



Samling af Afgørelser

DOMSTOLENS DOM (Store Afdeling)

20. september 2022*

[Tekst berigtiget ved kendelse af 27. oktober 2022]

»Præjudiciel forelæggelse – behandling af personoplysninger i den elektroniske kommunikationssektor – kommunikationshemmelighed – udbydere af elektroniske kommunikationstjenester – generel og udifferentieret lagring af trafikdata og lokaliseringsdata – direktiv 2002/58/EF – artikel 15, stk. 1 – Den Europæiske Unions charter om grundlæggende rettigheder – artikel 6, 7, 8 og 11 samt artikel 52, stk. 1 – artikel 4, stk. 2, TEU«

I de forenede sager C-793/19 og C-794/19,

angående anmodninger om præjudiciel afgørelse i henhold til artikel 267 TEUF, indgivet af Bundesverwaltungsgericht (forbundsdomstol i forvaltningsretlige sager, Tyskland) ved afgørelser af 25. september 2019, indgået til Domstolen den 29. oktober 2019, i sagen

Bundesrepublik Deutschland ved Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen,

mod

SpaceNet AG (C-793/19),

Telekom Deutschland GmbH (C-794/19),

har

DOMSTOLEN (Store Afdeling),

sammensat af præsidenten, K. Lenaerts, afdelingsformændene A. Arabadjiev, A. Prechal, S. Rodin, I. Jarukaitis og I. Ziemele og dommerne T. von Danwitz, M. Safjan, F. Biltgen, P.G. Xuereb (refererende dommer), N. Piçarra, L.S. Rossi og A. Kumin,

generaladvokat: M. Campos Sánchez-Bordona,

justitssekretær: kontorchef D. Dittert,

på grundlag af den skriftlige forhandling og efter retsmødet den 13. september 2021,

* Processprog: tysk.

efter at der er afgivet indlæg af:

- Bundesrepublik Deutschland ved Bundesnetzagentur für Elektrizität Gas, Telekommunikation, Post und Eisenbahnen ved C. Mögelin, som befuldmægtiget,
- [som berigtiget ved kendelse af 27. oktober 2022] SpaceNet AG ved Universitatsprofessor M. Backer,
- Telekom Deutschland GmbH ved Rechtsanwalt T. Mayen,
- den tyske regering ved J. Moller, F. Halibi, M. Hellmann, D. Klebs og E. Lankenau, som befuldmægtigede,
- den danske regering ved M. Jespersen, J. Nymann-Lindegren, V. Pasternak Jorgensen og M. Sondahl Wolff, som befuldmægtigede,
- den estiske regering ved A. Kalbus og M. Kriisa, som befuldmægtigede,
- Irland ved A. Joyce og J. Quaney, som befuldmægtigede, bistaet af D. Fennelly, BL, og P. Gallagher, SC,
- den spanske regering ved L. Aguilera Ruiz, som befuldmægtiget,
- den franske regering ved A. Daniel, D. Dubois, J. Illouz, E. de Moustier og T. Stehelin, som befuldmægtigede,
- Den cypriotiske regering ved I. Neophytou, som befuldmægtiget,
- den nederlandske regering ved K. Bulterman, A. Hanje og C.S. Schillemans, som befuldmægtigede,
- den polske regering ved B. Majczyna, D. Lutostańska og J. Sawicka, som befuldmægtigede,
- den finske regering ved A. Laine og M. Pere, som befuldmægtigede,
- den svenske regering ved H. Eklinder, A. Falk, J. Lundberg, C. Meyer-Seitz, R. Shahsavan Eriksson og H. Shev, som befuldmægtigede,
- Europa-Kommissionen ved G. Braun, S.L. Kaleda, H. Kranenborg, M. Wasmeier og F. Wilman, som befuldmægtigede,
- Den Europaiske Tilsynsforende for Databeskyttelse ved A. Buchta, D. Nardi, N. Stolič og K. Ujazdowski, som befuldmægtigede,

og efter at generaladvokaten har fremsat forslag til afgorelse i retsmødet den 18. november 2021, afsagt folgende

Dom

- 1 Anmodningerne om præjudiciel afgørelse vedrører fortolkningen af artikel 15, stk. 1, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation) (EFT 2002, L 201, s. 37), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 (EUT 2009, L 337, s. 11) (herefter »direktiv 2002/58«), sammenholdt med artikel 6-8 og 11 samt artikel 52, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder (herefter »chartret«) og artikel 4, stk. 2, TEU.
- 2 Anmodningerne er blevet indgivet i forbindelse med tvister mellem på den ene side Bundesrepublik Deutschland (Forbundsrepublikken Tyskland), ved Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (forbundsagentur for elektricitet, gas, telekommunikation og jernbaner, Tyskland), og på den anden side SpaceNet AG (sag C-793/19) og Telekom Deutschland GmbH (sag C-794/19) om den forpligtelse, som de sidstnævnte er pålagt, til at lagre deres trafikdata og lokaliseringsdata vedrørende deres kunders kommunikation.

Retsforskrifter

EU-retten

Direktiv 95/46/EF

- 3 Europa-Parlamentet og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT 1995, L 281, s. 31) blev med virkning fra den 25. maj 2018 ophævet ved Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT 2016, L 119, s. 1).
- 4 Artikel 3, stk. 2, i direktiv 95/46 bestemte:
 - »Dette direktiv gælder ikke for sådan behandling af personoplysninger,
 - som iværksættes med henblik på udøvelse af aktiviteter, der ikke er omfattet af fællesskabsretten, som f.eks. de aktiviteter, der er fastsat i afsnit V og VI i traktaten om Den Europæiske Union, og under ingen omstændigheder for behandling, der vedrører den offentlige sikkerhed, forsvar, statens sikkerhed (herunder statens økonomiske interesser, når behandlingen er forbundet med spørgsmål vedrørende statens sikkerhed) og statens aktiviteter på det strafferetlige område
 - som foretages af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter.«

Direktiv 2002/58

5 2., 6., 7. og 11. betragtning til direktiv 2002/58 har følgende ordlyd:

»(2) Dette direktiv søger at overholde de grundlæggende rettigheder og respektere de principper, der anerkendes i især [chartret]. Direktivet søger især at sikre fuld overholdelse af rettighederne i chartrets artikel 7 og 8.

[...]

(6) Internettet vender op og ned på de traditionelle markedsstrukturer, idet det udgør en fælles, global infrastruktur for fremføring af en lang række elektroniske kommunikationstjenester. Offentligt tilgængelige elektroniske kommunikationstjenester via internettet giver brugerne nye muligheder, men medfører også nye risikomomenter for deres personoplysninger og privatliv.

(7) Med hensyn til offentlige kommunikationsnet bør der træffes særlige foranstaltninger af lovgivningsmæssig, administrativ og teknisk art for at beskytte fysiske personers grundlæggende rettigheder og frihedsrettigheder og juridiske personers legitime interesser, navnlig mod den voksende risiko, der er forbundet med automatiseret opbevaring og behandling af oplysninger om abonnenter og brugere.

[...]

(11) Ligesom direktiv [95/46] finder dette direktiv ikke anvendelse på beskyttelse af grundlæggende rettigheder og frihedsrettigheder, der er forbundet med aktiviteter, der ikke er omfattet af fællesskabsretten. Det ændrer derfor ikke den nuværende balance mellem enkeltpersoners ret til privatlivets fred og medlemsstaternes mulighed for, jf. artikel 15, stk. 1, i dette direktiv, at træffe de foranstaltninger, der er nødvendige til beskyttelse af den offentlige sikkerhed, forsvaret, statens sikkerhed (herunder statens økonomiske interesser, når disse aktiviteter er forbundet med spørgsmål vedrørende statens sikkerhed) og statens aktiviteter på det strafferetlige område. Dette direktiv berører derfor ikke medlemsstaternes mulighed for lovligt at opfange elektronisk kommunikation eller træffe andre foranstaltninger, hvis det er nødvendigt med et af disse formål for øje og i overensstemmelse med den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder [undertegnet i Rom den 4. november 1950] som fortolket i Den Europæiske Menneskerettighedsdomstols retspraksis. Sådanne foranstaltninger skal være passende, stå i åbenbart rimeligt forhold til det mål, der forfølges, og være nødvendige i et demokratisk samfund, og foranstaltningerne bør omfattes af passende beskyttelsesordninger i overensstemmelse med den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder.«

6 Direktivets artikel 1 med overskriften »Anvendelsesområde og formål« fastsætter:

»1. Dette direktiv tager sigte på en harmonisering af nationale bestemmelser, der er nødvendig for at sikre et ensartet niveau i beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder og navnlig retten til privatliv og fortrolighed i forbindelse med behandling af personoplysninger inden for den elektroniske kommunikationssektor, og for at sikre fri omsætning af sådanne oplysninger og af elektronisk kommunikationsudstyr og elektroniske kommunikationstjenester i Fællesskabet.

2. Med henblik på at nå de i stk. 1 omhandlede mål specificerer og supplerer dette direktivs bestemmelser direktiv [95/46]. Nærværende bestemmelser beskytter desuden legitime interesser hos abonnenter, der er juridiske personer.

3. Dette direktiv gælder ikke for aktiviteter, der ikke er omfattet af [EUF-traktaten], som f.eks. de aktiviteter, der er omfattet af afsnit V og VI i [EU-traktaten], og under ingen omstændigheder for aktiviteter, der vedrører den offentlige sikkerhed, forsvaret, statens sikkerhed (herunder statens økonomiske interesser, når disse aktiviteter er forbundet med spørgsmål vedrørende statens sikkerhed) og statens aktiviteter på det strafferetlige område.«

7 Nævnte direktivs artikel 2 med overskriften »Definitioner« har følgende ordlyd:

»Medmindre andet angives, gælder i dette direktiv de definitioner, der er fastsat i direktiv [95/46] og Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002 om fælles rammebestemmelser for elektroniske kommunikationsnet og -tjenester (rammedirektivet) [(EFT 2002, L 108, s. 33)].

Følgende definitioner anvendes også:

- a) »bruger«: en fysisk person, som anvender en offentligt tilgængelig elektronisk kommunikationstjeneste i privat eller forretningsmæssigt øjemed, uden nødvendigvis at abonnere på den pågældende tjeneste
- b) »trafikdata«: data, som behandles med henblik på overføring af kommunikation i et elektronisk kommunikationsnet eller debitering heraf
- c) »lokaliseringsdata«: data, som behandles i et elektronisk kommunikationsnet eller af en elektronisk kommunikationstjeneste og angiver den geografiske placering af det terminaludstyr, som brugeren af en offentligt tilgængelig elektronisk kommunikationstjeneste anvender
- d) »kommunikation«: oplysninger, som udveksles eller overføres mellem et begrænset antal parter via en offentligt tilgængelig elektronisk kommunikationstjeneste. Dette omfatter ikke oplysninger, der overføres som del af en radio- og fjernsynstransmissionstjeneste til offentligheden via et elektronisk kommunikationsnet, medmindre oplysningerne kan kædes sammen med en identificerbar abonnent eller bruger, der modtager oplysningerne

[...]«

8 Artikel 3 i direktiv 2002/58 med overskriften »Omfattede tjenester« bestemmer:

»Dette direktiv finder anvendelse på behandling af persondata i forbindelse med, at offentligt tilgængelige elektroniske kommunikationstjenester stilles til rådighed via offentlige kommunikationsnet i Fællesskabet, herunder offentlige kommunikationsnet med dataindsamlings- og identifikationsudstyr.«

9 Dette direktivs artikel 5 med overskriften »Kommunikationshemmelighed« har følgende ordlyd:

»1. Medlemsstaterne sikrer kommunikationshemmeligheden ved brug af offentlige kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, både for så

vidt angår selve kommunikationen og de dermed forbundne trafikdata, via nationale forskrifter. De forbyder især aflytning, registrering, lagring og andre måder, hvorpå samtaler kan opfanges eller overvåges af andre end brugerne, uden at de pågældende brugere har indvilget heri, bortset fra tilfælde, hvor det er tilladt ifølge lovgivningen, jf. artikel 15, stk. 1. Dette stykke er ikke til hinder for teknisk lagring, som er nødvendig for overføring af en kommunikation, forudsat at princippet om kommunikationshemmelighed ikke berøres heraf.

[...]

3. Medlemsstaterne sikrer, at lagring af oplysninger eller opnåelse af adgang til oplysninger, der allerede er lagret i en abonnents eller brugers terminaludstyr, kun er tilladt på betingelse af, at abonnenten eller brugeren har givet sit samtykke hertil efter i overensstemmelse med direktiv [95/46] at have modtaget klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen. Dette er ikke til hinder for teknisk lagring eller adgang til oplysninger, hvis det alene sker med det formål at overføre kommunikation via et elektronisk kommunikationsnet eller er absolut påkrævet for at sætte udbyderen af en informationssamfundstjeneste, som abonnenten eller brugeren udtrykkelig har anmodet om, i stand til at levere denne tjeneste.«

10 Artikel 6 i direktiv 2002/58 med overskriften »Trafikdata« bestemmer:

»1. Trafikdata vedrørende abonnenter og brugere, som behandles og lagres af udbyderen af et offentligt kommunikationsnet eller en offentligt tilgængelig elektronisk kommunikationstjeneste, skal slettes eller gøres anonyme, når de ikke længere er nødvendige for fremføringen af kommunikationen, jf. dog stk. 2, 3 og 5, samt artikel 15, stk. 1.

2. Med henblik på debitering af abonnenten og afregning for samtrafik er det tilladt at behandle trafikdata. En sådan behandling er tilladt indtil udløbet af den lovbestemte forældelsesfrist for sådanne gældsforpligtelser eller fristen for anfægtelse af sådanne afregninger.

