Rättsfallssamlingen

FÖRSLAG TILL AVGÖRANDE AV GENERALADVOKAT
CAMPOS SÁNCHEZ-BORDONA
föredraget den 30 mars 2023 [1]

Mål C-162/22

A.G.
ytterligare deltagare i rättegången:
Lietuvos Respublikos generalinė prokuratūra

(begäran om förhandsavgörande från Lietuvos vyriausiasis administracinis teismas (Högsta förvaltningsdomstolen, Litauen))

”Begäran om förhandsavgörande – Telekommunikationer – Behandling av personuppgifter – Direktiv 2002/58/EG – Tillämpningsområde – Artikel 15.1 – Tillgång till uppgifter som har lagrats av leverantörer av elektroniska kommunikationstjänster och som samlats in inom ramen för förundersökningar – Senare användning av uppgifterna i samband med en utredning om tjänstefel”

1. Begäran om förhandsavgörande avser i huvudsak frågan huruvida personuppgifter som inhämtats under en brottsutredning senare kan användas i ett disciplinärt administrativt förfarande mot en offentlig tjänsteman.

2. Svaret på denna fråga ger domstolen ett nytt tillfälle att uttala sig om tillämpningsområdet för, å ena sidan, direktiv 2002/58/EG, [2] och, å andra sidan, direktiv (EU) 2016/680 [3] och förordning (EU) 2016/679 [4].

3. Vad gäller direktiv 2002/58 har domstolen utvecklat en numera fast rättspraxis avseende i vilka fall och på vilka villkor medlemsstaterna får begränsa omfattningen av de rättigheter och skyldigheter som föreskrivs i direktivet. [5]

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).

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 Utan att vara uttömmande kan följande exempel ges på de viktigaste målen i denna rättspraxis: dom av den 8 april 2014, Digital Rights Ireland m.fl. (C-293/12 och C-594/12, EU:C:2014:238), dom av den 21 december 2016, Tele2 Sverige och Watson m.fl. (C-203/15 och 698/15, EU:C:2016:970), 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), dom av den 2 mars 2021, Prokuratuur (Villkor för tillgång till uppgifter om elektronisk kommunikation) (C-746/18, EU:C:2021:152), och dom av den 5 april 2022, Commissioner of An Garda Síochána m.fl. (C-140/20, EU:C:2022:258) (nedan kallad domen Commissioner of An Garda Síochána).

I. Tillämpliga bestämmelser

A. Unionsrätt

1. Direktiv 2002/58

4. I artikel 1 (”Tillämpningsområde och syfte”) föreskrivs följande:

”1. Genom detta direktiv möjliggörs en harmonisering av nationella bestämmelser för att säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, särskilt rätten till integritet och konfidentialitet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation, samt för att säkerställa fri rörlighet för sådana uppgifter samt för utrustning och tjänster avseende elektronisk kommunikation inom gemenskapen.

2. Bestämmelserna i detta direktiv skall precisera och komplettera direktiv 95/46/EG[6] för de ändamål som avses i punkt 1. Bestämmelserna är vidare avsedda att skydda berättigade intressen för de abonnenter som är juridiska personer.

3. Detta direktiv skall inte tillämpas på verksamheter som faller utanför tillämpningsområdet för [FEUF], t.ex. de som omfattas av avdelningarna V och VI i [FEU], och inte i något fall på verksamheter som avser allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när verksamheten rör statens säkerhet) och statens verksamhet på straffrättens område.”

5. I artikel 5 (”Konfidentialitet vid kommunikation”) föreskrivs följande i punkt 1:

”Medlemsstaterna skall genom nationell lagstiftning säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. De skall särskilt förbjuda avlyssning, uppfångande med tekniskt hjälpmedel, lagring eller andra metoder som innebär att kommunikationen och de därmed förbundna trafikuppgifterna kan fångas upp eller övervakas av andra personer än användarna utan de berörda användarnas samtycke, utom när de har laglig rätt att göra detta i enlighet med artikel 15.1. Denna punkt får inte förhindra teknisk lagring som är nödvändig för överföring av kommunikationen utan att det påverkar principen om konfidentialitet.”

6. I artikel 15 (”Tillämpningen av vissa bestämmelser i direktiv 95/46/EG”) föreskrivs följande:

”1. Medlemsstaterna får genom lagstiftning vidta åtgärder för att begränsa omfattningen av de rättigheter och skyldigheter som anges i artikel 5, artikel 6, artikel 8.1, 8.2, 8.3 och 8.4 och artikel 9 i detta direktiv när en sådan begränsning i ett demokratiskt samhälle är nödvändig, lämplig och proportionell för att skydda nationell säkerhet (dvs. statens säkerhet), försvaret och allmän säkerhet samt för förebyggande, undersökning, avslöjande av och åtal för brott eller vid obehörig användning av ett elektroniskt kommunikationssystem enligt artikel 13.1 i direktiv 95/46/EG. Medlemsstaterna får för detta ändamål bland annat vidta lagstiftningsåtgärder som innebär att uppgifter får bevaras under en begränsad period som motiveras av de skäl som

[6] Europaparlamentets och rådets direktiv av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 1995, s. 31).

fastställs i denna punkt. Alla åtgärder som avses i denna punkt skall vara i enlighet med de allmänna principerna i gemenskapslagstiftningen, inklusive principerna i artikel 6.1 och 6.2 [FEU].

…

2. Bestämmelserna om rättslig prövning, ansvar och sanktioner i kapitel III i direktiv 95/46/EG skall gälla för de nationella bestämmelser som antas i enlighet med det här direktivet och för de individuella rättigheter som kan härledas från det här direktivet.

…”

2. GDPR

7. I artikel 2 (”Materiellt tillämpningsområde”) föreskrivs följande:

”1. Denna förordning ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register.

2. Denna förordning ska inte tillämpas på behandling av personuppgifter som

a) utgör ett led i en verksamhet som inte omfattas av unionsrätten,

…

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.

…”

8. I artikel 5 (”Principer för behandling av personuppgifter”) föreskrivs följande:

”1. Vid behandling av personuppgifter ska följande gälla:

…

b) De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska inte anses vara oförenlig med de ursprungliga ändamålen (ändamålsbegränsning).

…”

9. I artikel 6 (”Laglig behandling av personuppgifter”) föreskrivs följande:

”1. Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

…

e) Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

…

3. Den grund för behandlingen som avses i punkt 1 c och e ska fastställas i enlighet med

a) unionsrätten, eller

b) en medlemsstats nationella rätt som den personuppgiftsansvarige omfattas av.

