Rättsfallssamlingen

FÖRSLAG TILL AVGÖRANDE AV GENERALADVOKAT
MANUEL CAMPOS SÁNCHEZ-BORDONA
föredraget den 20 april 2023 [1]

Mål C-548/21

C. G.
mot
Bezirkshauptmannschaft Landeck

(begäran om förhandsavgörande från Landesverwaltungsgericht Tirol (Regionala förvaltningsdomstolen i Tyrolen, Österrike))

”Begäran om förhandsavgörande – Telekommunikation – Skydd av personuppgifter – Direktiv (EU) 2016/680 – Brottmålsförfarande – Försök från offentliga myndigheters sida att utan tillstånd från domstol eller oberoende administrativ myndighet få tillgång till uppgifter som finns lagrade i en mobiltelefon”

1. Begäran om förhandsavgörande avser i huvudsak de villkor som polismyndigheterna måste rätta sig efter för att få tillgång till uppgifter som lagrats i en persons mobiltelefon när personen är föremål för en brottsutredning.

2. Som jag kommer att försöka förklara är begäran om förhandsavgörande behäftad med väsentliga brister vad gäller frågan huruvida den kan tas upp till sakprövning. Om domstolen trots allt beslutar att pröva begäran om förhandsavgörande i sak, kommer den att behöva uttala sig om tillämpningsområdet för direktiv 2002/58/EG [2] respektive direktiv (EU) 2016/680. [3]

[1] Originalspråk: spanska.

[2] Europaparlamentets och rådets direktiv av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 2002, s. 37).

[3] Europaparlamentets och rådets direktiv av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 2016, s. 89).

I. Tillämpliga bestämmelser

A. Unionsrätt

1. Förordning (EU) 2016/679[4]

3. I punkt 2 i artikel 2 (”Materiellt tillämpningsområde”) anges följande:

”Denna förordning ska inte tillämpas på behandling av personuppgifter som

…

d) behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.”

2. Direktiv 2016/680

4. Skäl 2 har följande lydelse:

”Principerna och reglerna för skyddet för fysiska personer med avseende på behandling av deras personuppgifter bör … respektera deras rättigheter och grundläggande friheter, särskilt deras rätt till skydd av personuppgifter. Detta direktiv är avsett att bidra till att skapa ett område med frihet, säkerhet och rättvisa.”

5. Skäl 46 har följande lydelse:

”All begränsning av den registrerades rättigheter måste vara förenlig med stadgan och med Europakonventionen, tolkade enligt rättspraxis från domstolen respektive Europeiska domstolen för de mänskliga rättigheterna,[5] och i synnerhet respektera kärnan i dessa rättigheter och friheter.”

6. Skäl 49 har följande lydelse:

”När personuppgifter behandlas inom ramen för en brottsutredning eller domstolsförfaranden vid brottmål, bör medlemsstaterna kunna föreskriva att rätten till information, tillgång, rättelse och radering samt till begränsning av behandlingen utövas i enlighet med nationella bestämmelser om rättsliga förfaranden.”

7. I artikel 1 (”Syfte och mål”) föreskrivs följande:

”1. I detta direktiv fastställs bestämmelser om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av behöriga myndigheter i syfte att förebygga,

4 Europaparlamentets och rådets förordning av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 2016, s. 1) (nedan kallad GDPR).

5 Nedan kallad Europadomstolen.

förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.

2. Enligt detta direktiv ska medlemsstaterna

a) skydda fysiska personers grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter, och

…

3. Detta direktiv ska inte hindra medlemsstaterna från att föreskriva starkare skyddsåtgärder än de som fastställs i detta direktiv för skyddet av den registrerades rättigheter och friheter med avseende på behöriga myndigheters behandling av personuppgifter.”

8. I punkt 12 i artikel 2 (”Materiellt tillämpningsområde”) anges följande:

”Detta direktiv ska tillämpas på behandling av personuppgifter som utförs av behöriga myndigheter för de ändamål som anges i artikel 1.1.”

9. I artikel 3 (”Definitioner”) anges följande:

”I detta direktiv avses med

…

2) behandling: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,

…

7. behörig myndighet:

a) en offentlig myndighet som har behörighet att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, inklusive skydda mot eller förebygga hot mot den allmänna säkerheten, eller

…”.

10. I artikel 4, med rubriken ”Principer för behandling av personuppgifter”, föreskrivs följande i punkt 1:

”Medlemsstaterna ska föreskriva att personuppgifter ska

a) behandlas på ett lagligt och korrekt sätt,

b) samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte behandlas på ett sätt som står i strid med dessa ändamål,

c) vara adekvata, relevanta och inte för omfattande i förhållande till de syften för vilka de behandlas,

…

e) inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka de behandlas,

f) behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.”

11. Artikel 8 (”Laglig behandling av personuppgifter”) har följande lydelse:

”1. Medlemsstaterna ska föreskriva att behandling ska vara laglig endast om och i den mån behandlingen är nödvändig för att utföra en uppgift som utförs av en behörig myndighet för de ändamål som anges i artikel 1.1 och som sker på grundval av unionsrätt eller medlemsstaternas nationella rätt.

2. Medlemsstaternas nationella rätt som reglerar behandling inom tillämpningsområdet för detta direktiv ska åtminstone specificera syftet med behandlingen, vilka personuppgifter som ska behandlas och behandlingens ändamål.”

12. I artikel 13 (”Information som ska göras tillgänglig för eller lämnas till den registrerade”) föreskrivs följande:

”1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige ska göra åtminstone följande information tillgänglig för den registrerade:

…

d) Rätten att lämna in klagomål till en tillsynsmyndighet samt tillsynsmyndighetens kontaktuppgifter.

…

3. Medlemsstaterna får anta lagstiftningsåtgärder som gör att informationen till den registrerade enligt punkt 2 senareläggs, begränsas eller utelämnas, i den utsträckning och så länge som en sådan åtgärd är nödvändig och proportionell i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, i syfte att

a) undvika att hindra offentliga eller rättsliga utredningar, undersökningar eller förfaranden,

b) undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,

c) skydda den allmänna säkerheten,

d) skydda den nationella säkerheten,

e) skydda andra personers rättigheter och friheter.

…”

13. I artikel 15 (”Begränsningar av rätten till tillgång”) föreskrivs följande i punkt 1:

”Medlemsstaterna får anta lagstiftningsåtgärder som helt eller delvis begränsar den registrerades rätt till tillgång i den utsträckning och så länge en sådan partiell eller fullständig begränsning utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle med hänsyn tagen till den berörda fysiska personens grundläggande rättigheter och berättigade intressen, i syfte att

a) undvika att hindra offentliga eller rättsliga utredningar, undersökningar eller förfaranden,

b) undvika menlig inverkan på förebyggande, förhindrande, upptäckt, utredning eller lagföring av brott eller verkställighet av straffrättsliga påföljder,

c) skydda den allmänna säkerheten,

d) skydda den nationella säkerheten,

e) skydda andra personers rättigheter och friheter.”

