



# Rättsfallssamlingen

DOMSTOLENS DOM (stora avdelningen)

den 20 september 2022 \*

[Text rättad genom beslut av den 27 oktober 2022]

”Begäran om förhandsavgörande – Behandling av personuppgifter inom sektorn för elektronisk kommunikation – Konfidentialitet vid kommunikation – Leverantörer av elektroniska kommunikationstjänster – Generell och odifferentierad lagring av samtliga trafik- och lokaliseringsuppgifter – Direktiv 2002/58/EG – Artikel 15.1 – Europeiska unionens stadga om de grundläggande rättigheterna – Artiklarna 6, 7, 8, 11 och 52.1 – Artikel 4.2 FEU”

I de förenade målen C-793/19 och C-794/19,

angående beslut att begära förhandsavgörande enligt artikel 267 FEUF, från Bundesverwaltungsgericht (Federala högsta förvaltningsdomstolen, Tyskland), av den 25 september 2019, som inkom till domstolen den 29 oktober 2019, i målen

**Bundesrepublik Deutschland**, företrädd av Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen,

mot

**SpaceNet AG** (C-793/19),

**Telekom Deutschland GmbH** (C-794/19),

meddelar

DOMSTOLEN (stora avdelningen),

sammansatt av ordföranden K. Lenaerts, avdelningsordförandena A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis och I. Ziemele samt domarna T. von Danwitz, M. Safjan, F. Biltgen, P.G. Xuereb (referent), N. Piçarra, L.S. Rossi och A. Kumin,

generaladvokat: M. Campos Sánchez-Bordona,

justitiesekreterare: enhetschefen D. Dittert,

efter det skriftliga förfarandet och förhandlingen den 13 september 2021,

\* Rättegångsspråk: tyska.

med beaktande av de yttranden som avgetts av:

- Bundesrepublik Deutschland, företrädd av Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, genom C. Mögelin, i egenskap av ombud,
- [I rättad lydelse enligt beslut av den 27 oktober 2022] SpaceNet AG, genom M. Bäcker, Universitätsprofessor,
- Telekom Deutschland GmbH, genom T. Mayen, Rechtsanwalt,
- Tysklands regering, genom J. Möller, F. Halibi, M. Hellmann, D. Klebs och E. Lankenau, samtliga i egenskap av ombud,
- Danmarks regering, genom M. Jespersen, J. Nymann-Lindegren, V. Pasternak Jørgensen och M. Søndahl Wolff, samtliga i egenskap av ombud,
- Estlands regering, genom A. Kalbus och M. Kriisa, båda i egenskap av ombud,
- Irland, genom A. Joyce och J. Quaney, båda i egenskap av ombud, biträdda av D. Fennelly, BL, och P. Gallagher, SC,
- Spaniens regering, genom L. Aguilera Ruiz, i egenskap av ombud,
- Frankrikes regering, genom A. Daniel, D. Dubois, J. Illouz, E. de Moustier och T. Stéhelin, samtliga i egenskap av ombud,
- Cyperns regering, genom I. Neophytou, i egenskap av ombud,
- Nederländernas regering, genom K. Bulterman, A. Hanje och C.S. Schillemans, samtliga i egenskap av ombud,
- Polens regering, genom B. Majczyna, D. Lutostańska och J. Sawicka, samtliga i egenskap av ombud,
- Finlands regering, genom A. Laine och M. Pere, båda i egenskap av ombud,
- Sveriges regering, genom H. Eklinder, A. Falk, J. Lundberg, C. Meyer-Seitz, R. Shahsavan Eriksson och H. Shev, samtliga i egenskap av ombud,
- Europeiska kommissionen, genom G. Braun, S.L. Kaléda, H. Kranenborg, M. Wasmeier och F. Wilman, samtliga i egenskap av ombud,
- Europeiska datatillsynsmannen, genom A. Buchta, D. Nardi, N. Stolič och K. Ujazdowski, samtliga i egenskap av ombud,

och efter att den 18 november 2021 ha hört generaladvokatens förslag till avgörande,

följande

## Dom

- 1 Respektive begäran om förhandsavgörande avser tolkningen av 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) (EGT L 201, 2002, s. 37), i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 (EUT L 337, 2009, s. 11) (nedan kallat direktiv 2002/58), jämförd med artiklarna 6–8, 11 och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad stadgan) och artikel 4.2 FEU.
- 2 Respektive begäran har framställts i mål mellan å ena sidan Bundesrepublik Deutschland (Förbundsrepubliken Tyskland), företrädd av Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (federala myndigheten för el-, gas-, telekommunikations-, post- och järnvägsnät, Tyskland) och å andra sidan SpaceNet AG (mål C-793/19) och Telekom Deutschland GmbH (mål C-794/19) och rör den skyldighet som ålagts de sistnämnda att lagra trafik- och lokaliseringssuppgifter avseende deras kunders telekommunikationer.

### Tillämpliga bestämmelser

#### *Unionsrätt*

##### *Direktiv 95/46/EG*

- 3 Europaparlamentets och rådets direktiv 95/46/EG 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) upphävdes med verkan från och med den 25 maj 2018 genom 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 (allmän dataskyddsförordning) (EUT L 119, 2016, s. 1).
- 4 Artikel 3.2 i direktiv 95/46 hade följande lydelse:

”Detta direktiv gäller inte för sådan behandling av personuppgifter

  - som utgör ett led i en verksamhet som inte omfattas av gemenskapsrätten, exempelvis sådan verksamhet som avses i avdelningarna V och VI i Fördraget om Europeiska unionen, och inte under några omständigheter behandlingar som rör allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välbefinnande när behandlingen har samband med frågor om statens säkerhet) och statens verksamhet på straffrättens område,
  - av en fysisk person som ett led i verksamhet av rent privat natur eller som har samband med hans hushåll.”

*Direktiv 2002/58*

5 I skälen 2, 6, 7 och 11 i direktiv 2002/58 anges följande:

”(2) I detta direktiv eftersträvas respekt för de grundläggande rättigheterna och iakttagande av de principer som erkänns i synnerhet i [stadgan]. I synnerhet eftersträvas i detta direktiv att säkerställa full respekt för rättigheterna i artiklarna 7 och 8 i ... stadgan.

...

(6) Internet bryter upp traditionella marknadsstrukturer genom att tillhandahålla en gemensam, global infrastruktur för leverans av en mängd olika elektroniska kommunikationstjänster. Allmänt tillgängliga kommunikationstjänster via Internet öppnar nya möjligheter för användarna, men för även med sig nya risker för deras personuppgifter och integritet.

(7) När det gäller allmänna kommunikationsnät bör särskilda rättsliga och tekniska bestämmelser antas för att skydda fysiska personers grundläggande fri- och rättigheter samt juridiska personers berättigade intressen, särskilt med hänsyn till den ökade kapaciteten för automatisk lagring och behandling av uppgifter om abonnenter och användare.

...

(11) I likhet med direktiv 95/46... omfattar det här direktivet inte sådana frågor om skydd av grundläggande fri- och rättigheter som rör verksamhet som inte regleras av gemenskapslagstiftningen. Det ändrar därför inte den befintliga jämvikten mellan den enskildes rätt till integritet och medlemsstaternas möjligheter att vidta sådana åtgärder, enligt artikel 15.1 i det här direktivet, som krävs för att skydda allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välbefinnande när verksamheten rör statens säkerhet) och brottsbekämpning. Det här direktivet påverkar följaktligen inte medlemsstaternas möjlighet att utföra laglig avlyssning av elektronisk kommunikation eller att vidta andra åtgärder om det är nödvändigt för något av dessa ändamål och sker i enlighet med Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna [som undertecknades i Rom den 4 november 1950] i den tolkning dessa fått i rättspraxis från Europeiska domstolen för de mänskliga rättigheterna. Sådana åtgärder måste vara lämpliga, i strikt proportion till det avsedda ändamålet och nödvändiga i ett demokratiskt samhälle. De bör omfattas av lämpliga skyddsmekanismer i överensstämmelse med Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna.”

6 I artikel 1 i direktiv 2002/58, med rubriken ”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... 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 [EUF-fördraget], t.ex. de som omfattas av avdelningarna V och VI i [EU-fördraget], och inte i något fall på verksamheter som avser allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välbefinnande när verksamheten rör statens säkerhet) och statens verksamhet på straffrättens område.”

7 I artikel 2 i detta direktiv, med rubriken ”Definitioner”, anges följande:

”Om inte annat anges skall definitionerna i Europaparlamentets och rådets direktiv 95/46... och 2002/21/EG av den 7 mars 2002 om ett gemensamt regelverk för elektroniska kommunikationsnät och kommunikationstjänster (ramdirektiv) [(EGT L 108, 2002, s. 33)] gälla i detta direktiv.

Dessutom skall följande definitioner gälla:

- a) *användare*: en fysisk person som använder en allmänt tillgänglig elektronisk kommunikationstjänst för privat eller affärsmässigt bruk utan att nödvändigtvis ha abonnerat på denna tjänst.
- b) *trafikuppgifter*: alla uppgifter som behandlas i syfte att överföra en kommunikation via ett elektroniskt kommunikationsnät eller för att fakturera den.
- c) *lokaliseringssuppgifter*: alla uppgifter som behandlas i ett elektroniskt kommunikationsnät eller av en elektronisk kommunikationstjänst och som visar den geografiska positionen för terminalutrustningen för en användare av en allmänt tillgänglig elektronisk kommunikationstjänst.
- d) *kommunikation*: all information som utbyts eller överförs mellan ett begränsat antal parter genom en allmänt tillgänglig elektronisk kommunikationstjänst. Detta inbegriper inte information som överförs som del av en sändningstjänst för rundradio eller TV till allmänheten via ett elektroniskt kommunikationsnät utom i den mån informationen kan sättas i samband med den enskilde abonnenten eller användaren av informationen.

...”

8 I artikel 3 i direktiv 2002/58, med rubriken ”Berörda tjänster”, föreskrivs följande:

”Detta direktiv ska tillämpas på behandling av personuppgifter i samband med att allmänt tillgängliga elektroniska kommunikationstjänster tillhandahålls i allmänna kommunikationsnät inom gemenskapen, inbegripet allmänna kommunikationsnät som stöder datainsamling och identifieringsutrustning.”

9 I artikel 5 i direktivet, med rubriken ”Konfidentialitet vid kommunikation”, föreskrivs följande:

”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.

...

3. Medlemsstaterna ska se till att lagring av information eller tillgång till information som redan är lagrad i en abonnents eller användares terminalutrustning endast är tillåten på villkor att abonnenten eller användaren i fråga har gett sitt samtycke efter att ha fått tillgång till tydlig och fullständig information, i enlighet med direktiv 95/46..., bland annat om ändamålen med behandlingen av uppgifterna. Detta får inte förhindra någon teknisk lagring eller åtkomst som endast sker för att utföra överföringen av en kommunikation via ett elektroniskt kommunikationsnät eller det som är absolut nödvändigt för att leverantören ska kunna tillhandahålla en av informationssamhällets tjänster som användaren eller abonnenten uttryckligen har begärt.”

10 I artikel 6 i direktiv 2002/58, med rubriken ”Trafikuppgifter”, föreskrivs följande:

”1. Trafikuppgifter om abonnenter och användare som behandlas och lagras av leverantören av ett allmänt kommunikationsnät eller en allmänt tillgänglig elektronisk kommunikationstjänst skall utplånas eller avidentifieras när de inte längre behövs för sitt syfte att överföra en kommunikation, utan att det påverkar tillämpningen av punkterna 2, 3 och 5 i den här artikeln samt artikel 15.1.

2. Trafikuppgifter som krävs för abonnentfakturerings och betalning av samtrafikavgifter får behandlas. Sådan behandling är tillåten endast fram till utgången av den period under vilken det lagligen går att göra invändningar mot fakturan eller kräva betalning.

3. I syfte att saluföra elektroniska kommunikationstjänster eller i syfte att tillhandahålla mervärdestjänster får en leverantör av en allmänt tillgänglig elektronisk kommunikationstjänst behandla de uppgifter som avses i punkt 1 i den utsträckning och under den tidsperiod som är nödvändig för sådana tjänster eller sådan marknadsföring, om den abonnent eller användare som uppgifterna gäller i förväg har samtyckt till detta. Användare eller abonnenter ska ha möjlighet att när som helst dra tillbaka sitt samtycke till behandling av trafikuppgifter.

...

5. Behandlingen av trafikuppgifter skall, i enlighet med punkterna 1, 2, 3 och 4, begränsas till sådana personer som av leverantören av allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster getts i uppdrag att sköta fakturerings, trafikstyrning, kundförfrågningar, spårning av bedrägerier, marknadsföring av elektroniska kommunikationstjänster eller tillhandahållande av en mervärdestjänst, och behandlingen skall begränsas till sådant som är nödvändigt för dessa verksamheter.

...”