3. Med henblik på markedsføring af elektroniske kommunikationstjenester eller levering af værdiforøgende tjenester er det tilladt udbyderen af en offentligt tilgængelig elektronisk kommunikationstjeneste at behandle de i stk. 1 omtalte oplysninger i det omfang og tidsrum, som sådanne tjenester eller markedsføringen kræver, hvis den abonnent eller bruger, som oplysningerne vedrører, forudgående har givet sit samtykke hertil. Brugeren eller abonnenten skal på et hvilket som helst tidspunkt have mulighed for at trække sit samtykke til behandling af trafikdata tilbage.

[...]

5. Behandling af trafikdata i henhold til stk. 1, 2, 3 og 4 må kun foretages af personer, som handler efter bemyndigelse fra udbydere af de offentligt tilgængelige kommunikationsnet og -tjenester, og som er beskæftiget med debitering eller trafikstyring, kundeforespørgsler, afsløring af svig, markedsføring af elektroniske kommunikationstjenester eller levering af en tillægstjeneste, og skal begrænses til det for sådanne aktiviteter nødvendige.

[...]«

- 11 Direktivets artikel 9 med overskriften »Lokaliseringsdata, bortset fra trafikdata« fastsætter følgende i stk. 1:

»Hvis lokaliseringsdata, bortset fra trafikdata, vedrørende brugere af eller abonnenter på de offentlige kommunikationsnet eller offentligt tilgængelige elektroniske kommunikationstjenester, kan behandles, må disse data kun behandles, når de er gjort anonyme, eller når brugeren eller abonnenten har givet sit samtykke hertil, og da kun i det omfang og i det tidsrum, som er nødvendigt for levering af en tillægstjeneste. Tjenesteudbyderen skal, inden brugernes eller abonnenternes samtykke indhentes, underrette dem om, hvilken type lokaliseringsdata, bortset fra trafikdata, der behandles, hvorfor og hvor længe de behandles, og om de videregives til en tredjemand med henblik på levering af tillægstjenesten. [...]«

- 12 Artikel 15 i direktiv 2002/58 med overskriften »Anvendelsesområdet for visse bestemmelser i direktiv [95/46]« bestemmer i stk. 1:

»Medlemsstaterne kan vedtage retsfor skrifter med henblik på at indskrænke rækkevidden af de rettigheder og forpligtelser, der omhandles i artikel 5, artikel 6, artikel 8, stk. 1, 2, 3 og 4, og artikel 9, hvis en sådan indskrænkning er nødvendig, passende og forholdsmæssig i et demokratisk samfund af hensyn til den nationale sikkerhed (dvs. statens sikkerhed), forsvaret, den offentlige sikkerhed, eller forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager eller uautoriseret brug af det elektroniske kommunikationssystem efter artikel 13, stk. 1, i direktiv [95/46]. Med henblik herpå kan medlemsstaterne bl.a. vedtage retsfor skrifter om lagring af data i en begrænset periode, som kan begrundes i et af de hensyn, der er nævnt i dette stykke. Alle i dette stykke omhandlede for skrifter skal være i overensstemmelse med fællesskabsrettens generelle principper, herunder principperne i EU-traktatens artikel 6, stk. 1 og 2.«

Tysk ret

TKG

- 13 § 113a, stk. 1, første punktum, i Telekommunikationsgesetz (lov om telekommunikation) af 22. juni 2004 (BGBl. 2004 I, s. 1190) i den affattelse, der finder anvendelse på tvisterne i hovedsagerne, (herefter »TKG«), har følgende ordlyd:

»De i §§ 113b-113g definerede forpligtelser vedrørende lagring, anvendelse og sikkerhed med hensyn til trafikdata gør sig gældende for operatører, der leverer offentligt tilgængelige telekommunikationstjenester til slutbrugere.«

- 14 TKG's § 113b bestemmer:

»(1) De i § 113a, stk. 1, nævnte operatører skal lagre dataene på det nationale område på følgende måde:

1. i ti uger, hvis der er tale om de i stk. 2 og 3 omhandlede data.
2. i fire uger, hvis der er tale om de i stk. 4 omhandlede lokaliseringsdata.

(2) Udbydere af offentligt tilgængelige telefontjenester lagrer:

1. telefonnummeret eller en anden identitet for den, der ringer op, og den forbindelse, der ringes til, samt ved om- og viderestilling enhver anden involveret forbindelse
2. dato og klokkeslæt for kommunikationens begyndelse og ophør med angivelse af den anvendte tidszone
3. oplysninger om den benyttede tjeneste, hvis der i forbindelse med telefontjenesten kan benyttes forskellige tjenester
4. for mobile telefontjenester endvidere
 - a) den internationale identitet for mobile abonnenter for den, der ringer op, og den forbindelse, der ringes til
 - b) den internationale identitet for det terminaludstyr, der ringer op, og det der ringes til
 - c) dato og klokkeslæt for den første aktivering af tjenesten under angivelse af den anvendte tidszone, hvis der er blevet betalt tjenester på forhånd
5. for internettelefontjenester tillige IP-adresserne (internetprotokoladresserne) for den forbindelse, der ringer op, og den forbindelse, der ringes til, og tildelte brugeridentiteter.

Stk. 1 finder tilsvarende anvendelse

1. ved kommunikation med sms-, multimedie- eller lignende beskeder, i så fald erstattes de i stk. 1, nr. 2, nævnte oplysninger med tidspunkterne for afsendelse og modtagelse af beskeden
2. på ubesvarede eller forgæves opkald, der skyldes, at netværkssystemet har grebet ind [...]

(3) Udbydere af offentligt tilgængelige internetadgangstjenester lagrer

1. den IP-adresse, som abonnenten er blevet tildelt med henblik på brug af internettet
2. tydelig identifikation af den forbindelse, der giver adgang til internettet, samt det tildelte identifikationsnummer
3. dato og klokkeslæt for internetbenyttelsens begyndelse og ophør under den tildelte IP-adresse med angivelse af den anvendte tidszone

(4) Ved brug af mobile telefontjenester lagres betegnelsen for de radioceller, der blev anvendt ved forbindelsens begyndelse af den, der foretager opkaldet, og den, der modtager det. Hvad angår offentligt tilgængelige internetadgangstjenester lagres der i forbindelse med mobilt brug betegnelsen for de radioceller, der blev anvendt ved begyndelsen af internetforbindelsen. Der bør ligeledes lagres data, der gør det muligt at finde den geografiske placering og retningerne for den maksimale stråling fra de antenner, som betjener den pågældende mobiltelefon.

(5) Kommunikationens indhold, data om besøgte websteder og data fra e-mailtjenester kan ikke lagres i medfør af denne bestemmelse.

Data, der ligger til grund for de i § 99, stk. 2, omhandlede forbindelser, kan ikke lagres i overensstemmelse med denne bestemmelse. Dette finder tilsvarende anvendelse på telefonisk

kommunikation fra de i § 99, stk. 2, omhandlede enheder. § 99, stk. 2, andet til syvende punktum, finder tilsvarende anvendelse.

[...]«

15 De i TKG's § 99, stk. 2, nævnte forbindelser, hvortil TKG's § 113, stk. 6, henviser, er forbindelser med personer, myndigheder og organisationer af social eller religiøs karakter, som alene eller i det væsentlige tilbyder samtaleparterne, der i princippet forbliver anonyme, telefonisk assistance i tilfælde af kritiske psykologiske eller sociale situationer, og som selv eller hvis medarbejdere er omfattet af en særlig tavshedspligt i denne henseende. Den i TKG's § 99, stk. 2, andet og fjerde punktum, fastsatte undtagelse er betinget af, at den, der ringes til, registreres på en liste oprettet af forbundsagenturet for elektricitet, gas, telekommunikation og jernbaner, efter at indehaverne af opkaldsnumrene har godtgjort deres opgave ved at fremlægge en attest, der er udstedt af en offentligtretlig myndighed, organisme, institution eller stiftelse.

16 TKG's § 113c, stk. 1 og 2, har følgende ordlyd:

»(1) Data, der lagres i henhold til § 113b, kan

1. overføres til en retshåndhævende myndighed, når denne anmoder om overførsel under henvisning til en retlig bestemmelse, der bemyndiger den pågældende myndighed til at indsamle de i § 113b omhandlede data med henblik på bekæmpelse af særligt alvorlige strafbare handlinger
2. overføres til en sikkerhedsmyndighed på delstatsniveau, når denne anmoder om overførsel under henvisning til en retlig bestemmelse, der bemyndiger den pågældende myndighed til at indsamle de i § 113b omhandlede data med henblik på at forebygge en konkret risiko for en persons helbred, liv eller frihed eller for forbundsstatens eller en delstats beståen.

[...]

(2) Data, der lagres i overensstemmelse med § 113b, kan ikke anvendes af operatører, der er underlagt de i § 113a, stk. 1, fastsatte forpligtelser, til andre end de i stk. 1 omhandlede formål.«

17 TKG's § 113d bestemmer:

»Adressaten for den i § 113a, stk. 1, fastsatte forpligtelse skal ved hjælp af tekniske og organisatoriske foranstaltninger, der anvender den seneste teknologi, sikre, at data, der lagres i overensstemmelse med § 113b, stk. 1, som følge af forpligtelsen til lagring, er beskyttet mod uautoriseret kontrol og brug. Disse foranstaltninger omfatter navnlig:

1. anvendelse af en særligt sikker krypteringsprocedure
2. lagring i forskellige lagringsinfrastrukturer, der er adskilt fra de infrastrukturer, der anvendes til løbende driftsmæssige funktioner
3. lagring, der omfatter et øget niveau af beskyttelse mod cyberangreb, i ikke-forbundne it-systemer til databehandling

4. begrænsning af adgangen til anlæg, der anvendes til databehandling, til personer, der har en særlig bemyndigelse fra den aktør, der er ansvarlig for at opfylde forpligtelsen, og
5. en forpligtelse til, at der ved adgangen til dataene mindst deltager to personer, der har en særlig bemyndigelse fra den aktør, der er ansvarlig for at opfylde forpligtelsen.«
- 18 TKG's § 113e har følgende ordlyd:
- »(1) Den aktør, der er ansvarlig for at opfylde den i § 113a, stk. 1, fastsatte forpligtelse, skal sikre, at der med henblik på kontrol af databeskyttelse gives adgang, navnlig til læsning, kopiering, ændring, sletning og låsning, til data, der lagres i henhold til § 113b, stk. 1, i overensstemmelse med forpligtelsen til lagring. Følgende skal registreres
1. tidspunktet for adgangen
 2. de personer, der tilgår dataene
 3. adgangens formål og karakter.
- (2) De tilgæede data kan ikke anvendes til andre formål end til kontrol af databeskyttelsen.
- (3) Den aktør, der er ansvarlig for at opfylde den i § 113a, stk. 1, fastsatte forpligtelse, skal sikre, at de tilgæede data slettes efter et år.«
- 19 For at sikre et særligt højt niveau af beskyttelse og kvalitet for data fastsætter forbundsagenturet for elektricitet, gas, telekommunikation og jernbaner i overensstemmelse med TKG's § 113f, stk. 1, en række krav, som i henhold til denne lovs § 113f, stk. 2, skal vurderes kontinuerligt og eventuelt tilpasses. I henhold til TKG's § 113g skal konkrete sikkerhedsforanstaltninger integreres i den sammenfatning af sikkerhedspolitikken, som skal fremlægges af den aktør, der er ansvarlig herfor.

Strafferetsplejeloven

- 20 § 100g, stk. 2, sidste punktum, i Strafprozessordnung (strafferetsplejeloven) har følgende ordlyd:
- »Hvis det på grund af bestemte forhold mistænkes, at en person, i egenskab af ophavsmand eller medskyldig, har begået en af de særligt alvorlige strafbare handlinger, der er nævnt i andet punktum, eller i de tilfælde, hvor forsøg kan straffes, har forsøgt at begå en sådan strafbar handling, og såfremt den strafbare handling også er særligt alvorlig i det konkrete tilfælde, kan trafikdata, der lagres i overensstemmelse med [TKG's] § 113b, anvendes, hvis det er uforholdsmæssigt vanskeligt eller umuligt at efterforske de faktiske omstændigheder eller at lokalisere den undersøgte person med andre midler, eller hvis indsamlingen af data står i forhold til sagens betydning.«
- 21 Strafferetsplejelovens § 101a, stk. 1, gør indsamlingen af trafikdata i henhold til denne lovs § 100g betinget af, at der foreligger en retslig tilladelse. I henhold til strafferetsplejelovens § 101a, stk. 2, skal afgørelsens begrundelse indeholde de væsentligste betragtninger vedrørende spørgsmålet om, hvorvidt foranstaltningen er nødvendig og passende i det særlige omhandlede tilfælde. Strafferetsplejelovens § 101a, stk. 6, fastsætter en forpligtelse til at underrette deltagerne i den pågældende telekommunikation.