14. I artikel 27 (”Konsekvensbedömning avseende dataskydd”) föreskrivs följande:

”1. Om en typ av behandling, särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål, sannolikt leder till en hög risk för fysiska personers rättigheter och friheter, ska medlemsstaterna föreskriva att den personuppgiftsansvarige före behandlingen utför en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter.

2. Den bedömning som avses i punkt 1 ska åtminstone innehålla en allmän beskrivning av den planerade behandlingen, en bedömning av riskerna för de registrerades rättigheter och friheter, de åtgärder som planeras för att hantera dessa risker, skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifter och för att visa att detta direktiv efterlevs, med hänsyn till de registrerades och andra berörda personers rättigheter och berättigade intressen.”

15. I artikel 28 (”Förhandssamråd med tillsynsmyndigheten”) anges följande:

”1. Medlemsstaterna ska föreskriva att den personuppgiftsansvarige eller personuppgiftsbiträdet ska samråda med tillsynsmyndigheten före behandling av personuppgifter som kommer att ingå i ett nytt register som ska inrättas, om

a) en konsekvensbedömning avseende dataskydd enligt artikel 27 visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken, eller om

b) typen av behandling, särskilt vid användning av ny teknik eller nya rutiner eller förfaranden, medför en hög risk för de registrerades rättigheter och friheter.

…”.

16. I artikel 54 (”Rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde”) föreskrivs följande:

”Utan att det påverkar tillgängliga administrativa prövningsförfaranden eller prövningsförfaranden utanför domstol, inbegripet rätten att lämna in ett klagomål till en tillsynsmyndighet enligt artikel 52, ska medlemsstaterna föreskriva en rätt till effektiva rättsmedel för registrerade om han eller hon anser att deras rättigheter enligt de bestämmelser som antas enligt detta direktiv har kränkts som en följd av att hans eller hennes personuppgifter har behandlats på ett sätt som inte är förenligt med dessa bestämmelser.”

B. Nationell rätt

17. I 18 § i Strafprozessordnung[6] tilldelas kriminalpolisen uppgifter inom ramen för straffrättskipningen (punkt 1). Säkerhetsmyndigheterna ansvarar för de utredningar som genomförs av kriminalpolisen (punkt 2). Organen inom den offentliga säkerhetstjänsten ska tillhandahålla verkställande tjänster inom kriminalpolisen, vilket består i att utreda och lagföra brott (punkt 3).

18. Enligt 99 § i straffprocesslagen ska kriminalpolisen genomföra utredningar på eget initiativ eller efter klagomål och måste följa åklagarmyndighetens och domstolarnas beslut (punkt 1). Om en utredningsåtgärd kräver beslut från åklagarmyndigheten, får kriminalpolisen utöva motsvarande befogenhet även utan sådant beslut, om det föreligger överhängande fara. I ett sådant fall måste kriminalpolisen omedelbart ansöka om tillstånd (punkt 2).

19. Enligt 111 § punkt 2 i straffprocesslagen är, när information som är lagrad i datamedier ska bli föremål för insamling av personuppgifter, var och en skyldig att ge tillgång till denna information och att, på begäran, själv skapa eller tillåta att det skapas en elektronisk databärare i ett allmänt filformat. Denna person ska dessutom möjliggöra att det skapas en säkerhetskopia av den information som lagrats i databärarna.

II. Bakgrund, tvisten och tolkningsfrågorna

20. C.G. är tysk medborgare och arbetar och bor i Österrike.

21. I samband med en narkotikakontroll den 23 februari 2021 beslagtog tjänstemän vid tullkammaren i Innsbruck (Österrike) ett paket som var adresserat till C.G. och som innehöll 85 gram cannabis.

22. Den 6 mars 2021 förhörde två poliser C.G. om vem som var avsändare av paketet och genomsökte hans bostad. Under denna husrannsakan beslagtog de hans mobiltelefon (där det fanns ett SIM-kort och ett SD-kort) och överlämnade protokollet från beslaget till honom.

[6] Nedan kallad straffprocesslagen. BGBl nr 631/1975, i dess lydelse enligt Bundesgesetz BGBl I nr 24/2020.

23. C.G. ombads att ge tillgång till uppkopplingsuppgifter i sin mobiltelefon. C.G. vägrade att lämna ut dessa och vägrade även att uppge pinkoden till telefonen.

24. Poliskontoret i distriktet Landeck (Österrike) lyckades inte låsa upp mobiltelefonen. Telefonen skickades till Bundeskriminalamt (centrala kriminalpoliskontoret) i Wien, Österrike, där ytterligare ett försök gjordes, utan framgång, att låsa upp telefonen och få tillgång till de lagrade uppgifterna.

25. Vid den tidpunkt då polisen vidtog åtgärderna omfattades de varken av något beslut från åklagarmyndigheten eller av något domstolsavgörande.

26. Den 31 mars 2021 överklagade C.G. den tvångsåtgärd som vidtagits mot honom till Landesverwaltungsgericht Tirol (Regionala förvaltningsdomstolen i Tyrolen, Österrike) och motsatte sig att hans mobiltelefon tagits i beslag. Detta överklagande avslogs den 20 april 2021.

27. C.G. informerades inte om försöket att analysera mobiltelefonen. Han fick kännedom om det på grund av att den polistjänsteman som tog mobiltelefonen i beslag och därefter inledde den digitala analysen hördes som vittne under sanningsplikt. Dessa försök dokumenterades inte heller i kriminalpolisens akt.

28. Mot denna bakgrund ställde Landesverwaltungsgericht Tirol (Regionala förvaltningsdomstolen i Tyrolen) följande tolkningsfrågor till EU-domstolen:

”1) Ska artikel 15.1 (eventuellt jämförd med artikel 5) i direktiv 2002/58, i dess lydelse enligt direktiv 2009/136/EG, mot bakgrund av artiklarna 7 och 8 i stadgan …, tolkas så, att offentliga myndigheters tillgång till uppgifter som lagrats i mobiltelefoner utgör ett så allvarligt intrång i de grundläggande rättigheter som föreskrivs i dessa artiklar i stadgan, att sådan tillgång på området för förebyggande, utredning, upptäckt och lagföring av brottsliga handlingar bör begränsas till bekämpning av grov brottslighet?