11 Artikel 9 i direktiv 2002/58 har rubriken ”Andra lokaliseringssuppgifter än trafikuppgifter”. I artikel 9.1 föreskrivs följande:

”Om andra lokaliseringssuppgifter än trafikuppgifter som rör användare eller abonnenter av allmänna kommunikationsnät eller allmänt tillgängliga elektroniska kommunikationstjänster kan behandlas, får

dessa uppgifter endast behandlas sedan de har avidentifierats eller om användarna eller abonnenterna givit sitt samtycke, i den utsträckning och för den tid som krävs för tillhandahållandet av en mervärdestjänst. Innan användaren eller abonnenten ger sitt samtycke skall tjänsteleverantören informera denne om vilken typ av andra lokaliseringssuppgifter än trafikuppgifter som kommer att behandlas, behandlingens syfte och varaktighet samt om uppgifterna kommer att vidarebefordras till tredje part för tillhandahållande av mervärdestjänsten. ...”

- 12 I artikel 15 i direktiv 2002/58, med rubriken ”Tillämpningen av vissa bestämmelser i direktiv 95/46...”, anges följande i punkt 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... 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 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 i [FEU].”

### *Tysk rätt*

#### *TKG*

- 13 I 113a § punkt 1 första meningen i Telekommunikationsgesetz (lag om telekommunikationer) (BGBl. 2004 I, s. 1190), i den version som är tillämplig i de nationella målen (nedan kallad TKG), föreskrivs följande:

”De skyldigheter avseende trafikuppgifters lagring, användning och säkerhet som fastställs i 113b–113g §§ gäller för operatörer som tillhandahåller slutanvändarna allmänt tillgängliga telekommunikationstjänster.”

- 14 I 113b § TKG föreskrivs följande:

”1) De operatörer som avses i 113a § punkt 1 ska lagra uppgifterna inom landet på följande sätt:

1. I tio veckor om det rör sig om sådana uppgifter som avses i punkterna 2 och 3.
2. I fyra veckor och det rör sig om sådana lokaliseringssuppgifter som avses i punkt 4.

2) Den som tillhandahåller allmänt tillgängliga telefonitjänster ska lagra

1. telefonnumret eller något annat identifikationsnummer för det uppringande abonnemanget, det uppringda abonnemanget samt för om- och vidarekopplingar,
2. datum och klockslag då kommunikationen inleddes och avslutades, med uppgift om tidszon,

3. uppgifter om vilken tjänst som använts, i de fall då det är möjligt att använda olika tjänster inom ramen för telefonitjänsten,
4. om det rör sig om mobiltelefonitjänster dessutom
  - a) det internationella identifikationsnumret för mobilabonnenter till det uppringande och det uppringda abonnemanget,
  - b) det internationella identifikationsnumret för den uppringande och den uppringda ändustrustningen,
  - c) datum och klockslag för tjänstens första aktivering, med uppgift om tidszon när tjänster har betalats på förhand,
5. om det rör sig om internettelefonitjänster dessutom IP-adresserna (*internet protocol*) till det uppringande och det uppringda abonnemanget samt tilldelade identifieringsnummer.

Första stycket ska, efter nödvändig anpassning, tillämpas

1. om det rör sig om kommunikation via sms, multimediameddelande eller liknande meddelande; i det fallet ska de uppgifter som anges i första stycket led 2 ersättas av tidpunkter för sändande och mottagande av meddelandet,
2. på obesvarade samtal eller misslyckade uppringningsförsök på grund av att nätadministrationen har ingripit ...
- 3) Den som tillhandahåller allmänt tillgängliga internetanslutningstjänster ska lagra
  1. den IP-adress som tilldelats abonnenten för internetanvändning,
  2. en tydlig identifiering av den förbindelse som möjliggör internetanslutning, samt det tilldelade identifieringsnumret,
  3. datum och klockslag då internetanvändningen från den tilldelade IP-adressen inleddes och avslutades, med uppgift om tidszon.
- 4) Om det rör sig om mobiltelefonitjänster ska beteckningar på de celler som användes via det uppringande och det uppringda abonnemanget i början av kommunikationen lagras. Vad beträffar allmänt tillgängliga internetanslutningstjänster ska, vid mobilanvändning, beteckningen på de celler som användes i början av internetanslutningen lagras. Det är även lämpligt att lagra uppgifter som ger möjlighet att få kännedom om geografisk position och maximala strålningsriktningar för de antenner som betjänar den berörda cellen.
- 5) Kommunikationens innehåll, uppgifter om besökta webbplatser samt uppgifter om elektroniska posttjänster, får inte lagras med stöd av denna bestämmelse.
- 6) Uppgifter som ligger till grund för sådan kommunikation som avses i 99 § punkt 2 får inte lagras med stöd av denna bestämmelse. Detta gäller, i tillämpliga delar, även telefonkommunikation från sådana enheter som avses i 99 § punkt 2. 99 § punkt 2 meningarna 2–7 ska tillämpas, efter nödvändig anpassning.

...”



15 Den kommunikation som avses i 99 § punkt 2 TKG, till vilken det hänvisas i 113b § punkt 6 TKG, är kommunikation med personer, myndigheter och organisationer inom den sociala eller kyrkliga sfären som endast eller huvudsakligen erbjuder de som ringer, vilka i princip är anonyma, tjänster i form av telefonstöd i psykologiska eller sociala krissituationer, och som själva eller vars medarbetare omfattas av särskild tystnadsplikt. För att undantaget i 99 § punkt 2 andra–fjärde meningarna TKG ska vara tillämpligt krävs att de uppringda, på egen begäran, skrivs in i en förteckning som handhas av federala myndigheten för el-, gas-, telekommunikations-, post- och järnvägsnät, efter det att de uppringda numren styrkt vilken typ av tjänster som tillhandahålls genom ett intyg utfärdat av en offentligt rättslig myndighet, institution eller stiftelse eller ett offentligt rättsligt organ.

16 I 113c § punkterna 1 och 2 TKG föreskrivs följande:

”1) Uppgifter som lagras i enlighet med 113b § får

1. vidarebefordras till en straffrättslig myndighet när den begär att uppgifterna ska vidarebefordras med hänvisning till en lagbestämmelse som möjliggör för den att samla in sådana uppgifter som avses i 113b § i syfte att bekämpa särskilt allvarliga brott,
2. vidarebefordras till en delstatlig säkerhetsmyndighet när den begär att uppgifterna ska vidarebefordras med hänvisning till en lagbestämmelse som möjliggör för den att samla in sådana uppgifter som avses i 113b § i syfte att avvärja ett konkret hot mot en persons liv och lem eller frihet eller mot förbundsstatens eller en delstats fortlevnad,

...

2) Uppgifter som lagras i enlighet med 113b § får inte användas av den som omfattas av särskilda skyldigheter enligt 113a § punkt 1, för andra ändamål än de som avses i punkt 1.”

17 I 113d § TKG föreskrivs följande:

”Den som omfattas av den skyldighet som avses i 113a § punkt 1 ska se till att de uppgifter som på grund av lagringsskyldigheten lagras i enlighet med 113b § punkt 1, skyddas mot otillåten kontroll och användning genom tekniska och organisatoriska åtgärder i enlighet med den tekniska utvecklingen. Dessa åtgärder omfattar särskilt

1. användning av ett särskilt säkert krypteringsförfarande,
2. lagring i en särskild lagringsinfrastruktur som är avskild från den infrastruktur som används för löpande driftsfunktioner,
3. lagring med en hög nivå för skydd mot cyberangrepp, i fristående databehandlingssystem,
4. att endast personer med särskilt tillstånd utfärdat av den som ansvarar för skyldigheten ges tillgång till de anläggningar som används för att behandla uppgifter, och
5. en skyldighet att se till att minst två personer med särskilt tillstånd utfärdat av den som ansvarar för skyldigheten medverkar när tillgång ges till uppgifterna.”

18 I 113e § TKG föreskrivs följande:

”1) Den som ansvarar för den skyldighet som avses i 113a § punkt 1 ska, i syfte att kunna kontrollera uppgiftsskyddet, se till att varje tillgång antecknas och i synnerhet läsning, kopiering, ändring, radering och avslutning av uppgifter som lagras i enlighet med 113b § punkt 1 på grund av lagringsskyldigheten. Anteckning ska göras av

1. klockslag när tillgång ges till uppgifterna,
2. vilka personer som ges tillgång till uppgifterna,
3. syftet med tillgången och dess karaktär.

2) De antecknade uppgifterna får inte användas för andra ändamål än kontroll av uppgiftsskyddet.

3) Den som ansvarar för den skyldighet som avses i 113a § punkt 1 ska se till att de uppgifter som antecknas raderas efter ett år.”

19 I syfte att säkerställa en särskilt hög säkerhets- och skyddsnivå för personuppgifter fastställer federala myndigheten för el-, gas-, telekommunikations-, post- och järnvägsnät, i enlighet med 113f § punkt 1 TKG krav som, enligt artikel 113f § punkt 2 TKG fortgående ska utvärderas och i förekommande fall anpassas. I 113g § TKG krävs att särskilda säkerhetsåtgärder ska ingå i den redogörelse för policyn på säkerhetsområdet som ska läggas fram av den ansvarige.

#### *StPO*

20 I 100g § punkt 2 första meningen Strafprozessordnung (straffprocesslagen) (nedan kallad StPO) föreskrivs följande:

”Om det på grund av vissa omständigheter finns skäl att misstänka att någon i egenskap av gärningsman eller medhjälpare har begått ett sådant särskilt allvarligt brott som avses i andra meningen eller, i de fall där försök till brott är straffbart, har försökt att begå ett sådant brott och om brottet även är särskilt allvarligt i det konkreta fallet, får trafikuppgifter som lagrats med stöd av 113b § [TKB], samlas in om det skulle vara alltför svårt eller omöjligt att utreda brottet eller lokalisera den misstänkta personen på annat sätt och om insamlingen av uppgifterna står i proportion till sakens betydelse.”

21 Enligt 101a § punkt 1 StPO krävs domstols tillstånd för att samla in trafikuppgifter enligt 100g § StPO. Enligt 101a § punkt 2 StPO ska skälen för beslutet omfatta de väsentliga övervägandena för huruvida åtgärden är nödvändig och lämplig i det konkreta fallet. I 101a § punkt 6 StPO föreskrivs en skyldighet att informera deltagarna i den berörda telekommunikationen.

#### **Målet vid den nationella domstolen och tolkningsfrågan**

22 SpaceNet och Telekom Deutschland tillhandahåller allmänt tillgängliga internetanslutningstjänster i Tyskland. Telekom Deutschland tillhandahåller dessutom allmänt tillgängliga telefonitjänster i Tyskland.

- 23 Dessa tjänsteleverantörer väckte talan vid Verwaltungsgericht Köln (Förvaltningsdomstolen i Köln, Tyskland) och bestred skyldigheten, enligt 113a § punkt 1 jämförd med 113b § TKG, att lagra trafik- och lokaliseringssuppgifter hänförliga till sina kunders telekommunikationer från och med den 1 juli 2017.
- 24 I domar av den 20 april 2018 slog Verwaltungsgericht Köln (Förvaltningsdomstolen i Köln) fast att SpaceNet och Telekom Deutschland inte var skyldiga att lagra de uppgifter om telekommunikationstrafik som avses i 113b § punkt 3 TKG avseende kunder till vilka de tillhandahåller internetåtkomst och att Telekom Deutschland dessutom inte var skyldigt att lagra de uppgifter om telekommunikationstrafik som avses i 113b § punkt 2 första och andra meningen TKG avseende kunder till vilka företaget tillhandahåller allmänt tillgängliga telefonitjänster. Verwaltungsgericht Köln (Förvaltningsdomstolen i Köln) ansåg, mot bakgrund av domen av den 21 december 2016, Tele2 Sverige och Watson m.fl. (C-203/15 och C-698/15, EU:C:2016:970), att denna lagringsskyldighet stred mot unionsrätten.
- 25 Förbundsrepubliken Tyskland överklagade dessa domar till Bundesverwaltungsgericht (Federala högsta förvaltningsdomstolen, Tyskland), den hänskjutande domstolen.
- 26 Den hänskjutande domstolen anser att frågan huruvida den lagringsskyldighet som föreskrivs i 113a § punkt 1 jämförd med 113b § TKG strider mot unionsrätten beror på tolkningen av direktiv 2002/58.
- 27 Den hänskjutande domstolen påpekar i detta hänseende att EU-domstolen redan slutligt slagit fast, i domen av den 21 december 2016, Tele2 Sverige och Watson m.fl. (C-203/15 och C-698/15, EU:C:2016:970), att bestämmelser om lagring av trafik- och lokaliseringssuppgifter samt nationella myndigheters tillgång till dessa uppgifter i princip omfattas av tillämpningsområdet för direktiv 2002/58.
- 28 Den hänskjutande domstolen har även påpekat att den i de nationella målen aktuella lagringsskyldigheten, i den mån den begränsar de rättigheter som följer av artiklarna 5.1, 6.1 och artikel 9.1 i direktiv 2002/58, endast kan motiveras med stöd av artikel 15.1 i direktivet.
- 29 Den erinrar om att det av domen av den 21 december 2016, Tele2 Sverige och Watson m.fl. (C-203/15 och C-698/15, EU:C:2016:970), framgår att artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, ska tolkas på så sätt att den utgör hinder för en nationell lagstiftning som i brottsbekämpande syfte föreskriver en generell och odifferentierad lagring av samtliga trafik- och lokaliseringssuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel.
- 30 Enligt den hänskjutande domstolen krävs det enligt de nationella bestämmelser som är aktuella i de nationella målen, i likhet med de nationella bestämmelser som var aktuella i de mål som avgjordes genom nämnda dom, inte några skäl för att lagra uppgifterna eller något samband mellan de lagrade uppgifterna och ett brott eller en risk för den allmänna säkerheten. Den nationella lagstiftningen innebär nämligen att merparten av alla relevanta uppgifter om telekommunikationstrafik ska lagras, generellt och utan differentiering i fråga om person, tidpunkt eller geografisk plats, utan krav på skäl.
- 31 Den hänskjutande domstolen anser emellertid att det inte är uteslutet att den i de nationella målen aktuella lagringsskyldigheten kan vara motiverad med stöd av artikel 15.1 i direktiv 2002/58.