Twisterne i hovedsagerne og det præjudicielle spørgsmål

- 22 SpaceNet AG og Telekom Deutschland GmbH leverer offentligt tilgængelige internetadgangstjenester i Tyskland. Sidstnævnte selskab leverer ligeledes offentligt tilgængelige telefontjenester i Tyskland.
- 23 Disse tjenesteudbydere anfægtede for Verwaltungsgericht Köln (forvaltningsdomstolen i Köln, Tyskland) den forpligtelse, som de fra den 1. juli 2017 er pålagt ved TKG's § 113a, stk. 1, sammenholdt med denne lovs § 113b, til at lagre deres trafikdata og lokaliseringsdata vedrørende deres kunders telekommunikation.
- 24 Ved domme afsagt den 20. april 2018 fastslog Verwaltungsgericht Köln (forvaltningsdomstolen i Köln), at SpaceNet og Telekom Deutschland ikke var forpligtede til at lagre de trafikdata vedrørende telekommunikation, der er omhandlet i TKG's § 113b, stk. 3, for de kunder, til hvilke de leverer internetadgang, og at Telekom Deutschland endvidere ikke var forpligtet til at lagre de trafikdata vedrørende telekommunikation, som er nævnt i TKG's § 113b, stk. 2, første og andet punktum, for kunder, til hvilke dette selskab leverer adgang til offentligt tilgængelige telefontjenester. Denne retsinstans fastslog nemlig, at denne forpligtelse til lagring, henset til dom af 21. december 2016, Tele2 Sverige og Watson m.fl. (C-203/15 og C-698/15, EU:C:2016:970), var i strid med EU-retten.
- 25 Forbundsrepublikken Tyskland har iværksat appel med påstand om ophævelse af disse domme for Bundesverwaltungsgericht (forbundsdomstol i forvaltningsretlige sager, Tyskland), der er den forelæggende ret.
- 26 Forbundsrepublikken Tyskland har anført, at spørgsmålet om, hvorvidt den forpligtelse til lagring, der er pålagt ved TKG's § 113a, stk. 1, sammenholdt med denne lovs § 113b, er i strid med EU-retten, afhænger af fortolkningen af direktiv 2002/58.
- 27 Den forelæggende ret har i denne henseende anført, at Domstolen i dom af 21. december 2016, Tele2 Sverige og Watson m.fl. (C-203/15 og C-698/15, EU:C:2016:970), allerede endeligt har fastslået, at lovgivning, der vedrører lagring af trafikdata og lokaliseringsdata samt de nationale myndigheders adgang til disse data, principielt er omfattet af anvendelsesområdet for direktiv 2002/58.
- 28 Den forelæggende ret har ligeledes anført, at den i hovedsagerne omhandlede forpligtelse til lagring kun kan begrundes i henhold til artikel 15, stk. 1, i direktiv 2002/58, eftersom den begrænser de rettigheder, der følger af direktivets artikel 5, stk. 1, artikel 6, stk. 1, og artikel 9, stk. 1.
- 29 Den forelæggende ret har i denne henseende anført, at det følger af dom af 21. december 2016, Tele2 Sverige og Watson m.fl. (C-203/15 og C-698/15, EU:C:2016:970), at artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at denne bestemmelse er til hinder for en national lovgivning, der med henblik på bekæmpelse af kriminalitet fastsætter en generel og udifferentieret lagring af samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation.

- 30 Ifølge den forelæggende ret kræver den i hovedsagerne omhandlede nationale lovgivning ligesom i de sager, der gav anledning til nævnte dom, ikke nogen begrundelse for at lagre data eller nogen forbindelse mellem de lagrede data og en strafbar handling eller en risiko for den offentlige sikkerhed. Denne nationale lovgivning kræver nemlig en lagring af størstedelen af de relevante telekommunikationstrafikdata, som er uden anledning, generel samt personligt, tidsmæssigt og geografisk udifferentieret.
- 31 Den forelæggende ret er imidlertid af den opfattelse, at det ikke er udelukket, at den i hovedsagerne omhandlede forpligtelse til lagring kan være begrundet i henhold til artikel 15, stk. 1, i direktiv 2002/58.
- 32 I første række har den forelæggende ret anført, at den i hovedsagerne omhandlede nationale lovgivning i modsætning til de nationale lovgivninger, som var omhandlet i de sager, der gav anledning til dom af 21. december 2016, Tele2 Sverige og Watson m.fl. (C-203/15 og C-698/15, EU:C:2016:970), ikke kræver lagring af samtlige trafikdata vedrørende alle abonnenters og registrerede brugeres telekommunikation i forbindelse med samtlige midler til elektronisk kommunikation. Ikke blot er kommunikationens indhold udelukket fra forpligtelsen til lagring, men heller ikke data om besøgte websteder, data fra e-mailtjenester og data vedrørende meddelelser til eller fra telefontjenester af social eller religiøs karakter til eller fra bestemte linjer kan lagres, således som det fremgår af TKG's § 113b, stk. 5 og 6.
- 33 I anden række har den forelæggende ret anført, at der i TKG's § 113b, stk. 1, fastsættes en periode for lagring på fire uger for lokaliseringsdata og på ti uger for trafikdata, selv om Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15. marts 2006 om lagring af data genereret eller behandlet i forbindelse med tilvejebringelse af offentligt tilgængelige elektroniske kommunikationstjenester eller elektroniske kommunikationsnet og om ændring af direktiv 2002/58/EF (EUT 2006, L 105, s. 54), på hvilke de nationale lovgivninger, som var omhandlet i de sager, der gav anledning til dom af 21. december 2016, Tele2 Sverige og Watson m.fl. (C-203/15 og C-698/15, EU:C:2016:970), var støttet, fastsatte en periode for lagringen på mellem seks måneder og to år.
- 34 Den forelæggende ret har anført, at selv om visse kommunikationsmidler eller visse kategorier af data undtages lagringspligten, og perioden for lagringen begrænses, kan dette ikke fjerne enhver risiko for, at der kan udarbejdes en omfattende profil af de pågældende personer, men det kan i det mindste reducere denne risiko væsentligt i forbindelse med gennemførelsen af den i hovedsagerne omhandlede nationale lovgivning.
- 35 I tredje række indebærer denne lovgivning strenge begrænsninger med hensyn til beskyttelsen af de lagrede data og adgangen til disse. For det første sikrer den en effektiv beskyttelse af de lagrede data mod risici for misbrug samt mod enhver ulovlig adgang til disse data. For det andet må de lagrede data kun anvendes til bekæmpelsen af grov kriminalitet eller med henblik på at forebygge en konkret risiko for en persons helbred, liv eller frihed eller for forbundsstatens eller en delstats beståen.
- 36 I fjerde række kan en fortolkning af artikel 15, stk. 1, i direktiv 2002/58 i den forstand, at enhver ulovlig lagring af data generelt er uforenelig med EU-retten, være i strid med medlemsstaternes forpligtelse til at handle, som følger af den ret til sikkerhed, der er fastsat i chartrets artikel 6.

- 37 I femte række har den forelæggende ret anført, at såfremt artikel 15 i direktiv 2002/58 fortolkes således, at denne bestemmelse er til hinder for en generel lagring af data, er den nationale lovgivers handlemuligheder væsentligt begrænset på et område inden for strafforfølgelse og offentlig sikkerhed, som i henhold til artikel 4, stk. 2, TEU fortsat hører under de enkelte medlemsstaters enekompetence.
- 38 I sjette række har den forelæggende ret anført, at der skal tage hensyn til Den Europæiske Menneskerettighedsdomstols praksis, og at denne domstol har fastslået, at artikel 8 i den europæiske konvention til beskyttelse af menneskerettigheder og grundlæggende frihedsrettigheder (herefter »EMRK«) ikke var til hinder for nationale bestemmelser om masseopfangelse af den grænseoverskridende datatrafik, henset til de trusler, som mange stater aktuelt er udsat for, og til de tekniske værktøjer, som terrorister og kriminelle nu kan anvende for at begå strafbare handlinger.
- 39 På denne baggrund har Bundesverwaltungsgericht (forbundsdomstol i forvaltningsretlige sager) besluttet at udsætte sagerne og forelægge Domstolen følgende præjudicielle spørgsmål:

»Skal artikel 15 i direktiv [2002/58] i lyset af [chartrets] artikel 7, 8 og 11 samt artikel 52, stk. 1, [...] på den ene side og [chartrets] artikel 6 [...] og artikel 4 [TEU] på den anden side fortolkes således, at den er til hinder for en national bestemmelse, som forpligter udbyderne af offentligt tilgængelige elektroniske kommunikationstjenester til at lagre trafik- og lokaliseringsdata for slutbrugerne af disse tjenester, når

- 1) denne forpligtelse ikke forudsætter nogen specifik anledning i lokal, tidsmæssig eller geografisk henseende
- 2) genstanden for pligten til at lagre data i forbindelse med levering af offentligt tilgængelige telefontjenester – herunder formidling af sms-, multimedie- eller lignende beskeder samt ubesvarede eller forgæves opkald – er følgende data:
 - a) telefonnummeret eller en anden identitet for den, der ringer op, og den forbindelse, der ringes til, samt ved om- og viderestilling enhver anden involveret forbindelse
 - b) dato og klokkeslæt for begyndelse og afslutning af forbindelsen henholdsvis – i forbindelse med formidling af sms-, multimedie- eller lignende beskeder – tidspunkterne for afsendelse og modtagelse af beskeden med angivelse af den anvendte tidszone
 - c) oplysninger om den benyttede tjeneste, hvis der i forbindelse med telefontjenesten kan benyttes forskellige tjenester
 - d) for mobile telefontjenester endvidere
 - i) den internationale identitet for mobile abonnenter for den, der ringer op, og den forbindelse, der ringes til
 - ii) den internationale identitet for det terminaludstyr, der ringer op, og som der ringes til
 - iii) dato og klokkeslæt for den første aktivering af tjenesten under angivelse af den anvendte tidszone, hvis der er blevet betalt tjenester på forhånd
 - iv) betegnelserne for de radioceller, som blev benyttet af den forbindelse, der ringer op, og den forbindelse, der ringes til, ved forbindelsens begyndelse
 - e) for internettelefontjenester tillige internetprotokoladresserne for den forbindelse, der ringer op, og den forbindelse, der ringes til, og tildelte brugeridentiteter
- 3) genstanden for pligten til lagring i forbindelse med levering af offentligt tilgængelige internetadgangstjenester er følgende data:
 - a) den internetprotokoladresse, som er tildelt abonnenten til en internetbenyttelse

- b) en entydig identitet for den forbindelse, gennem hvilken internetbenyttelsen sker, samt en tildelt brugeridentitet
 - c) dato og klokkeslæt for internetbenyttelsens begyndelse og ophør under den tildelte internetprotokoladresse med angivelse af den anvendte tidszone
 - d) for mobil benyttelse betegnelsen for de radioceller, som benyttes ved internetforbindelsens begyndelse
- 4) følgende data ikke må lagres:
- a) kommunikationens indhold
 - b) data om besøgte internetsider
 - c) data fra elektroniske posttjenester
 - d) data, som er baseret på forbindelser til eller fra bestemte personers, myndigheders og organisationers forbindelser inden for sociale eller [religiøse] områder
- 5) perioden for lagring af lokaliseringsdata, dvs. betegnelsen for de benyttede radioceller, udgør fire uger, og for de øvrige data ti uger
- 6) der er sikret en effektiv beskyttelse af de lagrede data mod risici for misbrug samt mod enhver ulovlig adgang, og
- 7) de lagrede data kun må anvendes til at forfølge særligt grove straffelovsovertrædelser og til at forebygge en konkret fare for en persons liv og helbred eller frihed eller for forbundsstatens eller en delstats beståen, med undtagelse af den internetprotokoladresse, som er tildelt abonnenten til en internetbenyttelse, og som det er tilladt at anvende i forbindelse med en stamdataoplysning [...] med henblik på forfølgelse af enhver form for strafbare handlinger, for at forebygge en fare for den offentlige sikkerhed og orden samt for at opfylde efterretningstjenesternes opgaver?«

Retsforhandlingerne for Domstolen

- 40 Ved afgørelse truffet af Domstolens præsident den 3. december 2019 er sagerne C-793/19 og C-794/19 blevet forenet med henblik på retsforhandlingernes skriftlige og mundtlige del samt dommen.
- 41 Ved afgørelse truffet af Domstolens præsident den 14. juli 2020 er behandlingen af de forenede sager C-793/19 og C-794/19 blevet udsat i henhold til artikel 55, stk. 1, litra b), i Domstolens procesreglement indtil afsigelsen af dommen i sagen La Quadrature du Net m.fl. (C-511/18, C-512/18 og C-520/18).
- 42 Eftersom Domstolen den 6. oktober 2020 afsagde dom i sag La Quadrature du Net m.fl. (C-511/18, C-512/18 og C-520/18, EU:C:2020:791), har Domstolens præsident den 8. oktober 2020 truffet afgørelse om genoptagelse af sagens behandling i de forenede sager C-793/19 og C-794/19.
- 43 Den forelæggende ret, til hvilken Justitskontoret har meddelt denne dom, har anført, at den opretholdt sin anmodning om præjudiciel afgørelse.
- 44 Den forelæggende ret har i denne henseende indledningsvis anført, at den forpligtelse til lagring, der er fastsat i den i hovedsagerne omhandlede lovgivning, vedrører et mindre antal data og en kortere periode for lagring end det, der var fastsat i de nationale lovgivninger, som var omhandlet

i de sager, der gav anledning til dom af 6. oktober 2020, La Quadrature du Net m.fl. (C-511/18, C-512/18 og C-520/18, EU:C:2020:791). Disse særlige forhold reducerer risikoen for, at de lagrede data gør det muligt at drage særdeles præcise konklusioner vedrørende privatlivet hos de personer, hvis data er blevet lagret.

- 45 Den forelæggende ret har desuden atter anført, at den i hovedsagerne omhandlede nationale lovgivning sikrer de lagrede data en effektiv beskyttelse mod risikoen for misbrug og ulovlig adgang.
- 46 Endelig har den forelæggende ret fremhævet, at der fortsat er usikkerhed med hensyn til spørgsmålet om, hvorvidt den lagring af IP-adresser, der foreskrives i den i hovedsagerne omhandlede nationale lovgivning, er forenelig med EU-retten, idet der er en uoverensstemmelse mellem præmis 155 og 168 i dom af 6. oktober 2020, La Quadrature du Net m.fl. (C-511/18, C-512/18 og C-520/18, EU:C:2020:791). Ifølge den forelæggende ret indebærer denne dom således en usikkerhed med hensyn til spørgsmålet om, hvorvidt Domstolen med henblik på lagring af IP-adresser kræver en begrundelse for lagringen, der er knyttet til et formål med beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet eller forebyggelse af alvorlige trusler mod den offentlige sikkerhed, sådan som det fremgår af nævnte doms præmis 168, eller om det er tilladt at lagre IP-adresser uden en konkret begrundelse, idet alene anvendelsen af de lagrede data er begrænset af de nævnte formål, sådan som det fremgår af samme doms præmis 155.