…

4. Om en behandling för andra ändamål än det ändamål för vilket personuppgifterna samlades in inte grundar sig på den registrerades samtycke eller på unionsrätten eller medlemsstaternas nationella rätt som utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle för att skydda de mål som avses i artikel 23.1, ska den personuppgiftsansvarige för att fastställa huruvida behandling för andra ändamål är förenlig med det ändamål för vilket personuppgifterna ursprungligen samlades in bland annat beakta följande:

a) Kopplingar mellan de ändamål för vilka personuppgifterna har samlats in och ändamålen med den avsedda ytterligare behandlingen.

b) Det sammanhang inom vilket personuppgifterna har samlats in, särskilt förhållandet mellan de registrerade och den personuppgiftsansvarige.

c) Personuppgifternas art, särskilt huruvida särskilda kategorier av personuppgifter behandlas i enlighet med artikel 9 eller huruvida personuppgifter om fällande domar i brottmål och lagöverträdelser som innefattar brott behandlas i enlighet med artikel 10.

d) Eventuella konsekvenser för registrerade av den planerade fortsatta behandlingen.

…”

3. Direktiv 2016/680

10. I artikel 1 (”Syfte och mål”) föreskrivs följande i punkt 1:

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

11. I artikel 2 (”Tillämpningsområde”) föreskrivs följande i punkt 1:

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

12. I artikel 4 (”Principer för behandling av personuppgifter”) föreskrivs följande:

”1. Medlemsstaterna ska föreskriva att personuppgifter ska

…

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

…

2. Behandling som utförs av samma eller en annan personuppgiftsansvarig för något annat ändamål som anges i artikel 1.1 än det för vilket personuppgifterna samlas in ska tillåtas om

a) den personuppgiftsansvarige i enlighet med unionsrätten eller medlemsstaternas nationella rätt är bemyndigad att behandla sådana personuppgifter för ett sådant ändamål, och

b) behandlingen är nödvändig och står i proportion till detta andra ändamål i enlighet med unionsrätten eller medlemsstaternas nationella rätt.

…”

13. I artikel 9 (”Särskilda villkor för uppgiftsbehandling”) föreskrivs följande i punkt 1:

”Personuppgifter som samlas in av behöriga myndigheter för de ändamål som anges i artikel 1.1. ska inte behandlas för andra ändamål än de som anges i artikel 1.1 såvida inte sådan behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt. När personuppgifter behandlas för andra ändamål ska [GDPR] tillämpas, såvida inte behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten.”

B. Nationell rätt

1. Lietuvos Respublikos elektroninių ryšių įstatymas [7]

14. Enligt artikel 65.2 ska leverantörer av elektroniska kommunikationstjänster lagra de uppgifter som anges i bilaga 1 till samma lag och, i förekommande fall, göra uppgifterna tillgängliga för behöriga myndigheter så att de kan använda dem för att bekämpa grov brottslighet. [8]

[7] Republiken Litauens lag om elektronisk kommunikation, i dess lydelse enligt lag nr IX-2135 av den 15 april 2004, i dess lydelse enligt lag nr XIII-2172 av den 6 juni 2019 (nedan kallad lagen om elektronisk kommunikation).

[8] De uppgifter som räknas upp i nämnda bilaga (”Kategorier av uppgifter som ska skyddas”) är de uppgifter som är nödvändiga för att identifiera källa och slutmål för en kommunikation, dess datum, tid och varaktighet, typen av kommunikation och kommunikationsmediets plats (även för mobil kommunikation) hos användarna.

15. Enligt artikel 77.1 ska leverantörer av elektroniska kommunikationstjänster förse de behöriga myndigheterna med de uppgifter som de lagligen innehar och som är nödvändiga särskilt för att förebygga, upptäcka och lagföra brott.

16. I artikel 77.4 föreskrivs att om det finns ett motiverat rättsligt avgörande eller någon annan rättslig grund som föreskrivs i lag, ska leverantörer av elektroniska kommunikationstjänster göra det tekniskt möjligt, bland annat för brottsutredande myndigheter och förundersökningsmyndigheter, att på det sätt som föreskrivs i straffprocesslagstiftningen kontrollera innehållet i de kommunikationer som sprids via elektroniska kommunikationsnät.

2. Lietuvos Respublikos kriminalinės žvalgybos įstatymas [9]

17. Enligt artikel 6.3 led 1 får brottsutredande myndigheter [10] samla in information från leverantörer av elektroniska kommunikationstjänster om de villkor som uppställs i lagen om kriminalunderrättelser är uppfyllda och om de har tillstånd från åklagarmyndigheten eller en rättslig myndighet.

18. Enligt artikel 8.1 och 8.3 ska brottsutredande myndigheter agera så snart det finns tillgång till information om förberedelse eller genomförande av ett brott som är synnerligen allvarligt, allvarligt eller relativt allvarligt, varvid ett straffrättsligt förfarande omedelbart ska inledas om utredningen visar att ett brott har begåtts.

19. Enligt artikel 19.1 led 5 får information från brottsutredningar användas i de fall som avses i punkterna 3 och 4 i samma artikel och i andra fall som föreskrivs i lag.

20. Enligt artikel 19.3 får information om en gärning som uppfyller rekvisiten för korruptionsbrott i samråd med åklagarmyndigheten klassificeras om och användas inom ramen för en utredning om disciplinförseelser eller tjänstefel.

3. Lietuvos Respublikos baudžiamojo proceso kodeksa [11]

21. Enligt artikel 154 (”Kontroll, inspelning och lagring av information som sänts via elektroniska kommunikationsnät”), punkt 1, får en utredare, efter beslut av en förundersökningsdomare som fattar beslut på begäran av åklagarmyndigheten, lyssna på, registrera och lagra samtal som sprids via elektroniska kommunikationsnät, om det finns skäl att anta att det går att erhålla uppgifter om ett brott som är synnerligen allvarligt eller allvarligt om brottet vid tillfället förbereds, genomförs eller redan har genomförts, samt vid relativt allvarliga brott eller mindre allvarliga brott.

[9] Republiken Litauens lag om kriminalunderrättelser, i dess lydelse enligt lag nr XI-2234 av den 2 oktober 2012, i dess lydelse enligt lag nr XIII-1837 av den 20 december 2018 (nedan kallad lagen om kriminalunderrättelser).

