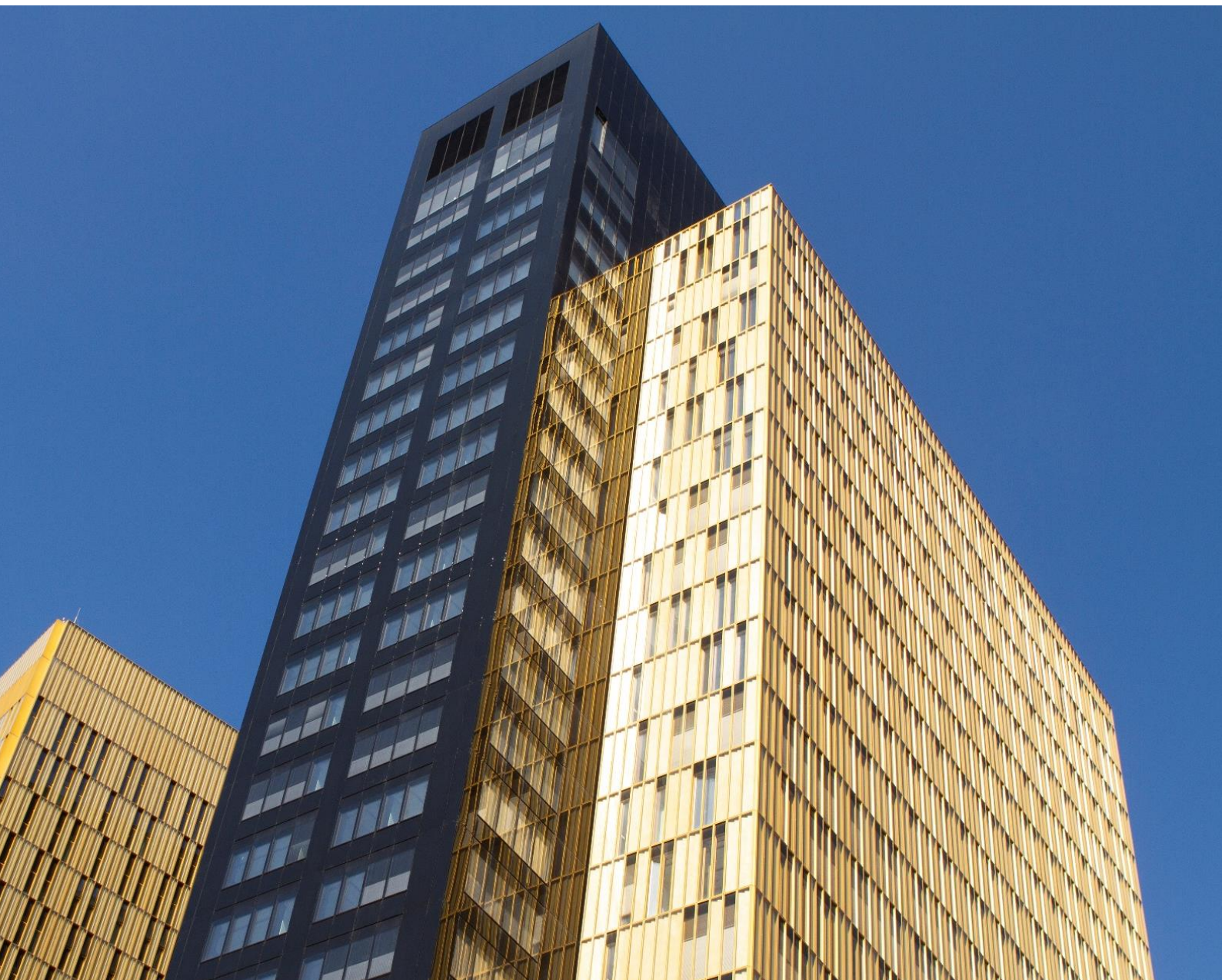




Faktablad

Beskyttelse af personoplysninger

Forord

Retten til beskyttelse af personoplysninger er en grundlæggende ret, hvis overholdelse er et vigtigt mål for Den Europæiske Union.

Denne ret er sikret ved den primære ret, navnlig i artikel 8 i Den Europæiske Unions charter om grundlæggende rettigheder (herefter »chartret«) og i artikel 16, stk. 1, i traktaten om Den Europæiske Unions funktionsmåde (TEUF). Denne grundlæggende ret er desuden tæt knyttet til retten til respekt for privatliv og familieliv, der er sikret ved chartrets artikel 7.

Med hensyn til den afledte ret fik Det Europæiske Fællesskab fra midten af 1990'erne forskellige instrumenter til sikring af beskyttelsen af personoplysninger. Direktiv 95/46/EF om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger ¹, der blev ophævet i 2018, udgjorde i denne henseende Fællesskabets vigtigste retsakt på området.

Direktiv 2002/58/EF ² supplerede dernæst direktiv 95/46/EF, idet det harmoniserede medlemsstaternes lovgivning om beskyttelse af retten til privatlivets fred, navnlig i forbindelse med behandling af personoplysninger i den elektroniske kommunikationssektor ³. Det bemærkes, at EU-lovgiver med henblik på at tage højde for nye udviklinger på det teknologiske og forretningsmæssige område i 2017 indledte en revision af dette direktiv ⁴, som på nuværende tidspunkt stadig pågår ⁵.

Den Europæiske Union ændrede i 2016 de overordnede retsforskrifter på området. Med henblik herpå vedtog den forordning (EU) 2016/679 ⁶ om databeskyttelse (herefter »databeskyttelsesforordningen«), der ophævede direktiv 95/46, og som har fundet

¹ Europa-Parlamentets og Rådets direktiv 95/46/EF af 24.10.1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT 1995, L 281, s. 6), konsolideret udgave af 20.11.2003, ophævet med virkning fra 25.5.2018 (jf. fodnote 6).

² Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12.7.2002 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), konsolideret udgave af 19.12.2009.

³ Direktiv 2002/58 blev ændret ved Europa-Parlamentets og Rådets direktiv 2006/24/EF af 15.3.2006 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). Domstolen erklærede dette direktiv ugyldigt i dom af 8.4.2014, Digital Rights Ireland og Seitlinger m.fl. (C-293/12 og C-594/12, [EU:C:2014:238](#)), med den begrundelse, at det indebærer en alvorlig risiko for retten til respekt for privatlivets fred og beskyttelsen af personoplysninger (se afsnit I.1 med overskriften »Den afledte EU-rets overensstemmelse med retten til beskyttelse af personoplysninger« i dette faktablad).

⁴ Kommissionen indgav den 10.1.2017 et forslag med henblik på at erstatte direktivet med en forordning om databeskyttelse inden for elektronisk kommunikation.

⁵ Den 10.1.2021 godkendte Rådet for Den Europæiske Union et mandat til at føre forhandlinger om en revision af bestemmelserne om beskyttelse af privatlivets fred og fortroligheden i brugen af elektroniske kommunikationstjenester, der gjorde det muligt at indlede forhandlingerne med Europa-Parlamentet. Teksten til forslag til Europa-Parlamentets og Rådets forordning om respekt for privatliv og beskyttelse af personoplysninger i forbindelse med elektronisk kommunikation og om ophævelse af direktiv 2002/58/EF (forordning om databeskyttelse inden for elektronisk kommunikation) er tilgængelig via af dette link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN

⁶ Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27.4.2016 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 (EUT 2016, L 119, s. 1).

anvendelse siden den 25. maj 2018, samt direktiv (EU) 2016/680⁷ om beskyttelse af disse oplysninger i straffesager, hvis bestemmelser har fundet anvendelse siden den 6. maj 2018.

Hvad angår behandlingen af personoplysninger i Unionens institutioner og organer har beskyttelsen heraf siden den 11. december 2018 navnlig været sikret ved forordning (EU) 2018/1725⁸. Af hensyn til en sammenhængende tilgang til beskyttelse af personoplysninger i hele Unionen sigter denne forordning så vidt muligt mod at tilpasse reglerne på området til den ordning, der blev indført med databeskyttelsesforordningen.

Endelig har EU-lovgiver med henblik på at tackle de udfordringer, der er forbundet med de nye teknologier, siden 2020 indledt vedtagelsen af nye lovgivningsmæssige foranstaltninger⁹, der har relation til de EU-retlige bestemmelserne om beskyttelse af personoplysninger.

Henset til Domstolens omfattende retspraksis vedrørende beskyttelsen af personoplysninger tager dette faktablad sigte på at præsentere et udvalg af principielle domme på området samt domme, der har haft stor betydning for udviklingen af denne retspraksis, med særligt fokus på de domme, der er afsagt af Domstolens Store Afdeling. Formålet med dette faktablad er nærmere bestemt både at dække retspraksis vedrørende den generelle lovgivning om behandling af personoplysninger, med udgangspunkt i fortolkningen af direktiv 95/46 og databeskyttelsesforordningen, og retspraksis vedrørende de sektorspecifikke regler, der navnlig omhandler den elektroniske kommunikationssektor og strafferetten. Derudover tilstræbes det at præsentere et udvalg af domme vedrørende de lovregler, der finder tværgående anvendelse, idet det på forhånd skal fremhæves, at chartret har spillet en afgørende rolle i udviklingen af retspraksis.

⁷ Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27.4.2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (EUT 2016, L 119, s. 89).

⁸ Europa-Parlamentets og Rådets forordning (EU) 2018/1725 af 23.10.2018 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i Unionens institutioner, organer, kontorer og agenturer og om fri udveksling af sådanne oplysninger og om ophævelse af forordning (EF) nr. 45/2001 og afgørelse nr. 1247/2002/EF (EUT 2018, L 295, s. 39).

⁹ I denne forbindelse skal navnlig nævnes tre lovgivningsinitiativer: i) Europa-Parlamentets og Rådets forordning (EU) 2022/868 af 30.5.2022 om europæisk datastyring og om ændring af forordning (EU) 2018/1724 (forordning om datastyring) (EUT 2022, L 152, s. 1) og Europa-Parlamentets og Rådets forordning (EU) 2023/2854 af 13.12.2023 om harmoniserede regler om fair adgang til og anvendelse af data og om ændring af forordning (EU) 2017/2394 og direktiv (EU) 2020/1828 (dataforordningen) (EUT L, 2023/2854, s. 1), ii) en lovgivningspakke om de digitale tjenester og markeder bestående af Europa-Parlamentet og Rådets forordning (EU) 2022/2065 af 19.10.2022 om et indre marked for digitale tjenester og om ændring af direktiv 2000/31/EF (forordning om digitale tjenester) (EUT 2022, L 277, s. 1) og Europa-Parlamentets og Rådets forordning 2022/1925 af 14.9.2022 om åbne og fair markeder i den digitale sektor og om ændring af direktiv (EU) 2019/1937 og (EU) 2020/1828 (forordningen om digitale markeder) (EUT 2022, L 265, s. 1), og iii) det allerførste lovgivningsforslag med henblik på at skabe en lovgivningsmæssig ramme på området for kunstig intelligens, som har udmøntet sig i en forordning om kunstig intelligens (EUT L, 2024/1689).