- 32 Den har, för det första, påpekat att den aktuella nationella lagstiftningen i förevarande mål, till skillnad från de nationella bestämmelser som var aktuella i de mål som avgjordes genom domen av den 21 december 2016, Tele2 Sverige och Watson m.fl. (C-203/15 och C-698/15, EU:C:2016:970), inte kräver lagring av samtliga uppgifter om telekommunikationstrafik avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel. Förutom att innehållet i kommunikationerna är undantaget från lagringsskyldigheten, så får inte heller uppgifter om de webbplatser som besökts, uppgifter om elektroniska posttjänster och uppgifter som ligger till grund för kommunikation av social eller kyrklig karaktär till eller från vissa linjer lagras, såsom framgår av 113b §.punkterna 5 och 6 TKG.
- 33 Den hänskjutande domstolen har, för det andra, angett att det i 113b § punkt 1 TKG föreskrivs en lagringstid på fyra veckor för lokaliseringssuppgifter och tio veckor för trafikuppgifter, medan det i Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG (EUT L 105, 2006, s. 54), vilket låg till grund för de nationella bestämmelser som var i fråga i de mål som avgjordes genom domen av den 21 december 2016, Tele2 Sverige och Watson m.fl. (C-203/15 och C-698/15, EU:C:2016:970), föreskrevs en lagringstid på mellan sex månader och två år.
- 34 Även om uteslutandet av vissa kommunikationsmedel eller vissa kategorier av uppgifter och begränsningen av lagringstiden inte räcker för att helt undanröja risken för att det ska vara möjligt att upprätta en fullständig profil för de berörda personerna, är denna risk enligt den hänskjutande domstolen i vart fall avsevärt mindre i samband med genomförandet av den nationella lagstiftning som är aktuell i de nationella målen.
- 35 För det tredje innehåller denna lagstiftning strikta begränsningar när det gäller skydd av och tillgång till lagrade uppgifter. Den säkerställer således dels att de lagrade uppgifterna åtnjuter ett effektivt skydd mot riskerna för missbruk och otillåten tillgång till uppgifterna. Dels får de lagrade uppgifterna endast användas för att bekämpa allvarliga brott eller för att förebygga en konkret risk mot en persons liv och lem eller frihet eller förbundsstatens eller en delstats fortlevnad.
- 36 För det fjärde skulle en tolkning av artikel 15.1 i direktiv 2002/58 som innebär att all lagring av uppgifter utan skäl rent generellt är oförenlig med unionsrätten kunna strida mot medlemsstaternas skyldighet att agera, vilken följer av rätten till säkerhet i artikel 6 i stadgan.
- 37 För det femte anser den hänskjutande domstolen att en tolkning av artikel 15 i direktiv 2002/58 som innebär att den utgör hinder för en generell lagring av uppgifter avsevärt skulle inskränka den nationella lagstiftarens handlingsutrymme på ett område som rör bekämpning av brott och allmän säkerhet, vilket enligt artikel 4.2 FEU faller under varje medlemsstats eget ansvar.
- 38 För det sjätte anser den hänskjutande domstolen att praxis från Europeiska domstolen för de mänskliga rättigheterna ska beaktas och har påpekat att den domstolen har slagit fast att artikel 8 i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna (Europakonventionen) inte utgör hinder för nationella bestämmelser som föreskriver massiv avläsning av gränsöverskridande dataflöden, med hänsyn till de hot som många stater för närvarande ställs inför och de tekniska verktyg som terrorister och kriminella framdeles kan använda sig av för att begå klandervärda handlingar.

39 Mot denna bakgrund beslutade Bundesverwaltungsgericht (Federala högsta förvaltningsdomstolen) att vilandeförklara målet och ställa följande frågor till EU-domstolen:

”Ska artikel 15 i direktiv 2002/58..., jämförd med dels artiklarna 7, 8, 11 och 52.1 i [stadgan], dels artikel 6 i [stadgan] och artikel 4 [FEU], tolkas så, att den utgör hinder för en nationell lagstiftning som ålägger operatörer av allmänt tillgängliga elektroniska kommunikationstjänster att lagra trafik- och lokaliseringssuppgifter avseende slutanvändare av nämnda tjänster, när denna skyldighet

1. inte villkoras av särskilda skäl i fråga om geografiska, tidsmässiga eller territoriella aspekter,
2. i samband med tillhandahållandet av allmänt tillgängliga telefonitjänster, inbegripet kommunikation via sms, multimediameddelande eller liknande meddelande samt samtal som inte besvaras eller når fram, avser följande uppgifter:
  - a) telefonnumret eller något annat identifikationsnummer för det uppringande abonnemanget, det uppringda abonnemanget samt för om- och vidarekopplingar,
  - b) datum och klockslag då kommunikationen inleddes och avslutades eller – om det rör sig om kommunikation via sms, multimediameddelande eller liknande meddelande – tidpunkter för sändande och mottagande av meddelandet, med uppgift om tidszon,
  - c) uppgifter om vilken tjänst som använts, i de fall då det är möjligt att använda olika tjänster inom ramen för telefonitjänsten,
  - d) om det rör sig om mobiltelefonitjänster dessutom
    - i) det internationella identifikationsnumret för mobilabonnenter till det uppringande och det uppringda abonnemanget,
    - ii) det internationella identifikationsnumret för den uppringande och den uppringda ändrustningen,
    - iii) datum och klockslag för tjänstens första aktivering, med uppgift om tidszon, när tjänster har betalats på förhand,
    - iv) beteckningar på de celler som användes via det uppringande och det uppringda abonnemanget i början av kommunikationen,
  - e) om det rör sig om internettelefonitjänster dessutom IP-adresserna (*internet protocol*) till det uppringande och det uppringda abonnemanget samt tilldelade identifieringsnummer,
3. i samband med tillhandahållandet av allmänt tillgängliga internetanslutningstjänster, avser följande uppgifter:
  - a) den IP-adress som tilldelats abonnenten för internetanvändning,
  - b) en tydlig identifiering av den förbindelse som möjliggör internetanslutning, samt det tilldelade identifieringsnumret,
  - c) datum och klockslag då internetanvändningen på den tilldelade IP-adressen inleddes och avslutades, med uppgift om tidszon,
  - d) vid mobilanvändning, beteckningen på de celler som användes i början av internetanslutningen,
4. innebär att följande uppgifter inte får lagras:
  - a) kommunikationens innehåll,
  - b) uppgifter om besökta webbplatser,
  - c) uppgifter om elektroniska posttjänster,
  - d) uppgifter som avser kommunikation till eller från vissa abonnemang som tillhör personer, myndigheter och organisationer inom den sociala eller kyrkliga sfären,

5. innebär att lagringstiden för lokaliseringssuppgifter, det vill säga beteckningen på de celler som använts, är fyra veckor, och för övriga uppgifter tio veckor,
- 6) säkerställer ett effektivt skydd av lagrade uppgifter mot risker för missbruk och otillåten tillgång, och
- 7) innebär att de lagrade uppgifterna endast får användas i syfte att bekämpa allvarliga brott eller avvärja ett konkret hot mot en persons liv och lem eller frihet eller förbundsstatens eller en delstats fortlevnad, med undantag för den IP-adress som tilldelats en abonnent för internetanvändning, vilken får användas inom ramen för en förfrågan om inventariedata för att lagföra alla brott, avvärja risker för säkerhet och allmän ordning samt generellt sett för att fullgöra underrättelsetjänstens uppgifter?”

### **Förfarandet vid domstolen**

- 40 Domstolens ordförande har genom beslut av den 3 december 2019 förenat målen C-793/19 och C-794/19 vad gäller det skriftliga och det muntliga förfarandet samt domen.
- 41 Genom beslut av domstolens ordförande av den 14 juli 2020 vilandeförklarades förfarandet i de förenade målen C-793/19 och C-794/19 med stöd av artikel 55.1 b i domstolens rättegångsregler till dess att dom meddelats i målet La Quadrature du Net m.fl. (C-511/18, C-512/18 och C-520/18).
- 42 Efter det att domstolen den 6 oktober 2020 meddelat sin dom i målet La Quadrature du Net m.fl. (C-511/18, C-512/18 och C-520/18, EU:C:2020:791), beslutade domstolens ordförande den 8 oktober 2020 att förfarandet i de förenade målen C-793/19 och C-794/19 skulle återupptas.
- 43 Den hänskjutande domstolen, till vilken kansliet hade skickat denna dom, angav att den vidhöll sin begäran om förhandsavgörande.
- 44 Den hänskjutande domstolen har i detta avseende påpekat att den lagringsskyldighet som föreskrivs i den lagstiftning som är aktuell i de nationella målen avser ett lägre antal uppgifter och en kortare lagringstid än vad som föreskrevs i de nationella bestämmelser som var aktuella i de mål som avgjordes genom domen 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). Dessa omständigheter minskar möjligheten för att man genom de lagrade uppgifterna kan dra mycket precisa slutsatser om privatlivet beträffande de personer vilkas uppgifter har lagrats.
- 45 Vidare har den hänskjutande domstolen åter angett att den nationella lagstiftning som är aktuell i de nationella målen säkerställer ett effektivt skydd mot missbruk av och otillåten tillgång till lagrade uppgifter.
- 46 Slutligen har den hänskjutande domstolen framhållit att det fortfarande råder osäkerhet om huruvida den lagring av IP-adresser som föreskrivs i den nationella lagstiftning som är aktuell i de nationella målen är förenlig med unionsrätten, på grund av bristande överensstämmelse mellan punkterna 155 och 168 i domen 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). Enligt den hänskjutande domstolen medför denna dom att det är oklart huruvida EU-domstolen, för att IP-adresser ska få lagras, kräver att skälet för lagringen ska vara kopplat till målet att skydda den nationella säkerheten, bekämpa allvarlig

brottslighet eller att förhindra allvarliga hot mot den allmänna säkerheten, såsom framgår av punkt 168 i nämnda dom, eller om lagring av IP-adresser är tillåten även om det inte finns några konkreta skäl för detta och kraven avseende nämnda mål endast begränsar användningen av de lagrade uppgifterna, såsom framgår av punkt 155 i nämnda dom.

### **Prövning av tolkningsfrågan**

- 47 Den hänskjutande domstolen har ställt sin tolkningsfråga för att få klarhet i huruvida artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 6–8, 11 och 52.1 i stadgan och artikel 4.2 FEU, ska tolkas så, att den utgör hinder för en nationell lagstiftning som, med vissa undantag, ålägger leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster att för de syften som räknas upp i artikel 15.1 i detta direktiv, och särskilt med avseende på bekämpning av allvarliga brott eller förebyggande av konkreta risker för den nationella säkerheten, generellt och odifferentierat lagra flertalet trafik- och lokaliseringssuppgifter avseende dessa tjänsters slutanvändare, och därvid föreskriver en lagringstid på flera veckor och regler som syftar till att säkerställa ett effektivt skydd mot missbruk av eller otillåten tillgång till de lagrade uppgifterna.

### ***Huruvida direktiv 2002/58 är tillämpligt***

- 48 När det gäller Irlands samt den franska, den nederländska, den polska och den svenska regeringens argument att den nationella lagstiftning som är aktuell i de nationella målen inte omfattas av tillämpningsområdet för direktiv 2002/58, eftersom den antagits i syfte att bland annat värna om den nationella säkerheten, räcker det att erinra om att en nationell lagstiftning vilken ålägger leverantörer av elektroniska kommunikationstjänster att lagra trafik- och lokaliseringssuppgifter i syfte att bland annat skydda nationell säkerhet och bekämpa brottslighet, såsom den lagstiftning som är aktuell i de nationella målen, omfattas av tillämpningsområdet för direktiv 2002/58 (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, punkt 104).