2) Ska artikel 15.1 i direktiv 2002/58, i dess lydelse enligt direktiv 2009/136/EG, mot bakgrund av artiklarna 7, 8 och 11 samt artikel 52.1 i stadgan …, tolkas så, att den utgör hinder för en nationell bestämmelse, såsom 18 §, jämförd med 99 § stycke 1 i straffprocesslagen, enligt vilken säkerhetsmyndigheter under en brottsutredning, utan godkännande av en domstol eller en oberoende administrativ myndighet, skaffar sig själva omfattande och okontrollerad tillgång till alla digitala uppgifter som finns lagrade i en mobiltelefon?

3) Ska artikel 47 i stadgan …, eventuellt jämförd med dess artiklar 41 och 52, med hänsyn till principen om jämlikhet i medel och med hänsyn till rätten till ett effektivt rättsmedel, tolkas så, att den utgör hinder för en nationell bestämmelse, såsom 18 § jämförd med 99 § stycke 1 i straffprocesslagen, som gör det möjligt att undersöka en mobiltelefon digitalt utan att den berörda personen dessförinnan, eller först efter det att åtgärden har vidtagits, underrättas därom?”

III. Förfarandet vid EU-domstolen

29. Begäran om förhandsavgörande inkom till domstolens kansli den 6 september 2021.

30. Den 20 oktober 2021 anmodade EU-domstolen den hänskjutande domstolen att ange huruvida direktiv 2016/680 kunde vara relevant i målet.

31. Den 11 november 2021 svarade den hänskjutande domstolen att direktiv 2016/680 skulle tillämpas i det nationella målet.

32. Skriftliga yttranden har inkommit från den tyska, den österrikiska, den cypriotiska, den danska, den estniska, den franska, den ungerska, den irländska, den nederländska, den norska, den polska och den svenska regeringen samt från Europeiska kommissionen.

33. Vid förhandlingen den 16 januari 2023 närvarade dessa intervenienter, med undantag för den tyska, den ungerska och den polska regeringen, vilka hade inkommit med skriftliga yttranden. Även den finländska regeringen närvarade. Domstolen uppmanade dem alla att koncentrera sina argument på direktiv 2016/680 och att muntligen besvara vissa frågor om detta.

IV. Bedömning

A. Huruvida begäran om förhandsavgörande kan tas upp till sakprövning

34. Den hänskjutande domstolen begärde inledningsvis endast förhandsavgörande gällande tolkningen av direktiv 2002/58. I stort sett samtliga intervenienter är emellertid överens om att detta direktiv inte är tillämpligt i förevarande mål och att en tolkning av det direktivet följaktligen inte heller är nödvändig för att avgöra tvisten.

35. Enligt artikel 3 i direktiv 2002/58 ska direktivet tillämpas på ”behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät inom [unionen], inbegripet allmänna kommunikationsnät som stöder datainsamling och identifieringsutrustning”.

36. Domstolen har slagit fast att ”[n]är medlemsstaterna … direkt genomför åtgärder som innebär undantag från konfidentialiteten vid elektronisk kommunikation, utan att ålägga tjänsteleverantörer av sådan kommunikation någon skyldighet att behandla uppgifter, omfattas skyddet av de berörda personernas uppgifter inte av direktiv 2002/58, utan enbart av nationell rätt, med förbehåll för tillämpningen av [direktiv 2016/680]”.[7]

37. I förevarande fall gjordes försöket att få tillgång till uppgifter direkt av de polismyndigheterna inom ramen för en brottsutredning. Det förekom inte något deltagande från leverantörerna av elektroniska kommunikationstjänster. Dessa ombads inte att lämna ut personuppgifter. Direktiv 2002/58/EG är därför inte tillämpligt.

38. Den unionsrättsliga rättsakt som reglerar denna situation är direktiv 2016/680, som enligt artikel 2.1 i samma direktiv ska tillämpas på behöriga myndigheters behandling av personuppgifter ”i syfte att … utreda … brott”.

[7] Dom av den 6 oktober 2020, La Quadrature du Net m.fl., C-511/18, C-512/18 och C-520/18, EU:C:2020:791 (nedan kallad domen La Quadrature du Net m.fl.), punkt 103.

39. Detta skulle räcka för att dra slutsatsen att begäran om förhandsavgörande, såsom den formulerats av den nationella domstolen, inte kan tas upp till sakprövning, eftersom den unionsrättsliga bestämmelse som den nationella domstolen begärt tolkning av inte var tillämplig i förevarande fall.

40. Det står dock klart att det enligt artikel 267 FEUF är tillåtet för domstolen att omformulera de frågor som hänskjutits till den eller att ange att det finns andra unionsrättsliga bestämmelser som kan vara relevanta, för att ge den nationella domstolen ett användbart svar. [8]

41. EU-domstolen vände sig till den hänskjutande domstolen och bad den att uttala sig om den eventuella relevansen av direktiv 2016/680. EU-domstolen gav således den hänskjutande domstolen möjlighet att själv komplettera eller omformulera sina frågor. I stället för att göra det har den hänskjutande domstolen begränsat sig till att konstatera att ”bestämmelserna i direktiv 2016/680 under alla omständigheter ska iakttas i förevarande mål”, utan att ange vilka bestämmelser i direktivet som den hyser tvivel om och utan att vidare utveckla andra överväganden. [9]

42. EU-domstolen har vid upprepade tillfällen slagit fast att ”[d]et är … av avgörande betydelse, såsom anges i artikel 94 c i domstolens rättegångsregler, att begäran om förhandsavgörande innehåller en redogörelse för skälen till att den hänskjutande domstolen undrar över tolkningen eller giltigheten av vissa unionsbestämmelser, och för det samband som den hänskjutande domstolen har funnit föreligga mellan unionsbestämmelserna och den nationella lagstiftning som är tillämplig i det nationella målet”. [10]

43. Det är tydligt i förevarande begäran om förhandsavgörande att kraven i 94 § i rättegångsreglerna inte har iakttagits, utifrån det ovan anförda. Även om EU-domstolen visar en viss flexibilitet i detta avseende, måste samarbetet med den hänskjutande domstolen vara ömsesidigt: om den hänskjutande domstolen utan giltigt skäl underlåter att samarbeta för att förklara sina tvivel beträffande tolkningen av den unionsrätt som den anser vara tillämplig (i förevarande fall direktiv 2016/680), anser jag att det är logiskt att avvisa begäran om förhandsavgörande. [11]

44. Mot bakgrund av det ovan anförda kan det konstateras att den hänskjutande domstolen

– inte har preciserat arten av den behandling som polismyndigheterna försökte utföra eller av de personuppgifter som specifikt efterfrågades. Inledningsvis tycks den ange att den begränsade sig till uppkopplingsuppgifter (det vill säga trafik- och lokaliseringsuppgifter), men sedan utesluter den inte att upplåsningen av telefonen gav tillgång till ”alla digitala uppgifter som finns lagrade”, [12] inbegripet innehållet i de samtal och elektroniska meddelanden som sänts till och från denna mobiltelefon. [13]

[8] Se, exempelvis, dom av den 28 april 2016, Oniors Bio (C-233/15, EU:C:2016:305, punkt 30).