Indhold

FORORD	3
I. RETTEN TIL BESKYTTELSE AF PERSONOPLYSNINGER, DER SIKRES VED DEN EUROPÆISKE UNIONS CHARTER OM GRUNDLÆGGENDE RETTIGHEDER	7
1. Den afledte EU-rets overensstemmelse med retten til beskyttelse af personoplysninger	7
2. Overholdelse af retten til beskyttelse af personoplysninger ved EU-rettens gennemførelse	19
II. BEHANDLING AF PERSONOPLYSNINGER SOM OMHANDLET I DEN GENERELLE LOVGIVNING PÅ OMRÅDET.....	20
1. Den generelle lovgivnings anvendelsesområde	20
2. Begrebet »personoplysninger«	26
3. Begrebet »behandling af personoplysninger«	29
4. Begrebet »register med personoplysninger«	34
5. Begrebet »den registeransvarlige for behandlingen af personoplysninger«	34
6. Begrebet »fælles dataansvarlig«	37
7. Betingelser for lovligheden af en behandling af personoplysninger	38
III. BEHANDLING AF PERSONOPLYSNINGER SOM OMHANDLET I SEKTORSPECIFIKKE REGLER	44
1. Behandling af personoplysninger i den elektroniske kommunikationssektor ...	44
2. Behandling af personoplysninger i straffesager	64
IV. VIDEREGIVELSE AF PERSONOPLYSNINGER TIL TREDJELANDE.....	68
V. BESKYTTELSE AF PERSONOPLYSNINGER PÅ INTERNETTET	76
1. Ret til at gøre indsigelse mod behandling af personoplysninger (»retten til at blive glemt«).....	76
2. Behandling af personoplysninger og intellektuelle ejendomsrettigheder	77
3. Fjernelse af personoplysninger	80
4. Samtykke fra brugeren af et internetwebsted til lagring af oplysninger	89
5. Behandling af personoplysninger på sociale onlinenetværk.....	91
VI. NATIONALE TILSYNSMYNDIGHEDER	94
1. Rækkevidden af kravet om uafhængighed.....	94
2. Fastlæggelse af den ret, der finder anvendelse, og den kompetente tilsynsmyndighed	97
3. De nationale tilsynsmyndigheders beføjelser	98
4. Betingelser for pålæggelse af administrative bøder	104

5. Forholdet mellem nationale tilsynsmyndigheders beføjelser og andre nationale myndigheders beføjelser.....	108
--	-----

I. Retten til beskyttelse af personoplysninger, der sikres ved Den Europæiske Unions charter om grundlæggende rettigheder

1. Den afledte EU-rets overensstemmelse med retten til beskyttelse af personoplysninger

Dom af 9. november 2010 (Store Afdeling), Volker und Markus Schecke og Eifert (C-92/09 og C-93/09, [EU:C:2010:662](#))

I denne sag var parterne i tvisten i hovedsagen landbrugere og Land Hessen, og tvisten vedrørte Bundesanstalt für Landwirtschaft und Ernährung (den tyske forbundsmyndighed for landbrug og fødevarer) offentliggørelse på dennes websted af landbrugernes personoplysninger, fordi de havde modtaget midler fra Den Europæiske Garantifond for Landbruget (EGFL) og Den Europæiske Landbrugsfond for Udvikling af Landdistrikterne (ELFUL). De pågældende landbrugere modsatte sig denne offentliggørelse, idet de navnlig gjorde gældende, at den ikke var begrundet i en tungtvejende offentlig interesse. Land Hessen var af den opfattelse, at offentliggørelsen af disse oplysninger var i overensstemmelse med forordning (EF) nr. 1290/2005¹⁰ og (EF) nr. 259/2008¹¹ om finansiering af den fælles landbrugspolitik, der indeholder krav om offentliggørelse af oplysninger om fysiske personer, der modtager midler fra EGFL og ELFUL.

På denne baggrund forelagde Verwaltungsgericht Wiesbaden (forvaltningsdomstolen i Wiesbaden, Tyskland) Domstolen flere spørgsmål om gyldigheden af visse af bestemmelserne i forordning nr. 1290/2005 og af forordning nr. 259/2008, der indeholder krav om, at offentligheden får adgang til sådanne oplysninger, navnlig via de nationale kontorers websteder.

Domstolen anførte vedrørende overensstemmelsen mellem retten til beskyttelse af personoplysninger, der sikres ved chartret, og forpligtelsen til åbenhed vedrørende de europæiske fonde, at offentliggørelsen af modtagernes navne og de beløb, som de har modtaget, på et websted på grund af tredjeparters adgang til webstedet krænker de pågældende modtageres ret til privatlivets fred i almindelighed og til beskyttelse af deres personoplysninger i særdeleshed.

¹⁰ Rådets forordning (EF) nr. 1290/2005 af 21.6.2005 om finansiering af den fælles landbrugspolitik (EUT 2005, L 209, s. 1), ophævet ved Europa-Parlamentets og Rådets forordning (EU) nr. 1306/2013 af 17.12.2013 om finansiering, forvaltning og overvågning af den fælles landbrugspolitik (EUT 2013, L 347, s. 549).

¹¹ Kommissionens forordning (EF) nr. 259/2008 af 18.3.2008 om gennemførelsesbestemmelser til Rådets forordning (EF) nr. 1290/2005 for så vidt angår offentliggørelsen af oplysninger om modtagerne af midler fra Den Europæiske Garantifond for Landbruget (EGFL) og Den Europæiske Landbrugsfond for Udvikling af Landdistrikterne (ELFUL) (EUT 2008, L 76, s. 28), ophævet ved Kommissionens gennemførelsesforordning (EU) nr. 908/2014 af 6.8.2014 om gennemførelsesbestemmelser til Europa-Parlamentets og Rådets forordning (EU) nr. 1306/2013 for så vidt angår betalingsorganer og andre organer, økonomisk forvaltning, regnskabsafslutning, regler om kontroller, sikkerhedsstillelse og åbenhed (EUT 2014, L 255, s. 59).

En sådan krænkelse skal for at være begrundet være fastlagt i lovgivningen, respektere disse rettigheders væsentligste indhold, og den skal under iagttagelse af proportionalitetsprincippet være nødvendig og faktisk svare til mål af almen interesse, der er anerkendt af Unionen, idet undtagelser fra og begrænsninger af disse rettigheder skal holdes inden for det strengt nødvendige. Domstolen fastslog i denne forbindelse, at selv om skatteyderne i et demokratisk samfund har ret til at blive informeret om anvendelsen af offentlige midler, forholder det sig ikke desto mindre således, at Rådet og Kommissionen var forpligtet til at foretage en rimelig afvejning mellem de omhandlede interesser, hvilket krævede, at de inden vedtagelsen af de bestemmelser, hvis gyldighed var bestridt, havde undersøgt, om offentliggørelsen på et enkelt websted for hver medlemsstat gik ud over, hvad der var nødvendigt for at nå de legitime formål, der forfølges.

Domstolen erklærede således nogle af bestemmelserne i forordning nr. 1290/2005 og forordning nr. 259/2008 i dens helhed for ugyldige, for så vidt som disse bestemmelser vedrørende fysiske personer, der modtager midler fra EGFL og ELFUL, indebar et krav om offentliggørelse af personoplysninger om enhver modtager uden at foretage en sontring i henhold til relevante kriterier, såsom i hvilken periode de havde modtaget disse midler, hyppigheden af en sådan modtagelse eller midlernes art og omfang. Domstolen anfægtede dog ikke virkningerne af offentliggørelsen af lister over modtagere af sådanne midler, der var foretaget af de nationale myndigheder på grundlag af de nævnte bestemmelser i perioden inden denne doms afsigelse.

Dom af 8. april 2014 (Store Afdeling), Digital Rights Ireland og Seitlinger m.fl. (forenede sager C-293/12 og C-594/12, [EU:C:2014:238](#))

Denne dom udspringer af anmodninger om præjudiciel afgørelse vedrørende foreneligheden af direktiv 2006/24/EF om lagring af data med de grundlæggende rettigheder om respekt for privatliv og beskyttelsen af personoplysninger, der var blevet fremsat i forbindelse med nationale tvister indbragt for en irsk og en østrigsk domstol. I sag C-293/12 var der blevet indbragt en tvist for High Court (ret i første instans, Irland) mellem selskabet Digital Rights og de irske myndigheder om lovligheden af nationale foranstaltninger, der angår lagring af data vedrørende elektronisk kommunikation. I sag C-594/12 var der blevet anlagt en række forfatningsretlige søgsmål ved Verfassungsgerichtshof (forfatningsdomstol, Østrig) med påstand om annullation af den nationale bestemmelse til gennemførelse af direktiv 2006/24 i østrigsk ret.

Den irske og den østrigske ret ønskede med deres anmodninger om præjudiciel afgørelse oplyst, om direktiv 2006/24 var foreneligt med chartrets artikel 7, 8 og 11. De pågældende retter ønskede nærmere bestemt oplyst, om den pligt, der i henhold til direktivet var pålagt udbydere af offentligt tilgængelige elektroniske kommunikationstjenester eller af et offentligt kommunikationsnet til i et nærmere bestemt tidsrum at lagre data vedrørende en persons privatliv og kommunikation og til at give de kompetente nationale myndigheder adgang hertil, udgjorde et uberettiget

indgreb i de pågældende grundlæggende rettigheder. De datatyper, der var tale om, var bl.a. data, der er nødvendige for at spore og identificere kilden til en kommunikation og dens bestemmelsessted, for at fastslå en kommunikations dato, klokkeslæt, varighed og type, og identificere brugernes kommunikationsudstyr og foretage en lokalisering af mobilt udstyr, dvs. data, der bl.a. omfatter navn og adresse på abonnenten eller den registrerede bruger, telefonnummer på den, der foretager opkaldet, og det kaldte nummer samt for internettjenester en IP-adresse. Disse data gør det bl.a. muligt at få kendskab til, med hvilken person og ved hjælp af hvilket kommunikationsmiddel en abonnent eller registreret bruger har kommunikeret, samt at tidsfæste kommunikationen og identificere det sted, hvorfra den har fundet sted. Desuden gør de det muligt at være bekendt med hyppigheden af abonnentens eller den registrerede brugers kommunikation med bestemte personer i en given periode.

Domstolen fastslog først og fremmest, at bestemmelserne i direktiv 2006/24 ved at pålægge udbyderne sådanne pligter indebar et meget vidtrækkende indgreb i de grundlæggende rettigheder til respekt for privatliv og beskyttelse af personoplysninger, som er sikret ved chartrets artikel 7 og 8. Domstolen konstaterede i denne forbindelse ganske vist, at dette indgreb kunne begrundes i forfølgelsen af et mål af almen interesse såsom bekæmpelse af organiseret kriminalitet. Domstolen bemærkede i denne forbindelse for det første, at den lagring af oplysninger, der krævedes i direktivet, ikke kunne indebære en krænkelse af det væsentligste indhold af de grundlæggende rettigheder til respekt for privatliv og beskyttelse af personoplysninger, for så vidt som denne lagring ikke gav adgang til at gøre sig bekendt med selve indholdet af de elektroniske kommunikationer, ligesom det fremgik, at udbydere af tjenester eller af net skulle respektere visse principper for databeskyttelse og datasikkerhed. Domstolen bemærkede for det andet, at lagring af oplysninger med henblik på eventuelt at give de kompetente nationale myndigheder adgang hertil reelt svarede til et mål af almen interesse, nemlig bekæmpelse af alvorlig kriminalitet, og i sidste ende den offentlige sikkerhed.

Domstolen fandt dog, at EU-lovgiver med vedtagelsen af direktivet om lagring af data havde overskredet de grænser, som overholdelsen af proportionalitetsprincippet kræver. Den erklærede derfor direktivet ugyldigt, idet den fastslog, at det indgreb i de grundlæggende rettigheder af en meget vidtrækkende og særlig alvorlig karakter, som direktivet indebar, ikke var præcist afgrænset af bestemmelser, der gjorde det muligt at sikre, at det faktisk var begrænset til det strengt nødvendige. Direktiv 2006/24 omfattede således generelt alle personer, alle elektroniske kommunikationsmidler og samtlige trafikdata, uden at der i direktivet blev foretaget nogen form for differentiering, begrænsning eller undtagelse under hensyn til målet om bekæmpelse af grov kriminalitet. Direktivet indeholdt desuden ikke noget objektivi kriterium, som gjorde det muligt at sikre, at de kompetente nationale myndigheder kun havde adgang til dataene og kun kunne anvende dem med henblik på forebyggelse, afsløring eller retsforfølgning af strafbare handlinger, der kunne anses for tilstrækkeligt grove til at begrunde et sådant indgreb, og desuden ingen materielle og processuelle betingelser for en sådan

adgang og en sådan anvendelse. Med hensyn til varigheden af datalagringen foreskrev direktivet endelig, at dataene skulle lagres i et tidsrum af mindst seks måneder, uden at der på nogen måde blev foretaget en sontring afhængigt af, hvilke personer der var berørt, eller af oplysningernes eventuelle relevans for det forfulgte mål.

Med hensyn til de krav, der følger af chartrets artikel 8, stk. 3, konstaterede Domstolen desuden, at direktiv 2006/24 ikke indeholdt tilstrækkelige garantier, der gjorde det muligt at sikre en effektiv beskyttelse af lagrede data mod risikoen for misbrug og mod enhver ulovlig adgang til og anvendelse af disse oplysninger, ligesom det ikke foreskrev, at de omhandlede oplysninger skulle lagres på Unionens område.

Direktivet garanterede derfor ikke fuldt ud, at overholdelsen af kravene vedrørende beskyttelse og sikkerhed blev kontrolleret af en uafhængig myndighed, således som det udtrykkeligt kræves i chartret.