### ***Tolkningen av artikel 15.1 i direktiv 2002/58***

#### ***Erinran om de principer som följer av domstolens praxis***

- 49 Det framgår av fast rättspraxis att det vid tolkningen av en unionsbestämmelse inte bara är lydelsen som ska beaktas, utan också sammanhanget och de mål som eftersträvas med de föreskrifter som bestämmelsen ingår i. Därutöver ska bland annat förarbetena till bestämmelserna beaktas (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 32 och där angiven rättspraxis).
- 50 Det framgår av själva ordalydelsen i artikel 15.1 i direktiv 2002/58 att de lagstiftningsåtgärder som medlemsstaterna får vidta enligt direktivet, på de villkor som där fastställs, endast får vidtas för att "begränsa omfattningen" av de rättigheter och skyldigheter som anges i bland annat artiklarna 5, 6 och 9 i direktiv 2002/58 (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 33).

- 51 Vad gäller det system som direktivet inrättat och som artikel 15.1 ingår i, erinrar domstolen om att medlemsstaterna enligt artikel 5.1 första och andra meningen i direktivet är skyldiga att genom sin nationella lagstiftning säkerställa konfidentialitet vid kommunikation och därmed förbundna trafikuppgifter via allmänna kommunikationsnät och allmänt tillgängliga elektroniska kommunikationstjänster. De ska 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 i samma direktiv (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 34).
- 52 EU-domstolen har i detta hänseende tidigare slagit fast att det i artikel 5.1 i direktiv 2002/58 fastställs att principen om konfidentialitet gäller för såväl elektronisk kommunikation som därmed förbundna trafikuppgifter. Detta innebär bland annat ett principiellt förbud för andra personer än användarna att, utan användarnas samtycke, lagra sådan kommunikation och sådana uppgifter (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, punkt 107, och dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 35).
- 53 Denna bestämmelse återspeglar det syfte som unionslagstiftaren eftersträvade vid antagandet av direktiv 2002/58. Det framgår nämligen av redogörelsen för skälen i förslaget till Europaparlamentets och rådets direktiv om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (KOM(2000) 385 slutlig), som låg till grund för direktiv 2002/58, att unionslagstiftaren avsett att ”garantera en fortsatt hög skyddsnivå för personuppgifter och privatliv för alla elektroniska kommunikationstjänster, oavsett vilken teknik som används”. Syftet med direktiv 2002/58 är sålunda, såsom framgår av bland annat skälen 6 och 7 däri, att skydda användarna av elektroniska kommunikationstjänster mot de risker för deras personuppgifter och integritet som ny teknik och särskilt den ökade kapaciteten för automatiserad lagring och behandling av uppgifter medför. Direktivet syftar särskilt, såsom anges i dess skäl 2, till att säkerställa full respekt för de rättigheter som anges i artiklarna 7 och 8 i stadgan avseende skydd för privatlivet respektive skydd av personuppgifter (se, för ett liknande resonemang, dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 36 och där angiven rättspraxis).
- 54 Genom att anta direktiv 2002/58 har unionslagstiftaren således konkretiserat dessa rättigheter på ett sådant sätt att användarna av elektroniska kommunikationsmedel i princip har rätt att förvänta sig att deras kommunikationer och därmed förbundna uppgifter förblir anonyma och inte kan registreras, såvida de inte har samtyckt till detta (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 punkt 109, och dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 37).
- 55 När det gäller trafikuppgifter om abonnenter och användare som behandlas och lagras av leverantörer av elektroniska kommunikationstjänster föreskrivs i artikel 6.1 i direktiv 2002/58 att dessa uppgifter ska utplånas eller avidentifieras när de inte längre behövs för sitt syfte att överföra en kommunikation. I punkt 2 i denna artikel anges att trafikuppgifter som krävs för abonnentfakturering och betalning av samtrafikavgifter endast får behandlas fram till utgången av den period under vilken det lagligen går att göra invändningar mot fakturan eller kräva betalning. I fråga om andra lokaliseringssuppgifter än trafikuppgifter, föreskrivs i artikel 9.1 i direktivet att dessa endast får behandlas på vissa villkor och sedan de har avidentifierats eller om användarna eller abonnenterna gett sitt samtycke.



- 56 Direktiv 2002/58 reglerar således inte bara tillgången till sådana uppgifter genom garantier i syfte att förhindra missbruk utan innehåller även, i synnerhet, ett förbud mot att de lagras av tredje part (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 39).
- 57 Eftersom artikel 15.1 i direktiv 2002/58 tillåter medlemsstaterna att genom lagstiftning vidta åtgärder för att "begränsa omfattningen" av rättigheter och skyldigheter enligt bland annat artiklarna 5, 6 och 9 i direktivet, såsom de som följer av principerna om konfidentialitet vid kommunikation och om förbud mot lagring av därmed förbundna uppgifter, enligt vad som angetts ovan i punkt 52, föreskriver den ett undantag från den allmänna regeln i bland annat artiklarna 5, 6 och 9 och ska således enligt fast rättspraxis tolkas restriktivt. En sådan bestämmelse kan således inte motivera att ett undantag från den principiella skyldigheten att säkerställa konfidentialiteten vid elektronisk kommunikation och för därmed förbundna uppgifter, och särskilt från det uttryckliga förbudet mot lagring av sådana uppgifter i artikel 5 i direktivet, görs till huvudregel. Detta skulle nämligen i stor utsträckning förta verkan av sistnämnda bestämmelse (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 40 och där angiven rättspraxis).
- 58 Vad gäller de mål som kan motivera en begränsning av de rättigheter och skyldigheter som föreskrivs i bland annat artiklarna 5, 6 och 9 i direktiv 2002/58, har domstolen tidigare slagit fast att uppräkningsåtgärden i artikel 15.1 första meningen i detta direktiv är uttömmande. En lagstiftningsåtgärd som har vidtagits med stöd av denna bestämmelse måste därför faktiskt och strikt hänföra sig till ett av dessa mål (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 41 och där angiven rättspraxis).
- 59 Det framgår dessutom av artikel 15.1 tredje meningen i direktiv 2002/58 att de åtgärder som medlemsstaterna vidtar enligt denna bestämmelse ska vara förenliga med de allmänna principerna i unionsrätten, däribland proportionalitetsprincipen, och säkerställa att de grundläggande rättigheter som garanteras i stadgan iakttas. Domstolen har i detta hänseende redan slagit fast att när en medlemsstat i nationell lagstiftning ålägger leverantörer av elektroniska kommunikationstjänster en skyldighet att lagra trafikuppgifter i syfte att, i förekommande fall, göra dem tillgängliga för behöriga nationella myndigheter väcker detta frågor om en sådan lagstiftnings förenlighet inte bara med artiklarna 7 och 8 i stadgan, utan även med artikel 11 i stadgan, som rör yttrandefriheten. Yttrandefriheten utgör nämligen en av grundvalarna för ett demokratiskt och pluralistiskt samhälle och ingår i de värden som Europeiska unionen enligt artikel 2 FEU bygger på (se, för ett liknande resonemang, dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkterna 42 och 43 samt där angiven rättspraxis).
- 60 Det ska i detta avseende preciseras att lagring av trafik- och lokaliseringsuppgifter i sig utgör dels ett undantag från förbudet i artikel 5.1 i direktiv 2002/58 för andra personer än användarna att lagra dessa uppgifter, dels ett ingrepp i de grundläggande rättigheterna till respekt för privatlivet och skydd av personuppgifter, vilka är stadfästa i artikel 7 respektive artikel 8 i stadgan, oberoende av om de uppgifter som avser privatlivet är av känslig art eller ej eller om de berörda har fått utstå eventuella olägenheter på grund av ingreppet samt oberoende av om de lagrade uppgifterna senare kommer eller inte kommer att användas (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 44 och där angiven rättspraxis).

- 61 Denna slutsats framstår som än mer motiverad med hänsyn till att trafik- och lokaliseringssuppgifter kan avslöja information om ett stort antal aspekter av de berörda personernas privatliv, inbegripet känslig information, såsom sexuell läggning, politisk åskådning, religiös, filosofisk eller annan övertygelse, samhällsåskådning samt hälsotillstånd, samtidigt som sådana uppgifter omfattas av ett särskilt skydd enligt unionsrätten. Dessa uppgifter kan sammantagna göra det möjligt att dra mycket precisa slutsatser om privatlivet för de personer vilkas uppgifter har lagrats, såsom deras vanor i vardagslivet, deras stadigvarande och tillfälliga uppehållsorter, deras dagliga förflyttningar och förflyttningar i övrigt, de aktiviteter de utövar, deras sociala relationer och de umgängeskretsar de rör sig i. Närmare bestämt gör dessa uppgifter det möjligt att upprätta en profil för de berörda personerna, och denna information är lika känslig ur integritetssynpunkt som själva innehållet i kommunikationerna (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 45 och där angiven rättspraxis).
- 62 Lagring av trafik- och lokaliseringssuppgifter för polisiära ändamål kan således i sig utgöra ett åsidosättande av rätten till respekt för kommunikationer, vilken är stadfäst i artikel 7 i stadgan, och avhålla användarna av elektroniska kommunikationsmedel från att utöva sin yttrandefrihet, vilken garanteras i artikel 11 i stadgan, verkningar som är desto allvarligare ju fler och mer varierade de uppgifter är som har lagrats. Med hänsyn till den stora mängd trafik- och lokaliseringssuppgifter som kan bli föremål för fortlöpande lagring genom en generell och odifferentierad lagringsåtgärd och till att den information som dessa uppgifter kan innehålla är känslig, medför den omständigheten att leverantörer av elektroniska kommunikationstjänster lagrar dessa uppgifter dessutom i sig en risk för missbruk och obehörig åtkomst (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 46 och där angiven rättspraxis).
- 63 Eftersom artikel 15.1 i direktiv 2002/58 ger medlemsstaterna möjlighet att begränsa de rättigheter och skyldigheter som avses ovan i punkterna 51–54, avspeglar denna artikel emellertid den omständigheten att de rättigheter som är stadfästa i artiklarna 7, 8 och 11 i stadgan inte är några absoluta rättigheter, utan måste bedömas utifrån deras funktion i samhället. Såsom framgår av artikel 52.1 i stadgan är det nämligen enligt stadgan tillåtet att begränsa utövandet av dessa rättigheter, under förutsättning att begränsningarna föreskrivs i lag, att de är förenliga med det väsentliga innehållet i dessa rättigheter och att de, med beaktande av proportionalitetsprincipen, är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller mot behovet av skydd för andra människors rättigheter och friheter. En tolkning av artikel 15.1 i direktiv 2002/58 mot bakgrund av stadgan kräver således även att det tas hänsyn till betydelsen av de rättigheter som är stadfästa i artiklarna 3, 4, 6 och 7 i stadgan och till den betydelse som målen att skydda nationell säkerhet och bekämpa grov brottslighet har för att bidra till skyddet för andra människors rättigheter och friheter (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 48 och där angiven rättspraxis).
- 64 Vad särskilt gäller den effektiva bekämpningen av brott som bland annat minderåriga och andra utsatta personer utsätts för, ska det beaktas att det av artikel 7 i stadgan kan följa positiva skyldigheter för statsmakten att vidta rättsliga åtgärder för att skydda privatlivet och familjelivet. Sådana skyldigheter kan även följa av nämnda artikel 7 vad gäller skyddet av bostaden och kommunikationer, och av artiklarna 3 och 4 vad gäller skyddet av personers fysiska och mentala integritet och förbudet mot tortyr och omänsklig och förnedrande behandling (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 49 och där angiven rättspraxis).