Om det præjudicielle spørgsmål

- 47 Med det præjudicielle spørgsmål ønsker den forelæggende ret nærmere bestemt oplyst, om artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 6-8, 11 og artikel 52, stk. 1, og artikel 4, stk. 2, TEU, skal fortolkes således, at denne bestemmelse er til hinder for en national lovgivning, som med visse undtagelser med de i dette direktivs artikel 15, stk. 1, opregnede formål, og navnlig med henblik på at bekæmpe alvorlige strafbare handlinger eller forebygge en konkret risiko for den nationale sikkerhed, pålægger udbyderne af offentligt tilgængelige elektroniske kommunikationstjenester at foretage en generel og udifferentieret lagring af disse tjenesters slutbrugeres væsentligste trafikdata og lokaliseringsdata, idet der foreskrives en periode for lagringen på flere uger samt regler for at sikre de lagrede data en effektiv beskyttelse mod risikoen for misbrug og mod enhver ulovlig adgang til disse data.

Spørgsmålet om, hvorvidt direktiv 2002/58 finder anvendelse

- 48 Med hensyn til den argumentation, som Irland og den franske, den nederlandske, den polske og den svenske regering har fremført, hvorefter den af hovedsagerne omhandlede nationale lovgivning ikke henhører under anvendelsesområdet for direktiv 2002/58, navnlig for så vidt som denne lovgivning blev vedtaget med henblik på beskyttelse af den nationale sikkerhed, er det tilstrækkeligt at bemærke, at en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester at lagre trafikdata og lokaliseringsdata med henblik på at beskytte den nationale sikkerhed og bekæmpe kriminalitet, såsom den i hovedsagerne omhandlede lovgivning, er omfattet af anvendelsesområdet for direktiv 2002/58 (dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 104).

Fortolkningen af artikel 15, stk. 1, i direktiv 2002/58

Resumé af de principper, der følger af Domstolens praksis

- 49 Det fremgår af fast retspraksis, at der ved fortolkningen af en EU-retlig bestemmelse ikke blot skal tages hensyn til dennes ordlyd, men også til den sammenhæng, hvori den indgår, og til de mål, der forfølges med den lovgivning, som den er en del af, og bl.a. til denne lovgivnings tilblivelse (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 32 og den deri nævnte retspraksis).
- 50 Det fremgår af selve ordlyden af artikel 15, stk. 1, i direktiv 2002/58, at de retsfor skrifter, som direktivet tillader medlemsstaterne at vedtage på de i direktivet fastsatte betingelser, kun må tage sigte på »at indskrænke rækkevidden« af de rettigheder og forpligtelser, der er omhandlet i bl.a. artikel 5, 6 og 9 i direktiv 2002/58 (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 33).
- 51 Hvad angår den ordning, der er indført ved dette direktiv, og hvori dets artikel 15, stk. 1, indgår, bemærkes, at medlemsstaterne i henhold til direktivets artikel 5, stk. 1, første og andet punktum, via nationale forskrifter skal sikre kommunikationshemmeligheden ved brug af offentlige kommunikationsnet og offentligt tilgængelige elektroniske kommunikationstjenester, både for så vidt angår selve kommunikationen og de dermed forbundne trafikdata. De har navnlig pligt til at forbyde aflytning, registrering, lagring og andre måder, hvorpå samtaler og de dermed forbundne trafikdata kan opfanges eller overvåges af andre end brugerne, uden at de pågældende brugere har indvilget heri, bortset fra tilfælde, hvor det er tilladt ifølge lovgivningen, jf. samme direktivs artikel 15, stk. 1 (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 34).
- 52 I denne henseende har Domstolen allerede fastslået, at artikel 5, stk. 1, i direktiv 2002/58 fastsætter princippet om fortrolighed i forbindelse med såvel elektronisk kommunikation som de dermed forbundne trafikdata og navnlig indebærer, at det for andre end brugerne principielt er forbudt for enhver at lagre denne kommunikation og disse data, uden at disse brugere har givet samtykke hertil (dom af 6.10.2020, *La Quadrature du Net m.fl.*, C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 107, og af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 35).
- 53 Denne bestemmelse afspejler det formål, som EU-lovgiver forfulgte ved vedtagelsen af direktiv 2002/58. Det fremgår nemlig af begrundelsen til forslaget til Europa-Parlamentets og Rådets direktiv om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (KOM(2000) 385 endelig), der lå til grund for direktiv 2002/58, at EU-lovgiver ønskede »at sikre, at der fortsat garanteres en høj grad af beskyttelse af personoplysninger og privatlivets fred i forbindelse med alle elektroniske kommunikationstjenester, uanset hvilken teknologi der anvendes«. Som det bl.a. fremgår af sjette og syvende betragtning til det nævnte direktiv, har dette således til formål at beskytte brugerne af elektroniske kommunikationstjenester mod de risikomomenter for deres personoplysninger og privatliv, der følger af anvendelsen af ny teknologi, og navnlig den øgede mulighed for at foretage automatiseret opbevaring og behandling af oplysninger. Som det fremgår af anden betragtning til samme direktiv, ønsker EU-lovgiver især at sikre fuld overholdelse af de rettigheder, der er nævnt i chartrets artikel 7 og 8 vedrørende henholdsvis respekt for privatlivet og beskyttelse af personoplysninger (jf. i denne retning dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 36 og den deri nævnte retspraksis).

- 54 Med vedtagelsen af direktiv 2002/58 har EU-lovgiver således konkretiseret disse rettigheder, hvilket indebærer, at brugerne af elektroniske kommunikationsmidler principielt med rette kan forvente, at deres kommunikation og de dermed forbundne data forbliver anonyme, så længe de ikke har givet deres samtykke, og ikke kan gøres til genstand for registrering (dom af 6.10.2020, La Quadrature du Net m.fl., C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 109, og af 5.4.2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, præmis 37).
- 55 Hvad navnlig angår den behandling og lagring af trafikdata vedrørende abonnenter og brugere, der foretages af udbydere af elektroniske kommunikationstjenester, er det i artikel 6, stk. 1, i direktiv 2002/58 fastsat, at sådanne data skal slettes eller gøres anonyme, når de ikke længere er nødvendige for fremføringen af kommunikationen, og i artikel 6, stk. 2, er det præciseret, at det med henblik på debitering af abonnenten og afregning for samtrafik kun er tilladt at behandle trafikdata indtil udløbet af den lovbestemte forældelsesfrist for sådanne gældsforpligtelser eller fristen for anfægtelse af sådanne afregninger. Hvad angår andre lokaliseringsdata end trafikdata bestemmer direktivets artikel 9, stk. 1, at disse data kun må behandles under visse betingelser og kun, når de er gjort anonyme, eller når brugeren eller abonnenten har givet sit samtykke hertil.
- 56 Direktiv 2002/58 fastlægger følgelig ikke blot rammerne for adgang til sådanne data i form af garantier, der skal forhindre misbrug, men fastsætter navnlig også et princip om forbud mod tredjemands lagring heraf (dom af 5.4.2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, præmis 39).
- 57 For så vidt som medlemsstaterne i henhold til artikel 15, stk. 1, i direktiv 2002/58 kan vedtage retsfor skrifter med henblik på at »indskrænke rækkevidden« af de rettigheder og forpligtelser, der omhandles i bl.a. direktivets artikel 5, 6 og 9, såsom dem, der følger af princippet om kommunikationshemmelighed og forbuddet mod lagring af de dermed forbundne data, jf. denne doms præmis 52, fastsætter denne bestemmelse en undtagelse til hovedreglen i bl.a. artikel 5, 6 og 9, og den skal således i overensstemmelse med fast retspraksis fortolkes strengt. En sådan bestemmelse kan således ikke begrunde, at en fravigelse af den principielle pligt til at sikre fortroligheden af elektronisk kommunikation og de dermed forbundne data, og navnlig af det forbud mod at lagre disse data, der er fastsat i dette direktivs artikel 5, bliver hovedreglen, idet rækkevidden af sidstnævnte bestemmelse i så fald i høj grad ville blive udhulet (dom af 5.4.2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, præmis 40 og den deri nævnte retspraksis).
- 58 Hvad angår de formål, som kan begrunde en begrænsning af de rettigheder og forpligtelser, der er fastsat i navnlig artikel 5, 6 og 9 i direktiv 2002/58, har Domstolen allerede fastslået, at opregningen af de formål, der er fastsat i dette direktivs artikel 15, stk. 1, første punktum, er udtømmende, således at en retsfor skrift, der er vedtaget i henhold til denne bestemmelse, faktisk og præcist skal opfylde et af disse formål (dom af 5.4.2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, præmis 41 og den deri nævnte retspraksis).
- 59 Det fremgår endvidere af artikel 15, stk. 1, tredje punktum, i direktiv 2002/58, at de for skrifter, som medlemsstaterne vedtager i henhold til denne bestemmelse, skal være i overensstemmelse med EU-rettens generelle principper, som bl.a. omfatter proportionalitetsprincippet, ligesom de grundlæggende rettigheder, der er sikret ved chartret, skal være overholdt. Domstolen har i denne henseende allerede fastslået, at den pligt, som en medlemsstat i henhold til en national lovgivning har pålagt udbydere af elektroniske kommunikationstjenester, til at lagre trafikdata med henblik på eventuelt at gøre dem tilgængelige for de kompetente nationale myndigheder, ikke blot rejser en række spørgsmål vedrørende overholdelsen af chartrets artikel 7 og 8, men

ligeledes vedrørende artikel 11, der omhandler ytringsfriheden, idet denne frihed udgør et af de væsentlige grundlag for et demokratisk og pluralistisk samfund og er en del af de værdier, som Den Europæiske Union i overensstemmelse med artikel 2 TEU er støttet på (jf. i denne retning dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 42 og 43 og den deri nævnte retspraksis).

- 60 Det skal i denne henseende præciseres, at lagring af trafikdata og lokaliseringsdata i sig selv udgør dels en undtagelse fra det forbud mod at lagre disse data, der er fastsat i artikel 5, stk. 1, i direktiv 2002/58, og som gælder for alle andre end brugerne, dels et indgreb i den grundlæggende ret til respekt for privatlivet og til beskyttelse af personoplysninger, der er sikret ved chartrets artikel 7 og 8, idet det ikke er afgørende, om de pågældende oplysninger vedrørende privatlivet er følsomme, om dette indgreb har medført eventuelle ubehageligheder for de berørte, eller om de lagrede data efterfølgende anvendes (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 44 og den deri nævnte retspraksis).
- 61 Denne konklusion forekommer så meget desto mere begrundet, som trafikdata og lokaliseringsdata kan afsløre oplysninger om en lang række forhold, der vedrører de berørte personers privatliv, herunder følsomme oplysninger, såsom oplysninger om seksuel orientering, politiske anskuelser, samfundsmæssige, filosofiske, religiøse og andre overbevisninger samt oplysninger om helbredstilstand, mens sådanne oplysninger i øvrigt nyder en særlig beskyttelse i EU-retten. De nævnte data vil tilsammen kunne gøre det muligt at drage meget præcise slutninger vedrørende privatlivet for de personer, hvis data er blevet lagret, såsom vaner i dagligdagen, midlertidige eller varige opholdssteder, daglige eller andre rejser, hvilke aktiviteter der udøves, disse personers sociale relationer og de sociale miljøer, de frekventerer. Særligt gør disse data det muligt at lave en profil af de berørte personer, hvilken oplysning, henset til retten til respekt for privatlivet, er lige så følsom som selve indholdet af kommunikationen (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 45 og den deri nævnte retspraksis).
- 62 For det første kan lagring af trafikdata og lokaliseringsdata med henblik på politimæssige formål medføre et indgreb i retten til respekt for kommunikation, der er sikret ved chartrets artikel 7, og have afskrækkende virkninger, der kan afholde brugerne af elektroniske kommunikationsmidler fra at udøve deres ret til ytringsfrihed, der er sikret ved chartrets artikel 11, og disse virkninger er desuden så meget desto mere alvorlige i betragtning af, at der er tale om store mængder af lagrede data af meget forskellig art. For det andet bemærkes, at henset til den store mængde trafikdata og lokaliseringsdata, der løbende kan lagres ved hjælp af en generel og udifferentieret lagringsforanstaltning, og den følsomme karakter af de oplysninger, som disse data kan give adgang til, medfører alene den omstændighed, at udbyderne af elektroniske kommunikationstjenester lagrer de nævnte data, en risiko for misbrug og ulovlig adgang (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 46 og den deri nævnte retspraksis).
- 63 Når dette er sagt, afspejler artikel 15, stk. 1, i direktiv 2002/58, for så vidt som denne bestemmelse giver medlemsstaterne mulighed for at begrænse de rettigheder og forpligtelser, der er henvist til i denne doms præmis 51-54, det forhold, at de rettigheder, der er sikret ved chartrets artikel 7, 8 og 11, ikke er absolutte rettigheder, men skal ses i sammenhæng med deres funktion i samfundet. Som det fremgår af chartrets artikel 52, stk. 1, tillader dette charter nemlig begrænsninger i udøvelsen af disse rettigheder, for så vidt som disse begrænsninger er fastlagt i lovgivningen og respekterer de nævnte rettigheders væsentligste indhold, og for så vidt som disse begrænsninger under iagttagelse af proportionalitetsprincippet er nødvendige og faktisk svarer til mål af almen

interesse, der er anerkendt af Unionen, eller et behov for beskyttelse af andres rettigheder og friheder. I forbindelse med fortolkningen af artikel 15, stk. 1, i direktiv 2002/58 i lyset af chartret skal der således også tages hensyn til betydningen af de rettigheder, der er sikret ved chartrets artikel 3, 4, 6 og 7, og den betydning, som formålene om beskyttelse af den nationale sikkerhed og om bekæmpelse af grov kriminalitet har som følge af, at de bidrager til beskyttelsen af andres rettigheder og friheder (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 48 og den deri nævnte retspraksis).