Dom af 21. juni 2022 (Store Afdeling), Ligue des droits humains (C-817/19, [EU:C:2022:491](#))

PNR-oplysninger (Passenger Name Record) er oplysninger om reservationer, som luftfartsselskaberne lagrer i deres reservations- og afgangskontrolsystemer. PNR-direktivet ¹² forpligter luftfartsselskaberne til at videregive oplysninger om alle passagerer, der benytter en flyvning uden for EU mellem et tredjeland og Den Europæiske Union, til passageroplysningsenheden i den medlemsstat, som det pågældende fly flyver til eller fra, med henblik på at bekæmpe terrorisme og grov kriminalitet. De PNR-oplysninger, der således videregives, underkastes nemlig en forudgående vurdering i passageroplysningsenheden ¹³ og opbevares herefter med henblik på en eventuel efterfølgende vurdering, som de kompetente myndigheder i den berørte medlemsstat eller en anden medlemsstat foretager. Medlemsstaterne kan beslutte også at anvende dette direktiv på flyvninger inden for EU ¹⁴.

¹² Europa-Parlamentets og Rådets direktiv (EU) 2016/681 af 27.4.2016 om anvendelse af passagerlisteoplysninger (PNR-oplysninger) til at forebygge, opdage, efterforske og retsforfølge terrorhandlinger og grov kriminalitet (EUT 2016, L 119, s. 132, herefter »PNR-direktivet«).

¹³ Denne forudgående vurdering har til formål at identificere personer, som det kræves, at de kompetente myndigheder undersøger nærmere, idet sådanne personer kan være involveret i en terrorhandling eller grov kriminalitet. Den foretages systematisk og automatisk ved, at PNR-oplysningerne sammenholdes med oplysninger i databaser, der er »relevante«, eller behandles efter forud fastsatte kriterier som omhandlet i PNR-direktivets artikel 6, stk. 2, litra a), og artikel 6, stk. 3.

¹⁴ Ved brug af muligheden i PNR-direktivets artikel 2.

Ligue des droits humains (en belgisk menneskerettighedsorganisation) anlagde ved Cour constitutionnelle (forfatningsdomstol, Belgien) et søgsmål med påstand om annulation af den belgiske lov, der gennemførte både PNR-direktivet og API-direktivet i belgisk ret ¹⁵. Sagsøgeren anførte, at denne lov tilsidesatte retten til respekt for privatlivet og til beskyttelse af personoplysninger. Sagsøgeren anfægtede dels det meget store omfang af PNR-oplysninger, dels den generelle karakter af indsamlingen, videregivelsen og behandlingen af disse oplysninger. Loven udgjorde efter sagsøgerens opfattelse ligeledes et indgreb i den frie bevægelighed for personer, idet den indirekte genindførte grænsekontrol ved at udvide PNR-systemet til at omfatte flyvninger inden for EU og transporter med andre midler inden for EU.

I denne sammenhæng forelagde den belgiske forfatningsdomstol Domstolen præjudicielle spørgsmål vedrørende navnlig gyldigheden af PNR-direktivet.

I dommen, der blev afsagt af Store Afdeling, bekræftede Domstolen gyldigheden af PNR-direktivet, for så vidt som dette kan fortolkes i overensstemmelse med chartret.

I denne henseende fastslog Domstolen, at da Domstolens fortolkning af PNR-direktivets bestemmelser i lyset af de grundlæggende rettigheder, som beskyttes ved chartrets artikel 7, 8 og 21 samt artikel 52, stk. 1, ¹⁶sikrer dette direktivs overensstemmelse med disse bestemmelser i chartret, havde undersøgelsen af de forelagte spørgsmål intet frembragt, der kunne rejse tvivl om direktivets gyldighed.

Domstolen bemærkede indledningsvis, at en EU-retsakt i videst muligt omfang skal fortolkes således, at dens gyldighed ikke drages i tvivl, og i overensstemmelse med hele den primære ret og navnlig med chartrets bestemmelser, og medlemsstaterne skal således sikre, at de ikke lægger en fortolkning heraf til grund, som kommer i konflikt med de grundlæggende rettigheder, der beskyttes ved Unionens retsorden, eller med andre generelle principper, som er anerkendt i denne retsorden. Hvad angår PNR-direktivet præciserede Domstolen, at mange betragtninger og bestemmelser heri kræver en sådan overensstemmende fortolkning, idet der er lagt vægt på den betydning, som EU-lovgiver, med henvisning til et højt databeskyttelsesniveau, tillægger den fulde respekt for de grundlæggende rettigheder, som er sikret ved chartret.

Domstolen konstaterede, at PNR-direktivet indebærer indgreb af en klart alvorlig karakter i de rettigheder, som er sikret ved chartrets artikel 7 og 8, bl.a. for så vidt som det har til formål at indføre et system til kontinuerlig, ikke-måltrettet og systematisk overvågning, der omfatter automatisk vurdering af personoplysninger vedrørende samtlige personer, der benytter lufttransporttjenester. Den bemærkede, at

¹⁵ Rådets direktiv 2004/82/EF af 29.4.2004 om transportvirksomheders forpligtelse til at fremsende oplysninger om passagerer (EUT 2004, L 261, s. 24, herefter »API-direktivet«). Dette direktiv regulerer luftfartsselskabernes videregivelse af forhåndsoplysninger om passagerer (såsom den anvendte rejselegitimations nummer og type samt nationalitet) til de kompetente nationale myndigheder med henblik på at forbedre grænsekontrollen og bekæmpe ulovlig indvandring.

¹⁶ I henhold til ordlyden af denne bestemmelse skal enhver begrænsning i udøvelsen af de rettigheder og friheder, der anerkendes ved dette charter, skal være fastlagt i lovgivningen og skal respektere disse rettigheds og friheders væsentligste indhold. Der kan endvidere kun indføres begrænsninger, såfremt disse 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.

medlemsstaternes mulighed for at begrunde et sådan indgreb skal vurderes ved at bedømme dets alvor og ved at kontrollere, at betydningen af det mål af almen interesse, der forfølges, står i forhold til denne alvor.

Domstolen konkluderede, at videregivelse, behandling og opbevaring af PNR-oplysninger som fastsat i dette direktiv kan anses for at være begrænset til det strengt nødvendige med henblik på bekæmpelse af terrorhandlinger og grov kriminalitet, forudsat at beføjelserne i henhold til direktivet fortolkes snævert. Domstolen fastslog i sin dom navnlig følgende:

- Det system, der er indført ved PNR-direktivet, bør kun omfatte klart identificerbare og afgrænsede oplysninger inden for de rubrikker, der er angivet i bilag I til direktivet, som har forbindelse til flyvningen og den pågældende passager, hvilket – for visse af rubrikkerne i dette bilag – indebærer, at alene udtrykkeligt omhandlede oplysninger er omfattet ¹⁷.
- Anvendelsen af det system, der er indført ved PNR-direktivet, skal begrænses til terrorhandlinger og alene de former for grov kriminalitet, som har en – i det mindste indirekte – objektiv forbindelse med luftbefordring af passagerer. Hvad angår disse former for kriminalitet kan anvendelsen af dette system ikke udvides til at omfatte overtrædelser, der – selv om de opfylder kriteriet i dette direktiv om alvorstærsklen og bl.a. er omhandlet i bilag II til direktivet – under hensyntagen til det nationale strafferetlige systems særlige kendetegn henhører under almindelig kriminalitet.
- En eventuel udvidelse af anvendelsen af PNR-direktivet til at omfatte alle eller en del af flyvningerne inden for EU, som en medlemsstat kan træffe bestemmelse om ved at udnytte beføjelsen i henhold til dette direktiv, skal være begrænset til det strengt nødvendige. Med henblik herpå skal den udvidede anvendelse kunne gøres til genstand for en effektiv prøvelse ved en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser. Domstolen præciserede i denne henseende følgende:
 - Kun i en situation, hvor den pågældende medlemsstat konstaterer, at der foreligger tilstrækkeligt konkrete omstændigheder til at antage, at den står over for en terrortrussel, som må anses for at være reel og aktuel eller forudsigelig, vil det ikke overskride grænserne for det strengt nødvendige at anvende dette direktiv på alle flyvninger inden for EU fra eller til medlemsstaten i en periode, som er tidsmæssigt begrænset til det strengt nødvendige, men som kan forlænges ¹⁸.

¹⁷ »[O]plysninger om betalingsformer« (bilagets nr. 6) skal således begrænses til betalingsformer og faktureringsadresse for flybilletten, med undtagelse af alle andre oplysninger, der ikke har direkte forbindelse med denne flyvning, og »[g]enerelle bemærkninger« kan kun omfatte de oplysninger, der er udtrykkeligt opregnet i dette nummer for så vidt angår mindreårige passagerer.

¹⁸ Den omstændighed, at der foreligger en sådan trussel, kan nemlig i sig selv godtgøre, at der består en forbindelse mellem videregivelsen og behandlingen af de pågældende oplysninger og bekæmpelsen af terrorisme. Det vil derfor ikke gå ud over grænserne for det strengt nødvendige

- Hvis en sådan terrortrussel ikke foreligger, kan anvendelsen af dette direktiv ikke udvides til at omfatte samtlige flyvninger inden for EU, men skal begrænses til flyvninger inden for EU i forbindelse med bl.a. bestemte flyforbindelser, rejseruter eller bestemte lufthavne, for hvilke den berørte medlemsstat vurderer, at der foreligger oplysninger, der kan begrunde denne anvendelse. Det skal regelmæssigt evalueres, om denne anvendelse på de således udvalgte flyvninger inden for EU er strengt nødvendig, i lyset af udviklingen i de forhold, der har begrundet valget af disse flyvninger.
- Med henblik på den forudgående vurdering af PNR-oplysninger, der har til formål at identificere personer, for hvilke det er nødvendigt at foretage en nærmere undersøgelse før deres ankomst eller afrejse, og som i første omgang foretages ved automatisk behandling af oplysningerne, må passageroplysningsenheden for det første kun sammenholde disse oplysninger med oplysninger i databaser vedrørende personer eller genstande, der eftersøges eller er indberettet ¹⁹. Disse databaser skal være ikke-diskriminerende og benyttes af de kompetente myndigheder i forbindelse med bekæmpelse af terrorhandlinger og grov kriminalitet, der har en – i det mindste indirekte – objektiv forbindelse med luftbefordring af passagerer. Hvad for det andet angår den forudgående vurdering efter forud fastsatte kriterier må passageroplysningsenheden ikke anvende teknologier inden for kunstig intelligens i forbindelse med selvlæringssystemer (machine learning), som uden menneskelig indgriben og kontrol kan ændre vurderingsprocessen og navnlig de vurderingskriterier, som resultatet af anvendelsen af denne proces er baseret på, samt vægtningen af disse kriterier. Disse kriterier skal være fastsat således, at de specifikt er målrettet personer, for hvilke der kan foreligge en rimelig mistanke om, at de deltager i terrorhandlinger eller grov kriminalitet, og således, at de tager hensyn til både »belastende« og »diskulperende« forhold, samtidig med at de ikke giver anledning til direkte eller indirekte forskelsbehandling ²⁰.
- Henset til den fejlmargen, som nødvendigvis er forbundet med en sådan automatisk behandling af PNR-oplysninger, og det ganske betydelige antal »falsk positive« resultater, der blev opnået efter automatisk behandling i 2018 og 2019, afhænger egnetheden af det system, der er indført ved PNR-direktivet, til at opfylde de forfulgte formål, i bund og grund af, om den kontrol af de positive resultater opnået ved denne behandling, som passageroplysningsenheden i anden omgang foretager manuelt, fungerer korrekt. I denne henseende skal

at fastsætte, at PNR-direktivet finder anvendelse på alle flyvninger inden for EU fra eller til den pågældende medlemsstat i et begrænset tidsrum, idet den afgørelse, hvorved der træffes bestemmelse herom, skal kunne gøres til genstand for en prøvelse ved en domstol eller en uafhængig administrativ enhed.

¹⁹ Nemlig databaser vedrørende personer eller genstande, der eftersøges eller er indberettet, som omhandlet i PNR-direktivets artikel 6, stk. 3, litra a). Derimod kan analyser på grundlag af andre databaser tage form af udvinding af oplysninger (data mining) og føre til en uforholdsmæssig anvendelse af disse oplysninger og gøre det muligt at tegne en præcis profil af de registrerede alene af den grund, at de agter at rejse med fly.