- 65 Mot bakgrund av dessa olika positiva skyldigheter är det således nödvändigt att göra en avvägning mellan de olika legitima intressen och rättigheter som är i fråga och att inrätta en rättslig ram som möjliggör denna avvägning (se, för ett liknande resonemang, dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 50 och där angiven rättspraxis).
- 66 Det framgår av själva ordalydelsen av artikel 15.1 första meningen i direktiv 2002/58 att medlemsstaterna får vidta en åtgärd som avviker från principen om konfidentialitet (se ovan i punkt 52) när en sådan åtgärd är ”nödvändig, lämplig och proportionerlig ... i ett demokratiskt samhälle”. I skäl 11 i direktivet anges att en åtgärd av detta slag ska stå i ”strikt” proportion till det avsedda ändamålet.
- 67 Det ska i detta avseende erinras om att skyddet för den grundläggande rätten till respekt för privatlivet enligt domstolens fasta praxis kräver att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt. Ett mål av allmänt samhällsintresse kan dessutom inte uppnås utan att det beaktas att detta mål måste vara förenligt med de grundläggande rättigheter som berörs av åtgärden, varvid en balanserad avvägning ska göras mellan, å ena sidan, målet av allmänt samhällsintresse, och, å andra sidan, rättigheterna i fråga (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 52 och där angiven rättspraxis).
- 68 Det följer närmare bestämt av domstolens praxis att medlemsstaternas möjlighet att motivera en begränsning av de rättigheter och skyldigheter som föreskrivs i bland annat artiklarna 5, 6 och 9 i direktiv 2002/58 ska bedömas med hänsyn till hur allvarligt det ingrepp är som en sådan begränsning medför, varvid det ska kontrolleras att betydelsen av det mål av allmänt samhällsintresse som eftersträvas med denna begränsning står i proportion till hur allvarligt ingreppet är (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 53 och där angiven rättspraxis).
- 69 För att kravet på proportionalitet ska vara uppfyllt måste det i nationell 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, vilket säkerställer att ingreppet begränsas till vad som är strängt nödvändigt. Behovet av sådana garantier är särskilt stort när personuppgifter är föremål för automatiserad behandling, särskilt när det föreligger en betydande risk för obehörig åtkomst till uppgifterna. Dessa överväganden äger särskild giltighet när det är fråga om skyddet av den särskilda kategori av personuppgifter som utgörs av känsliga uppgifter (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 54 och där angiven rättspraxis).
- 70 En nationell lagstiftning som föreskriver lagring av personuppgifter måste således alltid uppfylla objektiva kriterier, som fastställer ett samband mellan de uppgifter som ska lagras och det eftersträfvade målet (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 55 och där angiven rättspraxis).
- 71 Vad gäller sådana mål av allmänt intresse som kan motivera att en åtgärd med stöd av artikel 15.1 i direktiv 2002/58 vidtas framgår det av EU-domstolens praxis, i synnerhet av domen 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),

att det av proportionalitetsprincipen följer att det föreligger en hierarki mellan dessa mål beroende på deras betydelse och att betydelsen av det mål som eftersträvas med en sådan åtgärd måste stå i proportion till hur allvarligt ingreppet till följd av åtgärden är (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 56).

- 72 När det gäller målet att skydda nationell säkerhet, vilket har större betydelse än de övriga mål som avses i artikel 15.1 i direktiv 2002/58, har EU-domstolen således slagit fast att denna bestämmelse, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, inte utgör hinder för en lagstiftningsåtgärd som, för att skydda nationell säkerhet, tillåter att leverantörer av elektroniska kommunikationstjänster åläggs att på ett generellt och odifferentierat sätt lagra trafik- och lokaliseringssuppgifter i situationer där den berörda medlemsstaten står inför ett allvarligt hot mot nationell säkerhet som visat sig vara verkligt och aktuellt eller förutsebart. Ett sådant beslut om åläggande av nämnda lagringsskyldighet måste kunna bli föremål för en effektiv kontroll antingen av en domstol eller av en oberoende myndighet, vars avgörande har bindande verkan, i syfte att kontrollera om någon av dessa situationer föreligger och att de villkor och garantier som måste ställas upp är uppfyllda. Vidare får åläggandet endast meddelas för en period som måste vara tidsmässigt begränsad till vad som är strängt nödvändigt, men som kan förlängas om hotet fortfarande kvarstår (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 58 och där angiven rättspraxis).
- 73 Vad gäller målet att förebygga, undersöka, avslöja och lagföra brott har domstolen framhållit att det, i enlighet med proportionalitetsprincipen, endast är bekämpning av grov brottslighet och förebyggande av allvarliga hot mot allmän säkerhet som kan motivera allvarliga ingrepp i de grundläggande rättigheter som anges i artiklarna 7 och 8 i stadgan, såsom de ingrepp som följer av lagring av trafik- och lokaliseringssuppgifter. Målet att förebygga, undersöka, avslöja och lagföra brott i allmänhet kan således endast motivera sådana ingrepp i nämnda grundläggande rättigheter som inte är av allvarligt slag (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 59 och där angiven rättspraxis).
- 74 Vad gäller målet att bekämpa grov brottslighet har EU-domstolen slagit fast att en nationell lagstiftning som för detta ändamål föreskriver en generell och odifferentierad lagring av trafik- och lokaliseringssuppgifter går utöver vad som är strängt nödvändigt och inte kan anses vara motiverad i ett demokratiskt samhälle. Med hänsyn till den känsliga karaktären av den information som kan framkomma genom trafik- och lokaliseringssuppgifter, är det nämligen av grundläggande betydelse för rätten till respekt för privatlivet att dessa uppgifter är konfidentiella. Domstolen finner således, med beaktande dels av att en lagring av dessa uppgifter kan ha en avhållande inverkan på utövandet av de grundläggande rättigheter som anges i artiklarna 7 och 11 i stadgan, som nämns ovan i punkt 62, dels av att det ingrepp som en sådan lagring innebär är av allvarligt slag, att det i ett demokratiskt samhälle är viktigt att denna lagring utgör ett undantag och inte en huvudregel, i enlighet med vad som föreskrivs i det system som inrättats genom direktiv 2002/58, och att uppgifterna inte får lagras systematiskt och fortlöpande. Denna slutsats gäller även med avseende på målen att bekämpa grov brottslighet och att förebygga allvarliga hot mot allmän säkerhet samt den betydelse som ska tillmätas dem (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 65 och där angiven rättspraxis).
- 75 EU-domstolen har däremot preciserat att artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, inte utgör hinder för lagstiftningsåtgärder som, i syfte att bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, föreskriver

- en riktad lagring av trafik- och lokaliseringssuppgifter vilken, på grundval av objektiva och icke-diskriminerande faktorer, är avgränsad genom de kategorier av personer som berörs eller genom ett geografiskt kriterium, för en period som är tidsmässigt begränsad till vad som är strängt nödvändigt men som kan förlängas,
- en generell och odifferentierad lagring av IP-adresser som har tilldelats källan för en internetanslutning, för en period som är tidsmässigt begränsad till vad som är strängt nödvändigt,
- en generell och odifferentierad lagring av uppgifter om identiteten beträffande användare av elektroniska kommunikationsmedel, och
- att leverantörer av elektroniska kommunikationstjänster genom ett beslut från behörig myndighet, vilket är föremål för effektiv domstolskontroll, får åläggas att, under en begränsad tidsperiod, skyndsamt säkra (*quick freeze*) de trafik- och lokaliseringssuppgifter som dessa tjänsteleverantörer har tillgång till,

förutsatt att denna lagstiftning, genom klara och precisa regler, säkerställer att lagringen av uppgifterna i fråga iakttar tillämpliga materiella och formella villkor, och att de berörda personerna förfogar över effektiva garantier mot riskerna för missbruk (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 punkt 168, och dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 67).

*En åtgärd som innebär en generell och odifferentierad lagring av merparten av trafik- och lokaliseringssuppgifterna under flera veckor*

- 76 Det är dessa principiella överväganden som ska ligga till grund för prövningen av särdragen i den nationella lagstiftning som är aktuell i de nationella målen, vilka har framhållits av den hänskjutande domstolen.
- 77 Vad för det första gäller omfattningen av de lagrade uppgifterna framgår det av beslutet om hänskjutande att den lagringsskyldighet som föreskrivs i denna lagstiftning, i samband med tillhandahållande av telefonitjänster, bland annat avser de uppgifter som är nödvändiga för att identifiera en kommunikations källa och destination, datum och klockslag för kommunikationens början och slut eller – när det rör sig om kommunikation via sms, multimediameddelande eller liknande meddelande – tidpunkten för avsändandet och mottagandet av meddelandet och, vid mobilanvändning, beteckningen på de celler som användes av det uppringande och det uppringda abonnemanget i början av kommunikationen. I samband med tillhandahållande av internetuppkopplingstjänster avser lagringsskyldigheten bland annat den IP-adress som abonnenten tilldelats, datum och klockslag för när internetanvändningen inleds och avslutas från den tilldelade IP-adressen och, vid mobilanvändning, beteckningen på de celler som använts i början av internetanslutningen. Även de uppgifter som ger möjlighet att få kännedom om den geografiska positionen och riktningarna för den maximala strålningen för de antenner som betjänar den berörda cellen lagras.
- 78 Även om den nationella lagstiftning som är aktuell i de nationella målen undantar innehållet i kommunikationerna och uppgifterna om de webbplatser som besökts från lagringsskyldigheten och endast föreskriver lagring av den cellidentifikationskod som använts i början av kommunikationen, ska det påpekas att detsamma i princip gällde de nationella bestämmelser om

införlivande av direktiv 2006/24 som var i fråga i de mål som avgjordes genom domen 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). Trots dessa begränsningar fann domstolen i den domen att de kategorier av uppgifter som lagrats med stöd av direktivet och dessa nationella bestämmelser kunde göra det möjligt att dra mycket precisa slutsatser om de berörda personernas privatliv, såsom deras vanor i vardagslivet, deras stadigvarande och tillfälliga uppehållsorter, deras dagliga förflyttningar och förflyttningar i övrigt, de aktiviteter de utövar, deras sociala relationer och de umgängeskretsar de rör sig i, och närmare bestämt göra det möjligt att upprätta en profil för dessa personer.

- 79 Det ska dessutom konstateras att även om den lagstiftning som är aktuell i de nationella målen inte omfattar information om vilka webbplatser som besökts, föreskriver den icke desto mindre att IP-adresserna ska lagras. Eftersom IP-adresser kan användas för att bland annat på ett uttömmande sätt kartlägga en internetanvändares hela klickström, och därmed dennes online-aktivitet, är det emellertid möjligt att med användning av dessa uppgifter upprätta en detaljerad profil för internetanvändaren. Den lagring och analys av dessa IP-adresser som krävs för en sådan kartläggning utgör således allvarliga ingrepp i internetanvändarens grundläggande rättigheter enligt artiklarna 7 och 8 i stadgan (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 punkt 153).
- 80 Dessutom, såsom SpaceNet har påpekat i sitt skriftliga yttrande, utgör de uppgifter som avser elektroniska posttjänster, även om de inte omfattas av lagringsskyldigheten enligt den lagstiftning som är aktuell i de nationella målen, endast en mycket liten del av de aktuella uppgifterna.
- 81 Såsom generaladvokaten har påpekat i punkt 60 i sitt förslag till avgörande omfattar den lagringsskyldighet som föreskrivs i den nationella lagstiftning som är aktuell i de nationella målen en stor mängd trafik- och lokaliseringssuppgifter, vilka i huvudsak motsvarar de uppgifter som låg till grund för den fasta rättspraxis som det erinrats om i punkt 78 ovan.
- 82 Som svar på en fråga som ställdes under förhandlingen preciserade den tyska regeringen dessutom att endast 1 300 enheter fanns upptagna i förteckningen över personer, myndigheter eller organisationer av social eller kyrklig karaktär vilkas uppgifter om elektronisk kommunikation inte lagras enligt 99 § punkt 2 och 113b § punkt 6 TKG. Det är uppenbart att detta motsvarar en begränsad andel av samtliga de användare av telekommunikationstjänster i Tyskland vilkas uppgifter omfattas av den lagringsplikt som föreskrivs i den nationella lagstiftning som är aktuell i de nationella målen. Sålunda lagras bland annat uppgifter om användare som omfattas av tystnadsplikt, såsom advokater, läkare och journalister.
- 83 Det framgår således av beslutet om hänskjutande att den lagring av trafik- och lokaliseringssuppgifter som föreskrivs i den nationella lagstiftningen berör nästan alla personer som ingår i befolkningen, även om dessa inte, ens indirekt, befinner sig i en situation som kan leda till straffrättsliga påföljder. Det föreskrivs även att merparten av alla trafik- och lokaliseringssuppgifter ska lagras, generellt och utan differentiering i fråga om person, tidpunkt eller geografisk plats, utan krav på skäl. Dessa uppgifter motsvarar till sin omfattning i princip de lagrade uppgifter som var i fråga i den rättspraxis som avses i punkt 79 ovan.
- 84 Mot bakgrund av den rättspraxis som det hänvisas till i punkt 75 ovan kan en sådan lagringsskyldighet som den som är aktuell i de nationella målen följaktligen inte anses utgöra en riktad lagring av uppgifterna, i motsats till vad den tyska regeringen har hävdats.