[10] Jag kommer att använda termen ”information”, och inte ”underrättelseinformation”, för att beskriva de tjänster som tillhandahålls i utredningarna.

[11] Republiken Litauens straffprocessordning av den 14 mars 2002, i den lydelse som är tillämplig i det nationella målet (nedan kallad straffprocessordningen).

22. Enligt artikel 177 (”Sekretess för uppgifter från förundersökningar”) punkt 1 är uppgifterna i utredningen konfidentiella och får, till dess att ärendet prövas i domstol, endast lämnas ut efter tillstånd av åklagarmyndigheten och i den mån det är motiverat. [12]

II. Faktiska omständigheter, det nationella målet och tolkningsfrågan

23. Lietuvos Respublikos generalinė prokuratūra (Republiken Litauens riksåklagarmyndighet) (nedan kallad riksåklagarmyndigheten) inledde en intern utredning av A.G.:s handlingar. A.G. var då åklagare vid en Apygardos prokuratūra (regional åklagarmyndighet). Utredningen avsåg att det fanns uppgifter om att han hade agerat felaktigt i sin tjänsteutövning.

24. Riksåklagarmyndigheten drog slutsatsen att A.G. hade agerat felaktigt i sin tjänsteutövning och föreslog att A.G. skulle sägas upp från sin tjänst, som en disciplinåtgärd.

25. Beteendet hade fastställts på grundval av information som erhållits under det administrativa förfarandet och som härrörde från kriminalunderrättelseverksamhet, förklaringar från andra tjänstemän och klaganden samt de slutsatser som dragits vid två förundersökningar.

26. Det hade närmare bestämt förekommit telefonsamtal mellan A.G. och en misstänkt persons advokat inom ramen för en förundersökning som leddes av A.G. angående mål där denna advokat hade varit försvarare. [13]

27. Övervakningen och registreringen av information som överförts genom elektroniska kommunikationsnät hade godkänts genom domstolsbeslut.

28. Riksåklagarmyndigheten beslutade om uppsägning av A.G. som en sanktionsåtgärd. A.G. överklagade till Vilniaus apygardos administracinis teismas (Vilnius regionala förvaltningsdomstol, Litauen) och yrkade att detta beslut skulle upphävas.

29. Överklagandet ogillades genom dom av den 16 juli 2021, eftersom domstolen i första instans konstaterade att kriminalunderrättelsetjänsternas handlande varit tillåtet och att det även var tillåtet att, under disciplinärendet, använda de uppgifter som dessa tjänster hade inhämtat.

30. A.G. överklagade domen från första instans till Lietuvos vyriausiasis administracinis teismas (Högsta förvaltningsdomstolen, Litauen), som beslutade att hänskjuta följande tolkningsfråga till domstolen:

”Ska artikel 15.1 i … direktiv 2002/58 … jämförd med artiklarna 7, 8, 11 och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna [stadgan], tolkas så, att den innebär ett förbud för behöriga offentliga myndigheter att i utredningar om korruptionsrelaterade tjänstefel använda uppgifter som har lagrats av leverantörer av elektroniska kommunikationstjänster och som kan ge information om uppgifter om och kommunikation som har utförts av en användare

[12] Enligt Ikiteisminio tyrimo duomenų teikimo ir panaudojimo ne baudžiamojo persekiojimo tikslais ir ikiteisminio tyrimo duomenų apsaugos rekomendajos (Rekommendationer om tillhandahållande och användning av uppgifter från förundersökningar för andra ändamål än åtal samt skydd av uppgifter från förundersökningar), godkänd genom riksåklagarens order nr 1–279 av den 17 augusti 2017, senast ändrad genom order nr 1–211 av den 25 juni 2018, särskilt klausul 23, är det, när en begäran om tillgång till uppgifter från förundersökningar har mottagits, riksåklagaren som beslutar om huruvida uppgifterna ska göras tillgängliga. Om uppgifterna ska göras tillgängliga ska riksåklagaren ange hur de kan lämnas ut.

[13] Såsom påpekades vid förhandlingen är två brottmål fortfarande anhängiga mot A.G. och advokaten för dessa gärningar.

av ett elektroniskt kommunikationsmedel, oavsett om tillgång till dessa uppgifter i det specifika fallet har beviljats i syfte att bekämpa allvarlig brottslighet och förebygga allvarliga hot mot den allmänna säkerheten?”

III. Förfarandet vid EU-domstolen

31. Begäran om förhandsavgörande inkom till domstolens kansli den 3 mars 2022.

32. Skriftliga yttranden har inkommit från A.G. och den tjeckiska, den estniska, den ungerska, den irländska, den italienska och den litauiska regeringen samt från Europeiska kommissionen.

33. A.G., den franska, den ungerska, den irländska och den litauiska regeringen samt kommissionen deltog vid förhandlingen den 2 februari 2023.

IV. Bedömning

A. Frågan om begäran om förhandsavgörande kan upptas till sakprövning samt avgränsning av svaret på tolkningsfrågan

34. Den hänskjutande domstolen är en förvaltningsdomstol som är behörig att överpröva förvaltningsrättsliga beslut. Riksåklagarmyndighetens beslut, genom vilket en tjänsteman vid en regional åklagarmyndighet blev föremål för uppsägning som en sanktionsåtgärd på grund av tjänstefel, är ett sådant förvaltningsrättsligt beslut.

35. Den nationella tvisten avser således inte avgöranden av rättsliga myndigheter inom straffrätten. Även om sådana avgöranden förekommer samtidigt med det administrativa (disciplinära) förfarande som ledde till uppsägning,[14] ska det påpekas att tvisten endast gäller det administrativa förfarandet.

36. Det finns dock vissa oklarheter i beslutet om hänskjutande vad gäller de faktiska omständigheter i målet som beskriver det sammanhang som tolkningsfrågan ingår i.

37. Såsom den tjeckiska regeringen och kommissionen har påpekat är det inte möjligt att utifrån beslutet om hänskjutande med säkerhet fastställa huruvida de behöriga myndigheterna vände sig till leverantörer av elektroniska kommunikationstjänster för att få fram de omtvistade uppgifterna eller om de erhöll dessa uppgifter direkt på egen hand.