[9] Domstolen blev tvungen att uppmana parterna att ange ”vilka bestämmelser i direktiv 2016/680 som enligt dem är relevanta och mot bakgrund av vilka domstolen i förekommande fall ska omformulera de tre tolkningsfrågor som den hänskjutande domstolen har ställt” (fjärde frågan för muntligt svar vid förhandlingen).

[10] Dom av den 6 oktober 2021, Consorzio Italian Management och Catania Multiservizi (C-561/19, EU:C:2021:799, punkt 69).

[11] Jag håller med den franska regeringen i denna bedömning (punkterna 36–41 i dess skriftliga yttrande).

[12] Detta sker i den andra tolkningsfrågan.

[13] I beslutet om hänskjutande anges att ”när det gäller trafikuppgifter kan nästan alla kontakter rekonstrueras utifrån kommunikationens frekvens, tidpunkt och varaktighet, och när det gäller kommunikation via sms och andra meddelandetjänster kan också innehållet rekonstrueras; även genom undersökning av lagrade foton och webbhistorik går det att få en mycket intim inblick i den berörda personens privatliv”.

– hänvisar till såväl beslaget av telefonen och tillgången till, eller försöket att få tillgång till, de uppgifter som finns i denna som till senare ”utnyttjande” (*Auswertung*), det vill säga analys och läsning av dem. Den hänskjutande domstolen tillade att det senare ”innebär … en fullständigt okontrollerad tillgång till den berörda personens digitala kommunikation i dess helhet”, vilket gör det möjligt att ”rekonstruera en mycket detaljerad och djupgående bild av nästan alla områden av privatlivet”.

45. Under dessa omständigheter skulle EU-domstolen, i stället för att *omformulera* den hänskjutande domstolens frågor, göra en verklig *omstrukturering* av begäran om förhandsavgörande, vilken dessutom delvis skulle grunda sig på hypotetiska överväganden snarare än på fastställda faktiska omständigheter. Jag upprepar att detta dessutom sker efter att den hänskjutande domstolen har getts möjlighet att själv komplettera eller omformulera sina frågor.

46. Jag föreslår därför att begäran om förhandsavgörande ska avvisas, i enlighet med flera av de intervenerande medlemsstaternas yrkanden.

47. Även den omständigheten, som påpekades vid förhandlingen, att det vid den hänskjutande domstolen inte längre finns någon verklig tvist som kräver tolkning av unionsrättsliga bestämmelser, bör leda till ett sådant beslut om avvisning.

48. Den österrikiska regeringen (som är ansvarig för de polismyndigheter som var inblandade i utredningen) vidgår att dessa myndigheters agerande var olagligt och kränkte den berördes rättigheter. Eftersom klagandens överklagande till förvaltningsdomstolen, enligt beslutet om hänskjutande, avsåg just de polisiära åtgärder som den myndighet som är motpart ansåg vara otillåtna, föreligger inte längre den tvist som den hänskjutande domstolen hade att avgöra.

49. Under alla omständigheter kommer jag, för det fall domstolen inte skulle dela min uppfattning, att behandla de sakfrågor som ligger till grund för tolkningsfrågorna i andra hand.

50. Först och främst anser jag dock att det är nödvändigt att utesluta att det finns någon annan grund för den avvisning som vissa av intervenienterna i målet har argumenterat för.[14] Eftersom direktiv 2016/680 rör skydd för fysiska personer med avseende på *behandling* av deras uppgifter skulle det enligt deras mening inte gälla för fall som detta, där det inte har skett någon behandling, utan endast ett *försök att få tillgång* till uppgifter som inte kunde erhållas i slutändan.

51. Kommissionen anser tvärtom att det för den ändamålsenliga verkan av direktiv 2016/680 ska ges företräde åt en tolkning av direktivets syfte som inte är begränsad till behandling av uppgifter i strikt mening, utan även omfattar frågor som är direkt knutna till sådan behandling. En av dessa frågor är försök att få tillgång till de uppgifter som man vill behandla.[15]

[14] Jag tänker konkret på den österrikiska, den franska, den nederländska och den norska regeringen.

[15] Kommissionen anser att det inte ”spelar någon roll om försöken har varit framgångsrika eller inte. Förekomsten av tekniska svårigheter som förhindrar framgångsrika försök att få tillgång till uppgifter är en omständighet som inte kan kännas till i förväg och som inte påverkar riskerna för skyddet av personuppgifter”.

52. Utan att behöva tänja på gränserna för tillämpningsområdet för direktiv 2016/680 [16] anser jag att dess tillämpning i detta fall är motiverad, inte på grund av att mobiltelefonen beslagtogs, [17] utan på grund av polismyndigheternas efterföljande åtgärder för att få fram vissa personuppgifter om den registrerade från telefonen, vilket var syftet med att de försökte låsa upp den och ge tillgång till dess innehåll.

53. Bland de åtgärder som definieras som ”behandling” i artikel 3.2 i direktiv 2016/680 finns ”tillhandahållande på annat sätt” av personuppgifter när detta sker inom ramen för en brottsutredning. Jag anser att när polismyndigheten beslagtar en telefon där dessa uppgifter lagras och hanterar den för att få ut uppgifterna från den, påbörjar den en ”behandling”, även om den förhindras av skäl som har med den kryptografiska säkerheten att göra.

54. Ett fruktlöst försök att få tillgång till personuppgifter som lagrats i en mobiltelefon, i samband med en brottsutredning, regleras av direktiv 2016/680 av skäl motsvarande dem som föranledde EU-domstolen att förklara att direktiv 2002/58 är tillämpligt på *försök* (även ett fruktlöst sådant) att få tillstånd från domstol att erhålla vissa uppgifter från den person som är föremål för utredning och som innehas av en operatör för elektronisk kommunikation. [18]

55. Om den hänskjutande domstolen i detta sammanhang skulle pröva om polisens åtgärd var olaglig (vilket den österrikiska regeringen anser, såsom jag redan har förklarat), skulle prövningen kunna vara beroende av huruvida det avsedda syftet är lagligt, såväl om åtgärden lyckades som om den endast påbörjades men inte lyckades.