- 64 Hvad nærmere bestemt angår den effektive bekæmpelse af strafbare handlinger, som navnlig mindreårige og andre sårbare personer er ofre for, skal det således tages i betragtning, at der i medfør af chartrets artikel 7 kan påhvile de offentlige myndigheder positive forpligtelser til at vedtage retlige foranstaltninger, der har til formål at beskytte privatlivet og familielivet. Sådanne forpligtelser kan ligeledes følge af den nævnte artikel 7 med hensyn til den beskyttelse, der gælder for en persons hjem og kommunikation, af artikel 3 og 4 med hensyn til beskyttelsen af en persons fysiske og psykiske integritet og af forbuddet mod tortur og umenneskelig og nedværdigende behandling (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 49 og den deri nævnte retspraksis).
- 65 Som følge af disse forskellige positive forpligtelser er det derfor nødvendigt, at der foretages en afvejning mellem de omhandlede forskellige legitime interesser og rettigheder, og at der indføres en retlig ramme, der gør det muligt at foretage denne afvejning (jf. i denne retning dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 50 og den deri nævnte retspraksis).
- 66 I denne forbindelse følger det af selve ordlyden af artikel 15, stk. 1, første punktum, i direktiv 2002/58, at medlemsstaterne kan vedtage en forskrift, der fraviger det fortrolighedsprincip, der er nævnt i denne doms præmis 52, når en sådan forskrift er »nødvendig, passende og forholdsmæssig i et demokratisk samfund«, idet det i 11. betragtning til dette direktiv i denne henseende er anført, at en forskrift af denne art skal stå i »åbenbart« rimeligt forhold til det mål, der forfølges.
- 67 Det skal i denne henseende bemærkes, at det af Domstolens faste praksis fremgår, at beskyttelsen af den grundlæggende ret til respekt for privatlivet kræver, at undtagelserne til og begrænsningerne af beskyttelsen af personoplysninger holdes inden for det strengt nødvendige. Desuden kan et mål af almen interesse ikke forfølges uden hensyntagen til den omstændighed, at dette mål skal forenes med de grundlæggende rettigheder, der er berørt af foranstaltningen, ved at foretage en rimelig afvejning mellem målet af almen interesse og de pågældende rettigheder (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 52 og den deri nævnte retspraksis).
- 68 Det fremgår nærmere bestemt af Domstolens praksis, at medlemsstaternes mulighed for at begrunde en begrænsning af de rettigheder og forpligtelser, der navnlig er fastsat i artikel 5, 6 og 9 i direktiv 2002/58, skal vurderes ved at bedømme alvoren af det indgreb, som en sådan begrænsning indebærer, og ved at kontrollere, at betydningen af det mål af almen interesse, der forfølges med denne begrænsning, står i forhold til denne alvor (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 53 og den deri nævnte retspraksis).
- 69 For at opfylde kravet om proportionalitet skal en national lovgivning fastsætte klare og præcise regler, der regulerer rækkevidden og anvendelsen af den pågældende foranstaltning, og som opstiller en række mindstekrav, således at de personer, hvis personoplysninger er berørt, råder over tilstrækkelige garantier, der gør det muligt effektivt at beskytte disse oplysninger mod

risikoen for misbrug. Denne lovgivning skal være retligt bindende i national ret og navnlig angive, under hvilke omstændigheder og på hvilke betingelser der kan vedtages en foranstaltning om behandling af sådanne oplysninger, hvorved det sikres, at indgrebet begrænses til det strengt nødvendige. Nødvendigheden af at råde over sådanne garantier er så meget desto større, når personoplysningerne er undergivet en automatiseret behandling, navnlig når der eksisterer en betydelig risiko for ulovlig adgang til disse oplysninger. Disse betragtninger gør sig især gældende, når der er tale om beskyttelse af den særlige kategori af personoplysninger, som følsomme oplysninger udgør (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 54 og den deri nævnte retspraksis).

- 70 En lovgivning, der foreskriver lagring af personoplysninger, skal således altid opfylde objektive kriterier, som fastlægger et forhold mellem de oplysninger, der skal lagres, og det forfulgte mål (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 55 og den deri nævnte retspraksis).
- 71 Hvad angår de mål af almen interesse, der kan begrunde vedtagelse af en forskrift i henhold til artikel 15, stk. 1, i direktiv 2002/58, fremgår det af Domstolens praksis, og navnlig af dom af 6. oktober 2020, *La Quadrature du Net m.fl.* (C-511/18, C-512/18 og C-520/18, EU:C:2020:791), at der i overensstemmelse med proportionalitetsprincippet er et hierarki mellem disse mål, som er bestemt af deres respektive betydning, og at betydningen af det mål, der forfølges med en sådan forskrift, skal stå i forhold til alvoren af det indgreb, som den medfører (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 56).
- 72 Hvad angår beskyttelsen af den nationale sikkerhed, som overstiger de øvrige mål, der er omhandlet i artikel 15, stk. 1, i direktiv 2002/58, har Domstolen fastslået, at denne bestemmelse, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, ikke er til hinder for retsfor skrifter, der med henblik på beskyttelse af den nationale sikkerhed gør det muligt at pålægge udbydere af elektroniske kommunikationstjenester et påbud om at foretage generel og udifferentieret lagring af trafikdata og lokaliseringsdata i de situationer, hvor den pågældende medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig, når den afgørelse, der fastsætter dette påbud, kan gøres til genstand for en effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, med henblik på at kontrollere, om en af disse situationer foreligger, samt om de betingelser og garantier, der skal være fastsat, er overholdt, og når det nævnte påbud kun kan udstedes for en periode, der er tidsmæssigt begrænset til det strengt nødvendige, men som kan forlænges i tilfælde af, at denne trussel består (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 58 og den deri nævnte retspraksis).
- 73 Hvad angår formålet om forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger har Domstolen fastslået, at det i overensstemmelse med proportionalitetsprincippet kun er bekæmpelsen af grov kriminalitet og forebyggelsen af alvorlige trusler mod den offentlige sikkerhed, der kan begrunde alvorlige indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, såsom de indgreb, som lagring af trafikdata og lokaliseringsdata indebærer. Det er således kun de indgreb i de nævnte grundlæggende rettigheder, der ikke er alvorlige, som kan begrundes i formålet om forebyggelse, efterforskning, afsløring og retsforfølgning af strafbare handlinger i almindelighed (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 59 og den deri nævnte retspraksis).

74 Med hensyn til formålet om bekæmpelse af grov kriminalitet har Domstolen fastslået, at en national lovgivning, der med henblik herpå foreskriver generel og udifferentieret lagring af trafikdata og lokaliseringsdata, overskrider det strengt nødvendige og ikke kan anses for at være begrundet i et demokratisk samfund. Henset til den følsomme karakter af de oplysninger, som trafikdata og lokaliseringsdata kan give adgang til, er det nemlig af afgørende betydning for retten til respekt for privatlivet, at disse data behandles med fortrolighed. Når der henses til dels de afskrækkende virkninger for udøvelsen af de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 11, og som er nævnt i denne doms præmis 62, som lagringen af disse data kan have, dels alvoren af det indgreb, som en sådan lagring indebærer, er det i et demokratisk samfund således væsentligt, at dette indgreb, sådan som det er tilfældet for det system, der er indført ved direktiv 2002/58, udgør undtagelsen og ikke reglen, og at disse data ikke kan gøres til genstand for en systematisk og løbende lagring. Denne konklusion gælder selv med hensyn til formålene om bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed samt den betydning, som disse formål skal tillægges (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 65 og den deri nævnte retspraksis).

75 Til gengæld har Domstolen præciseret, at artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, ikke er til hinder for retsfor skrifter, der med henblik på bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed foreskriver

- målrettet lagring af de trafikdata og lokaliseringsdata, som på grundlag af objektive og ikke-diskriminerende forhold er afgrænset ud fra kategorier af berørte personer eller ved hjælp af et geografisk kriterium, i en periode, der er tidsmæssigt begrænset til det strengt nødvendige, men som kan forlænges
- generel og udifferentieret lagring af de IP-adresser, der er tildelt kilden til en forbindelse, i en periode, der er tidsmæssigt begrænset til det strengt nødvendige
- generel og udifferentieret lagring af de data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, og
- mulighed for, ved en afgørelse fra den kompetente myndighed, som er underlagt en effektiv domstolsprøvelse, at pålægge udbydere af elektroniske kommunikationstjenester et påbud om i en begrænset periode at foretage hurtig lagring (*quick freeze*) af de trafikdata og lokaliseringsdata, som disse tjenesteudbydere råder over,

for så vidt som disse foranstaltninger ved klare og præcise regler sikrer, at lagringen af de omhandlede data er underlagt overholdelsen af de dermed forbundne materielle og proceduremæssige betingelser, og at de berørte personer råder over effektive garantier mod risikoen for misbrug (dom af 6.10.2020, *La Quadrature du Net m.fl.*, C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 168, og af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 67).

En forskrift, der pålægger generel og udifferentieret lagring af størstedelen af trafik- og lokaliseringsdata i flere uger

76 Det er i lyset af disse principielle betragtninger, at der skal foretages en undersøgelse af de kendetegn ved den i hovedsagerne omhandlede nationale lovgivning, som den forelæggende ret har fremhævet.

- 77 For det første fremgår det med hensyn til omfanget af de lagrede data af forelæggelsesafgørelsen, at som led i udbuddet af telefontjenester omfatter den pligt til lagring, der er fastsat ved denne lovgivning, navnlig de data, der er nødvendige for at identificere kilden til en kommunikation og bestemmelsesstedet for denne eller – i tilfælde af kommunikation via sms-, multimedie- eller lignende beskeder – tidspunktet for afsendelsen eller modtagelsen af beskeden samt ved mobilt brug betegnelserne for de radioceller, som blev benyttet af den forbindelse, der ringer op, og den forbindelse, der ringes til, ved forbindelsens begyndelse. I forbindelse med levering af internetadgangstjenester vedrører forpligtelsen til lagring bl.a. den IP-adresse, som abonnenten er blevet tildelt, dato og klokkeslæt for internetbenyttelsens begyndelse og ophør under den tildelte IP-adresse og, i forbindelse med mobilt brug, betegnelsen for de radioceller, der blev anvendt ved begyndelsen af internetforbindelsen. Data, der gør det muligt at finde den geografiske placering og retningerne for den maksimale stråling fra de antenner, som betjener den pågældende radiocelle, lagres ligeledes.
- 78 Selv om den i hovedsagerne omhandlede nationale lovgivning udelukker kommunikationens indhold og data vedrørende de besøgte internetsider og kun pålægger lagring af mobilidentiteten ved kommunikationens begyndelse, skal det bemærkes, at det samme i det væsentlige gjorde sig gældende for de nationale lovgivninger til gennemførelse af direktiv 2006/24, som var omhandlet i de sager, der gav anledning til dom af 6. oktober 2020, *La Quadrature du Net m.fl.* (C-511/18, C-512/18 og C-520/18, EU:C:2020:791). På trods af disse begrænsninger fastslog Domstolen i denne dom, at de kategorier af data, der lagres i henhold til nævnte direktiv og disse nationale lovgivninger, kunne gøre det muligt at drage præcise slutninger vedrørende privatlivet for de berørte personer, såsom vaner i dagligdagen, midlertidige eller varige opholdssteder, daglige eller andre rejser, hvilke aktiviteter der udøves, disse personers sociale relationer og de sociale miljøer, de frekventerer, og navnlig ved at give midler til at udarbejde en profil af disse personer.
- 79 Det skal endvidere fastslås, at selv om den i hovedsagerne omhandlede lovgivning ikke omfatter data vedrørende besøgte internetsider, foreskriver den ikke desto mindre lagring af IP-adresser. Eftersom disse IP-adresser kan anvendes til bl.a. at foretage en udtømmende sporing af en internetbrugers søgemønstre og dermed af den pågældendes onlineaktiviteter, gør disse oplysninger det muligt at skabe en detaljeret profil af denne internetbruger. Den lagring og analyse af de nævnte IP-adresser, som en sådan sporing kræver, udgør således alvorlige indgreb i internetbrugerens grundlæggende rettigheder, som er sikrede ved chartrets artikel 7 og 8 (jf. i denne retning dom af 6.10.2020, *La Quadrature du Net m.fl.*, C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 153).
- 80 Som SpaceNet har anført i sine skriftlige indlæg, udgør data vedrørende e-mailtjenester, selv om de ikke er omfattet af den pligt til lagring, der er fastsat i den i hovedsagerne omhandlede lovgivning, kun en ubetydelig del af de pågældende data.
- 81 Som generaladvokaten i det væsentlige har anført i punkt 60 i forslaget til afgørelse, gælder den pligt til lagring, der er fastsat i den i hovedsagerne omhandlede nationale lovgivning, således for en meget bred vifte af trafikdata og lokaliseringsdata, som i det væsentlige svarer til de data, som har ført til den retspraksis, der er nævnt i denne doms præmis 78.
- 82 Som svar på et spørgsmål stillet i retsmødet har den tyske regering desuden præciseret, at alene 1 300 enheder var registreret på listen over personer, myndigheder eller organisationer af social eller religiøs karakter, hvis data vedrørende elektronisk kommunikation ikke må lagres i henhold til TKG's § 99, stk. 2, og § 113b, stk. 6, hvilket tydeligvis udgør en begrænset andel af alle de bru-

gere af telekommunikationstjenester i Tyskland, hvis data henhører under den pligt til lagring, der er fastsat i den i hovedsagerne omhandlede nationale lovgivning. Således lagres bl.a. data fra brugere, der er undergivet tavshedspligt, såsom advokater, læger og journalister.