²⁰ De forud fastsatte kriterier skal være målrettede, stå i rimeligt forhold til målet og være konkrete, ligesom de skal evalueres regelmæssigt (PNR-direktivets artikel 6, stk. 4). Den forudgående vurdering efter forud fastsatte kriterier skal udføres på en ikke-diskriminerende måde. Ifølge PNR-direktivets artikel 6, stk. 4, må kriterierne må under ingen omstændigheder være baseret på en persons race eller etniske oprindelse, politiske anskuelser, religiøse eller filosofiske overbevisning, medlemskab af en fagforening, sundhed, seksualitet eller seksuel orientering.

medlemsstaterne fastsætte klare og præcise regler, der bestemmer grundlaget og rammerne for den analyse, som de medarbejdere i passageroplysningsenheden, der er ansvarlige for denne individuelle gennemgang, foretager, med henblik på at sikre den fulde respekt for de grundlæggende rettigheder, som er sikret ved chartrets artikel 7, 8 og 21, og navnlig sikre en konsekvent administrativ praksis i passageroplysningsenheden under overholdelse af princippet om forbud mod forskelsbehandling. De skal navnlig sikre, at passageroplysningsenheden fastsætter objektive kriterier for gennemgangen, som gør det muligt for dens medarbejdere at kontrollere dels, om og i hvilket omfang et hit faktisk vedrører en person, som kan være involveret i terrorhandlinger eller grov kriminalitet, dels at den automatiske behandling ikke er af en diskriminerende karakter. I denne sammenhæng fremhævede Domstolen også, at de kompetente myndigheder skal sikre sig, at den berørte kan forstå, hvordan disse forud fastsatte vurderingskriterier og de programmer, som anvender dem, fungerer, således at den pågældende på grundlag af et fuldt kendskab til sagen kan afgøre, om vedkommende vil gøre brug af sin klageadgang. I forbindelse med en sådan klage skal det være muligt for den dommer, der skal foretage legalitetsprøvelsen af den afgørelse, som de kompetente myndigheder har truffet, og – undtagen i tilfælde, hvor der er tale om trusler mod statens sikkerhed – for den berørte selv at få kendskab til såvel den fulde begrundelse som de beviser, på grundlag af hvilke denne afgørelse er truffet, herunder til de forud fastsatte vurderingskriterier og til, hvordan de programmer, som anvender disse kriterier, fungerer.

- Den efterfølgende videregivelse og vurdering af PNR-oplysningerne, dvs. efter den registreredes ankomst eller afrejse, må kun ske på grundlag af nye omstændigheder og objektive forhold, der enten kan begrunde en rimelig mistanke om, at den pågældende er involveret i grov kriminalitet, der har en – i det mindste indirekte – objektiv forbindelse med luftbefordring af passagerer, eller gør det muligt at antage, at disse PNR-oplysninger i en konkret sag kan bidrage effektivt til bekæmpelsen af terrorhandlinger med en sådan forbindelse. Videregivelse af PNR-oplysninger med henblik på en sådan efterfølgende vurdering skal principielt, undtagen i behørigt begrundede hastende tilfælde, være undergivet en forudgående kontrol, der foretages af enten en domstol eller en uafhængig administrativ enhed på grundlag af en begrundet anmodning fra de kompetente myndigheder, uanset om denne anmodning er blevet indgivet før eller efter udløbet af fristen på seks måneder efter videregivelsen af disse PNR-oplysninger til passageroplysningsenheden ²¹.

²¹ Ifølge PNR-direktivets artikel 12, stk. 1 og 3, er en sådan kontrol kun udtrykkeligt fastsat for anmodninger om videregivelse af PNR-oplysninger, der indgives efter udløbet af fristen på seks måneder efter videregivelsen af disse oplysninger til passageroplysningsenheden.

Dom af 22. november 2022 (Store Afdeling), Luxembourg Business Registers (C-37/20 og C-601/20, [EU:C:2022:912](#))

Med henblik på bekæmpelse og forebyggelse af hvidvask af penge og finansiering af terrorisme pålægger hvidvaskdirektivet²² medlemsstaterne at føre et register med oplysninger om de reelle ejere²³ af selskaber og andre juridiske enheder, der er etableret på deres område. Efter en ændring af dette direktiv ved direktiv 2018/843²⁴ skal visse af disse oplysninger i alle tilfælde gøres tilgængelige for ethvert medlem af offentligheden. I overensstemmelse med det således ændrede hvidvaskdirektiv (herefter »det ændrede hvidvaskdirektiv«) blev der ved luxembourgsk lovgivning oprettet et register over reelle ejere (herefter »RBE«) med henblik på opbevaring og tilrådighedsstillelse af en række oplysninger om de reelle ejere af de registrerede enheder, som enhver skal kunne tilgå.

På denne baggrund blev der anlagt to sager ved tribunal d'arrondissement de Luxembourg (kredsdomstolen i Luxembourg) af henholdsvis WM og Sovim SA, som anfægtede afslaget fra Luxembourg Business Registers, der forvalter RBE, på deres anmodninger om at forhindre offentlighedens adgang til oplysningerne vedrørende, i den første sag, WM som reel ejer af et privatretligt ejendomsselskab og, i den anden sag, Sovim SA's reelle ejer. I forbindelse med disse to sager, der bl.a. rejste tvivl om gyldigheden af de EU-retlige bestemmelser, der indførte ordningen om offentlighedens adgang til oplysninger om reelle ejere, forelagde tribunal d'arrondissement de Luxembourg (kredsdomstolen i Luxembourg) Domstolen et præjudicielt spørgsmål vedrørende bestemmelsernes gyldighed.

Ved sin dom fastslog Domstolen (Store Afdeling), at direktiv 2018/843 var ugyldigt, for så vidt som dette direktiv ændrede hvidvaskdirektivet, således at medlemsstaterne skulle sikre, at oplysninger om reelt ejerskab af selskaber og andre juridiske enheder, der er etableret på deres område, i alle tilfælde er tilgængelige for ethvert medlem af offentligheden²⁵.

I første række fastslog Domstolen, at offentlighedens adgang til oplysninger om de reelle ejere, der var fastsat i det ændrede hvidvaskdirektiv, udgjorde et alvorligt indgreb i de grundlæggende rettigheder til respekt for privatlivet og til beskyttelse af personoplysninger, der er sikret i henholdsvis chartrets artikel 7 og 8.

²² Europa-Parlamentets og Rådets direktiv (EU) 2015/849 af 20.5.2015 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme, om ændring af Europa-Parlamentets og Rådets forordning (EU) nr. 648/2012 og om ophævelse af Europa-Parlamentets og Rådets direktiv 2005/60/EF samt Kommissionens direktiv 2006/70/EF (EUT 2015, L 141, s. 73, herefter »hvidvaskdirektivet«).

²³ I henhold til hvidvaskdirektivets artikel 3, nr. 6), er de reelle ejere den eller de fysiske personer, der i sidste ende ejer eller kontrollerer kunden og/eller den eller de fysiske personer, på hvis vegne en transaktion eller en aktivitet gennemføres.

²⁴ Europa-Parlamentets og Rådets direktiv (EU) 2018/843 af 30.5.2018 om ændring af direktiv (EU) 2015/849 om forebyggende foranstaltninger mod anvendelse af det finansielle system til hvidvask af penge eller finansiering af terrorisme og om ændring af direktiv 2009/138/EF og 2013/36/EU (EUT 2018, L 156, s. 43).

²⁵ Ugyldighed af artikel 1, nr. 15), litra c), i direktiv 2018/843, der ændrede hvidvaskdirektivets artikel 30, stk. 5, første afsnit, litra c).

Domstolen bemærkede i denne henseende, at eftersom de omhandlede oplysninger indeholder oplysninger om identificerede fysiske personer, nemlig de reelle ejere af selskaber og andre juridiske enheder etableret på medlemsstaternes område, berører tilgængeligheden af disse oplysninger for ethvert medlem af offentligheden den grundlæggende ret til respekt for privatlivet. Oplysningernes tilrådighedsstillelse for offentligheden udgør desuden en behandling af personoplysninger. Domstolen tilføjede, at en sådan tilrådighedsstillelse for offentligheden udgør et indgreb i de to ovennævnte grundlæggende rettigheder, uanset hvad de videregivne oplysninger efterfølgende bruges til.

Hvad angår alvoren af dette indgreb bemærkede Domstolen, at for så vidt som de oplysninger, der stilles til rådighed for offentligheden, vedrører identiteten af den reelle ejer samt arten og omfanget af den reelle ejers rettigheder i selskaber eller andre juridiske enheder, kan oplysningerne gøre det muligt at tegne en profil vedrørende visse personlige identifikationsoplysninger, den pågældendes økonomiske situation samt de økonomiske sektorer, lande og virksomheder, som den pågældende reelle ejer har investeret i. Disse oplysninger bliver endvidere tilgængelige for et potentielt ubegrænset antal personer, således at en sådan behandling af personoplysninger ligeledes kan gøre det muligt for personer – der af andre hensyn end det mål, der forfølges med denne foranstaltning, ønsker at få oplysninger om bl.a. en reel ejers materielle og økonomiske situation – frit at få adgang til de nævnte oplysninger. Denne mulighed er så meget desto lettere, når oplysningerne kan tilgås på internettet. Endvidere forværres de potentielle konsekvenser for de registrerede, der følger af et eventuelt misbrug af deres oplysninger, af det forhold, at disse oplysninger, når de først er gjort tilgængelige for offentligheden, ikke blot kan tilgås frit, men også lagres og spredes, og at det bliver endnu vanskeligere eller endog illusorisk for de pågældende personer at forsvare sig effektivt mod misbrug.

I anden række bemærkede Domstolen i forbindelse med undersøgelsen af, om det omhandlede indgreb var begrundet, for det første, at legalitetsprincippet var overholdt i det foreliggende tilfælde. Begrænsning af udøvelsen af de ovennævnte grundlæggende rettigheder, der følger af offentlighedens adgang til oplysninger om de reelle ejere, var således fastsat i en lovgivningsmæssig retsakt, nemlig det ændrede hvidvaskdirektiv. Desuden præciserede det nævnte direktiv dels, at disse oplysninger skulle være passende, nøjagtige og aktuelle, og opregnede udtrykkeligt visse oplysninger, som skulle være tilgængelige for offentligheden. Dels fastsatte direktivet de betingelser, hvorunder medlemsstaterne kunne indrømme undtagelser til en sådan adgang.

For det andet bemærkede Domstolen, at det omhandlede indgreb ikke skader det væsentligste indhold af de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8. Selv om det var korrekt, at det ændrede hvidvaskdirektiv ikke indeholdt en udtømmende opregning af de oplysninger, som ethvert medlem af offentligheden skulle have adgang til, og at medlemsstaterne kan give adgang til supplerende oplysninger, forholdt det sig ikke desto mindre således, at kun passende oplysninger om de reelle

ejere og de reelle ejeres rettigheder blev indhentet, opbevaret og følgelig gjort tilgængelige for offentligheden, hvilket navnlig udelukkede informationer, der ikke står i et passende forhold til hvidvaskdirektivets formål. Det fremgik ikke, at tilrådighedsstillelse for offentligheden af oplysninger, der står i et sådant passende forhold, på nogen måde kunne skade det væsentligste indhold af de pågældende grundlæggende rettigheder.

For det tredje bemærkede Domstolen, at EU-lovgiver ved at fastsætte offentlighedens adgang til oplysninger om de reelle ejere har til hensigt at forebygge hvidvask af penge og finansiering af terrorisme ved gennem øget gennemsigtighed at skabe et miljø, der i mindre grad kan anvendes til disse formål, hvilket udgør et mål af almen interesse, der kan begrunde endog alvorlige indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8.

For det fjerde fastslog Domstolen i forbindelse med undersøgelsen af, om det omhandlede indgreb var egnet, nødvendigt og forholdsmæssigt, at offentlighedens adgang til oplysningerne om de reelle ejere ganske vist er egnet til at bidrage til virkeliggørelsen af dette formål.

Domstolen fandt imidlertid, at dette indgreb ikke kunne anses for at være begrænset til det strengt nødvendige. Dels kunne den strenge nødvendighed af det nævnte indgreb ikke godtgøres ved at støtte sig på den omstændighed, at kriteriet om »legitim interesse« – som enhver person, der ønskede at få adgang til oplysningerne om de reelle ejere, skulle godtgøre i henhold til hvidvaskdirektivet som affattet forud for ændringen ved direktiv 2018/843 – var vanskeligt at gennemføre, og at dets anvendelse ville kunne give anledning til vilkårlige afgørelser. Eventuelle vanskeligheder ved at opstille de præcise tilfælde og betingelser, hvorunder offentligheden kan tilgå oplysningerne om reelle ejere, kan nemlig ikke begrunde, at EU-lovgiver foreskriver, at offentligheden har adgang til disse oplysninger.

Dels kunne betragtningerne til direktiv 2018/843 heller ikke godtgøre, at det omhandlede indgreb var strengt nødvendigt ²⁶. For så vidt som det i disse betragtninger var anført, at offentlig adgang til oplysninger om reelt ejerskab skal give civilsamfundet, herunder pressen eller civilsamfundsorganisationer, bedre mulighed for at kontrollere oplysninger, bemærkede Domstolen, at såvel pressen som civilsamfundsorganisationer, der har en forbindelse til forebyggelsen og bekæmpelsen af hvidvask af penge og finansiering af terrorisme, har en legitim interesse i at tilgå de omhandlede oplysninger. Det samme gælder de personer, der ønsker at få kendskab til identiteten af de reelle ejere af et selskab eller en anden juridisk enhed, fordi de overvejer at indgå i transaktioner med disse, eller finansieringsinstitutter og myndigheder, der er involveret i bekæmpelsen af lovovertrædelser i forbindelse med hvidvask af penge eller finansiering af terrorisme.