38. Frågan är absolut inte oviktig. Det är den som avgör vilken unionslagstiftning som är relevant för att besvara tolkningsfrågan. Följande respektive direktiv ska tillämpas, beroende på om uppgifterna inkom på det ena eller det andra sättet:

– Direktiv 2002/58 om de uppgifter som erhölls är resultatet av en skyldighet att behandla uppgifter vilken åligger leverantörer av elektroniska kommunikationstjänster.

– Direktiv 2016/680 om uppgifterna erhölls direkt av den offentliga myndigheten utan att dessa leverantörer ålades några skyldigheter.

[14] Se fotnot 13 ovan.

39. I det andra fallet skulle skyddet av personuppgifterna regleras av nationell rätt, utan att det påverkar tillämpningen av direktiv 2016/680.[15] Tolkningsfrågan skulle därför, genom att lägga tonvikten på direktiv 2002/58, ha haft en felaktig utgångspunkt.

40. Den ungerska regeringen är övertygad om att personuppgifterna erhölls genom telefonavlyssning av kriminalunderrättelseverksamheten och har ifrågasatt att begäran om förhandsavgörande kan tas upp till sakprövning, eftersom direktiv 2002/58 i och med detta inte är tillämpligt.

41. Kommissionen anser emellertid att

– direktiv 2016/680 gäller i den mån det är fråga om att, till en senare utredning, använda personuppgifter som samlats in och lagrats direkt av myndigheterna i samband med en föregående brottsutredning.

– direktiv 2002/58 är tillämpligt om, såsom den nationella domstolen har angett,[16] åtminstone vissa av uppgifterna har behövt samlas in och lagras med stöd av en nationell bestämmelse som antagits med stöd av artikel 15.1 i direktivet. Direktiv 2002/58 skulle därmed vara relevant för utgången i målet.

42. Jag delar kommissionens uppfattning, som för övrigt är den enda som gör det möjligt att klargöra de (berättigade) tvivel som beslutet om hänskjutande ger upphov till vad gäller frågan huruvida begäran om förhandsavgörande kan tas upp till sakprövning.

43. Om tolkningsfrågan förstås på detta sätt gäller följande för frågan om direktiv 2002/58 är relevant för svaret:

– Relevansen följer av den inneboende presumtionen att varje begäran om förhandsavgörande är nödvändig, vilket det ankommer på den hänskjutande domstolen att pröva.[17]

– Den kan medges i den mån det endast är med avseende på direktiv 2002/58, som den nationella domstolen anser vara avgörande för målets avgörande, som domstolens tolkning har begärts.[18]

44. Enligt den hänskjutande domstolen är nämligen följande relevant i den tvist som anhängiggjorts vid den:

”i) Tillgången till *uppgifter som har lagrats av leverantörer av elektroniska kommunikationstjänster* även i andra syften än att bekämpa grov brottslighet och förebygga allvarliga hot mot den allmänna säkerheten.

[15] Domen La Quadrature du Net, punkt 103: ”När medlemsstaterna däremot 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].”

[16] Punkt 37 i beslutet om hänskjutande.

[17] Se dom av den 4 december 2018, Minister for Justice and Equality och Commissioner of An Garda Síochána (C-378/17, EU:C:2018:979, punkt 26), och dom av den 22 december 2022, Airbnb Ireland och Airbnb Payments UK (C-83/21, EU:C:2022:1018, punkt 82).

[18] Den otvetydiga hänvisningen till direktiv 2002/58 i avgörandedelen i beslutet om hänskjutande och den omständigheten att direktiv 2016/680 inte nämns i motiveringen talar för samma sak. Domstolen kan emellertid, utan att överskrida gränserna för frågan, ge den hänskjutande domstolen vägledning som är användbar för dess avgörande, med hänvisning till andra unionsrättsliga bestämmelser. Se, för ett liknande resonemang, dom av den 18 september 2019, VIPA (C-222/18, EU:C:2019:751, punkt 50 och där angiven rättspraxis).

ii) A*nvändning* i utredningen om tjänstefel i samband med korruption *av lagrade uppgifter* som har inhämtats i syfte att bekämpa grov brottslighet och för att förebygga allvarliga hot mot den allmänna säkerheten”.[19]

45. Allt tyder således på att det, oberoende av den eventuella förekomsten av personuppgifter vars behandling inte skulle kunna omfattas av tillämpningsområdet för direktiv 2002/58 (utan omfattas av tillämpningsområdet för direktiv 2016/680), i den utredning som gav upphov till den ålagda disciplinåtgärden användes personuppgifter som samlats in av leverantörer av elektroniska kommunikationstjänster.

46. Domstolens svar ska begränsas till den hänskjutande domstolens begäran såsom den har framställts av den hänskjutande domstolen. Det ska således fastställas huruvida personuppgifter som erhållits och behandlats i enlighet med artikel 15.1 i direktiv 2002/58 inom ramen för en brottsutredning därefter kan användas i ett (administrativt) disciplinärt förfarande mot en offentlig tjänsteman.

47. Efter denna avgränsning av villkoren för begäran om förhandsavgörande, är den andra sidan av vad som sagts ovan att följande frågor inte omfattas av begäran om förhandsavgörande:

– För det första, frågor som avser lagenligheten av det *ursprungliga erhållandet* av personuppgifterna med stöd av artikel 15.1 i direktiv 2002/58. Den hänskjutande domstolens fråga är begränsad till *den senare användningen* av dessa uppgifter i det disciplinära förfarandet, utan ifrågasättande av lagenligheten av erhållandet av dem från början.[20]

– För det andra, frågor som avser användning av uppgifter som har erhållits och behandlats direkt av offentliga myndigheter i samband med tidigare brottsutredningar. På denna punkt, som regleras av nationell rätt och direktiv 2016/680, hyser den hänskjutande domstolen inte heller några tvivel.

48. Sammanfattningsvis ska det inte göras någon tolkning av direktiv 2016/680 när det gäller prövningen i sak.[21] Vad gäller direktiv 2002/58 kommer sakprövningen att begränsa sig till användning av personuppgifter som har erhållits enligt direktivet genom behandlingar som ska anses vara tillåtna från början, eftersom den inte har ifrågasatts i det nationella målet.

[19] Punkt 35 i beslutet om hänskjutande. Min kursivering.

