhang met de artikelen 41 en 52 ervan) zich verzet tegen een regeling als de Oostenrijkse [34], die „toestaat dat een mobiele telefoon digitaal wordt uitgelezen zonder dat de betrokkene daarvan vooraf of op zijn minst na de toepassing van de maatregel in kennis wordt gesteld”.

[32] Arrest Prokuratuur, punt 17.

[33] Arrest Prokuratuur, punt 52.

[34] De verwijzende rechter verwijst opnieuw naar § 18 StPO juncto § 99 StPO.

96. Mijns inziens is de in die bewoordingen geformuleerde vraag mogelijk niet nodig voor de beslechting van het geding, aangezien de betrokkene het in artikel 47 van het Handvest gewaarborgde recht heeft kunnen uitoefenen door de verwijzende rechter te verzoeken de handelingen van de politie met de in beslag genomen telefoon, die ook het latere (en mislukte) uitlezen van de daarop bewaarde gegevens omvatten, nietig te verklaren.

97. In verband met de twee relevante momenten van het politieoptreden moet onderscheid worden gemaakt tussen:

– wat de inbeslagneming van de telefoon zelf betreft, de informatie in het dossier waaruit blijkt dat de betrokkene daar kennis van had en weigerde de ontgrendelingscode aan de politie te verstrekken nadat hij was aangehouden;

– wat de poging tot analyse van de gegevens betreft, het feit – waar alles op lijkt te wijzen – dat de verwerkingsverantwoordelijke de betrokkene niet van deze handeling in kennis heeft gesteld, ofschoon de Oostenrijkse regering verklaart dat de betrokkene bekend was met een verslag waarin het optreden van de recherche ten aanzien van de telefoon was vastgelegd [35].

98. Rond het uitlezen van de gegevens en de kennisneming daarvan door de betrokkene bestaan dus nog steeds bepaalde onzekerheden die, zoals ik reeds heb opgemerkt, door de verwijzende rechter hadden moeten worden verduidelijkt in zijn verwijzingsbeslissing en die een nuttig antwoord op de derde vraag in de weg staan.

99. Niettemin zal ik mij over deze vraag uitspreken voor het geval het Hof niet van oordeel is dat deze vraag niet ontvankelijk is. In dat geval zou die vraag, gelet op de niet-toepasselijkheid van richtlijn 2002/58, moeten worden geherformuleerd in het licht van richtlijn 2016/680, waarvan de artikelen 13, 15 en 54 de elementen bevatten voor de beantwoording ervan.

100. Ingevolge richtlijn 2016/680 is de informatie over de verwerking van gegevens van de betrokkene die aan hem moet worden verstrekt, die welke onder meer nodig is om a) een klacht in te dienen bij de toezichthoudende autoriteit [artikel 13, lid 1, onder d)], en b) een doeltreffende voorziening in rechte in te stellen in geval van een schending van de door richtlijn 2016/680 gewaarborgde rechten, onverminderd andere mogelijkheden van administratief of buitengerechtelijk beroep (artikel 54).

101. Niet vergeten mag echter worden dat zowel artikel 13, lid 3, als artikel 15, lid 1, van richtlijn 2016/680 de lidstaten toestaat wettelijke maatregelen te treffen om:

– de verstrekking van de in artikel 13, lid 2, bedoelde informatie aan de betrokkene uit te stellen, te beperken of achterwege te laten;

– het inzagerecht van de betrokkene geheel of gedeeltelijk te beperken, voor zover en zolang die volledige of gedeeltelijke beperking een noodzakelijke en evenredige maatregel is om – onder meer – belemmering van officiële of gerechtelijke onderzoeken of procedures te voorkomen of nadelige gevolgen voor het onderzoek van strafbare feiten te voorkomen [36].

[35] Punt 37 van de schriftelijke opmerkingen van de Oostenrijkse regering.