B. Prövning i sak

1. Den första tolkningsfrågan

56. Den hänskjutande domstolen vill få klarhet i huruvida, enligt artikel 15.1 i direktiv 2002/58 (eventuellt jämförd med artikel 5), mot bakgrund av artiklarna 7 och 8 i stadgan, ”offentliga myndigheters tillgång till uppgifter som lagrats i mobiltelefoner utgör ett så allvarligt intrång i de grundläggande rättigheter som föreskrivs i dessa artiklar i stadgan, att sådan tillgång på området för förebyggande, utredning, upptäckt och lagföring av brottsliga handlingar bör begränsas till bekämpning av grov brottslighet”.

57. Om begäran om förhandsavgörande skulle kunna tas upp till sakprövning skulle det, på grund av att direktiv 2002/58 inte är tillämpligt, vara nödvändigt att omformulera den första frågan, så att domstolens svar skulle tillhandahålla en tolkning av direktiv 2016/680.

58. Detta svar skulle i tur och ordning behöva klargöra om det kan röra sig om kränkning i fall som det förevarande och, om det föreligger kränkning, om det enligt direktiv 2016/680 krävs att åtkomsten till uppgifterna ska vara begränsad till bekämpningen av grov brottslighet.

[16] I synnerhet anser jag att den hänvisning till artiklarna 27 och 28 i direktiv 2016/680 som kommissionen föreslår i sitt skriftliga yttrande inte är nödvändig. ”[K]onsekvensbedömningen avseende dataskydd” som föreskrivs i artikel 27 avser generellt ”en typ av behandling” och inte specifika eller särskilda behandlingar. Därför anges följande i skäl 58 i direktiv 2016/680: ”[k]onsekvensbedömningarna bör omfatta relevanta system och processer för behandling *men inte enskilda fall*” (min kursivering). Vid förhandlingen nyanserade kommissionen sin hänvisning till dessa två bestämmelser, som den endast citerade för att understryka hur direktiv 2016/680 även avser situationer som föregår behandlingen av uppgifterna i egentlig mening.

[17] Direktiv 2016/680 omfattar inte beslag av telefonen som bevismedel inom ramen för en brottsutredning.

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

59. Behandling av uppgifter kan per definition äventyra rätten till respekt för privatlivet (artikel 7 i stadgan) och skyddet av personuppgifter (artikel 8 i stadgan). Offentliga myndigheter måste således iaktta de villkor som föreskrivs i artikel 52.1 i stadgan för att motivera sitt ingrepp i utövandet av dessa grundläggande rättigheter.

60. Intrång i de rättigheter som skyddas genom artiklarna 7 och 8 i stadgan är av desto större vikt dels eftersom det begärs tillgång till uppgifter av känslig karaktär som vanligtvis lagras i mobiltelefoner och som om de blir kända kan avslöja aspekter av innehavarnas liv som bör hållas hemliga för tredje part, dels för att tillgång till innehållet i kommunikation möjliggörs.

61. Ur allmän synvinkel och med hänsyn till dess innehåll kan direktiv 2016/680 inte tolkas så, att den behandling av uppgifter som direktivet avser är begränsad till fall av bekämpning av grov brottslighet.

62. Direktiv 2016/680 avser all behandling av personuppgifter [19] som utförs av behöriga myndigheter i syfte att förebygga, utreda, avslöja eller lagföra *alla typer* av brott.

63. Det framgår inte av de principer som införts genom direktiv 2016/680 kring behandlingen av personuppgifter med detta syfte (artikel 4) eller villkoren för att behandlingen ska vara tillåten (artikel 8) att behandling av personuppgifter som regel endast är möjlig vid grov brottslighet.

64. En långtgående begränsning till fall av bekämpning av grov brottslighet kan inte heller grundas på att man helt enkelt extrapolerar EU-domstolens praxis avseende direktiv 2002/58 [20] till fall som det nu aktuella.

65. Jag anser att detta inte går, eftersom denna rättspraxis, utan att det påverkar vad jag kommer att förklara nedan, avser en generaliserad och urskillningslös lagring av personuppgifter från en allmän och obestämd grupp, som systematiskt utförs av leverantörer av elektroniska kommunikationstjänster. Omfattningen av det ingrepp som denna typ av lagring utgör för samhället i dess helhet förklarar varför domstolen har varit särskilt sträng och förbjudit sådan lagring och sedan föreskrivit undantag till detta förbud.

66. Så är inte fallet när den tillgång som eftersträvas inte avser hela befolkningen eller stora befolkningsgrupper (det vill säga en allmän och obestämd grupps personuppgifter), utan information som är lagrad på en enskild mobiltelefon, inom ramen för ett brottsutredningsförfarande som också är unikt, för vilket direktiv 2016/680 är särskilt tillämpligt.

67. Syftet med direktiv 2016/680 är inget annat än behöriga myndigheters behandling av uppgifter för att förebygga, utreda, avslöja eller lagföra brott; alla slags brott, inte enbart grova.

68. Såsom vissa intervenienter i målet om förhandsavgörande har betonat skulle direktiv 2016/680, i avsaknad av uppgifter om hur allvarliga brotten är, kunna få en tillämpning i medlemsstaterna som inte är enhetlig, eftersom de bedömningar som görs i varje nationell rätt av straffbara gärningars olika allvar väsentligen skiljer sig åt. [21]

[19] Begreppet ”åtgärder” som används i artikel 3.2 i direktiv 2016/680 är mycket brett. Se punkt 9 ovan där jag återger denna artikel.

[20] Domen Quadrature du Net och domen av den 21 december 2016, Tele2 Sverige och Watson m.fl. (C-203/15 och C-698/15, EU:C:2016:970) (nedan kallad Tele2 Sverige och Watson); dom av den 2 oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788), dom av den 6 oktober 2020, Privacy International (C-623/17, EU:C:2020:790), och dom av den 2 mars 2021, Prokuratuur (Villkor för tillgång till uppgifter om elektronisk kommunikation) (C-746/18, EU:C:2021:152) (nedan kallad domen Prokuratuur).

[21] Den franska regeringen nämner som exempel brott som rör innehav och handel med narkotika, vars allvarlighetsgrad skiljer sig åt mellan de österrikiska och franska straffbestämmelserna. Den svenska regeringen har yttrat sig på liknande sätt.

69. Direktiv 2016/680 uppställer således inte som ett villkor för laglighet att den behandling av personuppgifter som föreskrivs i direktivet endast ska godtas i syfte att bekämpa grov brottslighet.

70. Detta påverkar inte den omständigheten att den behandling av uppgifter som de behöriga myndigheterna avser att utföra inom ramen för direktiv 2016/680, med tillämpning av proportionalitetsprincipen och från fall till fall, ska mildras med hänsyn dels till arten av de brott som lagförs, dels till den typ av personuppgifter som behandlingen avser.