[20] Det är således inte nödvändigt att EU-domstolen uttalar sig om huruvida dessa tidigare åtgärder är tillåtna. Om så blir fallet ska det upprepas att *tillgång* till uppgifter som innehas av leverantörer av elektroniska kommunikationstjänster endast kan ges om *lagringen* av uppgifterna är förenlig med artikel 15.1 i direktiv 2002/58. Se, för ett liknande resonemang, domen La Quadrature du Net, punkt 167. Denna bestämmelse, jämförd med artiklarna 7, 8 och 11 samt artikel 52.1 i stadgan, utgör hinder för lagstiftningsåtgärder som för dessa ändamål i preventivt syfte föreskriver en generell och odifferentierad lagring av trafikuppgifter och lokaliseringsuppgifter (domen La Quadrature du Net, punkt 168).

[21] Jag återkommer emellertid till detta i andra hand i den avslutande delen av detta förslag till avgörande.

B. Prövning i sak

1. Sammanfattning av domstolens praxis avseende tillämpningen av direktiv 2002/58

49. Det framgår av artikel 15.1 första meningen i direktiv 2002/58 att medlemsstaterna får vidta en åtgärd som avviker från den princip om konfidentialitet som fastställs i artikel 5.1 i direktivet om den ”i ett demokratiskt samhälle är nödvändig, lämplig och proportionell” och är i ”strikt” proportion till det avsedda ändamålet. [22]

50. I synnerhet ska medlemsstaternas möjlighet att motivera en begränsning av de rättigheter och skyldigheter som föreskrivs i artiklarna 5, 6 och 9 i direktiv 2002/58 bedömas med hänsyn till allvaret i det ingrepp som denna inskränkning innebär och genom en kontroll av att vikten av det mål av allmänt intresse som eftersträvas med begränsningen står i proportion till ingreppets allvar. [23]

51. ”För att kravet på proportionalitet ska vara uppfyllt måste det i lagstiftning föreskrivas klara och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden samt anges minimikrav, så att de personer vars personuppgifter berörs har tillräckliga garantier för att uppgifterna på ett effektivt sätt är skyddade mot riskerna för missbruk. Denna lagstiftning ska vara rättsligt bindande enligt nationell rätt och i synnerhet ange under vilka omständigheter och på vilka villkor en åtgärd avseende behandling av sådana uppgifter får vidtas…”. [24]

52. När det gäller skäl av allmänintresse som gör det möjligt att motivera en åtgärd som vidtagits med stöd av artikel 15.1 i direktiv 2002/58, är målen i enlighet med proportionalitetsprincipen ordnade i en hierarki utifrån målens betydelse: vikten av att vidta en sådan åtgärd måste stå i proportion till ingreppets allvar. [25]

53. I denna målhierarki är skyddet för den nationella säkerheten, tolkat mot bakgrund av artikel 4.2 FEU, överordnat de övriga mål som anges i artikel 15.1 i direktiv 2002/58, nämligen försvar, allmän säkerhet samt förebyggande, undersökning, avslöjande av och åtal för brott eller obehörig användning av ett elektroniskt kommunikationssystem. Målet att bekämpa brottslighet i allmänhet, även allvarlig sådan, och att skydda den allmänna säkerheten, återfinns i denna andra kategori. [26]

54. Utifrån denna kategorisering av målen kan följande slutsatser dras:

– Målet att försvara den nationella säkerheten, vilket ligger högst i den hierarki som EU-domstolen har angett, tillåter lika allvarliga ingrepp som dem som följer av lagstiftningsåtgärder som gör det möjligt att ålägga leverantörer av elektroniska

[22] Domen La Quadrature du Net, punkt 129.

[23] Domen La Quadrature du Net, punkt 131 och där angiven rättspraxis.

[24] Domen Commissioner of An Garda Síochána, punkt 54.

[25] Domen Commissioner of An Garda Síochána, punkt 56.

[26] Domen La Quadrature du Net, punkterna 135 och 136, där det förklaras att den nationella säkerheten är statens eget ansvar och att det svarar mot det grundläggande intresset av att skydda statens väsentliga funktioner och samhällets grundläggande intressen när den står inför verksamhet som allvarligt kan störa de grundläggande konstitutionella, politiska, ekonomiska eller sociala strukturerna i ett land och i synnerhet direkt hota samhället, befolkningen eller staten som sådan, såsom bland annat terrorverksamhet. Sådana hot skiljer sig, till sin art och på grund av sitt särskilda allvar, från risken i allmänhet för oroligheter eller störningar, även allvarliga sådana, av den allmänna säkerheten. Målet att skydda nationell säkerhet kan således motivera åtgärder som innebär mer långtgående ingrepp i de grundläggande rättigheterna än dem som dessa övriga mål skulle kunna motivera.

kommunikationstjänster en skyldighet att generellt och utan åtskillnad lagra trafikuppgifter och lokaliseringsuppgifter. [27]

– Det näst viktigaste målet, nämligen kampen mot grov brottslighet, kan motivera ingrepp såsom exempelvis selektiv lagring av trafik- och lokaliseringsuppgifter eller av IP-adresser som hänförs till en anslutnings källa, under en tidsperiod som begränsas till vad som är absolut nödvändigt. [28]

2. Tillämpning av denna rättspraxis inom ramen för förevarande begäran om förhandsavgörande

55. Enligt den hänskjutande domstolen har de aktuella uppgifterna erhållits genom allvarliga ingrepp i de rättigheter som garanteras genom artiklarna 7, 8 och 11 i stadgan. [29]

56. Det ska upprepas att det i detta hänseende inte är fråga om att undersöka den ursprungliga tillåtligheten av inhämtandet av dessa uppgifter, det vill säga att bedöma huruvida ingreppet var tillräckligt motiverat med hänsyn till hur allvarlig den aktuella överträdelsen var.

57. På dessa två punkter (ingreppets allvar och överträdelsens allvar) har den hänskjutande domstolen uttalat sig på ett sätt som inte har ifrågasatts i det nationella förfarandet och som således inte är relevant för begäran om förhandsavgörande.

58. Det som nu är av betydelse är, enligt den nationella domstolen, huruvida dessa uppgifter a) även kan användas i samband med efterföljande utredningar som syftar till att bekämpa brottslighet i allmänhet (varvid det antas att det handlande som är föremål för den omtvistade disciplinåtgärden omfattas av detta begrepp), eller b) endast får användas vid utredningar som syftar till att bekämpa allvarlig brottslighet.

59. Den tjeckiska och den irländska regeringen har undersökt om det aktuella beteendet vid den hänskjutande domstolen förtjänar att kvalificeras som ett ”allvarligt brott” och har kommit fram till att så är fallet.