²⁶ Der var tale om betragtningerne i 30. betragtning til direktiv 2018/843.

Desuden var det omhandlede indgreb heller ikke forholdsmæssigt. I denne henseende fastslog Domstolen, at de materielle regler, der regulerede indgrebet, ikke opfyldte kravet om klarhed og præcision. Det ændrede hvidvaskdirektiv bestemte nemlig, at ethvert medlem af offentligheden »mindst« skulle have adgang til de deri omhandlede oplysninger, og gav medlemsstaterne mulighed for at give adgang til supplerende oplysninger, hvilket som »minimum« omfattede den reelle ejers fødselsdato eller kontaktoplysninger. Ved anvendelsen af udtrykkene »mindst« og »minimum«, gav dette direktiv mulighed for, at oplysninger, der ikke er tilstrækkeligt definerede eller identificerbare, blev stillet til rådighed for offentligheden.

Hvad i øvrigt angår afvejningen af alvoren af dette indgreb og vigtigheden af det pågældende formål af almen interesse anerkendte Domstolen, at dette formål, henset til dets vigtighed, kan begrunde endog alvorlige indgreb i de grundlæggende rettigheder, som er sikret ved chartrets artikel 7 og 8.

For det første påhviler bekæmpelsen af hvidvask af penge og finansiering af terrorisme imidlertid først og fremmest offentlige myndigheder samt enheder, såsom kreditinstitutter eller finansieringsinstitutter, der på grund af deres aktiviteter er underlagt særlige forpligtelser på dette område. Af denne grund bestemte det ændrede hvidvaskdirektiv, at oplysningerne om reelt ejerskab i alle tilfælde skulle være tilgængelige for kompetente myndigheder og finansielle efterretningsenheder uden nogen begrænsninger samt for forpligtede enheder inden for rammerne af kundekendskabsproceduren ²⁷.

For det andet – i sammenligning med den tidligere ordning, der ud over kompetente myndigheders og visse enheders adgang til oplysningerne om de reelle ejere fastsatte adgang for enhver person eller organisation, der kunne godtgøre at have en legitim interesse heri – udgjorde den ordning, der blev indført med direktiv 2018/843, et langt mere alvorligt indgreb i de grundlæggende rettigheder, der er sikret ved chartrets artikel 7 og 8, uden at dette mere alvorlige indgreb kunne opvejes ved de eventuelle fordele, som denne sidstnævnte ordning kunne medføre i forhold til førstnævnte ordning for så vidt angår bekæmpelsen af hvidvask af penge og finansiering af terrorisme.

²⁷ Det ændrede hvidvaskdirektivs artikel 30, stk. 5, første afsnit, litra a) og b).

2. Overholdelse af retten til beskyttelse af personoplysninger ved EU-rettens gennemførelse

Dom af 21. december 2016 (Store Afdeling), Tele2 Sverige (forenede sager C-203/15 og C-698/15, [EU:C:2016:970](#))

I forlængelse af dommen i sagen Digital Rights Ireland og Seitlinger m.fl., hvorved direktiv 2006/24 blev erklæret ugyldigt (se ovenfor), blev der indbragt to sager for Domstolen angående den generelle forpligtelse til lagring af data om denne kommunikation, der i Sverige og i Det Forenede Kongerige påhvilede udbydere af elektroniske kommunikationstjenester en lagring, der var foreskrevet i henhold til det ugyldige direktiv.

Dagen efter, at dommen i sagen Digital Rights Ireland og Seitlinger m.fl. var blevet afsagt, meddelte telekommunikationsvirksomheden Tele2 Sverige den svenske myndighed for post- og teletilsyn, at den havde besluttet at ophøre med at lagre oplysninger, og at den agtede at slette allerede registrerede oplysninger (sag C-203/15). I henhold til svensk ret var udbydere af elektroniske kommunikationstjenester forpligtet til systematisk og uafbrudt og uden undtagelse at lagre samtlige trafikdata og lokaliseringsdata vedrørende samtlige abonnenter og registrerede brugere i forbindelse med samtlige midler til elektronisk kommunikation. I sag C-698/15 havde tre personer anlagt sag til prøvelse af den britiske ordning for lagring af oplysninger, der gav indenrigsministeren mulighed for at pålægge offentlige teleoperatører at lagre alle kommunikationsdata i en periode på højst 12 måneder, men ikke indholdet af kommunikationen.

Kammarrätten i Stockholm (appeldomstolen for forvaltningsretlige sager i Stockholm, Sverige) og Court of Appeal (England and Wales) (Civil Division) (appeldomstol (England og Wales) (afdelingen for civile sager, Det Forenede Kongerige)) anmodede Domstolen om en fortolkning af artikel 15, stk. 1, i direktiv 2002/58, det såkaldte »direktiv om databeskyttelse inden for elektronisk kommunikation«, der giver medlemsstaterne mulighed for at indskrænke den i direktivet omhandlede pligt til at sikre fortroligheden i forbindelse med elektronisk kommunikationen og de dermed forbundne trafikdata.

Domstolen fastslog i sin dom først og fremmest, at artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1, er til hinder for en national lovgivning, som den i Sverige omhandlede, 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 alle elektroniske kommunikationsmidler. Ifølge Domstolen overskrider en sådan lovgivning det strengt nødvendige og kan i et demokratisk samfund ikke anses for at være begrundet, således som det er påkrævet i henhold til den nævnte artikel 15, stk. 1, sammenholdt med de nævnte artikler i chartret.

Samme bestemmelse, sammenholdt med de samme artikler i chartret, er ligeledes til hinder for en national lovgivning, der regulerer beskyttelsen af og sikkerheden vedrørende trafikdata og lokaliseringsdata, og navnlig de kompetente nationale myndigheders adgang til de lagrede data, uden i forbindelse med bekæmpelsen af kriminalitet at begrænse denne adgang til målet om bekæmpelse af grov kriminalitet, uden at undergive den nævnte adgang en forudgående kontrol foretaget af en domstol eller af en uafhængig administrativ myndighed og uden at stille et krav om, at de pågældende data lagres på Unionens område.

Domstolen fastslog derimod, at artikel 15, stk. 1, i direktiv 2002/58 ikke er til hinder for, at en medlemsstat vedtager en lovgivning, der som en forebyggende foranstaltning muliggør en målrettet lagring af data af denne art med henblik på bekæmpelse af grov kriminalitet, forudsat at lagringen af disse data begrænses til det strengt nødvendige for så vidt angår kategorierne af data, der skal lagres, de omhandlede kommunikationsmidler, de berørte personer og den fastsatte varighed af lagringen. For at opfylde disse krav skal en sådan national lovgivning for det første fastsætte klare og præcise regler, der gør det muligt effektivt at beskytte deres personlige oplysninger mod risikoen for misbrug. Lovgivningen skal navnlig angive, under hvilke omstændigheder og på hvilke betingelser der i forebyggende øjemed kan vedtages en foranstaltning om lagring af data, hvorved det sikres, at en sådan foranstaltning begrænses til det strengt nødvendige. Hvad for det andet angår de materielle betingelser, som en national lovgivning skal opfylde, for at det sikres, at den er begrænset til det strengt nødvendige, skal lagringen af disse data altid opfylde objektive kriterier, som fastlægger et forhold mellem de data, der skal lagres, og det forfulgte mål. Navnlig skal sådanne betingelser i praksis være af en sådan art, at de faktisk kan afgrænse omfanget af foranstaltningen og følgelig den berørte personkreds. Hvad angår denne afgrænsning skal den nationale lovgivning være baseret på objektive forhold, der gør det muligt at fokusere målrettet på en personkreds, hvis data kan afsløre en forbindelse, i det mindste indirekte, til grov kriminalitet, bidrage til bekæmpelse af grov kriminalitet på den ene eller den anden måde eller forhindre en alvorlig fare for den offentlige sikkerhed.

II. Behandling af personoplysninger som omhandlet i den generelle lovgivning på området

1. Den generelle lovgivnings anvendelsesområde

Dom af 30. maj 2006 (Store Afdeling), Parlamentet mod Rådet (C-317/04 og C-318/04, [EU:C:2006:346](#))

Efter terrorangrebene den 11. september 2001 vedtog USA en lovgivning, hvorefter luftfartsselskaber, der foretager flyvninger til, fra eller over USA, skulle give de

amerikanske myndigheder elektronisk adgang til oplysningerne i luftfartsselskabernes reservations-/afgangskontrolsystemer, dvs. deres »Passenger Name Records« (PNR).

Kommissionen var af den opfattelse, at disse bestemmelser kunne være i strid med EU-lovgivningen og medlemsstaternes lovgivning om databeskyttelse, og indledte derfor forhandlinger med de amerikanske myndigheder. Efter afslutningen af disse forhandlinger vedtog Kommissionen den 14. maj 2004 beslutning 2004/535/EF²⁸, hvori den konstaterede, at United States Bureau of Customs and Border Protection (USA's told- og grænsekontrolmyndighed, herefter »CBP«) sikrer en passende beskyttelse af de PNR-oplysninger, der overføres fra Fællesskabet (herefter »beslutningen om tilstrækkelig beskyttelse«). Dernæst vedtog Rådet den 17. maj 2004 afgørelse 2004/496/EF²⁹ om godkendelse af indgåelsen af en aftale mellem Det Europæiske Fællesskab og USA om medlemsstaternes luftfartsselskabers behandling og overførsel til CBP af PNR-oplysninger.

Europa-Parlamentet nedlagde påstand om, at Domstolen annullerede ovennævnte beslutning og afgørelse, og gjorde navnlig gældende, at beslutningen om tilstrækkelig beskyttelse var blevet vedtaget ved overskridelse af Kommissionens beføjelser, at artikel 95 EF (nu artikel 114 TEUF) ikke udgjorde den rette hjemmel for afgørelsen om indgåelse af aftalen, og at de grundlæggende rettigheder i begge tilfælde var blevet tilsidesat.

Med hensyn til beslutningen om tilstrækkelig beskyttelse undersøgte Domstolen først, om Kommissionen gyldigt kunne vedtage sin beslutning på grundlag af direktiv 95/46. Domstolen konstaterede i denne forbindelse, at det fulgte af beslutningen om tilstrækkelig beskyttelse, at videregivelsen af PNR-oplysninger til CBP udgør en behandling, der vedrører den offentlige sikkerhed og statens aktiviteter på det strafferetlige område. Domstolen fastslog, at, selv om PNR-oplysningerne først blev indsamlet af luftfartsselskaberne som led i en aktivitet, der er underlagt EU-retten, nemlig salg af en flybillet, der giver ret til en tjenesteydelse, var den behandling af oplysningerne, der var tale om i beslutningen om tilstrækkelig beskyttelse, imidlertid af en helt anden art. Beslutningen vedrørte således ikke en behandling af oplysninger, der var nødvendig for at levere en tjenesteydelse, men en behandling, som anses for nødvendig for at beskytte den offentlige sikkerhed og for at nå retshåndhævende mål.

Domstolen bemærkede i denne forbindelse, at den omstændighed, at PNR-oplysningerne blev indsamlet af private erhvervsdrivende til kommercielle formål, og at det var disse erhvervsdrivende, som forestod oplysningernes videregivelse til en tredjestat, ikke var til hinder for, at den omhandlede overførsel kunne anses for en behandling, der var udelukket fra direktivets anvendelsesområde. Videregivelsen skete

²⁸ Kommissionens beslutning 2004/535/EF af 14.5.2004 om tilstrækkelig beskyttelse af personoplysninger, der er indeholdt i registre over flypassagerer, og som videregives til Amerikas Forenede Staters told- og grænsekontrolmyndighed (Bureau of Customs and Border Protection) (EUT 2004, L 235, s. 11).

²⁹ Rådets afgørelse 2004/496/EF af 17.5.2004 om indgåelse af en aftale mellem Det Europæiske Fællesskab og Amerikas Forenede Stater om luftfartsselskabers behandling og overførsel af PNR-oplysninger til United States Department of Homeland Security, Bureau of Customs and Border Protection (EUT 2004, L 183, s. 168).

nemlig inden for rammer, der var indført af de statslige myndigheder, og som vedrørte den offentlige sikkerhed. Domstolen fastslog derfor, at beslutningen om tilstrækkelig beskyttelse ikke var omfattet af direktivets anvendelsesområde, idet den vedrørte en behandling af personoplysninger, der var udelukket fra dette anvendelsesområde. Domstolen annullerede derfor beslutningen om tilstrækkelig beskyttelse.