- 85 Vad för det andra gäller lagringstiden för uppgifterna framgår det av artikel 15.1 andra meningen i direktiv 2002/58 att den lagringstid som föreskrivs i en nationell bestämmelse som föreskriver en generell och odifferentierad lagring förvisso är en relevant faktor bland andra för att avgöra huruvida unionsrätten utgör hinder för en sådan åtgärd, eftersom det i nämnda mening krävs att lagringstiden ska vara ”begränsad”.
- 86 I förevarande fall är det riktigt att dessa tidsperioder, som enligt 113b § punkt 1 TKG uppgår till fyra veckor för lokaliseringssuppgifter och till tio veckor för övriga uppgifter, är betydligt kortare än de tidsperioder som föreskrevs i de nationella lagstiftningar med krav på en generell och odifferentierad lagringsskyldighet som prövades av domstolen i domen av den 21 december 2016, Tele2 Sverige och Watson m.fl. (C-203/15 och C-698/15, EU:C:2016:970), domen 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), och domen av den 5 april 2022, Commissioner of An Garda Síochána m.fl. (C-140/20, EU:C:2022:258).
- 87 Det framgår emellertid av den rättspraxis som det hänvisas till i punkt 61 ovan att frågan hur allvarligt ingreppet är beror på hur stor risken är för att det med hjälp av de sammantagna lagrade uppgifterna, bland annat med hänsyn till deras antal och mångfald, blir möjligt att dra mycket precisa slutsatser om privatlivet för den eller de personer vilkas uppgifter har lagrats och, i synnerhet, att upprätta en profil för den eller de berörda personerna, och att denna information är lika känslig med avseende på rätten till respekt för privatlivet som själva innehållet i kommunikationerna.
- 88 Lagring av trafik- eller lokaliseringssuppgifter som kan ge information om kommunikation som en användare av elektronisk kommunikationsutrustning har utfört, eller om lokaliseringen av den terminalutrustning som vederbörande använder, är dock alltid av allvarlig art, oberoende av lagringstidens längd och mängden eller arten av de uppgifter som lagras, för det fall att dessa samlade uppgifter gör det möjligt att dra mycket specifika slutsatser om den eller de berörda personernas privatliv (se, med avseende på tillgång till sådana uppgifter, dom av den 2 mars 2021, Prokuratuur (Villkor för att ge tillgång till uppgifter avseende elektronisk kommunikation), C-746/18, EU:C:2021:152, punkt 39).
- 89 I detta avseende kan även lagring av ett begränsat antal trafik- eller lokaliseringssuppgifter eller lagring av dessa uppgifter under en kort tidsperiod ge mycket exakt information om privata angelägenheter beträffande en användare av elektronisk kommunikationsutrustning. Det är dessutom inte möjligt att få en uppfattning om mängden tillgängliga uppgifter och den mycket exakta information om den berörda personens privatliv som följer av dessa uppgifter förrän efter det att man tagit del av dem. Det ingrepp som lagringen av uppgifterna resulterar i äger dock nödvändigtvis rum innan man kan ta del av de uppgifter och den information som följer därav. Bedömningen av hur allvarligt det ingrepp som lagringen av uppgifterna utgör måste därför göras med hänsyn till den risk för de berörda personernas privatliv som normalt sett är knuten till den kategori av uppgifter som lagras, varvid det saknar betydelse huruvida den information om personens privatliv som är möjlig att utläsa av uppgifterna är känslig eller ej (se, för ett liknande resonemang, dom av den 2 mars 2021, Prokuratuur (Villkor för att ge tillgång till uppgifter avseende elektronisk kommunikation), C-746/18, EU:C:2021:152, punkt 40).
- 90 Såsom framgår av punkt 77 ovan, och som bekräftades vid förhandlingen, kan i förevarande fall en mängd trafik- och lokaliseringssuppgifter som lagrats under tio respektive fyra veckor göra det möjligt att dra mycket precisa slutsatser om privatlivet för de personer vilkas uppgifter lagrats, såsom deras vanor i vardagslivet, deras stadigvarande och tillfälliga uppehållsorter, deras dagliga

förflyttningar och förflyttningar i övrigt, de aktiviteter de utövar, deras sociala relationer och de umgängeskretsar de rör sig i, och i synnerhet göra det möjligt att upprätta en profil för dessa personer.

- 91 Vad för det tredje gäller de garantier som föreskrivs i den nationella lagstiftning som är aktuell i de nationella målen och som syftar till att skydda de lagrade uppgifterna mot riskerna för missbruk och otillåten åtkomst, påpekar domstolen att lagringen av och tillgången till uppgifterna, såsom framgår av den rättspraxis som det erinrats om i punkt 60 ovan, utgör separata ingrepp i de grundläggande rättigheter som garanteras i artiklarna 7 och 11 i stadgan, vilka kräver en separat motivering enligt artikel 52.1 i stadgan. Av detta följer att även om en nationell lagstiftning säkerställer ett fullständigt iakttagande av de villkor som följer av rättspraxis avseende tolkningen av bestämmelserna i direktiv 2002/58 när det gäller *tillgång* till lagrade uppgifter, kan detta inte betyda att denna lagstiftning, för den skull, på grund av att den har denna beskaffenhet, vare sig begränsar eller ens avhjälp det allvarliga ingrepp som en sådan generell lagring av dessa uppgifter som avses i denna nationella lagstiftning innebär i de rättigheter som garanteras i artiklarna 5 och 6 i direktivet och i de grundläggande rättigheter som dessa artiklar konkretiserar (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 47).
- 92 För det fjärde och slutligen, när det gäller Europeiska kommissionens argument att särskilt allvarlig brottslighet kan likställas med ett hot mot den nationella säkerheten, har EU-domstolen redan tidigare slagit fast att målet att skydda den nationella säkerheten motsvarar det grundläggande intresset av att skydda statens väsentliga funktioner och samhällets grundläggande intressen och inbegriper förebyggande och beivrande av 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 (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 61 och där angiven rättspraxis).
- 93 Till skillnad från brottslighet, även om den är särskilt allvarlig, måste ett hot mot den nationella säkerheten vara verkligt och faktiskt eller åtminstone förutsebart, vilket förutsätter att det föreligger tillräckligt konkreta omständigheter, för att motivera en generell och odifferentierad lagring av trafik- och lokaliseringssuppgifter under en begränsad tid. Ett sådant hot skiljer sig således till sin art, sitt allvar och den specifika karaktären på de omständigheter som hotet består i, från den allmänna och ständiga risken för oroligheter eller störningar, även allvarliga sådana, av den allmänna säkerheten eller risken för allvarliga brott (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 62 och där angiven rättspraxis).
- 94 Således kan brottslighet, även allvarlig sådan, inte likställas med ett hot mot den nationella säkerheten. Ett sådant likställande skulle nämligen kunna införa en mellanliggande kategori mellan nationell säkerhet och allmän säkerhet i syfte att på den sistnämnda kategorin tillämpa de krav som följer av den förstnämnda (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 63).



*Åtgärder som avser riktad lagring, skyndsamt säkrande av uppgifter eller lagring av IP-adresser*

- 95 Flera regeringar, däribland den franska regeringen, har understrukit att endast en generell och odifferentierad lagring gör det möjligt att effektivt uppnå de mål som eftersträvas med lagringsåtgärderna, och den tyska regeringen har i huvudsak preciserat att en sådan slutsats inte vederläggs av att medlemsstaterna kan använda sig av sådana riktade lagringsåtgärder och sådant skyndsamt säkrande av uppgifter som avses i punkt 75 i förevarande dom.
- 96 Det ska i detta hänseende för det första påpekas att en effektiv lagföring som regel inte beror på en enda utredningsmetod, utan på alla de utredningsmetoder som behöriga nationella myndigheter förfogar över för det ändamålet (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 69).
- 97 För det andra möjliggör artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, enligt tolkningen i den rättspraxis som det erinrats om ovan i punkt 75, för medlemsstaterna att, i syfte att bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, vidta inte bara åtgärder avseende riktad lagring och skyndsamt säkrande av uppgifter, utan även åtgärder som föreskriver en generell och odifferentierad lagring av dels identitetsuppgifter om användare av elektroniska kommunikationsmedier, dels IP-adresser som tilldelas källan till en anslutning (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 70).
- 98 Det är i det avseendet vedertaget att lagring av identitetsuppgifter om användare av elektroniska kommunikationsmedel kan bidra till bekämpandet av grov brottslighet, i den mån uppgifterna gör det möjligt att identifiera de personer som använt sådana medel i samband med förberedandet eller utförandet av en handling som utgör grov brottslighet (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 71).
- 99 Direktiv 2002/58 utgör inte hinder för generell lagring av identitetsuppgifter om personer i syfte att bekämpa brottslighet i allmänhet. Under dessa omständigheter preciserar domstolen att varken detta direktiv eller någon annan unionsrättsakt utgör hinder för en nationell lagstiftning som syftar till att bekämpa grov brottslighet, enligt vilken elektroniska kommunikationsmedel, såsom ett förbetalt SIM-kort, endast får förvärvas på villkor att det görs en kontroll av officiella handlingar som visar köparens identitet och att säljaren registrerar den information som kommit fram vid denna kontroll, och enligt vilken säljaren i förekommande fall är skyldig att ge behöriga nationella myndigheter tillgång till dessa uppgifter (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 72).
- 100 Det ska dessutom erinras om att en generell lagring av IP-adresser som tilldelats källan till internetanslutningen utgör ett allvarligt ingrepp i de grundläggande rättigheter som är stadfästa i artiklarna 7 och 8 i stadgan, eftersom dessa IP-adresser kan användas för att dra exakta slutsatser om privatlivet för användaren av det elektroniska kommunikationsmedlet i fråga och kan ha en avskräckande effekt på utövandet av den yttrandefrihet som garanteras i artikel 11 i stadgan. Vad gäller sådan lagring har EU-domstolen emellertid konstaterat att det, vid den avvägning som ska göras mellan de legitima intressena och rättigheterna, enligt den rättspraxis som avses ovan i punkterna 65–68, ska beaktas att lagring av IP-adressen, när det är fråga om brott som begåtts på internet, och särskilt när det gäller förvärv, spridning, överföring eller uppladdning på internet av barnpornografi, i den mening som avses i artikel 2 c i Europaparlamentets och rådets direktiv 2011/93/EU av den 13 december 2011 om bekämpande av sexuella övergrepp mot barn, sexuell exploatering av barn och barnpornografi samt om ersättande av rådets

rambeslut 2004/68/RIF (EUT L 335, 2011, s. 1, och rättelse i EUT L 18, 2012, s. 7), kan utgöra den enda utredningsmetod som gör det möjligt att identifiera den person, till vilken denna adress var tilldelad vid den tidpunkt då brottet begicks (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 73).

- 101 Under dessa omständigheter – och även om det är riktigt att en lagstiftning som föreskriver att IP-adresser ska lagras för samtliga fysiska personer som äger en terminalutrustning från vilken det går att få åtkomst till internet omfattar personer som vid första anblicken inte har något samband, i den mening som avses i den rättspraxis som anges i punkt 70 ovan, med de eftersträvade målen och att internetanvändare, i enlighet med vad som konstateras i punkt 54 ovan, på grundval av artiklarna 7 och 8 i stadgan, har rätt att förvänta sig att deras identitet i princip inte kommer att avslöjas – strider en lagstiftning som föreskriver generell och odifferentierad lagring av enbart de IP-adresser som har tilldelats källan till en internetanslutning i princip inte mot artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan. Detta gäller under förutsättning att denna möjlighet används med beaktande av de stränga materiella och formella villkor som måste styra användningen av dessa uppgifter (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 punkt 155).
- 102 Med hänsyn till det allvarliga ingrepp i de grundläggande rättigheter i artiklarna 7 och 8 i stadgan som denna lagring innebär, är det endast bekämpning av grov brottslighet och förebyggande av allvarliga hot mot allmän säkerhet som, i likhet med skyddet av nationell säkerhet, kan motivera detta ingrepp. Lagringstiden får inte heller överstiga den tid som är strängt nödvändig med hänsyn till det eftersträvade målet. Slutligen måste en åtgärd av detta slag föreskriva stränga villkor och garantier vad gäller utnyttjandet av dessa uppgifter, bland annat genom kartläggning av de berörda personernas kommunikation och aktivitet på internet (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 punkt 156).
- 103 I motsats till vad den hänskjutande domstolen har understrukit finns det således ingen motsättning mellan punkterna 155 och 168 i domen 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). Såsom generaladvokaten påpekade i punkterna 81 och 82 i sitt förslag till avgörande framgår det nämligen klart av punkt 155, jämförd med punkterna 156 och 168 i den domen, att det endast är bekämpning av grov brottslighet och förebyggande av allvarliga hot mot allmän säkerhet som, i likhet med skyddet av den nationella säkerheten, kan motivera en generell lagring av IP-adresser som tilldelats källan till en internetanslutning, oberoende av om de berörda personerna har en, åtminstone indirekt, koppling till de eftersträvade målen.
- 104 Vad för det tredje gäller de lagstiftningsåtgärder som föreskriver en riktad lagring och ett skyndsamt säkrande av trafik- och lokaliseringssuppgifter, framgår det av vissa synpunkter som medlemsstaterna har framfört mot sådana åtgärder att räckvidden av dessa åtgärder har tolkats mer restriktivt än i den rättspraxis som det hänvisas till ovan i punkt 75. Även om dessa lagringsåtgärder, i enlighet med vad som har angetts ovan i punkt 57, ska utgöra ett undantag inom ramen för det system som inrättats genom direktiv 2002/58, krävs det enligt detta direktiv, jämfört med de grundläggande rättigheter som stadfästs i artiklarna 7, 8, 11 och 52.1 i stadgan, för möjligheten att utfärda ett föreläggande om riktad lagring inte att det redan är känt var ett allvarligt brott kan komma att utspelas eller vilka personer som kan misstänkas vara inblandande i en sådan gärning. Direktivet innehåller inte heller något krav på att föreläggandet om skyndsamt

säkran ska vara begränsat till misstänkta som redan har identifierats före utfärdandet av ett sådant föreläggande (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 75).