60. Enligt min mening är detta emellertid en fråga som domstolen inte behöver uttala sig om, eftersom kvalificeringen av beteendet omfattas av den hänskjutande domstolens behörighet.

61. Den hänskjutande domstolen har angett att om användningen av de uppgifter som erhållits genom ett allvarligt ingrepp i de grundläggande rättigheterna endast kunde vara motiverad i kampen mot grov brottslighet och för att förebygga allvarliga hot mot den allmänna säkerheten, skulle dessa uppgifter inte kunna användas vid utredningar av disciplinära fel i samband med korruption, [30] det vill säga i sådana undersökningar som är i fråga i detta mål.

[27] Domen Commissioner of An Garda Síochána, punkt 58.

[28] Domen La Quadrature du Net, punkt 168.

[29] Detta framgår av punkt 46 i beslutet om hänskjutande. Där hänvisas till uppgifter som kan tillhandahålla information om kommunikation som har utförts av en användare av elektroniska kommunikationsmedel eller platsen där vederbörande har använt terminalutrustning och som gör det möjligt att dra precisa slutsatser om de berörda personernas privatliv.

[30] Beslutet om hänskjutande, punkt 46, *in fine*.

62. Utifrån denna bedömning är det intressanta att få klarhet i huruvida de disciplinära förseelser, för vars utredning vissa personuppgifter är avsedda att användas, kvalitativt sett, med hänsyn till sitt allvar, måste motsvara de brott som motiverade insamling av dessa uppgifter. [31]

63. Vid förhandlingen medgav den litauiska regeringen att uppsägningen hade skett på grund av att åklagaren hade begått ett etiskt fel. Bedömningen av huruvida detta fel (otillåtet utlämnande av uppgifter om en förundersökning) kan likställas med ett allvarligt brott eller medföra en allvarlig risk för skyddet av den allmänna säkerheten beror på en rad omständigheter som endast den hänskjutande domstolen kan kontrollera. [32]

64. Vid förhandlingen gjordes åtskilliga hänvisningar till kampen mot korruption, som är en företeelse som ligger till grund för sådana beteenden som det som är i fråga i förevarande mål. På denna punkt krävs en del nyansering av diskussionen, med hänsyn till den noggrannhet som krävs för alla uttryck för statens makt att utdela straff. Det ska exempelvis fastställas huruvida begreppet ”korruption” används i allmän mening eller om det hänvisas till en specifik typ av beteende i vilket det teoretiskt sett vore orimligt att inkludera ett blott åsidosättande av tystnadsplikten om det inte har medfört en fördel för tjänstemannen. [33]

65. Om den hänskjutande domstolen skulle finna att den överträdelse av etiska regler för vilken en påföljd här har ålagts är mindre allvarlig än det brott vars utredning motiverade den åtgärd som vidtogs med stöd av artikel 15 i direktiv 2002/58, följer svaret på tolkningsfrågan under alla omständigheter av dessa förklaringar av domstolen:

– ”[Å]tkomst till trafik- och lokaliseringsuppgifter som lagrats av leverantörer med tillämpning av en åtgärd som vidtagits med stöd av artikel 15.1 i direktiv 2002/58, vilken ska ske med iakttagande av de villkor som följer av rättspraxis avseende tolkningen av direktiv 2002/58, [kan] i princip endast … motiveras av det mål av allmänt samhällsintresse som ligger till grund för leverantörernas skyldighet att lagra uppgifterna. Så förhåller det sig alltid såvida inte syftet med åtkomsten till uppgifterna är av större betydelse än det mål som ligger till grund för lagringen”. [34]

– ”[I] synnerhet [kan] åtkomst till sådana uppgifter i syfte att lagföra och beivra ordinära brott inte i något fall … medges när lagringen av dem har motiverats med målet att bekämpa grov brottslighet eller, i ännu högre grad, målet att skydda nationell säkerhet.” [35]

[31] Europadomstolens dom av den 18 januari 2022, Adomaitis mot Litauen (CE:ECHR:2022:0118JUD001483318) (nedan kallad Europadomstolens dom Adomaitis), angående avlyssning av elektroniska kommunikationer vid kontinuerligt maktmissbruk från en kriminalvårdsanstalts sida, tillhandahåller metoder för att bedöma huruvida sådan likvärdighet föreligger.

[32] Straffbara handlingar som prövas i ett straffrättsligt förfarande kan som regel inte likställas med rent etiska fel för vilka påföljder formaliseras genom ett disciplinärt förfarande. Brottmålsförfarandet och det disciplinära förfarandet skiljer sig åt vad gäller sina föremål och arten av och allvaret i det beteende för vilket en påföljd har utgått. Skillnaderna mellan förfarandena visar i detta avseende på hur deras respektive föremål är olika allvarliga.

[33] I Konvention utarbetad på grundval av artikel K 3.2 c i Fördraget om Europeiska unionen om kamp mot korruption som tjänstemän i Europeiska gemenskaperna eller Europeiska unionens medlemsstater är delaktiga i (EGT C 195, 1997, s. 2) anges fall av mutbrott (”varje avsiktlig handling som utförs av en tjänsteman för att, direkt eller genom tredje man, för egen räkning eller för tredje mans räkning, begära eller ta emot förmåner, oavsett art, eller att acceptera löften härom för att på ett sätt som strider mot hans officiella förpliktelser utföra eller underlåta att utföra en handling i tjänsten eller vid utövandet av tjänsten”) och bestickning (”varje avsiktlig handling som utförs av en person för att direkt eller genom tredje man utlova eller bevilja en förmån, oavsett art, till en tjänsteman, för egen räkning eller för tredje mans räkning, för att denne på ett sätt som strider mot hans officiella förpliktelser skall utföra eller underlåta att utföra en handling i tjänsten eller vid utövandet av tjänsten”) som ska klassificeras som brott.

[34] Domen Commissioner of An Garda Síochána, punkt 98.

[35] Domen La Quadrature du Net, punkt 166.

66. Här gäller således ett slags princip om likvärdighet mellan å ena sidan de mål av allmänintresse som motiverar *insamlande* av personuppgifter och å andra sidan dem som motiverar att personuppgifterna senare *används*. Det enda undantaget från denna princip är, såsom angetts ovan, när betydelsen av det mål som eftersträvas genom tillgången är större än betydelsen av det mål som låg till grund för bevarandet.