71. I linje med detta håller jag med om vissa av den tyska regeringens påståenden om begränsningen av tillgången till uppgifter från beslagtagna telefoner, när uppgifterna gör det möjligt att skapa en fullständig bild av ägarnas personlighet utifrån det digitala innehållet i telefonerna. Enligt den tyska regeringen bör sådan tillgång begränsas till uppgifter som är nödvändiga som bevis i ett specifikt fall, och kan vara olämplig vid faktorer som ”den mindre allvarliga karaktären av det brott som utreds eller det svaga bevisvärdet hos de uppgifter som ska erhållas”. [22]

72. *I abstrakt mening* innebär därför inte direktiv 2016/680 att det som regel är olagligt att få tillgång till personuppgifter som lagrats i en mobiltelefon i syfte att underlätta utredningen av beteenden som kan falla inom ramen för allmän brottslighet. Om sådan tillgång *i ett konkret fall* ska ges, är det något som den berörda myndigheten ska bedöma från fall till fall mot bakgrund av dess nödvändighet och med beaktande av det proportionalitetskriterium som jag precis hänvisade till.

73. Detta framgår, enligt min mening, av bestämmelserna i direktiv 2016/680 som fastställer villkoren för att behandling av personuppgifter inom ramen för brottsbekämpningen ska vara laglig:

– Artikel 4.1 a, enligt vilken uppgifterna måste ”behandlas på ett lagligt … sätt”.

– Artikel 8.1, i vilken det framhålls att behandlingen ska vara *nödvändig* och grunda sig på unionsrätten eller medlemsstatens lagstiftning.

2. Den andra tolkningsfrågan

74. Den hänskjutande domstolen har ställt den andra frågan för att få klarhet i huruvida artikel 15.1 i direktiv 2002/58, mot bakgrund av artiklarna 7, 8 och 11 samt artikel 52.1 i stadgan, ”utgör hinder för en nationell bestämmelse, såsom 18 §, jämförd med 99 § stycke 1 i straffprocesslagen, enligt vilken säkerhetsmyndigheter under en brottsutredning, utan godkännande av en domstol eller en oberoende administrativ myndighet, skaffar sig själva omfattande och okontrollerad tillgång till alla digitala uppgifter som finns lagrade i en mobiltelefon”.

75. Frågan är något tvetydigt formulerad. Den hänskjutande domstolen

– medger att det i 110 § punkt 2 i straffprocesslagen föreskrivs att beslag av egendom i regel kräver tillstånd från åklagarmyndigheten. Polismyndigheten får genomföra sådana beslag utan ett sådant tillstånd endast under de exceptionella omständigheter som anges i punkt 3 i bestämmelsen (vilka inte tycks föreligga i det aktuella fallet).

[22] Den tyska regeringens yttrande, punkt 20.

– tillägger dock att analys av den information som lagrats i mobiltelefoner ”inte är entydigt reglerad straffprocesslagen” och kan göras av säkerhetsmyndigheterna på eget initiativ, utan föregående tillstånd.

76. Den österrikiska regeringen har angett en version av de nationella bestämmelserna som inte överensstämmer med den version som anges i beslutet om hänskjutande. I synnerhet anger den att det enligt nationell lagstiftning endast är möjligt att beslagta telefonen (utom i nödsituationer) och analysera de uppgifter som finns lagrade på den om åklagarmyndigheten gett tillstånd till detta.[23] Utan ett beslut från åklagarmyndigheten är det olagligt för polisen att bearbeta de uppgifter som finns lagrade i telefonen.

77. Det ankommer på den hänskjutande domstolen att kontrollera villkoren i nationell rätt. Enligt det förfarande som föreskrivs i artikel 267 FEUF är domstolen inte behörig att tolka nationell rätt, utan det är endast den hänskjutande domstolen som har att fastställa den exakta omfattningen av nationella lagar och andra författningar.[24]

78. Utan att vilja delta i diskussionen kring tolkningen av österrikisk rätt, anser jag att det är svårt att utifrån de bestämmelser som den hänskjutande domstolen har angett (18 § straffprocesslagen jämförd med 99 § stycke 1 i samma lag) dra den slutsats som den domstolen drar. Det är dock som sagt endast den hänskjutande domstolen som kan avgöra detta.

79. Under alla omständigheter anser den hänskjutande domstolen att domen Prokuratuur,[25] avseende en domstols eller en oberoende myndighets förhandskontroll av tillgången till lagrade uppgifter, kan överföras på ett sådant fall som det nu aktuella.

80. Den nederländska regeringen anser tvärtom att denna praxis ska förstås mot bakgrund av en nationell lagstiftning som ger de behöriga myndigheterna *allmän* tillgång till *samtliga* trafikuppgifter och lokaliseringsuppgifter som lagrats. Detta skulle förklara kravet på ett förhandstillstånd från en domstol, vilket dock kanske inte är motiverat när det gäller tillgång till uppgifter från en enda mobiltelefon.

81. På samma sätt hävdar den norska regeringen att bland de många skyddsgarantier som fastställs i direktiv 2016/680[26] finns inte kravet på förhandstillstånd från en oberoende rättslig eller administrativ myndighet uttryckligen med.

82. Med utgångspunkt i att bestämmelserna i direktiv 2016/680 ska tolkas mot bakgrund av stadgan gör kommissionen gällande att den skyldighet som åläggs medlemsstaterna genom artikel 8.1 i detta direktiv (villkor för att behandlingen ska vara laglig) medför att de grundläggande rättigheter som garanteras i artiklarna 7 och 8 i stadgan måste iakttas.

[23] Punkt 19 i den tyska regeringens skriftliga yttrande. Den åberopar Oberster Gerichtshofs (Österrikes högsta domstol) beslut av den 13 oktober 2020 (mål 11 Os 56/20z), enligt vilket det anses olagligt, i den mån det kränker den berörda personens subjektiva rättigheter, att kriminalpolisen analyserar uppgifter i en mobiltelefon utan tillstånd från åklagarmyndigheten.

[24] Se exempelvis dom av den 28 april 2022, SeGEC m.fl. (C-277/21, EU:C:2022:318, punkt 21).

[25] Domen Prokuratuur, punkt 51: ”[det är] väsentligt att behöriga nationella myndigheters tillgång till de lagrade uppgifterna är underkastad förhandskontroll av en domstol eller en oberoende myndighet, och att domstolen meddelar sitt avgörande eller myndigheten antar sitt beslut till följd av att dessa myndigheter har framställt en motiverad begäran inom ramen för exempelvis ett förfarande för förebyggande, avslöjande eller lagföring av brott”.