- 105 När det gäller riktad lagring har EU-domstolen slagit fast att artikel 15.1 i direktiv 2002/58 inte utgör hinder för en nationell lagstiftning som på grundval av objektiva faktorer gör det möjligt att ta sikte på en personkrets vars trafik- och lokaliseringssuppgifter kan avslöja en, åtminstone indirekt, koppling till grov brottslighet, bidra till att bekämpa grov brottslighet eller förhindra en allvarlig risk för allmän säkerhet eller en risk för nationell säkerhet (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 76 och där angiven rättspraxis).
- 106 EU-domstolen har i detta avseende preciserat att även om dessa objektiva faktorer kan variera utifrån vilka åtgärder som vidtas för att förebygga, undersöka, avslöja eller lagföra grov brottslighet, kan de personer som är föremål för lagring av uppgifter bland annat vara personer som, inom ramen för tillämpliga nationella förfaranden och på grundval av objektiva och icke-diskriminerande kriterier, tidigare har identifierats som en person som utgör ett hot mot allmän säkerhet eller nationell säkerhet i den berörda medlemsstaten (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 77).
- 107 Medlemsstaterna har således bland annat möjlighet att vidta lagringsåtgärder avseende personer som på grund av en sådan identifiering är föremål för utredning eller andra aktuella övervakningsåtgärder eller som förekommer i det nationella kriminalregistret på grund av en tidigare fällande dom för allvarliga brott som kan vara en indikation på att det föreligger en hög återfallsrisk. När en sådan identifiering grundar sig på objektiva och icke-diskriminerande faktorer som definieras i nationell rätt är riktad lagring av uppgifter om personer som identifierats på detta sätt motiverad (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 78).
- 108 En riktad lagringsåtgärd av trafik- och lokaliseringssuppgifter kan, beroende på den nationella lagstiftarens val och med strikt iakttagande av proportionalitetsprincipen, även grundas på ett geografiskt kriterium när behöriga nationella myndigheter på grundval av objektiva och icke-diskriminerande faktorer, bedömer att det i ett eller flera geografiska områden finns en förhöjd risk för förberedelse eller genomförande av grov brottslighet. Dessa områden kan bland annat utgöras av platser som utmärks av att det där begås ett stort antal allvarliga brott, platser vilka är särskilt utsatta med avseende på grov brottslighet, såsom platser och infrastruktur som regelbundet besöks eller nyttjas av ett stort antal personer, eller strategiskt viktiga platser, såsom flygplatser, järnvägsstationer, kusthamnar eller vägtullstationer (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 79 och där angiven rättspraxis).
- 109 Det ska understrykas att behöriga nationella myndigheter, i fråga om de områden som avses i föregående punkt, enligt denna rättspraxis kan vidta en riktad lagringsåtgärd som grundar sig på ett geografiskt kriterium, såsom bland annat den genomsnittliga graden av brottslighet inom ett geografiskt område, utan att de nödvändigtvis har några konkreta indikationer på att allvarliga brott håller på att förberedas eller begås i de berörda områdena. I och med att en riktad lagring som grundar sig på ett sådant kriterium, beroende på den grova brottslighet som avses och situationen i respektive medlemsstat, kan beröra både platser som kännetecknas av ett stort antal allvarliga brott och platser som är särskilt utsatta ur brottsynpunkt, är den i princip inte heller av sådan art att den kan ge upphov till diskriminering, eftersom kriteriet avseende den

genomsnittliga graden av allvarlig brottslighet i sig inte har något samband med potentiellt diskriminerande omständigheter (dom av den 5 april 2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, punkt 80).

- 110 En riktad lagringsåtgärd som avser platser eller infrastrukturer som regelbundet besöks av ett mycket stort antal personer eller strategiska platser, såsom flygplatser, tågstationer, kusthamnar eller vägtullstationer, gör det dessutom möjligt för de behöriga myndigheterna att samla in trafikuppgifter och särskilt lokaliseringssuppgifter för alla personer som vid en viss tidpunkt använder elektroniska kommunikationsmedel på någon av dessa platser. En sådan riktad lagringsåtgärd kan således göra det möjligt för nämnda myndigheter att, genom att få tillgång till de lagrade uppgifterna, få information om dessa personers närvaro på de platser eller inom de geografiska områden som omfattas av åtgärden och om deras förflyttningar mellan eller inom dessa områden och att, i syfte att bekämpa grov brottslighet, dra slutsatser om deras närvaro och förehavanden på dessa platser eller inom dessa geografiska områden vid en viss tidpunkt under lagringsperioden (dom av den 5 april 2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, punkt 81).
- 111 Det ska även påpekas att de geografiska områden som berörs av en sådan riktad lagring kan och, i förekommande fall, ska ändras beroende på hur den situation som motiverade att de valdes ut utvecklas, vilket bland annat gör det möjligt att reagera på hur kampen mot allvarlig brottslighet utvecklas. Domstolen har nämligen tidigare slagit fast att de riktade lagringsåtgärder som beskrivs i punkterna 105–110 ovan inte får pågå längre än vad som är strängt nödvändigt med hänsyn till det eftersträvade målet och de omständigheter som motiverar dem, utan att detta påverkar möjligheten att förnya åtgärderna om nämnda lagring fortsätter att vara nödvändig (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, punkt 151, och dom av den 5 april 2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, punkt 82).
- 112 När det gäller möjligheten att föreskriva andra särskiljande kriterier än ett personligt eller geografiskt kriterium för att genomföra en riktad lagring av trafik- och lokaliseringssuppgifter, kan det inte uteslutas att andra objektiva och icke-diskriminerande kriterier kan aktualiseras för att säkerställa att omfattningen av en riktad lagring begränsas till vad som är absolut nödvändigt och att det, åtminstone indirekt, finns ett samband mellan de allvarliga brotten och de personer vilkas uppgifter lagras. Eftersom artikel 15.1 i direktiv 2002/58 avser lagstiftningsåtgärder som vidtas av medlemsstaterna, ankommer det på medlemsstaterna och inte på EU-domstolen att identifiera sådana kriterier, varvid det inte kan bli fråga om att på detta sätt på nytt införa en generell och odifferentierad lagring av trafik- och lokaliseringssuppgifter (dom av den 5 april 2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, punkt 83).
- 113 Såsom generaladvokaten påpekade i punkt 50 i sitt förslag till avgörande kan i vilket fall som helst den eventuella förekomsten av svårigheter att exakt fastställa i vilka situationer och under vilka villkor en riktad lagring kan utföras inte motivera att medlemsstaterna gör ett undantag till huvudregel genom att föreskriva en generell och odifferentierad lagring av trafik- och lokaliseringssuppgifter (dom av den 5 april 2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, punkt 84).
- 114 Vad för det andra gäller skyndsamt säkrande av trafik- och lokaliseringssuppgifter som behandlas och lagras av leverantörer av elektroniska kommunikationstjänster med stöd av artiklarna 5, 6 och 9 i direktiv 2002/58, eller med stöd av lagstiftning enligt artikel 15.1 i direktivet, ska dessa uppgifter i princip antingen utplånas eller avidentifieras vid utgången av de lagstadgade

tidsperioder inom vilka behandling och lagring får ske i enlighet med de nationella bestämmelser som införlivar direktivet. Domstolen har emellertid slagit fast att det under behandlingen och lagringen av uppgifterna kan uppkomma situationer där det krävs att uppgifterna fortsätter att lagras efter utgången av dessa tidsperioder för att klarlägga allvarliga brott eller hot mot nationell säkerhet. Så kan vara fallet både i situationer där ovannämnda brott eller hot redan har kunnat konstateras och i situationer där de, efter en objektiv bedömning av samtliga relevanta omständigheter, rimligen kan misstänkas (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 85).

- 115 I en sådan situation står det medlemsstaterna fritt att, mot bakgrund av den avvägning som ska göras mellan de rättigheter och intressen som är i fråga (se punkterna 65–68 ovan), i lagstiftning som antas med stöd av artikel 15.1 i direktiv 2002/58 föreskriva en möjlighet, genom ett beslut av den behöriga myndigheten vilket ska kunna bli föremål för en effektiv domstolsprövning, att ålägga leverantörer av elektroniska kommunikationstjänster att för en bestämd tidsperiod skyndsamt säkra de trafik- och lokaliseringssuppgifter som de har tillgång till (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, punkt 163, och dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 86).
- 116 I den mån ändamålet med ett sådant skyndsamt säkrande inte längre motsvarar de ändamål för vilka uppgifterna inledningsvis samlades in och lagrades, och eftersom varje behandling av uppgifter enligt artikel 8.2 i stadgan ska ske för bestämda ändamål, måste medlemsstaterna i sin lagstiftning precisera det ändamål för vilket det får företas ett skyndsamt säkrande av uppgifter. Med hänsyn till det allvarliga ingrepp i de grundläggande rättigheterna enligt artiklarna 7 och 8 i stadgan som en sådan lagring kan medföra, är det endast bekämpningen av grov brottslighet och, i ännu högre grad, skyddet av den nationella säkerheten som kan motivera detta ingrepp, under förutsättning att åtgärden och tillgången till de lagrade uppgifterna inte överskrider gränserna för vad som är strängt nödvändigt, såsom dessa framgår av punkterna 164–167 i domen 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) (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 87).
- 117 Domstolen har preciserat att en sådan lagringsåtgärd inte behöver begränsas till uppgifter om personer som på förhand har identifierats som ett hot mot den allmänna säkerheten eller den berörda medlemsstatens nationella säkerhet eller till uppgifter om personer som konkret misstänks för att ha begått ett allvarligt brott eller vidtagit handlingar till men för den nationella säkerheten. EU-domstolen har nämligen fastställt att en sådan åtgärd – med iakttagande av den ram som fastställs i artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan samt med beaktande av övervägandena i punkt 70 ovan – i enlighet med den nationella lagstiftarens val och förutsatt att gränserna för vad som är strängt nödvändigt inte överskrids, får utsträckas till att omfatta trafik- och lokaliseringssuppgifter för andra personer än dem som misstänks ha planerat eller begått ett allvarligt brott alternativt misstänks ha planerat att vidta eller ha vidtagit handlingar till men för nationell säkerhet, under förutsättning att dessa uppgifter, på grundval av objektiva och icke-diskriminerande faktorer, kan bidra till att klarlägga ett sådant brott eller en sådan handling till men för den nationella säkerheten. Det kan härvidlag röra sig om uppgifter om offret och om offrets sociala bekantskapskrets eller yrkeskontakter (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, punkt 165, och dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 88).

- 118 En lagstiftningsåtgärd kan således tillåta att leverantörer av elektroniska kommunikationstjänster föreläggs att skyndsamt säkra trafik- och lokaliseringssuppgifter med avseende på bland annat personer som ett offer, genom sina elektroniska kommunikationsmedel, har haft kontakt med innan en handling som utgör ett allvarligt hot mot den allmänna säkerheten har utförts eller ett allvarligt brott har begåtts (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 89).
- 119 Ett sådant skyndsamt säkrande kan, enligt domstolens praxis som det hänvisas till ovan i punkt 117 och på samma villkor som de som avses i den punkten, även utsträckas till att omfatta bestämda geografiska områden, såsom platsen där brottet begicks och platsen där förberedelserna för det aktuella brottet eller handlingarna till men för den nationella säkerheten vidtogs. Det ska preciseras att även trafik- och lokaliseringssuppgifter som rör den plats där en person som eventuellt är offer för grov brottslighet har försvunnit kan omfattas av en sådan åtgärd, under förutsättning att åtgärden och tillgången till de således lagrade uppgifter iakttar gränserna för vad som är absolut nödvändigt för att bekämpa grov brottslighet eller för att skydda den nationella säkerheten, såsom dessa anges i punkterna 164–167 i domen 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) (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 90).
- 120 Det ska dessutom preciseras att artikel 15.1 i direktiv 2002/58 inte utgör hinder för att de behöriga nationella myndigheterna förordnar om skyndsamt säkrande av uppgifter redan i det första skedet av utredningen av ett allvarligt hot mot den allmänna säkerheten eller av ett eventuellt allvarligt brott, det vill säga från och med den tidpunkt då dessa myndigheter, enligt relevanta bestämmelser i nationell rätt, kan inleda en sådan utredning (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 91).
- 121 När det vidare gäller mångfalden av de åtgärder för lagring av trafik- och lokaliseringssuppgifter som avses i punkt 75 ovan, ska det preciseras att dessa olika åtgärder, enligt den nationella lagstiftarens val och med iakttagande av gränserna för vad som är strängt nödvändigt, kan tillämpas samtidigt. Under dessa omständigheter utgör artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan, såsom den har tolkats i domen 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), inget hinder för att dessa åtgärder kombineras (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 92).
- 122 För det fjärde och slutligen ska det understrykas att proportionaliteten av de åtgärder som vidtas enligt artikel 15.1 i direktiv 2002/58, enligt den fasta rättspraxis som sammanfattats i domen 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), kräver ett iakttagande av inte bara kraven på att de ska vara lämpliga och nödvändiga, utan även kravet på att åtgärderna ska vara proportionerliga i förhållande till det eftersträlvade målet (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 93).
- 123 I detta sammanhang erinrar EU-domstolen om att den, i punkt 51 i domen av den 8 april 2014, *Digital Rights Ireland m.fl.* (C-293/12 och C-594/12, EU:C:2014:238), fann att även om bekämpningen av grov brottslighet är av största betydelse för att garantera allmän säkerhet och även om dess effektivitet i stor utsträckning kan vara beroende av användningen av moderna utredningstekniker, kan ett sådant mål av allmänt samhällsintresse emellertid, trots sin grundläggande betydelse, inte i sig motivera att en åtgärd i form av en generell och

odifferentierad lagring av trafik- och lokaliseringssuppgifter, såsom den som infördes genom direktiv 2006/24, ska anses vara nödvändig (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 94).