67. En annan bedömning skulle innebära att skyddssystemet i direktiv 2002/58 snedvrids: de rättigheter som direktivet skyddar skulle kunna bli föremål för allvarliga ingrepp i andra fall än dem som föreskrivs i artikel 15 och på de villkor som fastställts i domstolens rättspraxis.

68. I synnerhet är det endast legitimt att offra rätten till konfidentiell kommunikation mot bakgrund av det särskilda mål av allmänt intresse som det tjänar. Det är därför rätten att få tillgång till de lagrade uppgifterna ska bedömas från fall till fall, varvid det ska göras en avvägning mellan å ena sidan hur allvarligt ingreppet är och å andra sidan betydelsen av det mål av allmänt intresse som eftersträvas med detta ingrepp.

69. Det som inte kan godtas som en tolkning av direktiv 2002/58 är att det, när tillgång har beviljats i ett giltigt motiverat första fall, är fritt fram för senare tillgång (i själva verket ett vidareautnyttjande av insamlade uppgifter) som grundar sig på ett mål som hierarkiskt sett ligger lägre än syftet med det ursprungliga fallet.

70. De krav som uppställs för den ursprungliga tillgången (inklusive de krav som domstolen ställer i fråga om tillåtligheten av den) [36] kan i detta syfte överföras på andra myndigheters senare användning av samma uppgifter.

C. I andra hand: relevansen av direktiv 2016/680

71. Jag har hittills redogjort för vad jag anser lämpligast för att besvara begäran om förhandsavgörande såsom den är formulerad, det vill säga genom att ge den hänskjutande domstolen en tolkning av direktiv 2002/58, såsom den hänskjutande domstolen har begärt.

72. Om de uppgifter som är tvistiga i detta mål inte hade inhämtats med stöd av artikel 15 i direktiv 2002/58, utan direkt av medlemsstatens kriminalunderrättelseverksamhet, inom ramen för ett straffrättsligt förfarande, skulle detta scenario vara annorlunda.

73. I ett sådant fall skulle bestämmelserna i nationell rätt vara tillämpliga, utan att det påverkar tillämpningen av direktiv 2016/680 när det gäller behandling av personuppgifter som samlats in i samband med en brottsutredning. Jag antar att kriminalunderrättelseverksamheten i ett sådant fall omfattas av direktiv 2016/680. Detta bekräftades vid förhandlingen.

74. Jag förklarade följande i mitt förslag till avgörande i målet Inspektor v Inspektorata kam Vissy sahan savet (Ändamål för behandlingen av uppgifter – Brottsutredning) [37]: ”Den allmänna dataskyddsförordningen och direktiv 2016/680 utgör ett sammanhängande system där

– den allmänna dataskyddsförordningen innehåller *allmänna bestämmelser* för att skydda fysiska personer i samband med behandling av deras personuppgifter,

[36] Domen Commissioner of An Garda Síochána, punkt 106, med hänvisning till domen Prokuratuur, punkt 51.

[37] C-180/21 (EU:C:2022:406) (nedan kallat förslaget Inspektor v Inspektorata).

– direktiv 2016/680 innehåller *särskilda bestämmelser* för behandling av sådana uppgifter på områdena för straffrättsligt samarbete och polissamarbete.” [38]

75. Jag påpekade då [39] följande:

– ”Det system som utgörs av dessa båda rättsakter ger ett skydd som bygger på principerna om laglighet, rättvisa och insyn samt, i det här aktuella sammanhanget, principen om att personuppgifter bara ska samlas in och behandlas för lagstadgade ändamål.”

– ”Närmare bestämt föreskrivs i artikel 5.1 b i den allmänna dataskyddsförordningen att personuppgifter 'ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål *och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål*'. Vad beträffar *lex specialis* återfinns samma formulering i artikel 4.1 b i direktiv 2016/680.”

– ”Personuppgifter får således inte samlas in eller behandlas generellt, utan bara för vissa ändamål och på vissa laglighetsvillkor som fastställts av unionslagstiftaren.” [40]

– ”Principen om att det ska finnas ett strikt samband mellan, å ena sidan, insamling och behandling av personuppgifter och, å andra, sidan ändamålen för denna insamling och behandling är inte absolut. Såväl den allmänna dataskyddsförordningen som direktiv 2016/680 medger en viss flexibilitet…”

76. Såsom domstolen har tolkat artikel 4.2 i direktiv 2016/680 [41] kan det knappast godtas att personuppgifter som samlats in inom ramen för ett straffrättsligt förfarande används *för samma ändamål* i samband med ett senare disciplinärt förfarande mot en offentlig tjänsteman.

77. Det ska emellertid påpekas att enligt artikel 4.2 i direktiv 2016/680 ska ”[b]ehandling som utförs av samma eller en annan personuppgiftsansvarig för något annat ändamål som anges i artikel 1.1 än det för vilket personuppgifterna samlas in … tillåtas om:

– den personuppgiftsansvarige i enlighet med unionsrätten eller medlemsstaternas nationella rätt är bemyndigad att behandla sådana personuppgifter för ett sådant ändamål, och

– behandlingen är nödvändig och står i proportion till detta andra ändamål i enlighet med unionsrätten eller medlemsstaternas nationella rätt”.

78. Utifrån denna utgångspunkt ska den hänskjutande domstolen pröva huruvida (*det särskilda*) syftet med den senare behandlingen omfattas av de syften som föreskrivs i artikel 1.1 i direktiv 2016/680 eller om det faller utanför dessa.

– I det första fallet (*internt* hänförande) ska det kontrolleras att de två villkor som föreskrivs i artikel 4.2 i direktiv 2016/680 är uppfyllda.

[38] Förslaget Inspektor v Inspektorata, punkt 35.

[39] Förslaget Inspektor v Inspektorata, punkt 36–39.

[40] Kravet på ”laglighet” uppställs i artikel 5.1 a i dataskyddsförordningen (artikel 4.1 a i direktiv 2016/680), genom att det i artikel 6 i dataskyddsförordningen förklaras vilka villkor som gäller för detta. Vad gäller det som är av intresse här och i enlighet med led e i den sistnämnda bestämmelsen ska behandlingen vara nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i en myndighetsutövning som utförs av den personuppgiftsansvarige (av själva behandlingen).

[41] Dom av den 8 december 2022, Inspektor v Inspektorata kam Visshia sadeben savet (”Ändamål för behandlingen av uppgifter – Brottsutredning”), C-180/21 (EU:C:2022:967) (nedan kallad domen Inspektor v Inspektorata).