- 83 Det fremgår således af forelæggelsesafgørelsen, at den lagring af trafikdata og lokaliseringsdata, der foreskrives ved denne nationale lovgivning, vedrører næsten samtlige de personer, som befolkningen udgøres af, uden at de – end ikke indirekte – befinder sig i en situation, der vil kunne give anledning til strafferetlig forfølgning. På samme måde pålægger denne lovgivning uden anledning en generel samt personligt, tidsmæssigt og geografisk udifferentieret lagring af størstedelen af trafikdata og lokaliseringsdata, hvoraf omfanget i det væsentlige svarer til omfanget af de data, som blev lagret i de sager, der gav anledning til den retspraksis, der er nævnt i denne doms præmis 78.
- 84 Henset til den retspraksis, der er nævnt i denne doms præmis 75, kan en pligt til lagring af data som den i hovedsagerne omhandlede i modsætning til, hvad den tyske regering har gjort gældende, således ikke anses for at være en målrettet lagring af data.
- 85 For det andet følger det hvad angår perioden for lagringen af data af artikel 15, stk. 1, andet punktum, i direktiv 2002/58, at den periode for lagringen, som er fastsat ved nationale forskrifter, der pålægger en pligt til generel og udifferentieret lagring, ganske vist er én blandt flere relevante faktorer med henblik på at afgøre, om EU-retten er til hinder for en sådan forskrift, idet det i nævnte punktum kræves, at denne periode skal være »begrænset«.
- 86 I det foreliggende tilfælde er det korrekt, at disse perioder, som i henhold til TKG's § 113b, stk. 1, udgør fire uger for lokaliseringsdata og ti uger for andre data, er væsentligt kortere end de perioder, der var fastsat i de nationale lovgivninger om pålæggelse af en pligt til generel og udifferentieret lagring, som Domstolen undersøgte i dom af 21. december 2016, *Tele2 Sverige og Watson m.fl.* (C-203/15 og C-698/15, EU:C:2016:970), af 6. oktober 2020, *La Quadrature du Net m.fl.* (C-511/18, C-512/18 og C-520/18, EU:C:2020:791), og af 5. april 2022, *Commissioner of An Garda Síochána m.fl.* (C-140/20, EU:C:2022:258).
- 87 Som det fremgår af den retspraksis, der er nævnt i denne doms præmis 61, følger alvoren af indgrebet, navnlig i betragtning af dataenes antal og forskelligartethed, af risikoen for, at de lagrede data samlet set gør det muligt at drage meget præcise slutninger vedrørende privatlivet for den eller de personer, hvis data er blevet lagret, og især giver midler til at udarbejde en profil for den eller de berørte personer, som, henset til respekten for privatlivet, er en lige så følsom oplysning som selve indholdet af kommunikationen.
- 88 Dermed er lagringen af trafikdata eller lokaliseringsdata, der kan tilvejebringe oplysninger om den kommunikation, som en bruger har foretaget ved hjælp af et elektronisk kommunikationsmiddel, eller om placeringen af det terminaludstyr, som den pågældende gør brug af, imidlertid under alle omstændigheder af alvorlig karakter, uanset varigheden af perioden for lagringen og mængden eller arten af de lagrede data, når denne samling af data kan gøre det muligt at drage meget præcise slutninger vedrørende privatlivet for den eller de berørte personer (jf. med hensyn til adgangen til sådanne data dom af 2.3.2021, *Prokuratuur* (Betingelser for adgang til oplysninger om elektronisk kommunikation), C-746/18, EU:C:2021:152, præmis 39).
- 89 I denne henseende kan selv lagringen af en begrænset mængde trafikdata eller lokaliseringsdata eller lagringen af data i en kort periode gøre det muligt at tilvejebringe præcise oplysninger om privatlivet for en bruger af et elektronisk kommunikationsmiddel. Hvor stor mængden af

tilgængelige oplysninger er, og hvilke præcise oplysninger om den berørte persons privatliv der kan udledes heraf, kan desuden først vurderes, efter at de nævnte data er blevet gennemgået. Det indgreb, der følger af lagringen af de nævnte data, finder nødvendigvis sted, før de data og de oplysninger, der kan udledes heraf, kan gennemgås. Vurderingen af alvoren af det indgreb, som lagringen indebærer, skal således nødvendigvis foretages på grundlag af den risiko, der for de berørte personers privatliv generelt er forbundet med den kategori af data, der er lagret, uden at det i øvrigt er væsentligt at vide, om de oplysninger om privatlivet, der kan udledes heraf, eventuelt er følsomme i det konkrete tilfælde (jf. i denne retning dom af 2.3.2021, Prokuratuur (Betingelser for adgang til oplysninger om elektronisk kommunikation), C-746/18, EU:C:2021:152, præmis 40).

- 90 I det foreliggende tilfælde kan samling af trafikdata og lokaliseringsdata, som lagres i henholdsvis ti og fire uger, sådan som det fremgår af denne doms præmis 77, og som det er blevet bekræftet i retsmødet, gøre det muligt at drage meget præcise slutninger vedrørende privatlivet for de personer, hvis data lagres, såsom vaner i dagligdagen, midlertidige eller varige opholdssteder, daglige eller andre rejser, hvilke aktiviteter der udøves, disse personers sociale relationer og de sociale miljøer, de frekventerer, og navnlig at udarbejde en profil af disse personer.
- 91 For det tredje skal det hvad angår de garantier, som er fastsat i den i hovedsagerne omhandlede nationale lovgivning, der tilsigter at beskytte de lagrede data mod risikoen for misbrug og mod enhver form for ulovlig adgang, fremhæves, at lagring af sådanne data og adgang hertil, således som det fremgår af den retspraksis, der er nævnt i denne doms præmis 60, udgør særskilte indgreb i de grundlæggende rettigheder, som beskyttes af chartrets artikel 7 og 11, og kræver særskilte begrundelser i henhold til chartrets artikel 52, stk. 1. Heraf følger, at en national lovgivning, der sikrer, at de betingelser, der følger af den retspraksis, hvori bestemmelserne i direktiv 2002/58 om adgang til lagrede data er blevet fortolket, overholdes fuldt ud, i sagens natur hverken kan begrænse eller endsige afhjælpe det alvorlige indgreb, der ville følge af en generel lagring af sådanne data som fastsat i denne nationale lovgivning, i de rettigheder, der er sikret i dette direktivs artikel 5 og 6 og ved de grundlæggende rettigheder, som konkretiseres i disse artikler (dom af 5.4.2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, præmis 47).
- 92 For det fjerde og endelig har Domstolen hvad angår Europa-Kommissionens argument om, at særlig grov kriminalitet kan sidestilles med en trussel mod den nationale sikkerhed, allerede fastslået, at formålet om beskyttelse af den nationale sikkerhed svarer til den primære interesse i at beskytte statens væsentlige funktioner og grundlæggende samfundsinteresser gennem forebyggelse og bekæmpelse af aktiviteter, der alvorligt kan destabilisere et lands grundlæggende forfatningsmæssige, politiske, økonomiske eller sociale strukturer og navnlig direkte true samfundet, befolkningen eller staten som sådan, såsom bl.a. terrorvirksomhed (dom af 5.4.2022, Commissioner of An Garda Síochána m.fl., C-140/20, EU:C:2022:258, præmis 61 og den deri nævnte retspraksis).
- 93 Til forskel fra selv særlig grov kriminalitet skal en trussel mod den nationale sikkerhed være reel og aktuel eller i det mindste forudsigelig, hvilket forudsætter, at der foreligger tilstrækkeligt konkrete omstændigheder til at kunne begrunde en forskrift om generel og udifferentieret lagring af trafikdata og lokaliseringsdata i et begrænset tidsrum. En sådan trussel adskiller sig derfor på grund af sin art, sin alvorlige karakter og den særlige karakter af de omstændigheder, som udgør den, fra den generelle og vedvarende risiko i form af spændinger eller forstyrrelser, selv

alvorlige, for den offentlige sikkerhed og alvorlige strafbare handlinger (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 62 og den deri nævnte retspraksis).

- 94 Selv særlig grov kriminalitet kan således ikke sidestilles med en trussel mod den nationale sikkerhed. En sådan sidestilling ville nemlig svare til at indføre en mellemkategori mellem den nationale sikkerhed og den offentlige sikkerhed og anvende de krav, der gælder for førstnævnte, på sidstnævnte (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 63).

Forskrifter, der foreskriver en målrettet lagring, hurtig lagring eller lagring af IP-adresser

- 95 Flere regeringer, herunder den franske, har fremhævet, at alene en generel og udifferentieret lagring gør det muligt effektivt at gennemføre de formål, der er omhandlet af forskrifterne om lagring, idet den tyske regering i det væsentlige har præciseret, at en sådan konklusion ikke svækkes af den omstændighed, at medlemsstaterne kan anvende de forskrifter om målrettet og hurtig lagring, der er nævnt i denne doms præmis 75.
- 96 I denne henseende bemærkes for det første, at effektiviteten af strafforfølgningen generelt ikke afhænger af et enkelt efterforskningsredskab, men af alle de efterforskningsredskaber, som de kompetente nationale myndigheder har til rådighed i efterforskningsøjemed (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 69).
- 97 For det andet kan medlemsstaterne i henhold til artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, som fortolket i den retspraksis, der er nævnt i denne doms præmis 75, med henblik på bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed vedtage ikke alene forskrifter om målrettet lagring og hurtig lagring, men også forskrifter om generel og udifferentieret lagring af dels de data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, dels de IP-adresser, der er tildelt kilden til en forbindelse (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 70).
- 98 I denne henseende er det ubestridt, at lagring af de data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, kan bidrage til bekæmpelsen af grov kriminalitet, for så vidt som disse data gør det muligt at identificere de personer, der har anvendt sådanne midler i forbindelse med planlægningen eller udførelsen af en handling, der sorterer under grov kriminalitet (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 71).
- 99 Direktiv 2002/58 er dog ikke til hinder for generel lagring af identitetsdata med henblik på bekæmpelse af kriminalitet generelt. På denne baggrund skal det præciseres, at hverken dette direktiv eller nogen anden EU-retsakt er til hinder for en national lovgivning, der har til formål at bekæmpe grov kriminalitet, og hvorefter erhvervelse af et elektronisk kommunikationsmiddel, såsom et forudbetalt SIM-kort, betinges af en kontrol af officielle dokumenter, der fastslår køberens identitet, og af sælgerens registrering af oplysningerne herom, idet sælgeren har pligt til i givet fald at give de kompetente nationale myndigheder adgang til disse oplysninger (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 72).

- 100 Desuden bemærkes, at generel lagring af IP-adresserne på kilden til forbindelsen udgør et alvorligt indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, eftersom disse IP-adresser kan gøre det muligt at drage præcise slutninger om privatlivet for brugeren af det pågældende elektroniske kommunikationsmiddel og have en afskrækkende virkning på udøvelsen af ytringsfriheden som sikret ved chartrets artikel 11. Hvad angår en sådan lagring har Domstolen imidlertid fastslået, at der med henblik på at foretage den nødvendige afvejning af de omhandlede legitime rettigheder og interesser, som kræves i henhold til den retspraksis, der er nævnt i denne doms præmis 65-68, skal tages hensyn til den omstændighed, at IP-adressen i tilfælde, hvor en lovovertrædelse er begået online, og især i tilfælde af erhvervelse, udbredelse, transmission eller tilrådighedsstillelse online af børnepornografi som omhandlet i artikel 2, litra c), i Europa-Parlamentets og Rådets direktiv 2011/93/EU af 13. december 2011 om bekæmpelse af seksuelt misbrug og seksuel udnyttelse af børn og børnepornografi og om erstatning af Rådets rammeafgørelse 2004/68/RIA (EUT 2011, L 335, s. 1), kan udgøre det eneste efterforskningsmiddel, der kan gøre det muligt at identificere den person, som denne adresse var tildelt på det tidspunkt, hvor den pågældende overtrædelse blev begået (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 73).
- 101 På denne baggrund, og selv om det er korrekt, at en retsforordning, der foreskriver lagring af IP-adresser på alle de fysiske personer, der ejer terminaludstyr, hvorfra det er muligt at tilgå internettet, vil omfatte personer, der ikke umiddelbart har en forbindelse som omhandlet i den retspraksis, der er nævnt i denne doms præmis 70, til de forfulgte formål, og at internetbrugere i overensstemmelse med, hvad der er fastslået i denne doms præmis 54, har ret til i henhold til chartrets artikel 7 og 8 at forvente, at deres identitet principielt ikke afsløres, forekommer en retsforordning, der foreskriver generel og udifferentieret lagring af de IP-adresser, der er tildelt kilden til en forbindelse, principielt ikke at være i strid med artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, under forudsætning af, at denne mulighed er betinget af en streng overholdelse af de materielle og proceduremæssige betingelser, der skal gælde for brugen af disse data (dom af 6.10.2020, *La Quadrature du Net m.fl.*, C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 155).
- 102 Henset til den alvorlige karakter af det indgreb i de grundlæggende rettigheder, der er sikrede ved chartrets artikel 7 og 8, som denne lagring indebærer, er det kun bekæmpelsen af grov kriminalitet og forebyggelsen af alvorlige trusler mod den offentlige sikkerhed, der i lighed med beskyttelsen af den nationale sikkerhed kan begrunde dette indgreb. Lagringsperioden må endvidere ikke overstige, hvad der er strengt nødvendigt for at nå det forfulgte formål. Endelig skal en forordning af denne art indeholde strenge betingelser og garantier for så vidt angår brugen af disse data, navnlig ved hjælp af sporing, med hensyn til de kommunikationer og de aktiviteter, som de berørte personer foretager online (dom af 6.10.2020, *La Quadrature du Net m.fl.*, C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 156).
- 103 I modsætning til, hvad den forelæggende ret har fremhævet, er der således ikke uoverensstemmelse mellem præmis 155 og 168 i dom af 6. oktober 2020, *La Quadrature du Net m.fl.* (C-511/18, C-512/18 og C-520/18, EU:C:2020:791). Som generaladvokaten i det væsentlige har anført i punkt 81 og 82 i forslaget til afgørelse, fremgår det nemlig klart af præmis 155, sammenholdt med denne doms præmis 156 og 168, at det kun er bekæmpelsen af grov kriminalitet og forebyggelsen af alvorlige trusler mod den offentlige sikkerhed, der i lighed med beskyttelsen af den nationale sikkerhed kan begrunde generel lagring af de IP-adresser, der er tildelt kilden til en forbindelse, uanset om de berørte personer kan have en endog indirekte forbindelse med de forfulgte mål.