- 124 Enligt samma logik klargjorde EU-domstolen, i punkt 145 i domen 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), att inte ens de positiva skyldigheter för medlemsstaterna som, beroende på omständigheterna i det enskilda fallet, kan följa av artiklarna 3, 4 och 7 i stadgan och som, såsom påpekats i punkt 64 ovan, avser införande av bestämmelser som möjliggör en effektiv bekämpning av brott, kan medföra att det anses motiverat med så allvarliga ingrepp i de grundläggande rättigheter som är stadfästa i artiklarna 7 och 8 i stadgan som följer av en lagstiftning om lagring av praktiskt taget hela befolkningens trafik- och lokaliseringssuppgifter, utan att det finns ett, åtminstone indirekt, samband mellan de berörda personerna och det eftersträvade målet (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 95).
- 125 De domar från Europadomstolen av den 25 maj 2021, *Big Brother Watch m.fl. mot Förenade kungariket* (CE:ECHR:2021:0525JUD 005817013) och av den 25 maj 2021, *Centrum för Rättvisa mot Sverige* (CE:ECHR:2021:0525JUD 003525208), som vissa regeringar åberopade vid förhandlingen till stöd för att Europakonventionen inte utgör hinder för nationella bestämmelser som i huvudsak föreskriver en generell och odifferentierad lagring av trafik- och lokaliseringssuppgifter, påverkar inte den tolkning av artikel 15.1 i direktiv 2002/58 som följer av ovanstående resonemang. I dessa domar var det nämligen fråga om massavläsning av uppgifter avseende internationell kommunikation. Som kommissionen påpekade vid förhandlingen uttalade sig Europeiska domstolen för de mänskliga rättigheterna, i nämnda domar, således inte om huruvida det var förenligt med Europakonventionen att generellt och odifferentierat lagra trafikuppgifter och lokaliseringssuppgifter på det nationella territoriet eller att göra en omfattande avläsning av dessa uppgifter i syfte att förebygga, upptäcka och utreda allvarliga brott. Det ska under alla omständigheter erinras om att artikel 52.3 i stadgan syftar till att säkerställa att rättigheterna i stadgan och motsvarande rättigheter enligt Europakonventionen stämmer överens med varandra, enligt vad som är påkallat, utan att undergräva unionsrättens och Europeiska unionens domstols autonomi. Detta innebär att det endast är i egenskap av en lägsta skyddsnivå som de motsvarande rättigheterna i Europakonventionen ska beaktas vid tolkningen av stadgan (dom av den 17 december 2020, *Centraal Israëlitisch Consistorie van België m.fl.*, C-336/19, EU:C:2020:1031, punkt 56).

#### *Tillgång till uppgifter som lagrats generellt och odifferentierat*

- 126 Under förhandlingen gjorde den danska regeringen gällande att behöriga nationella myndigheter, i syfte att bekämpa grov brottslighet, bör kunna få tillgång till trafik- och lokaliseringssuppgifter som har lagrats på ett generellt och odifferentierat sätt, i enlighet med den rättspraxis som framgår av domen 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, punkterna 135–139), för att kunna hindra ett allvarligt hot mot den nationella säkerheten som är verkligt och aktuellt eller förutsägbart.
- 127 Domstolen påpekar inledningsvis att om tillgång till trafik- och lokaliseringssuppgifter som har lagrats på ett generellt och odifferentierat sätt beviljas i syfte att bekämpa grov brottslighet, blir tillgången till dessa uppgifter avhängig omständigheter som ligger utanför detta syfte, beroende på huruvida det föreligger ett sådant allvarligt hot mot den nationella säkerheten som avses i föregående punkt eller inte i den berörda medlemsstaten, trots att det enbart med hänsyn till syftet att bekämpa grov brottslighet, som ska motivera lagringen av och tillgången till

uppgifterna, inte finns något som motiverar olika behandling, i synnerhet mellan medlemsstaterna (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 97).

- 128 Domstolen har redan slagit fast att tillgång till trafik- och lokaliseringssuppgifter som lagrats av leverantörer av elektroniska kommunikationstjänster till följd av en åtgärd som vidtagits med stöd av artikel 15.1 i direktiv 2002/58, vilken ska genomföras med iakttagande av de villkor som följer av rättspraxis avseende tolkningen av detta direktiv, i princip endast kan 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 tillgången till uppgifterna är av större betydelse än det mål som ligger till grund för lagringen (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 98).
- 129 Den danska regeringens argument avser emellertid en situation där syftet med den planerade begäran om tillgång, det vill säga bekämpning av grov brottslighet, i rangordningen av de allmänna målen av samhällsintresse, är av mindre betydelse än det syfte som låg till grund för lagringen, nämligen skyddet för den nationella säkerheten. Att i en sådan situation tillåta tillgång till lagrade uppgifter skulle strida mot hur de mål av allmänt samhällsintresse, som det erinrats om i föregående punkt och i punkterna 68, 71, 72 och 73 ovan, har rangordnats (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 99).
- 130 Dessutom och framför allt kan trafik- och lokaliseringssuppgifter, i enlighet med den rättspraxis som det erinrats om i punkt 74 i förevarande dom, inte lagras på ett generellt och odifferentierat sätt i syfte att bekämpa grov brottslighet, och tillgång till dessa uppgifter kan således inte motiveras av dessa syften. När dessa uppgifter undantagsvis har lagrats på ett generellt och odifferentierat sätt, i syfte att skydda den nationella säkerheten mot ett verkligt och aktuellt eller förutsebart hot, under de förutsättningar som anges i punkt 71 ovan, kan de nationella brottsbekämpande myndigheterna inte ha rätt att få tillgång till dessa uppgifter inom ramen för straffrättsliga förfaranden, eftersom det skulle betyda att förbudet mot en sådan lagring i syfte att bekämpa allvarlig brottslighet, som det erinras om i punkt 74 ovan, förlorade sin ändamålsenliga verkan (dom av den 5 april 2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, punkt 100).
- 131 Mot bakgrund av samtliga överväganden ovan ska frågan besvaras enligt följande. Artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan ska tolkas på så sätt, att den utgör hinder för nationella lagstiftningsåtgärder som i förebyggande syfte, för att bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, föreskriver att det ska ske en generell och odifferentierad lagring av trafik- och lokaliseringssuppgifter. Nämnda artikel 15.1, jämförd med artiklarna 7, 8 och 11 och 52.1 i stadgan ska tolkas på så sätt, att den däremot inte utgör hinder för lagstiftning
- som, för att skydda nationell säkerhet, tillåter att leverantörer av elektroniska kommunikationstjänster åläggs att på ett generellt och odifferentierat sätt lagra trafik- och lokaliseringssuppgifter i situationer där den berörda medlemsstaten står inför ett allvarligt hot mot nationell säkerhet som har visat sig vara verkligt och aktuellt eller förutsebart, varvid beslutet om åläggande av nämnda lagringsskyldighet måste kunna bli föremål för effektiv kontroll antingen av en domstol eller av en oberoende myndighet, vars avgörande har bindande verkan, i syfte att kontrollera om någon av dessa situationer föreligger och att de villkor och garantier som måste ställas upp är uppfyllda, och varvid åläggandet endast får meddelas för en



period som måste vara tidsmässigt begränsad till vad som är strängt nödvändigt, men som kan förlängas om hotet fortfarande kvarstår,

- som, för att skydda nationell säkerhet, bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, föreskriver en riktad lagring av trafik- och lokaliseringssuppgifter vilken, på grundval av objektiva och icke-diskriminerande faktorer, är avgränsad genom de kategorier av personer som berörs eller genom ett geografiskt kriterium, för en period som är tidsmässigt begränsad till vad som är strängt nödvändigt men som kan förlängas,
- som, för att skydda nationell säkerhet, bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, föreskriver en generell och odifferentierad lagring av IP-adresser som har tilldelats källan till en internetanslutning, för en period som är tidsmässigt begränsad till vad som är strängt nödvändigt,
- som, för att skydda nationell säkerhet, bekämpa brottslighet och skydda allmän säkerhet, föreskriver en generell och odifferentierad lagring av uppgifter om identiteten beträffande användare av elektroniska kommunikationsmedel, och
- som, för att bekämpa grov brottslighet eller, i ännu högre grad, skydda nationell säkerhet, tillåter att leverantörer av elektroniska kommunikationstjänster genom ett beslut från behörig myndighet, vilket ska kunna bli föremål för en effektiv domstolskontroll, åläggs att, under en begränsad tidsperiod, skyndsamt säkra de trafik- och lokaliseringssuppgifter som dessa tjänsteleverantörer har tillgång till,

förutsatt att denna lagstiftning, genom klara och precisa regler, säkerställer att lagringen av uppgifterna i fråga iakttar tillämpliga materiella och formella villkor, och att de berörda personerna förfogar över effektiva garantier mot riskerna för missbruk.

### **Rättegångskostnader**

- 132 Eftersom förfarandet i förhållande till parterna i de nationella målen utgör ett led i beredningen av samma mål, ankommer det på den hänskjutande domstolen att besluta om rättegångskostnaderna. De kostnader för att avge yttrande till domstolen som andra än nämnda parter har haft är inte ersättningsgilla.

Mot denna bakgrund beslutar domstolen (stora avdelningen) följande:

**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), i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009, jämförd med artiklarna 7, 8, 11 och 52.1 i Europeiska unionens stadga om de grundläggande rättigheterna,**

**ska tolkas på så sätt**

**att den utgör hinder för nationella lagstiftningsåtgärder som i förebyggande syfte, för att bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, föreskriver att det ska ske en generell och odifferentierad lagring av trafik- och lokaliseringssuppgifter,**

### **att den inte utgör hinder för lagstiftning**

- som, för att skydda nationell säkerhet, tillåter att leverantörer av elektroniska kommunikationstjänster åläggs att på ett generellt och odifferentierat sätt lagra trafik- och lokaliseringssuppgifter i situationer där den berörda medlemsstaten står inför ett allvarligt hot mot nationell säkerhet som har visat sig vara verkligt och aktuellt eller förutsebart, varvid beslutet om åläggande av nämnda lagringsskyldighet måste kunna bli föremål för effektiv kontroll antingen av en domstol eller av en oberoende myndighet, vars avgörande har bindande verkan, i syfte att kontrollera om någon av dessa situationer föreligger och att de villkor och garantier som måste ställas upp är uppfyllda, och varvid åläggandet endast får meddelas för en period som måste vara tidsmässigt begränsad till vad som är strängt nödvändigt, men som kan förlängas om hotet fortfarande kvarstår,
- som, för att skydda nationell säkerhet, bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, föreskriver en riktad lagring av trafik- och lokaliseringssuppgifter vilken, på grundval av objektiva och icke-diskriminerande faktorer, är avgränsad genom de kategorier av personer som berörs eller genom ett geografiskt kriterium, för en period som är tidsmässigt begränsad till vad som är strängt nödvändigt men som kan förlängas,
- som, för att skydda nationell säkerhet, bekämpa grov brottslighet och förhindra allvarliga hot mot allmän säkerhet, föreskriver en generell och odifferentierad lagring av IP-adresser som har tilldelats källan till en internetanslutning, för en period som är tidsmässigt begränsad till vad som är strängt nödvändigt,
- som, för att skydda nationell säkerhet, bekämpa brottslighet och skydda allmän säkerhet, föreskriver en generell och odifferentierad lagring av uppgifter om identiteten beträffande användare av elektroniska kommunikationsmedel, och
- som, för att bekämpa grov brottslighet eller, i ännu högre grad, skydda nationell säkerhet, tillåter att leverantörer av elektroniska kommunikationstjänster genom ett beslut från behörig myndighet, vilket ska kunna bli föremål för en effektiv domstolskontroll, åläggs att, under en begränsad tidsperiod, skyndsamt säkra de trafik- och lokaliseringssuppgifter som dessa tjänsteleverantörer har tillgång till,

förutsatt att denna lagstiftning, genom klara och precisa regler, säkerställer att lagringen av uppgifterna i fråga iakttar tillämpliga materiella och formella villkor, och att de berörda personerna förfogar över effektiva garantier mot riskerna för missbruk.

Underskrifter