– I det andra fallet (*externt* hänförande) är det artikel 9.1 i direktiv 2016/680 som är aktuell.

1. Användning av uppgifterna enligt artikel 4.2 i direktiv 2016/680

79. Vad gäller det *första* av de två villkor som uppställs i denna bestämmelse ska det endast prövas om medlemsstatens lagstiftning kommer till uttryck i en lag [42] som reglerar när den ansvarige får behandla personuppgifter. Denna lag ska dessutom innehålla tvingande, klara och precisa bestämmelser. [43]

80. Det är emellertid en fråga som det naturligtvis ankommer på den hänskjutande domstolen att kontrollera, efter att ha analyserat artikel 177 i straffprocessordningen, artikel 19.3 i lagen om kriminalunderrättelser och Riksåklagarens rekommendationer. [44] Med hjälp av dessa uppgifter ska det bedömas i vilken mån den nationella lagstiftningen tillåter att uppgifter som samlats in inom ramen för ett straffrättsligt förfarande under vissa förutsättningar kan användas inom ramen för utredningen om disciplinförseelser. Vid denna kontroll kan övervägandena i Europadomstolens dom Adomaitis vara användbara för den. [45]

81. Vad gäller det *andra* villkoret ska den hänskjutande domstolen bedöma huruvida ingreppet är nödvändigt och proportionerligt i behandlingen av de uppgifter som är i fråga i det aktuella målet. [46]

82. Återigen skulle det som anges i Europadomstolens dom Adomaitis kunna bidra till denna bedömning:

– Vad gäller nödvändigheten ska det göras en avvägning av i vilken mån det förhållandet att de övriga uppgifter som fanns tillgängliga under det disciplinära förfarandet inte var tillräckliga som bevisning verkligen gjorde det nödvändigt att använda sig av de omtvistade uppgifterna för att den pågående utredningen skulle bli framgångsrik. [47]

– Vad gäller proportionaliteten ska det göras en bedömning av hur allvarlig den överträdelse som ligger till grund för det disciplinära förfarandet är, med beaktande av att användningen av personuppgifter, såsom den litauiska regeringen har gjort gällande och som framgår av Europadomstolens dom Adomaitis [48], är förbehållen överträdelser för vilka den strängaste disciplinåtgärden, det vill säga uppsägning, föreskrivs.

[42] Jag delar kommissionens uppfattning att eftersom en senare användning av personuppgifter som samlats in under en brottsutredning utgör ett ingrepp i de grundläggande rättigheter som garanteras genom artiklarna 7 och 8 i stadgan, är det enligt artikel 52.1 i stadgan nödvändigt att den är föreskrivet i lag.

[43] Punkt 51 ovan.

[44] Fotnot 12 ovan.

[45] Dom i vilken det i punkt 83 anses vara tillräckligt att säkerställa lagenligheten av det ingrepp som garanteras genom nationella lagbestämmelser och litauisk konstitutionell rättspraxis.

[46] Som kommissionen har påpekat skiljer sig inte detta mål väsentligt från det mål som prövades i Europadomstolens dom av den 16 juni 2016, Versini-Campinchi och Crasnianski mot Frankrike (CE:ECHR:2016:0616JUD004917611). Enligt punkt 57 i denna dom svarar det mot ett berättigat mål, i den mening som avses i artikel 8 i Europakonventionen, att inom ramen för ett disciplinärt förfarande om åsidosättande av tystnadsplikten använda kommunikation inom ramen för ett straffrättsligt förfarande. Det nära materiella sambandet mellan syftena med det straffrättsliga förfarandet och det disciplinära förfarandet leder till en gemensam legitimitet för målen för båda två.

[47] Europadomstolens dom Adomaitis, punkt 85.

[48] Europadomstolens dom Adomaitis, punkt 87.

2. Användning av uppgifterna enligt artikel 9 i direktiv 2016/680

83. Enligt artikel 9.1 i direktiv 2016/680 får personuppgifter som samlas in av behöriga myndigheter för de ändamål som anges i artikel 1.1 i direktivet behandlas för andra ändamål än de som anges i artikel 1.1, om sådan behandling är tillåten enligt unionsrätten eller medlemsstaternas nationella rätt. I det fallet ska GDPR tillämpas, såvida inte behandlingen utförs som ett led i en verksamhet som inte omfattas av unionsrätten. [49]

84. För det fall den hänskjutande domstolen skulle finna att artikel 4.2 i direktiv 2016/680 inte är tillämplig, ska det hänvisas till GDPR. I enlighet med GDPR ska det, utöver det förhållandet att behandlingen ska vara föreskriven i lag, fastställas huruvida åtminstone ett av de villkor som uttömmande räknas upp i artikel 6.1 i förordningen för att behandling av personuppgifter ska vara tillåten är uppfyllt.

V. Förslag till avgörande

85. Mot bakgrund av det ovan anförda föreslår jag att domstolen besvarar de frågor som Lietuvos vyriausiasis administracinis teismas (Högsta förvaltningsdomstolen, Litauen) har ställt enligt följande:

1. Artikel 15.1 i Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation), jämförd med artiklarna 7, 8, 11 och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna

   ska tolkas så,

   att den inte tillåter att behöriga offentliga myndigheter samlar in uppgifter som lagrats av leverantörer av elektroniska kommunikationstjänster vilka kan tillhandahålla detaljerad information om en användare, och använder dessa i samband med utredningar av handlingar som utgör mindre allvarliga förseelser än de handlingar för vars utredning tillgång till uppgifterna kunde motiveras.

2. I andra hand:

   Artikel 9.1 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, jämförd med artiklarna 6 och 10 i Europaparlamentets och rådets förordning (EU) 2016/679 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, mot bakgrund av artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna,

   ska tolkas så,

[49] Detta undantag tolkades restriktivt i domen av den 22 juni 2021, Latvijas Republikas Saeima (Prickning vid överträdelser av trafikregler) (C-439/19, EU:C:2021:504, punkt 66).

att den inte utgör hinder för att i ett administrativt disciplinärt förfarande använda personuppgifter som samlats in lagenligt och direkt av offentliga myndigheter i samband med en brottsutredning, förutsatt att det, enligt klara, precisa och tvingande regler i nationell rätt, finns ett samband mellan detta förfarande och denna utredning, och så länge användningen av uppgifterna sker för ett legitimt ändamål och är nödvändig och proportionerlig, vilket det ankommer på den rättsliga myndigheten att fastställa.