- 104 For det tredje afspejler visse af de betragtninger, som medlemsstaterne har anført vedrørende retsfor skrifter om målrettet lagring og hurtig lagring af trafikdata og lokaliseringsdata, en mere snæver forståelse af rækkevidden af disse forskrifter end den, som er lagt til grund i den retspraksis, der er nævnt i denne doms præmis 75. Selv om disse lagringsforanstaltninger i overensstemmelse med det anførte i denne doms præmis 57 skal have undtagelsens karakter i det system, der er indført ved direktiv 2002/58, gør dette direktiv, sammenholdt med de grundlæggende rettigheder, der er sikret ved chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, nemlig ikke muligheden for at udstede et påbud om målrettet lagring betinget af, at det på forhånd er kendt, hvor en groft kriminell handling eventuelt vil blive begået, eller hvem der mistænkes for at være involveret i en sådan handling. Direktivet kræver heller ikke, at et påbud om hurtig lagring begrænses til at omfatte mistænkte, der er identificeret forud for et sådant påbud (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 75).
- 105 Hvad indledningsvis angår den målrettede lagring har Domstolen fastslået, at artikel 15, stk. 1, i direktiv 2002/58 ikke er til hinder for en national lovgivning, der er baseret på objektive forhold, som gør det muligt at fokusere målrettet på de personer, hvis trafikdata og lokaliseringsdata kan afsløre en forbindelse, i det mindste indirekte, til groft kriminelle handlinger, bidrage til bekæmpelse af grov kriminalitet eller forhindre en alvorlig fare for den offentlige sikkerhed eller endog en risiko for den nationale sikkerhed (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 76 og den deri nævnte retspraksis).
- 106 Domstolen har i denne henseende præciseret, at selv om disse objektive forhold kan variere i forhold til de forskrifter, der vedtages med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af grov kriminalitet, kan de således omhandlede personer bl.a. være sådanne, som på forhånd inden for rammerne af de gældende nationale procedurer og på grundlag af objektive og ikke-diskriminerende forhold er blevet identificeret som en trussel mod den pågældende medlemsstats offentlige sikkerhed eller nationale sikkerhed (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 77).
- 107 Medlemsstaterne kan således bl.a. træffe lagringsforanstaltninger vedrørende personer, der i forbindelse med en sådan identifikation er genstand for efterforskning eller andre igangværende overvågningsforanstaltninger eller er opført i det nationale strafferegister med angivelse af en tidligere dom for groft kriminelle handlinger, der kan indebære en høj risiko for gentagelse. Når en sådan identifikation er baseret på objektive og ikke-diskriminerende forhold, der er fastsat i national ret, er målrettet lagring af data om således identificerede personer begrundet (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 78).
- 108 En forskrift om målrettet lagring af trafikdata og lokaliseringsdata kan efter den nationale lovgivers valg og under streng overholdelse af proportionalitetsprincippet ligeledes baseres på et geografisk kriterium, når de kompetente nationale myndigheder på grundlag af objektive og ikke-diskriminerende forhold finder, at der i et eller flere geografiske områder foreligger en situation, der er kendetegnet ved en høj risiko for, at der planlægges eller begås groft kriminelle handlinger. Disse områder kan navnlig være steder, der er kendetegnet ved et højt antal tilfælde af groft kriminelle handlinger, steder, hvor der i særlig grad kan begås groft kriminelle handlinger, såsom steder eller infrastrukturer, der regelmæssigt besøges af et meget stort antal personer, eller strategiske steder, såsom lufthavne, banegårde, havne eller vejafgiftsområder (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 79 og den deri nævnte retspraksis).

- 109 Det skal fremhæves, at de kompetente nationale myndigheder ifølge denne retspraksis i forhold til de områder, der er nævnt i den foregående præmis, kan vedtage en forskrift om målrettet lagring baseret på et geografisk kriterium, såsom bl.a. den gennemsnitlige kriminalitetsrate i et geografisk område, uden at de nødvendigvis råder over konkrete indicier for, at der planlægges eller begås groft kriminelle handlinger i de pågældende områder. For så vidt som en målrettet lagring, der er baseret på et sådant kriterium – afhængigt af, hvilke alvorlige strafbare handlinger der er tale om, og hvilken situation der foreligger i de respektive medlemsstater – både kan berøre steder, der er kendetegnet ved et højt antal tilfælde af groft kriminelle handlinger, og steder, som i særlig grad er udsatte for sådan kriminalitet, kan den principielt heller ikke give anledning til forskelsbehandling, idet kriteriet om gennemsnitsraten for grov kriminalitet ikke i sig selv har nogen forbindelse med potentielt diskriminerende forhold (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 80).
- 110 Endvidere og navnlig gør en forskrift om målrettet lagring rettet mod steder eller infrastrukturer, der regelmæssigt besøges af et meget stort antal personer, eller strategiske steder, såsom lufthavne, banegårde, havne eller vejafgiftsområder, det muligt for de kompetente myndigheder at indsamle trafikdata og navnlig lokaliseringsdata om alle de personer, der på et givet tidspunkt har benyttet et elektronisk kommunikationsmiddel på et af disse steder. En sådan forskrift om målrettet lagring kan således gøre det muligt for de nævnte myndigheder, gennem adgangen til de således lagrede data, at indhente oplysninger om disse personers tilstedeværelse på de steder eller i de geografiske områder, som forskriften omfatter, og om deres bevægelser mellem eller inden for disse, og med henblik på bekæmpelse af grov kriminalitet heraf drage konklusioner om deres tilstedeværelse og aktivitet på disse steder eller i disse geografiske områder på et givet tidspunkt i løbet af lagringsperioden (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 81).
- 111 Det skal endvidere bemærkes, at de geografiske områder, der er omfattet af en sådan målrettet lagring, kan og i givet fald skal tilpasses udviklingen i de forhold, der har begrundet valget af dem, således at der bl.a. kan reageres på udviklingen i bekæmpelsen af grov kriminalitet. Domstolen har nemlig allerede fastslået, at varigheden af de forskrifter om målrettet lagring, der er beskrevet i denne doms præmis 105-110, ikke må overstige, hvad der er strengt nødvendigt i forhold til det forfulgte formål og de omstændigheder, der begrunder dem, dog med forbehold af muligheden for at forlænge forskriften som følge af, at det fortsat er nødvendigt at foretage en sådan lagring (dom af 6.10.2020, *La Quadrature du Net m.fl.*, C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 151, og af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 82).
- 112 Hvad angår muligheden for at fastsætte andre særlige kriterier end personlige eller geografiske kriterier ved iværksættelsen af en målrettet lagring af trafikdata og lokaliseringsdata kan det ikke udelukkes, at andre objektive og ikke-diskriminerende kriterier vil kunne komme på tale for at sikre, at rækkevidden af en målrettet lagring begrænses til det strengt nødvendige, og for at godtgøre en forbindelse, i det mindste indirekte, mellem groft kriminelle handlinger og de personer, hvis data lagres. Når dette er sagt, er det, eftersom artikel 15, stk. 1, i direktiv 2002/58 vedrører retsfor skrifter, der vedtages af medlemsstaterne, disse og ikke Domstolen, der skal fastlægge sådanne kriterier, idet der dog ikke kan blive tale om herigennem at genindføre en generel og udifferentieret lagring af trafikdata og lokaliseringsdata (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 83).

- 113 Som generaladvokaten har anført i punkt 50 i forslaget til afgørelse, kan eventuelle vanskeligheder ved at opstille de præcise tilfælde og betingelser, hvorunder der kan ske en målrettet lagring, under alle omstændigheder ikke begrunde, at medlemsstaterne gør undtagelsen til en regel og foreskriver generel og udifferentieret lagring af trafikdata og lokaliseringsdata (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 84).
- 114 Hvad desuden angår hurtig lagring af de trafikdata og lokaliseringsdata, som behandles og lagres af udbydere af elektroniske kommunikationstjenester på grundlag af artikel 5, 6 og 9 i direktiv 2002/58 eller på grundlag af de retsfor skrifter, der er vedtaget i henhold til dette direktivs artikel 15, stk. 1, skal det bemærkes, at disse data principielt, alt efter omstændighederne, skal slettes eller gøres anonyme efter udløbet af de lovbestemte frister, inden for hvilke disse data skal behandles og lagres i overensstemmelse med de nationale bestemmelser, der gennemfører dette direktiv. Domstolen har ikke desto mindre fastslået, at der under denne behandling og lagring kan opstå situationer, hvori det er nødvendigt at lagre de nævnte data ud over disse frister for at opklare alvorlige strafbare handlinger eller angreb mod den nationale sikkerhed, såvel i den situation, hvor disse strafbare handlinger eller disse angreb allerede har kunnet konstateres, som i den situation, hvor der efter en objektiv undersøgelse af samtlige relevante omstændigheder foreligger rimelig grund til at mistænke, at der er begået sådanne strafbare handlinger eller angreb (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 85).
- 115 I en sådan situation står det, henset til den nødvendige afvejning af de omhandlede legitime rettigheder og interesser, der er nævnt i denne doms præmis 65-68, medlemsstaterne frit for i en lovgivning, der vedtages i henhold til artikel 15, stk. 1, i direktiv 2002/58, at fastsætte muligheden for ved en afgørelse fra den kompetente myndighed, som er underlagt en effektiv domstolsprøvelse, at pålægge udbydere af elektroniske kommunikationstjenester i en begrænset periode at foretage hurtig lagring af de trafikdata og lokaliseringsdata, som de råder over (dom af 6.10.2020, *La Quadrature du Net m.fl.*, C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 163, og af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 86).
- 116 For så vidt som formålet med en sådan hurtig lagring ikke længere svarer til de formål, hvortil dataene oprindeligt blev indsamlet og lagret, og da enhver behandling af data i henhold til chartrets artikel 8, stk. 2, skal opfylde udtrykkeligt angivne formål, skal medlemsstaterne i deres lovgivning præcisere det formål, med henblik på hvilket en hurtig lagring af data kan finde sted. Henset til den alvorlige karakter af det indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, som en sådan lagring kan indebære, er det kun bekæmpelsen af grov kriminalitet og så meget desto mere beskyttelsen af den nationale sikkerhed, der kan begrunde dette indgreb, på den betingelse, at denne foranstaltning og adgangen til de således lagrede data holder sig inden for grænserne af det strengt nødvendige, således som disse er angivet i præmis 164-167 i dom af 6. oktober 2020, *La Quadrature du Net m.fl.* (C-511/18, C-512/18 og C-520/18, EU:C:2020:791) (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 87).
- 117 Domstolen har præciseret, at en lagringsforanstaltning af denne art ikke skal begrænses til data om de personer, der på forhånd er blevet identificeret som en trussel mod den pågældende medlemsstats offentlige sikkerhed eller nationale sikkerhed, eller om de personer, der konkret er mistænkt for at have begået en groft kriminell handling eller et angreb mod den nationale sikkerhed. Under overholdelse af den ramme, der er fastsat ved artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, og under hensyn til

de betragtninger, der er anført i denne doms præmis 70, kan en sådan foranstaltning nemlig ifølge Domstolen, afhængigt af det valg, som den nationale lovgiver træffer, og såfremt den holder sig inden for det strengt nødvendige, udvides til at omfatte de trafikdata og lokaliseringsdata, der vedrører andre personer end dem, der mistænkes for at have planlagt eller begået en alvorlig strafbar handling eller et angreb mod den nationale sikkerhed, for så vidt som disse data på grundlag af objektive og ikke-diskriminerende forhold kan bidrage til at opklare en sådan strafbar handling eller et sådant angreb mod den nationale sikkerhed, såsom oplysninger om offeret for den strafbare handling eller om den pågældendes sociale og arbejdsmæssige omgangskreds (dom af 6.10.2020, *La Quadrature du Net m.fl.*, C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 165, og af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 88).

- 118 En retsforordning kan således tillade, at der pålægges udbydere af elektroniske kommunikationstjenester et påbud om hurtig lagring af trafikdata og lokaliseringsdata om navnlig personer, som et offer, før der foreligger en alvorlig trussel mod den offentlige sikkerhed, eller før der er begået en groft kriminell handling, har været i kontakt med ved hjælp af sine elektroniske kommunikationsmidler (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 89).
- 119 En sådan hurtig lagring kan i henhold til den praksis fra Domstolen, der er nævnt i denne doms præmis 117, og på samme betingelser som de i denne præmis anførte, ligeledes udvides til at omfatte bestemte geografiske områder, såsom de steder, hvor den omhandlede strafbare handling eller det omhandlede angreb mod den nationale sikkerhed blev begået eller planlagt. Det skal præciseres, at en sådan foranstaltning også kan omfatte trafikdata og lokaliseringsdata om det sted, hvor en person, der potentielt er offer for en groft kriminell handling, er forsvundet, på betingelse af, at denne foranstaltning og adgangen til de således lagrede data holder sig inden for grænserne af det strengt nødvendige med henblik på bekæmpelse af grov kriminalitet eller beskyttelse af den nationale sikkerhed, således som disse er angivet i præmis 164-167 i dom af 6. oktober 2020, *La Quadrature du Net m.fl.* (C-511/18, C-512/18 og C-520/18, EU:C:2020:791) (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 90).
- 120 Det skal i øvrigt præciseres, at artikel 15, stk. 1, i direktiv 2002/58 ikke er til hinder for, at de kompetente nationale myndigheder anordner en forordning om hurtig lagring allerede fra det første stadium af efterforskningen vedrørende en alvorlig trussel mod den offentlige sikkerhed eller en eventuel groft kriminell handling, dvs. fra det tidspunkt, hvor myndighederne i henhold til de relevante bestemmelser i national ret kan indlede en sådan efterforskning (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 91).
- 121 Hvad angår de forskellige forskrifter om lagring af trafikdata og lokaliseringsdata, der er nævnt i denne doms præmis 75, skal det præciseres, at disse forskellige forskrifter, efter den nationale lovgivers valg og inden for grænserne af det strengt nødvendige, kan finde anvendelse samtidig. Under disse omstændigheder er artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, som fortolket i retspraksis i henhold til dom af 6. oktober 2020, *La Quadrature du Net m.fl.* (C-511/18, C-512/18 og C-520/18, EU:C:2020:791), ikke til hinder for en kombination af disse forskrifter (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 92).