[26] Utöver dem som anges i artiklarna 4 och 8 finns de i kapitlen III (”Den registrerades rättigheter”), IV (”Personuppgiftsansvarig och personuppgiftsbiträde”), VI (”Oberoende tillsynsmyndigheter”) och VIII (”Rättsmedel, ansvar och sanktioner”).

83. Jag håller med kommissionen om att de nationella lagstiftarna, samtidigt som de iakttar dessa principer i stadgan, är skyldiga att fastställa de regler som krävs för att se till att tillgången till uppgifter är motiverad i varje enskilt fall och begränsad till vad som är absolut nödvändigt och proportionerligt.

84. Sådana nationella bestämmelser behöver emellertid inte nödvändigtvis vara specifika för tillgång till personuppgifter som ingår i en mobiltelefon, såsom i förevarande fall, utan kan vara allmänt föreskrivna i nationell rätt om bevisupptagning.

85. I detta avseende har jag redan återgett punkt 103 i domen La Quadrature du Net vad gäller medlemsstaternas åtgärder som rör konfidentialitet vid elektronisk kommunikation men där leverantörer av sådana kommunikationstjänster inte åläggs skyldigheter gällande behandlingen av sådan kommunikation. [27]

86. Utan att det därför är nödvändigt att utifrån direktiv 2016/680 härleda *särskilda* regler av förfarandekaraktär som garanti för att tillgången till uppgifter som lagras i en mobiltelefon är laglig, [28] kommer de nationella regler som reglerar utövandet av befogenheter att göra husrannsakan och beslag i samband med brottsutredningar att vara tillämpliga. [29]

87. Hänvisningen till bestämmelser i nationell rätt för att säkerställa att tillgång enligt direktiv 2016/680 är laglig är för övrigt förenlig med Europadomstolens praxis. Det var just i ett fall som avsåg Republiken Österrike gällande artikel 8 i Europakonventionen (rätten till respekt för privatlivet och familjelivet samt hemmet och skriftväxlingen) som Europadomstolen konstaterade att den österrikiska lagstiftningen om beslag av föremål, särskilt handlingar, är tillämplig på husrannsakan och beslag av uppgifter som lagrats på datamedier. [30]

88. Om polismyndigheterna, såsom den österrikiska regeringen hävdar med hänvisning till Oberster Gerichtshofs (Högsta domstolen, Österrike) rättspraxis, inte har rätt att få tillgång till de uppgifter som finns lagrade i en viss mobiltelefon utan tillstånd från åklagaren, förlorar den andra frågan om förhandsavgörande en stor del av sin mening.

89. Under alla omständigheter kan svaret på denna fråga inte utesluta att tillgången till personuppgifterna i den telefon som beslagtagits leder till att ”rekonstruera en mycket detaljerad och djupgående bild av nästan alla områden av privatlivet” hos den berörda personen. [31] Om så är fallet kan polismyndigheterna inte avstå från det förhandstillstånd som avses i domen Prokuratuur.

90. Vid en första anblick verkar detta uttalande inte vara förenligt med att direktiv 2002/58 inte ska tillämpas i ett sådant fall (enligt tolkningen i domen Prokuratuur), som jag har hävdat ovan. Jag anser emellertid att *ändamålet* med denna dom talar för samma lösning.

[27] Se punkt 36 ovan.

[28] Kommissionens ansträngningar i punkterna 34–39 i dess skriftliga yttrande för att bidra till att fastställa tydliga och exakta regler för fastställande av gränser och lämpliga skyddsåtgärder när det gäller tillgång till uppgifter från mobiltelefoner är en bra illustration av svårigheten med detta åtagande.

[29] Regler som, som exempelvis den danska och irländska regeringen påpekar, ligger utanför EU-rättens tillämpningsområde, men som kan tjäna till att uppfylla ett krav som följer av unionsrätten.

[30] Europadomstolens dom av den 16 oktober 2007, Wieser och Bicos Beteiligungen mot Österrike (CE:ECHR:2007:1016JUD007433601), § 54: ”the Austrian Code of Criminal Procedure does not contain specific provisions for the search and seizure of electronic data. However, it contains detailed provisions for the seizure of objects and, in addition, specific rules for the seizure of documents. It is established in the domestic courts’ case-law that these provisions also apply to the search and seizure of electronic data”.

[31] Se den hänskjutande domstolens överväganden som återges i punkt 44 ovan.

91. I det mål som gav upphov till domen Prokuratuur var det, som här, fråga om en enskild brottsutredning mot en viss person, även om tillgången hade erhållits genom tillgång till uppgifter (metadata) från leverantörer av elektroniska kommunikationstjänster. Det rörde sig om insamling av ”uppgifter rörande ett flertal … telefonnummer och … internationella identiteter för mobil utrustning”. [32]

92. Enligt min mening kan två aspekter urskiljas i domen Prokuratuur: dels ifrågasättandet av en medlemsstats allmänna bestämmelser om generell och odifferentierad lagring och senare tillgång till uppgifter som innehas av tjänsteleverantörerna, dels förhandskontrollen, i ett enskilt fall, av tillgången till dessa metadata, när dessa gör det möjligt att skapa detaljerad bild av en persons privatliv.

93. Den omständigheten att de uppgifter som i förevarande mål avslöjar en persons privatliv inte innehas av tjänsteleverantörerna och att de erhålls (eller att någon försöker erhålla dem) från en enda telefon som har beslagtagits är enligt min mening av underordnad betydelse i förhållande till syftet med det krav på förhandskontroll som slås fast i domen Prokuratuur.

94. Denna förhandskontroll har sitt yttersta stöd i det skydd som garanteras genom artiklarna 7 och 8 i stadgan. Det organ som genomför den ska kunna ”säkerställa en korrekt balans mellan intressen som inom ramen för brottsbekämpning gör sig gällande för att svara mot utredningens behov, å ena sidan, och de grundläggande rättigheter avseende respekt för privatlivet och skydd av personuppgifter som tillkommer de personer vars uppgifter kan komma att lämnas ut, å den andra sidan”. [33]

3. Den tredje tolkningsfrågan

95. Den hänskjutande domstolen har ställt den tredje tolkningsfrågan för att få klarhet i huruvida artikel 47 i stadgan (eventuellt jämförd med artiklarna 41 och 52) utgör hinder för en sådan lagstiftning som den österrikiska lagstiftningen [34] som ”som gör det möjligt att undersöka en mobiltelefon digitalt utan att den berörda personen dessförinnan, eller först efter det att åtgärden har vidtagits, underrättas därom”.