[36] Zie in dit verband arrest Tele2 Sverige en Watson, punt 121. De daarin ontwikkelde rechtspraak van het Hof betreffende richtlijn 2002/58 kan ook worden toegepast op richtlijn 2016/680 waar het gaat om het waarborgen van de rechterlijke bescherming van de rechten van personen van wie gegevens worden verwerkt.

102. Hoe dan ook is de rechtmatigheid van de verwerking van gegevens niet afhankelijk van de naleving door de bevoegde autoriteiten van de (latere) verplichtingen die hun door artikel 13 van richtlijn 2016/680 worden opgelegd, maar van de rechtmatigheid van het doel waarvoor de verwerking plaatsvond, dus van de vraag of die bestuursorganen gemachtigd waren om de persoonsgegevens te verwerken.

103. Vanuit dit oogpunt is er op zichzelf geen verband tussen het feit dat de betrokkene al dan niet op de hoogte is gesteld van de pogingen om toegang tot de op de in beslag genomen telefoon opgeslagen gegevens te krijgen en de materiële rechtmatigheid van het politieoptreden. Dat het gedrag van de verwerkingsverantwoordelijke mogelijkerwijs niet strookt met de hem bij artikel 13 van richtlijn 2016/680 opgelegde verplichtingen, kan andere gevolgen hebben, maar heeft – zoals gezegd – geen invloed op de rechtmatigheid of onrechtmatigheid van de verwerking zelf.

104. Het staat aan de verwijzende rechter om na te gaan of de nationale regeling de doeltreffende uitoefening van de genoemde rechten door de betrokkene mogelijk maakt.

V. Conclusie

105. Gelet op een en ander geef ik het Hof in overweging om het verzoek om een prejudiciële beslissing van het Landesverwaltungsgericht Tirol niet-ontvankelijk te verklaren.

Subsidiair stel ik voor om dat verzoek te beantwoorden als volgt:

„1) Artikel 4, lid 1, onder a), en artikel 8, lid 1, van richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van kaderbesluit 2008/977/JBZ van de Raad, gelezen in samenhang met de artikelen 7, 8 en 52 van het Handvest van de grondrechten van de Europese Unie,

moeten aldus worden uitgelegd dat

de toegang van overheidsinstanties tot op een mobiele telefoon opgeslagen persoonsgegevens met het oog op de verwerking ervan, in het kader van een strafrechtelijk onderzoek niet is beperkt tot gevallen waarin het doel van die toegang de bestrijding van ernstige criminaliteit is.

De toegang moet in elk afzonderlijk geval gerechtvaardigd zijn en moet beperkt blijven tot wat strikt noodzakelijk en evenredig is, hetgeen afhankelijk is van de aard van de vervolgde strafbare feiten en de persoonsgegevens waarop de beoogde toegang betrekking heeft.

De politiediensten mogen zich in het kader van een strafrechtelijk onderzoek niet op eigen initiatief en zonder voorafgaande toestemming van een rechterlijke instantie volledige en ongecontroleerde toegang tot alle op een mobiele telefoon opgeslagen gegevens verschaffen wanneer uit die gegevens een nauwkeurig beeld van de persoonlijke levenssfeer van een persoon kan worden verkregen.

2) De artikelen 13, 15 en 54 van richtlijn 2016/680, gelezen in samenhang met de artikelen 47 en 52 van het Handvest,

moeten aldus worden uitgelegd dat

de bezitter van een mobiele telefoon, onverminderd de beperkingen die zijn toegestaan door artikel 15, lid 1, van richtlijn 2016/680 of andere mogelijkheden van administratief of buitengerechtelijk beroep, in kennis moet worden gesteld van de verwerking door de betreffende instanties van de op die telefoon opgeslagen persoonsgegevens op het tijdstip dat en de wijze die nodig zijn om de uitoefening van zijn recht op een doeltreffende voorziening in rechte tegen een eventuele schending van de door richtlijn 2016/680 verleende rechten te waarborgen."