- 122 For det fjerde og sidste skal det fremhæves, at kravet om, at de forskrifter, der vedtages i henhold til artikel 15, stk. 1, i direktiv 2002/58, skal være forholdsmæssige, ifølge Domstolens faste praksis, således som denne er sammenfattet i dom af 6. oktober 2020, *La Quadrature du Net m.fl.* (C-511/18, C-512/18 og C-520/18, EU:C:2020:791), indebærer, at ikke alene kravene om egnethed og nødvendighed, men også det krav, der vedrører disse forskrifters forholdsmæssighed i forhold til det forfulgte formål, skal være overholdt (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 93).
- 123 Det skal i denne forbindelse bemærkes, at Domstolen i præmis 51 i dom af 8. april 2014, *Digital Rights Ireland m.fl.* (C-293/12 og C-594/12, EU:C:2014:238), fastslog, at selv om bekæmpelse af grov kriminalitet er af afgørende betydning for at sikre den offentlige sikkerhed, og selv om effektiviteten heraf i vidt omfang kan være afhængig af anvendelse af moderne efterforskningsteknikker, kan et sådant mål af almen interesse imidlertid ikke, hvor grundlæggende det end er, i sig selv begrunde, at en forskrift om generel og udifferentieret lagring af trafikdata og lokaliseringsdata som den, der blev indført ved direktiv 2006/24, anses for nødvendig (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 94).
- 124 I samme retning præciserede Domstolen i præmis 145 i dom af 6. oktober 2020, *La Quadrature du Net m.fl.* (C-511/18, C-512/18 og C-520/18, EU:C:2020:791), at selv de positive forpligtelser for medlemsstaterne, som alt efter omstændighederne kan følge af chartrets artikel 3, 4 og 7, og som, således som det er anført i denne doms præmis 64, vedrører indførelsen af regler, der gør det muligt effektivt at bekæmpe strafbare handlinger, ikke kan begrunde indgreb, der er så alvorlige som de indgreb, som en lovgivning, der foreskriver lagring af trafikdata og lokaliseringsdata, indebærer i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, og som berører praktisk talt hele befolkningen, uden at de berørte personers data kan afsløre en forbindelse, endog ikke indirekte, til det forfulgte formål (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 95).
- 125 I øvrigt kan Menneskerettighedsdomstolens domme af 25. maj 2021, *Big Brother Watch m.fl. mod Det Forenede Kongerige* (CE:ECHR:2021:0525JUD 005817013) og *Centrum för Rättvisa mod Sverige* (CE:ECHR:2021:0525JUD 003525208), som visse regeringer har påberåbt sig i retsmødet for at gøre gældende, at EMRK ikke er til hinder for nationale bestemmelser, der i det væsentlige foreskriver generel og udifferentieret lagring af trafikdata og lokaliseringsdata, ikke rejse tvivl om den fortolkning af artikel 15, stk. 1, i direktiv 2002/58, der følger af de ovenfor anførte betragtninger. Disse domme omhandlede nemlig masseopfangelse af data vedrørende international kommunikation. Som Kommissionen har anført i retsmødet, traf Den Europæiske Menneskerettighedsdomstol i de nævnte domme således ikke afgørelse om, hvorvidt en generel og udifferentieret lagring af trafikdata og lokaliseringsdata på det nationale område er forenelig med EMRK, eller om dette er tilfældet for en vidtrækkende opfangelse af disse data med henblik på forebyggelse, afsløring og efterforskning af alvorlige strafbare handlinger. Det skal under alle omstændigheder bemærkes, at chartrets artikel 52, stk. 3, har til formål at sikre den nødvendige sammenhæng mellem de i chartret indeholdte rettigheder og de tilsvarende ved EMRK sikrede rettigheder, uden at dette berører EU-retten og Den Europæiske Unions Domstols autonomi, hvorfor der med henblik på fortolkningen af chartret alene skal tages hensyn til de tilsvarende rettigheder i EMRK som en tærskel for minimumsbeskyttelse (dom af 17.12.2020, *Centraal Israëlitisch Consistorie van België m.fl.*, C-336/19, EU:C:2020:1031, præmis 56).

Adgangen til data, som er blevet lagret generelt og udifferentieret

- 126 I retsmødet har den danske regering anført, at de kompetente nationale myndigheder med henblik på bekæmpelse af grov kriminalitet bør kunne få adgang til trafikdata og lokaliseringsdata, i overensstemmelse med retspraksis i henhold til dom af 6. oktober 2020, *La Quadrature du Net m.fl.* (C-511/18, C-512/18 og C-520/18, EU:C:2020:791, præmis 135-139), for at håndtere en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig.
- 127 Indledningsvis bemærkes, at såfremt der med henblik på bekæmpelse af grov kriminalitet gives adgang til trafikdata og lokaliseringsdata, som er blevet lagret generelt og udifferentieret, vil denne adgang komme til at afhænge af omstændigheder, som er dette formål uvedkommende, afhængigt af, om der i den pågældende medlemsstat foreligger eller ikke foreligger en alvorlig trussel mod den nationale sikkerhed som omhandlet i den foregående præmis, selv om der med hensyn til det ene formål at bekæmpe grov kriminalitet, som skal begrunde lagring og adgang til disse data, ikke er noget, der kan begrunde en forskellig behandling, især mellem medlemsstaterne (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 97).
- 128 Som Domstolen allerede har fastslået, kan adgang til de trafikdata og lokaliseringsdata, som udbyderne af elektroniske kommunikationstjenester lagrer som følge af en forskrift vedtaget i henhold til artikel 15, stk. 1, i direktiv 2002/58, der skal gennemføres under fuld overholdelse af de betingelser, der følger af den retspraksis, hvori dette direktiv er blevet fortolket, i princippet kun begrundes i det mål af almen interesse, med henblik på hvilket disse udbydere er blevet pålagt at foretage denne lagring. Anderledes forholder det sig kun, såfremt det formål, der forfølges med adgangen, er vigtigere end det, der har begrundet lagringen (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 98).
- 129 Den danske regerings argumentation vedrører imidlertid en situation, hvor formålet med den pågældende anmodning om adgang, nemlig bekæmpelse af grov kriminalitet, har mindre betydning i hierarkiet af mål af almen interesse end det, der har begrundet lagringen, nemlig beskyttelse af den nationale sikkerhed. Såfremt der i en sådan situation blev givet adgang til de lagrede data, ville det være i strid med dette hierarki af mål af almen interesse, som er nævnt i den foregående præmis og i denne doms præmis 68, 71, 72 og 73 (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 99).
- 130 Endvidere og navnlig kan trafikdata og lokaliseringsdata i overensstemmelse med den retspraksis, der er nævnt i denne doms præmis 74, ikke gøres til genstand for en generel og udifferentieret lagring med henblik på bekæmpelse af grov kriminalitet, og adgang til disse data kan derfor ikke begrundes i dette formål. Når disse data undtagelsesvis er blevet lagret generelt og udifferentieret med henblik på at beskytte den nationale sikkerhed mod en trussel, som må anses for at være reel og aktuel eller forudsigelig, under de betingelser, som er omhandlet i denne doms præmis 71, kan de kompetente nationale myndigheder på området for strafferetlig efterforskning ikke få adgang til disse data i forbindelse med strafferetlig forfølgning, idet det forbud mod at foretage en sådan lagring med henblik på bekæmpelse af grov kriminalitet, der er omtalt i nævnte præmis 74, herved vil blive berøvet sin effektive virkning (dom af 5.4.2022, *Commissioner of An Garda Síochána m.fl.*, C-140/20, EU:C:2022:258, præmis 100).

131 Henset til samtlige ovenstående betragtninger skal det præjudicielle spørgsmål besvares med, at artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal fortolkes således, at denne bestemmelse er til hinder for nationale retsfor skrifter, der med henblik på bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed i forebyggende øjemed foreskriver generel og udifferentieret lagring af trafikdata og lokaliseringsdata. Den nævnte artikel 15, stk. 1, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, skal derimod fortolkes således, at denne bestemmelse ikke til hinder for nationale retsfor skrifter:

- der med henblik på beskyttelse af den nationale sikkerhed gør det muligt at pålægge udbydere af elektroniske kommunikationstjenester et påbud om at foretage generel og udifferentieret lagring af trafikdata og lokaliseringsdata i de situationer, hvor den pågældende medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig, når den afgørelse, der fastsætter dette påbud, kan gøres til genstand for en effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, med henblik på at kontrollere, om en af disse situationer foreligger, samt om de betingelser og garantier, der skal være fastsat, er overholdt, og når det nævnte påbud kun kan udstedes for en periode, der er tidsmæssigt begrænset til det strengt nødvendige, men som kan forlænges i tilfælde af, at denne trussel består
- der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed foreskriver målrettet lagring af de trafikdata og lokaliseringsdata, som på grundlag af objektive og ikke-diskriminerende forhold er afgrænset ud fra kategorier af berørte personer eller ved hjælp af et geografisk kriterium, i en periode, der er tidsmæssigt begrænset til det strengt nødvendige, men som kan forlænges
- der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed foreskriver generel og udifferentieret lagring af de IP-adresser, der er tildelt kilden til en forbindelse, i en periode, der er tidsmæssigt begrænset til det strengt nødvendige
- der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og beskyttelse af den offentlige sikkerhed foreskriver generel og udifferentieret lagring af de data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, og
- der med henblik på bekæmpelse af grov kriminalitet og a fortiori med henblik på beskyttelsen af den nationale sikkerhed gør det muligt ved en afgørelse fra den kompetente myndighed, som er underlagt en effektiv domstolsprøvelse, at pålægge udbydere af elektroniske kommunikationstjenester et påbud om i en begrænset periode at foretage hurtig lagring af de trafikdata og lokaliseringsdata, som disse tjenesteudbydere råder over,

for så vidt som disse forskrifter ved klare og præcise regler sikrer, at lagringen af de omhandlede data er underlagt overholdelsen af de dermed forbundne materielle og proceduremæssige betingelser, og at de berørte personer råder over effektive garantier mod risikoen for misbrug.

Sagsomkostninger

- 132 Da sagernes behandling i forhold til hovedsagernes parter udgør et led i de sager, der verserer for den forelæggende ret, tilkommer det denne at træffe afgørelse om sagsomkostningerne. Bortset fra de nævnte parters udgifter kan de udgifter, som er afholdt i forbindelse med afgivelse af indlæg for Domstolen, ikke erstattes.

På grundlag af disse præmisser kender Domstolen (Store Afdeling) for ret:

Artikel 15, stk. 1, i Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation), som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009, sammenholdt med artikel 7, 8 og 11 samt artikel 52, stk. 1, i Den Europæiske Unions charter om grundlæggende rettigheder,

skal fortolkes således, at

denne bestemmelse er til hinder for nationale retsfor skrifter, der med henblik på bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed i forebyggende øjemed foreskriver generel og udifferentieret lagring af trafikdata og lokaliseringsdata

denne bestemmelse er ikke til hinder for nationale retsfor skrifter:

- der med henblik på beskyttelse af den nationale sikkerhed gør det muligt at pålægge udbydere af elektroniske kommunikationstjenester et påbud om at foretage generel og udifferentieret lagring af trafikdata og lokaliseringsdata i de situationer, hvor den pågældende medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed, som må anses for at være reel og aktuel eller forudsigelig, når den afgørelse, der fastsætter dette påbud, kan gøres til genstand for en effektiv prøvelse enten ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, med henblik på at kontrollere, om en af disse situationer foreligger, samt om de betingelser og garantier, der skal være fastsat, er overholdt, og når det nævnte påbud kun kan udstedes for en periode, der er tidsmæssigt begrænset til det strengt nødvendige, men som kan forlænges i tilfælde af, at denne trussel består
- der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed foreskriver målrettet lagring af de trafikdata og lokaliseringsdata, som på grundlag af objektive og ikke-diskriminerende forhold er afgrænset ud fra kategorier af berørte personer eller ved hjælp af et geografisk kriterium, i en periode, der er tidsmæssigt begrænset til det strengt nødvendige, men som kan forlænges
- der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed foreskriver generel og udifferentieret lagring af de IP-adresser, der er tildelt kilden til en forbindelse, i en periode, der er tidsmæssigt begrænset til det strengt nødvendige

- der med henblik på beskyttelse af den nationale sikkerhed, bekæmpelse af grov kriminalitet og beskyttelse af den offentlige sikkerhed foreskriver generel og udifferentieret lagring af de data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler, og
- der med henblik på bekæmpelse af grov kriminalitet og a fortiori med henblik på beskyttelsen af den nationale sikkerhed gør det muligt ved en afgørelse fra den kompetente myndighed, som er underlagt en effektiv domstolsprøvelse, at pålægge udbydere af elektroniske kommunikationstjenester et påbud om i en begrænset periode at foretage hurtig lagring af de trafikdata og lokaliseringsdata, som disse tjenesteudbydere råder over,

for så vidt som disse forskrifter ved klare og præcise regler sikrer, at lagringen af de omhandlede data er underlagt overholdelsen af de dermed forbundne materielle og proceduremæssige betingelser, og at de berørte personer råder over effektive garantier mod risikoen for misbrug.

Underskrifter