Med hensyn til Rådets afgørelse fastslog Domstolen, at artikel 95 EF, sammenholdt med artikel 25 i direktiv 95/46, ikke gav Fællesskabet kompetence til at indgå den pågældende aftale med USA. Aftalen vedrørte nemlig samme videregivelse af oplysninger, som var omhandlet i beslutningen om tilstrækkelig beskyttelse, og dermed vedrørte aftalen behandling af oplysninger, der var udelukket fra direktivets anvendelsesområde. Domstolen annullerede derfor Rådets afgørelse om godkendelse af indgåelse af aftalen.

Dom af 13. maj 2014 (Store Afdeling), Google Spain og Google (C-131/12, [EU:C:2014:317](#))

I 2010 indgav en spansk statsborger en klage til Agencia Española de Protección de Datos (databeskyttelsesagenturet, herefter »AEPD«) over La Vanguardia Ediciones SL, som udgiver en avis med et stort oplagstal, og over Google Spain og Google. Den pågældende gjorde gældende, at internetbrugere ved en søgning på hans navn på Googlekoncernens søgemaskine fik vist et link til to sider i avisen La Vanguardia fra 1998 med en annonce vedrørende en tvangsauktion over fast ejendom i forbindelse med en beslaglæggelse på grund af gæld. Med klagen krævede den pågældende for det første, at La Vanguardia blev pålagt enten at fjerne eller ændre disse sider eller at anvende visse værktøjer i søgemaskinerne til beskyttelse af disse oplysninger. For det andet krævede den pågældende, at Google Spain eller Google blev pålagt at fjerne eller skjule hans personoplysninger, således at de ikke længere indgik i søgeresultaterne og ikke længere fremgik af linkene til La Vanguardia.

AEPD afviste klagen over La Vanguardia, idet dennes offentliggørelse af de omhandlede oplysninger var retligt begrundet, men for så vidt angik Google Spain og Google fik den pågældende derimod medhold i klagen, og de to selskaber blev pålagt at træffe de nødvendige foranstaltninger med henblik på at fjerne personoplysninger fra deres indeks og forhindre fremtidig adgang. De to selskaber anlagde to søgsmål ved Audiencia Nacional (domstol i visse straffe-, forvaltnings- og arbejdsretlige sager, Spanien) med påstand om annullation af AEPD's afgørelse, og den spanske domstol forelagde Domstolen en række spørgsmål.

I denne dom udtalte Domstolen sig ligeledes om det territoriale anvendelsesområde for direktiv 95/46.

Domstolen fastslog således, at behandling af personoplysninger foretages som led i aktiviteter, der inden for en medlemsstats område udføres af en registeransvarligs virksomhed som omhandlet i direktiv 95/46, når en søgemaskineudbyder, selv om denne har sit hovedsæde i et tredjeland, etablerer en filial eller et datterselskab i en

medlemsstat, der skal sørge for reklame og salg af reklameplads i søgemaskinen, og hvis aktivitet er rettet mod indbyggerne i denne medlemsstat.

Under sådanne omstændigheder er søgemaskineudbyderens aktiviteter og de aktiviteter, der foretages af søgemaskineudbyderens virksomhed eller organ i en medlemsstat, nemlig uløseligt forbundne, eftersom aktiviteterne vedrørende reklameplads udgør midlet, der gør den omhandlede søgemaskine økonomisk rentabel, og denne søgemaskine samtidig er det middel, der gør det muligt at gennemføre aktiviteterne.

Dom af 11. december 2014, Ryneš (C-212/13, [EU:C:2014:2428](#))

Efter at være blevet angrebet flere gange havde František Ryneš installeret et overvågningskamera på sit hus. Efter et nyt angreb mod huset var det takket være kamerasystemet muligt at identificere to mistænkte, hvilke der blev indledt en straffesag imod. En af de anklagede bestred lovligheden af behandlingen af data fra overvågningskameraet ved det tjekkiske kontor for beskyttelse af personoplysninger, og kontoret konstaterede, at František Ryneš havde overtrådt reglerne for beskyttelse af personoplysninger, og pålagde ham en bøde.

František Ryneš iværksatte appel af en afgørelse fra Městský soud v Praze (byretten i Prag, Den Tjekkiske Republik), der havde stadfæstet kontorets afgørelse, ved Nejvyšší správní soud (øverste domstol i forvaltningsretlige sager, Den Tjekkiske Republik), som forelagde Domstolen et spørgsmål om, hvorvidt František Ryneš' optagelse med henblik på at beskytte sit liv, sin sundhed og sin ejendom udgjorde en databehandling, der ikke var omfattet af direktiv 95/46 med den begrundelse, at denne optagelse var blevet foretaget af en fysisk person med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter som omhandlet i direktivets artikel 3, stk. 2, andet led.

Domstolen fastslog, at anvendelse af et kamerasystem til at optage videoer af personer, der kontinuerligt bliver opbevaret på en optagerenhed, såsom en harddisk, hvilket system er blevet installeret af en fysisk person på den pågældendes familiebolig med henblik på at beskytte boligens ejeres ejendom, sundhed og liv, idet dette system også overvåger et offentligt rum, ikke udgør behandling af personoplysninger, som foretages med henblik på udøvelse af rent personlige eller familiemæssige aktiviteter.

Den fremhævede i denne forbindelse, at beskyttelsen af den grundlæggende ret til respekt for privatlivet som sikret ved chartrets artikel 7 kræver, at undtagelserne fra og begrænsningerne af beskyttelsen af personoplysninger skal holdes inden for det strengt nødvendige. Henset til, at bestemmelserne i direktiv 95/46, for så vidt som de omhandler behandling af personoplysninger, der kan krænke de grundlæggende frihedsrettigheder og navnlig privatlivets fred, nødvendigvis skal fortolkes under hensyntagen til de grundlæggende rettigheder, som er opført i nævnte charter, skal undtagelsen i direktivets artikel 3, stk. 2, andet led, undergives en streng fortolkning. Endvidere kan det af selve bestemmelsens ordlyd udledes, at behandlingen af

oplysninger med henblik på udøvelse af »rent« personlige eller familiemæssige aktiviteter ikke er omfattet af anvendelsesområdet for direktiv 95/46. Hvis en videoovervågning dækker et offentligt område – om end kun delvist – og derfor optager uden for det private rum, som den, der gennem overvågningen foretager behandlingen af disse oplysninger, befinder sig i, kan den ikke anses for en rent »personlig eller familiemæssig« aktivitet som omhandlet i nævnte bestemmelse.

Dom af 16. januar 2024 (Store Afdeling), Österreichische Datenschutzbehörde (C-33/22, [EU:C:2024:46](#))

Med henblik på at undersøge, om Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (forbundsautoritet til beskyttelse af forfatningen og bekæmpelse af terrorisme, Østrig)³⁰ eventuelt var blevet udsat for politisk påvirkning, nedsatte Nationalrat (nationalrådet, Østrig) en undersøgelseskommission (herefter »undersøgelseskommissionen vedrørende forbundskontoret«). Denne kommission hørte WK som vidne. Til trods for WK's anmodning om anonymitet blev referatet af denne høring, hvori WK's fulde for- og efternavn var nævnt, offentliggjort på Parlament Österreichs (det østrigske parlament) websted. WK indgav en klage til Österreichische Datenschutzbehörde (databeskyttelsesmyndighed, Østrig) (herefter »Datenschutzbehörde«), idet han gjorde gældende, at en sådan videregivelse af hans identitet var i strid med databeskyttelsesforordningen og østrigsk lovgivning. Ved afgørelse af 18. september 2019 fandt Datenschutzbehörde, at den ikke havde kompetence til at træffe afgørelse om klagen, idet den anførte, at princippet om magtadskillelse udelukkede, at denne myndighed som et organ under den udøvende magt kunne kontrollere undersøgelseskommissionen vedrørende forbundskontoret, der henhører under den lovgivende magt.

Efter at Bundesverwaltungsgericht (forbundsdomstol i forvaltningsretlige sager, Østrig) havde taget stilling til sagen, idet den tog WK's søgsmål til følge og annullerede Datenschutzbehörde's afgørelse, iværksatte WK revisionsanke ved Verwaltungsgerichtshof (forvaltningsdomstol, Østrig) til prøvelse af afgørelsen fra Bundesverwaltungsgericht (forbundsdomstol i forvaltningsretlige sager).

I denne sammenhæng forelagde den forelæggende ret Domstolen spørgsmålet om, hvorvidt de aktiviteter, der udøves af en undersøgelseskommission, som er nedsat af en medlemsstats parlament, er omfattet af databeskyttelsesforordningens anvendelsesområde, og om denne forordning finder anvendelse, når disse aktiviteter vedrører beskyttelsen af statens sikkerhed.

For det første fremhævede Domstolen, at databeskyttelsesforordningens artikel 2, stk. 2, litra a), som fastsætter, at denne forordning ikke finder anvendelse på behandling af

³⁰ Den 1.12.2021 blev denne enhed til »Direktion Staatsschutz und Nachrichtendienst« (direktorat for statens sikkerhed og efterretningstjenester, Østrig).

personoplysninger i forbindelse med en aktivitet, der ikke er omfattet af EU-rettens anvendelsesområde, udelukkende har til formål at udelukke behandling, der foretages af statslige myndigheder under udøvelse af en aktivitet, som tilsigter at beskytte statens sikkerhed, eller som henhører under samme kategori, fra dens anvendelsesområde. Den omstændighed alene, at en aktivitet er statens eller en offentlig myndigheds, er således ikke tilstrækkelig til automatisk at udelukke, at databeskyttelsesforordningen kan finde anvendelse på en sådan aktivitet.

Denne fortolkning, der følger af den manglende sondring på grundlag af identiteten af den, der har foretaget den pågældende behandling, bekræftes af databeskyttelsesforordningens artikel 4, nr. 7)³¹.

Domstolen præciserede, at den omstændighed, at undersøgelseskommissionen vedrørende forbundskontoret havde parlamentarisk karakter, ikke indebar, at de aktiviteter, som denne undersøgelseskommission udførte, var udelukket fra databeskyttelsesforordningens anvendelsesområde. Den undtagelse, der er fastsat i denne forordnings artikel 2, stk. 2, litra a), henviser nemlig kun til kategorier af aktiviteter, der som følge af deres art ikke er omfattet af EU-rettens anvendelsesområde, og ikke til kategorier af personer. Den omstændighed, at behandlingen af personoplysninger foretages af en undersøgelseskommission, der er nedsat af en medlemsstats parlament under udøvelsen af dette parlaments beføjelse til at kontrollere den udøvende magt, gør det derfor ikke i sig selv muligt at godtgøre, at denne behandling foretages i forbindelse med en aktivitet, der ikke er omfattet af EU-rettens anvendelsesområde.

For det andet bemærkede Domstolen, at selv om det tilkommer medlemsstaterne at fastsætte deres væsentlige sikkerhedsinteresser og at træffe de nødvendige foranstaltninger til at beskytte deres sikkerhed³², kan alene den omstændighed, at en national foranstaltning er blevet truffet med henblik på at beskytte den nationale sikkerhed, ikke medføre, at EU-retten ikke finder anvendelse, og fritage medlemsstaterne fra at sikre den nødvendige overholdelse af denne ret. Den undtagelse, der er fastsat i databeskyttelsesforordningens artikel 2, stk. 2, litra a), henviser imidlertid kun til kategorier af aktiviteter, der som følge af deres art ikke er omfattet af EU-rettens anvendelsesområde. I denne henseende er den omstændighed, at den dataansvarlige er en offentlig myndighed, hvis hovedaktivitet er at varetage statens sikkerhed, ikke i sig selv tilstrækkelig til at udelukke den behandling af personoplysninger, som denne myndighed foretager i forbindelse med andre aktiviteter, fra databeskyttelsesforordningens anvendelsesområde.

I det foreliggende tilfælde syntes den politiske kontrol, som undersøgelseskommissionen vedrørende forbundskontoret udførte, ikke som sådan at

³¹ I denne bestemmelse defineres begrebet »dataansvarlig« som en henvisning til »en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger«.

³² I overensstemmelse med artikel 4, stk. 2, TEU.

udgøre en aktivitet, der har til formål at beskytte statens sikkerhed, eller som henhører under samme kategori. Med forbehold for den forelæggende rets efterprøvelse faldt denne aktivitet således ikke uden for databeskyttelsesforordningens anvendelsesområde.