96. Jag anser att den fråga som formulerats på detta sätt kanske inte är nödvändig för att lösa tvisten, eftersom den berörda personen kunde utöva sin rätt enligt artikel 47 i stadgan genom att begära att den hänskjutande domstolen ska ogiltigförklara polisens åtgärder avseende den telefon som togs i beslag, vilket innefattar den senare (och misslyckade) användningen av de uppgifter som var lagrade i telefonen.

97. När det gäller dessa två tillfällen av polisinsatser bör man göra en åtskillnad mellan två saker:

– När det gäller beslaget av själva telefonen visar uppgifterna i målet att den registrerade var medveten om beslaget och att han vägrade att ge polismyndigheterna koden för att låsa upp telefonen när den beslagtogs.

– När det gäller försöket att analysera uppgifterna tyder allt på att den som ansvarade för behandlingen inte informerade den registrerade om denna åtgärd, även om den österrikiska

[32] Domen Prokuratuur, punkt 17.

[33] Domen Prokuratuur, punkt 52.

[34] Här hänvisar den återigen till 18 § i straffprocesslagen jämförd med 99 § i samma lag.

regeringen uppger att den registrerade kände till en rapport där det konstaterades att kriminalpolisen hade vidtagit åtgärder avseende telefonen. [35]

98. Det kvarstår således vissa oklarheter om användningen av uppgifterna och den registrerades kännedom om dem, vilka, som jag redan har påpekat, borde ha klargjorts av den hänskjutande domstolen i beslutet om hänskjutande och som hindrar att ett användbart svar ges på den tredje tolkningsfrågan.

99. För det fall domstolen inte skulle anse att denna fråga inte kan tas upp till sakprövning kommer jag i vart fall att uttala mig om den. I ett sådant fall, och med beaktande av att direktiv 2002/58 inte är tillämpligt, är det nödvändigt att omformulera frågan mot bakgrund av direktiv 2016/680, vars artiklar 13, 15 och 54 erbjuder vägar för att svara på den.

100. Enligt direktiv 2016/680 är den information om behandlingen av personuppgifter som måste lämnas till den registrerade den information som är nödvändig bland annat för att, å ena sidan, lämna in ett klagomål till tillsynsmyndigheten (artikel 13.1 d), och, å andra sidan, att komma i åtnjutande av ett effektivt rättsligt skydd mot kränkningar av de rättigheter som garanteras i direktiv 2016/680, utan att det påverkar tillgängliga administrativa eller utomrättsliga rättsmedel (artikel 54).

101. Det bör dock inte glömmas bort att både artikel 13.3 och artikel 15.1 i direktiv 2016/680 ger medlemsstaterna rätt att anta lagstiftningsåtgärder genom vilka:

– informationen till den registrerade enligt artikel 13.2 senareläggs, begränsas eller utelämnas.

– den registrerades rätt till tillgång till de uppgifter som behandlas begränsas helt eller delvis, förutsatt att en sådan begränsning utgör en nödvändig och proportionerlig åtgärd *bland annat* för att undvika att hindra offentliga eller rättsliga utredningar, undersökningar eller förfaranden, eller att utredningen av brottsliga handlingar påverkas menligt. [36]

102. Under alla omständigheter beror lagligheten av behandlingen av uppgifter inte på huruvida de behöriga myndigheterna har uppfyllt de (senare) skyldigheter som ålagts dem genom artikel 13 i direktiv 2016/680, utan på lagligheten av det ändamål som motiverade behandlingen, det vill säga huruvida dessa administrativa myndigheter hade rätt att behandla personuppgifterna.

103. Ur detta perspektiv har det faktum att den registrerade har informerats om försöken att få tillgång till de uppgifter som finns lagrade i den telefon som beslagtogs från honom i sig inget samband med huruvida polisens åtgärder är lagliga på materiella grunder. Den personuppgiftsansvariges beteende som kan strida mot de skyldigheter som åläggs den personuppgiftsansvarige enligt artikel 13 i direktiv 2016/680 kan få andra konsekvenser, men det påverkar som sagt inte i sig lagligheten eller olagligheten av själva behandlingen.

104. Det ankommer på den hänskjutande domstolen att avgöra om den nationella lagstiftningen gör det möjligt för den berörda personen att utöva dessa rättigheter på ett effektivt sätt.

[35] Punkt 37 i dess skriftliga yttrande.

[36] Se domen Tele2 Sverige och Watson, punkt 121. Dess praxis i förhållande till direktiv 2002/58 kan överföras på direktiv 2016/680 i syfte att säkerställa rättsligt skydd för att rättigheterna för dem vars uppgifter behandlas skyddas.

V. Förslag till avgörande

105. Mot bakgrund av ovanstående föreslår jag att domstolen ska avvisa begäran om förhandsavgörande från Landesverwaltungsgericht Tirol (regionala förvaltningsdomstolen i Tyrolen, Österrike).

Alternativt föreslår jag att domstolen svarar på begäran om förhandsavgörande på följande sätt:

1) Artiklarna 4.1 a och 8.1 i Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, jämförda med artiklarna 7, 8 och 52 i Europeiska unionens stadga om de grundläggande rättigheterna,

   ska tolkas så,

   att inom ramen för en brottsutredning är offentliga myndigheters tillgång till personuppgifter som lagrats i en mobiltelefon, vilken syftar till att behandla dessa uppgifter, inte begränsad till fall av bekämpning av grov brottslighet.

   Sådan tillgång måste vara motiverad i varje enskilt fall och begränsas till vad som är absolut nödvändigt och proportionerligt, med hänsyn till arten av de brott som lagförs och de personuppgifter som dessa myndigheter vill få tillgång till.

   Polismyndigheterna får inte, inom ramen för en brottsutredning, på egen hand och utan föregående tillstånd från ett rättsligt organ, skaffa sig fullständig och obegränsad tillgång till alla uppgifter som finns lagrade i en mobiltelefon, när dessa uppgifter kan ge en detaljerad bild av en persons privatliv.

2) Artiklarna 13, 15 och 54 i direktiv 2016/680, jämförda med artiklarna 47 och 52 i stadgan,

   ska tolkas så,

   att utan att det påverkar de begränsningar som tillåts enligt artikel 15.1 i direktiv 2016/680, eller andra tillgängliga administrativa prövningsförfaranden eller prövningsförfaranden utanför domstol, ska innehavaren av en mobiltelefon informeras om de aktuella myndigheternas behandling av personuppgifter som lagrats i telefonen, vid den tidpunkt och på de villkor som är nödvändiga för att säkerställa ett effektivt utövande av den registrerades rätt att söka rättsligt skydd mot ett eventuellt åsidosättande av de rättigheter som erkänns i direktiv 2016/680.