Når dette er sagt, kan en parlamentarisk undersøgelseskommision få adgang til personoplysninger, som af hensyn til statens sikkerhed skal nyde særlig beskyttelse. I denne henseende kan der ved lovgivningsmæssige foranstaltninger fastsættes begrænsninger for de forpligtelser og rettigheder, der følger af databeskyttelsesforordningen, bl.a. af hensyn til statens sikkerhed ³³. På dette grundlag er det således muligt at begrunde begrænsninger vedrørende indsamling af personoplysninger, underretning af de registrerede og disses adgang til de nævnte oplysninger eller videregivelse af disse oplysninger uden de registreredes samtykke til andre personer end den dataansvarlige, for så vidt som sådanne begrænsninger respekterer det væsentligste indhold af de registreredes grundlæggende rettigheder og frihedsrettigheder og er en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund.

Domstolen bemærkede imidlertid, at det af de oplysninger, som Domstolen rådede over, ikke fremgik, at undersøgelseskommisionen vedrørende forbundskontoret havde hævdet, at videregivelse af den registreredes personoplysninger var nødvendig for at beskytte statens sikkerhed og var baseret på en national lovgivningsmæssig foranstaltning, der var fastsat med henblik herpå, hvilket det tilkom den forelæggende ret at efterprøve.

2. Begrebet »personoplysninger«

Dom af 19. oktober 2016, Breyer (C-582/14, [EU:C:2016:779](#))

Patrick Breyer havde anlagt et søgsmål ved de tyske civile domstole med påstand om, at Forbundsrepublikken Tyskland forbydes at opbevare eller gennem tredjemand at opbevare de elektroniske oplysninger, der overføres ved hver søgning på de tyske forbundsinstitutioners websteder. Med henblik på at afværge angreb og gøre det muligt at forfølge »angriberne« strafferetligt registrerede udbyderen af online-medietjenester til de tyske forbundsinstitutioner oplysninger i form af en »dynamisk« IP-adresse, dvs. en IP-adresse, der ændres ved hver ny tilslutning til internettet, samt dato og tidspunkt for søgningen på siden. Til forskel fra statiske IP-adresser gør de dynamiske IP-adresser det ikke umiddelbart muligt ved hjælp af filer, der er tilgængelige for offentligheden, at foretage en kobling mellem en given computer og den fysiske tilslutning til det net, som

³³ Ifølge databeskyttelsesforordningens artikel 23.

anvendes af internetudbyderen. De registrerede oplysninger alene var ikke nok til, at udbyderen af online-medietjenester kunne identificere brugeren. Internetudbyderen var derimod i besiddelse af supplerende oplysninger, der sammenholdt med IP-adressen gjorde det muligt at identificere den pågældende bruger.

Bundesgerichtshof (forbundsdomstol, Tyskland), for hvilken der var iværksat en »revisionsanke«, forelagde Domstolen et spørgsmål om, hvorvidt en IP-adresse, som en udbyder af online-medietjenester lagrer i forbindelse med en søgning på dennes websted, udgør en personoplysning for denne udbyders vedkommende.

Domstolen fastslog først, at det, for at en oplysning kan kvalificeres som »personoplysning« som omhandlet i artikel 2, litra a), i direktiv 95/46, ikke er påkrævet, at alle de oplysninger, der gør det muligt at identificere den registrerede, skal befinde sig hos en enkelt person. Det forhold, at den yderligere viden, som kræves for at identificere brugeren af en internetseite, indehaves ikke af udbyderen af online-medietjenester, men af denne brugers internetudbyder, synes således ikke at kunne udelukke, at de dynamiske IP-adresser, der er registreret af udbyderen af online-medietjenester, for denne udgør personoplysninger som omhandlet i artikel 2, litra a), i direktiv 95/46.

Domstolen konstaterede derfor, at en dynamisk IP-adresse, som en udbyder af online-medietjenester registrerer i forbindelse med en søgning foretaget af en person på en internetseite, som denne udbyder gør tilgængelig for offentligheden, i forhold til den nævnte udbyder udgør en personoplysning som omhandlet i artikel 2, litra a), i direktiv 95/46, når udbyderen råder over lovlige hjælpemidler, der gør det muligt for denne at få identificeret den registrerede gennem den yderligere viden om personen, som denne persons internetudbyder råder over.

Dom af 20. december 2017, Nowak (C-434/16, [EU:C:2017:994](#))

Peter Nowak, en regnskabs elev, var dumpet til en eksamen tilrettelagt af brancheorganisationen for Irlands revisorer/skatterådgivere (herefter »CAI«). Han indgav en anmodning om indsigt i henhold til databeskyttelseslovens section 4 med hensyn til alle personoplysninger om ham, som CAI var i besiddelse af. CAI sendte nogle dokumenter til Peter Nowak, men afslog at udlevere hans prøvebesvarelse med den begrundelse, at den ikke indeholdt personoplysninger som omhandlet i databeskyttelsesloven.

Da den tilsynsførende for databeskyttelse heller ikke imødekom Peter Nowaks anmodning om aktindsigt, anlagde han sag ved de nationale domstole. Supreme Court (øverste domstol, Irland), ved hvilken Peter Nowak havde iværksat appel, forelagde Domstolen et spørgsmål, hvorved den nærmere bestemt ønskede oplyst, om artikel 2, litra a), i direktiv 95/46 skal fortolkes således, at en skriftlig besvarelse, som en deltager har givet i forbindelse med en faglig prøve, og eksaminators eventuelle rettelser og kommentarer til denne besvarelse under omstændigheder som de i hovedsagen omhandlede udgør personoplysninger i denne bestemmelses forstand.

For det første fastslog Domstolen, at det, for at en oplysning kan kvalificeres som »personoplysning« som omhandlet i artikel 2, litra a), i direktiv 95/46, ikke er påkrævet, at alle de oplysninger, der gør det muligt at identificere den registrerede, skal befinde sig hos en enkelt person. I det tilfælde, hvor eksaminator ikke kender deltagerens identitet ved rettelsen af den pågældendes besvarelse i forbindelse med en prøve, råder den enhed, som afholder prøven, her CAI, derimod over de nødvendige oplysninger til uden vanskeligheder eller tvivl at identificere deltageren ved hjælp af den pågældendes identifikationsnummer, som er anbragt på prøvebesvarelsen eller på dennes omslag, og således til at tillægge denne besvarelse.

For det andet konstaterede Domstolen, at en skriftlig besvarelse, som en deltager har givet i forbindelse med en faglig prøve, udgør personoplysninger. Indholdet af denne besvarelse afspejler således deltagerens viden og kompetence inden for et givent område samt i givet fald hans tankegang, dømmekraft og kritiske sans. I øvrigt har indsamlingen af disse besvarelser til formål at evaluere deltagerens faglige kompetencer og hans evne til at udøve det pågældende erhverv. Desuden kan brugen af denne information, som bl.a. udmønter sig i, at deltageren består eller dumper til den pågældende prøve, have indvirkning på dennes rettigheder og interesser, idet denne brug f.eks. kan afgøre eller påvirke hans chancer for at få adgang til det erhverv eller den stilling, der ønskes opnået. Konstateringen af, at den skriftlige besvarelse, som en deltager har givet i forbindelse med en faglig prøve, udgør information om denne deltager som følge af dens indhold, formål og virkning, gælder i øvrigt også, når der er tale om en prøve med alle hjælpemidler.

For det tredje bemærkede Domstolen hvad angår eksaminators rettelser og kommentarer til deltagerens besvarelse, at disse ligesom den besvarelse, som deltageren har givet i forbindelse med prøven, udgør information om denne deltager, eftersom de afspejler eksaminators mening om eller bedømmelse af deltagerens individuelle præstation til prøven og især af hans viden og kompetence på det pågældende område. Rettelserne og kommentarerne har i øvrigt netop til formål at dokumentere eksaminators evaluering af deltagerens præstation og kan således have virkninger for sidstnævnte.

For det fjerde fastslog Domstolen, at den skriftlige besvarelse, som en deltager har givet i forbindelse med en faglig prøve, og eksaminators eventuelle rettelser og kommentarer til besvarelsen kan underkastes en efterprøvelse især med hensyn til deres nøjagtighed og nødvendigheden af deres opbevaring som omhandlet i artikel 6, stk. 1, litra d) og e), i direktiv 95/46 og kan berigtiges eller slettes i henhold til direktivets artikel 12, litra b). Den omstændighed, at en deltager gives ret til indsigt i denne besvarelse og disse rettelser og kommentarer i medfør af direktivets artikel 12, litra a), har til formål at sikre beskyttelsen af deltagerens ret til privatliv i forbindelse med behandlingen af hans personoplysninger, uafhængigt af om deltageren også har en sådan ret til indsigt i medfør af den nationale lovgivning, som finder anvendelse på prøven. Domstolen fremhævede imidlertid, at retten til indsigt og til berigtigelse i artikel 12, litra a) og b), i

direktiv 95/46 ikke omfatter eksamensspørgsmålene, der ikke som sådan udgør deltagerens personoplysninger.

Henset hertil konkluderede Domstolen, at en skriftlig besvarelse, som en deltager har givet i forbindelse med en faglig prøve, og eksaminators eventuelle rettelser og kommentarer til denne besvarelse, under omstændigheder som de i hovedsagen omhandlede udgør personoplysninger som omhandlet i artikel 2, litra a), i direktiv 95/46.

3. Begrebet »behandling af personoplysninger«

Dom af 6. november 2003 (Store Afdeling), Lindqvist (C-101/01, [EU:C:2003:596](#))

Bodil Lindqvist, der arbejdede som frivillig i en protestantisk sognekirke i Sverige, havde fra sin egen computer oprettet internetsider, hvorpå hun offentliggjorde personoplysninger vedrørende en række personer, der ligesom hun arbejdede som frivillige i den pågældende sognekirke. Bodil Lindqvist blev idømt en bøde med den begrundelse, at hun havde behandlet personoplysninger elektronisk uden først at have indgivet skriftlig anmeldelse til Datainspektionen (offentligt organ, der beskytter elektronisk overførte oplysninger), at hun uden tilladelse havde videregivet personoplysningerne til et tredjeland, og at hun havde behandlet følsomme personoplysninger.

I forbindelse med den appel, som Bodil Lindqvist iværksatte af denne afgørelse ved Göta hovrätt (appeldomstolen for Götaland, Sverige), indgav denne en anmodning om en præjudiciel afgørelse til Domstolen, idet den nærmere bestemt ønskede oplyst, om Bodil Lindqvist havde foretaget »behandling af personoplysninger, der helt eller delvis foretages ved hjælp af edb« i den forstand, hvori udtrykket er anvendt i direktiv 95/46.

Domstolen konstaterede, at en operation, der består i på en internetside at henvise til forskellige personer, og i at identificere dem ved navn eller på anden måde, f.eks. ved at oplyse deres telefonnummer eller ved at give oplysninger om deres arbejdsforhold og fritidsinteresser, udgør en »behandling af personoplysninger, der helt eller delvis foretages ved hjælp af edb« i den forstand, hvori udtrykket er anvendt i direktivet. En sådan behandling af personoplysninger, der foretages i forbindelse med udøvelse af frivillige eller religiøse aktiviteter, er ikke omfattet af nogen af undtagelserne fra direktivets anvendelsesområde, for så vidt som der hverken er tale om aktiviteter, der vedrører den offentlige sikkerhed, eller om rent personlige eller familiemæssige aktiviteter, der ikke er omfattet af direktivets anvendelsesområde.

Dom af 13. maj 2014 (Store Afdeling), Google Spain og Google (C-131/12, [EU:C:2014:317](#))

I denne dom (se ligeledes afsnit II.1 med overskriften »Den generelle lovgivnings anvendelsesområde«) havde Domstolen lejlighed til at præcisere begrebet »behandling af personoplysninger« på internettet i forhold til direktiv 95/46.

Domstolen fastslog således, at en søgemaskines aktivitet, der består i at finde oplysninger, der er offentliggjort eller lagt på internettet af tredjemand, indeksere disse automatisk, lagre dem midlertidigt og sluttelig gøre dem tilgængelige for internetbrugerne i en vis prioriteret orden, skal kvalificeres som behandling af personoplysninger, når oplysningerne indeholder personoplysninger. Domstolen fremhævede endvidere, at de operationer, der er omhandlet i direktivet, skal kvalificeres som behandling, også når de udelukkende vedrører oplysninger, der som sådan allerede har været offentliggjort i medierne. En generel undtagelse fra at anvende direktivet i dette tilfælde ville i vid udstrækning gøre direktivet indholdsløst.

Dom af 10. juli 2018 (Store Afdeling), Jehovan todistajat (C-25/17, [EU:C:2018:551](#))

Den finske databeskyttelsesmyndighed havde truffet en afgørelse, som forbød trossamfundet Jehovas Vidner at indsamle eller behandle personoplysninger i forbindelse med dets medlemmers forkyndelsesvirksomhed fra dør til dør uden at overholde de i den finske lovgivning om behandling af sådanne oplysninger fastsatte betingelser. Medlemmerne af dette trossamfund tager nemlig i forbindelse med deres forkyndelsesvirksomhed fra dør til dør notater om besøgene hos personer, som de pågældende selv og trossamfundet ikke har kendskab til. Disse oplysninger indsamles som en hukommelseshjælp med henblik på at kunne hentes frem igen i forbindelse med et eventuelt senere besøg, uden at de berørte personer har givet tilladelse dertil eller er blevet informeret derom. I denne forbindelse har trossamfundet Jehovas Vidner givet sine medlemmer retningslinjer vedrørende disse notater, som er gengivet i mindst ét af trossamfundets tidsskrifter om forkyndelsesvirksomhed.

Domstolen fastslog, at et trossamfunds medlemmers indsamling af personoplysninger i forbindelse med forkyndelsesvirksomhed fra dør til dør og den efterfølgende behandling af disse personoplysninger ikke er omfattet af undtagelserne fra anvendelsesområdet for direktiv 95/46, eftersom disse aktiviteter hverken udgør behandling af personoplysninger, som foretages under udøvelsen af aktiviteter som omhandlet i direktivets artikel 3, stk. 2, første led, eller behandling af personoplysninger foretaget af fysiske personer ved udøvelsen af en rent personlig eller familiemæssig aktivitet som omhandlet i direktivets artikel 3, stk. 2, andet led.

Dom af 22. juni 2021 (Store Afdeling), Latvijas Republikas Saeima (Strafpoint) (C-439/19, [EU:C:2021:504](#))

En fysisk person, B, var blevet pålagt strafpoint som følge af en eller flere færdselsforseelser. Ceļu satiksmes drošības direkcija (direktoratet for færdselssikkerhed, Letland) (herefter »CSDD«) indførte disse strafpoint i det nationale register over køretøjer og førere.

I henhold til den lettiske færdselslov³⁴ var oplysningerne om de strafpoint, som blev pålagt bilister, og som var indeholdt i dette register, tilgængelige for offentligheden, og CSDD videregav disse oplysninger til enhver, der anmodede herom, uden at vedkommende skulle godtgøre en særlig interesse i at få de nævnte oplysninger, herunder erhvervsdrivende med henblik på videreanvendelse. Eftersom B nærede tvivl om lovligheden af denne lovgivning, anlagde B et forfatningssøgsmål ved Latvijas Republikas Satversmes tiesa (forfatningsdomstol, Letland), med henblik på at denne domstol skulle undersøge denne lovgivnings forenelighed med retten til respekt for privatlivet.

Latvijas Republikas Satversmes tiesa (forfatningsdomstol) fandt, at den som led i sin forfatningsretlige bedømmelse skulle tage hensyn til databeskyttelsesforordningen. Den anmodede derfor Domstolen om at afklare rækkevidden af flere af databeskyttelsesforordningens bestemmelser med henblik på at afgøre, om den lettiske færdselslov var forenelig med denne forordning.

Med sin dom, der blev afsagt i Store Afdeling, fastslog Domstolen, at behandlingen af personoplysninger vedrørende strafpoint udgør »behandling af personoplysninger vedrørende straffedomme og lovovertrædelser«³⁵, for hvilken databeskyttelsesforordningen fastsatte en øget beskyttelse som følge af de pågældende oplysningers særlige følsomhed.

Domstolen bemærkede i denne forbindelse indledningsvis, at oplysninger vedrørende strafpoint udgør personoplysninger, og at CSDD's videregivelse heraf til tredjemand udgjorde behandling, som henhørte under databeskyttelsesforordningens materielle anvendelsesområde. Dette anvendelsesområde er nemlig meget vidt, og behandlingen henhørte ikke under undtagelserne til forordningens anvendelighed.

Denne behandling var således for det første ikke omfattet af undtagelsen om, at databeskyttelsesforordningen ikke finder anvendelse på behandling foretaget som led i aktiviteter, der ikke er omfattet af EU-retten³⁶. Denne undtagelse skal anses for alene at have til formål at udelukke statslige myndigheders behandling af personoplysninger under udøvelse af en aktivitet, som tilsigter at beskytte den nationale sikkerhed, eller en aktivitet, som kan henføres til samme kategori, fra anvendelsesområdet for denne

³⁴ Artikel 14¹, stk. 2, i Ceļu satiksmes likums (færdselsloven) af 1.10.1997 (Latvijas Vēstnesis, 1997, nr. 274/276).

³⁵ Databeskyttelsesforordningens artikel 10.

³⁶ Databeskyttelsesforordningens artikel 2, stk. 2, litra a).

forordning. Disse aktiviteter omfatter navnlig de aktiviteter, hvis formål er at beskytte centrale statslige funktioner og samfundets grundlæggende interesser. Aktiviteter vedrørende trafiksikkerheden forfølger ikke dette formål og kan derfor ikke henføres under samme kategori som de aktiviteter, som har til formål at sikre den nationale sikkerhed.

Videregivelsen af personoplysninger vedrørende strafpoint udgjorde for det andet endvidere heller ikke en behandling, der var omfattet af den undtagelse, der fastsætter, at databeskyttelsesforordningen ikke finder anvendelse på de kompetente myndigheders behandling af personoplysninger på det strafferetlige område³⁷. Domstolen fastslog nemlig, at CSDD ved at foretage denne videregivelse ikke kunne anses for at være en sådan »kompetent myndighed«³⁸.

Med henblik på at fastslå, om aktindsigt i personoplysninger vedrørende færdselsforseelser, såsom strafpoint, udgør behandling af personoplysninger vedrørende »lovovertrædelser«³⁹, som nyder øget beskyttelse, fastslog Domstolen, idet den bl.a. henviste til databeskyttelsesforordningens tilblivelseshistorie, at dette begreb alene henviser til strafbare handlinger. Den omstændighed, at færdselsforseelser i den lettiske retsorden kvalificeres som administrative forseelser, er ikke afgørende for at vurdere, om disse forseelser henhørte under begrebet »strafbar handling«, for så vidt som der er tale om et selvstændigt EU-retligt begreb, der skal undergives en selvstændig og ensartet fortolkning i hele Unionen. Efter at have erindret om de tre relevante kriterier for at vurdere, om en lovovertrædelse har karakter af en strafbar handling, nemlig den retlige kvalificering af lovovertrædelsen i national ret, lovovertrædelsens art og stregheden af den pålagte sanktion, fandt Domstolen derfor, at de pågældende færdselsforseelser henhørte under begrebet »lovovertrædelse« som omhandlet i databeskyttelsesforordningen. Hvad angår de to første kriterier fastslog Domstolen, at selv om overtrædelser ikke kvalificeres som »strafferetlige« i national ret, kan en sådan karakter følge af selve overtrædelsens art og navnlig det repressive formål, der forfølges med den sanktion, som overtrædelsen kan medføre. I det foreliggende tilfælde havde tildelingen af strafpoint for færdselsforseelser ligesom andre sanktioner, som begåelsen heraf kunne medføre, bl.a. et sådant repressivt formål. Hvad angår det tredje kriterium bemærkede Domstolen, at alene færdselsforseelser af en vis grovhed fører til tildeling af strafpoint, og at sådanne overtrædelser derfor kan medføre sanktioner af en vis streghed. Pålæggelsen af sådanne point var endvidere generelt et supplement til den sanktion, der blev pålagt, og kumulationen af disse point havde i sig selv retsvirkninger, som endog kunne omfatte et kørselsforbud.

³⁷ Databeskyttelsesforordningens artikel 2, stk. 2, litra d).

³⁸ Artikel 3, stk. 7, i Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27.4.2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (EUT 2016, L 119, s. 89).

³⁹ Databeskyttelsesforordningens artikel 10.

Dom af 5. december 2023 (Store Afdeling), Nacionalinis visuomenės sveikatos centras (C-683/21, [EU:C:2023:949](#))

I 2020 besluttede de litauiske myndigheder at tilrettelægge erhvervelsen af en IT-mobilapplikation for at håndtere covid-19-pandemien bedre. Denne applikation skulle bidrage til en epidemiologisk overvågning ved at gøre det muligt at registrere og overvåge oplysninger om personer, der var udsat for covid-19-virusset.

Med henblik herpå kontaktede Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (det nationale folkesundhedscenter under sundhedsministeriet, Litauen, herefter »det nationale folkesundhedscenter«), der stod for erhvervelsen, selskabet UAB »IT sprendimai sėkmei« (herefter »ITSS«) og anmodede det om at udvikle en sådan mobilapplikation. Herefter sendte ansatte i folkesundhedscentret e-mails vedrørende bl.a. de spørgsmål, der skulle stilles i applikationen, til dette selskab.

I perioden fra april til maj 2020 var den mobilapplikation, som ITSS udviklede, tilgængelig for offentligheden. Som følge heraf gjorde 3 802 personer brug af applikationen og afgav forskellige oplysninger, som applikationen krævede om dem. På grund af manglende finansiering tildelte det nationale folkesundhedscenter imidlertid ikke ITSS nogen offentlig kontrakt vedrørende den officielle erhvervelse af selskabets mobilapplikation, og centret afsluttede proceduren vedrørende denne erhvervelse.

I mellemtiden indledte den nationale tilsynsmyndighed en undersøgelse af behandlingen af personoplysninger som følge af anvendelsen af denne applikation. Ved en afgørelse, som denne myndighed vedtog efter undersøgelsen, blev både det nationale folkesundhedscenter og ITSS, der blev anset for at være fælles dataansvarlig, pålagt administrative bøder.

Det nationale folkesundhedscenter anlagde sag til prøvelse af denne afgørelse ved Vilniaus apygardos administracinis teismas (den regionale domstol i forvaltningsretlige sager i Vilnius, Litauen). Da denne var i tvivl om fortolkningen af flere bestemmelser i databeskyttelsesforordningen, forelagde den Domstolen en anmodning om en præjudiciel afgørelse.

Domstolen (Store Afdeling) anførte i sin dom bl.a. nogle præciseringer vedrørende begrebet »behandling«. Domstolen anførte, at brug af personoplysninger til IT-testning af en mobilapplikation udgør en behandling som omhandlet i databeskyttelsesforordningen. Det forholder sig imidlertid anderledes, hvis oplysningerne er gjort anonyme på en sådan måde, at den registrerede ikke eller ikke længere kan identificeres, eller hvis der er tale om fiktive oplysninger, som ikke vedrører en eksisterende fysisk person.

Spørgsmålet om, hvorvidt personoplysninger bruges til IT-testning eller til et andet formål, er nemlig for det første uden betydning for kvalificeringen af aktiviteten som »behandling«. For det andet kan alene behandling, der vedrører personoplysninger,

kvalificeres som »behandling« som omhandlet i databeskyttelsesforordningen. Fiktive eller anonyme oplysninger udgør ikke personoplysninger.

4. Begrebet »register med personoplysninger«

Dom af 10. juli 2018 (Store Afdeling), Jehovan todistajat (C-25/17, [EU:C:2018:551](#))

I denne dom (se ligeledes afsnit II.3 med overskriften »Den generelle lovgivnings anvendelsesområde«) præciserede Domstolen begrebet »register« som omhandlet i artikel 2, litra c), i direktiv 95/46.

Først erindrede Domstolen således om, at dette direktiv kun finder anvendelse på ikke-elektronisk behandling af personoplysninger, når de behandlede oplysninger er eller vil blive indeholdt i et register, hvorpå den fastslog, at nævnte begreb omfatter en samling af personoplysninger, der er indsamlet i forbindelse med forkyndelsesvirksomhed fra dør til dør, og som omfatter navne og adresser samt andre oplysninger vedrørende de opsøgte personer, når disse oplysninger er struktureret i henhold til kriterier, der i praksis gør det muligt let at hente disse frem til senere brug. Det er ikke nødvendigt, for at en sådan samling kan være omfattet af dette begreb, at den omfatter kartotekskort, konkrete fortegninger eller andre søgesystemer.

5. Begrebet »den registeransvarlige for behandlingen af personoplysninger«

Dom af 10. juli 2018 (Store Afdeling), Jehovan todistajat (C-25/17, [EU:C:2018:551](#))

I denne sag (se ligeledes afsnit II.3 med overskriften »Begrebet »behandling af personoplysninger«« og II.4. med overskriften »Begrebet »register med personoplysninger««) udtalte Domstolen sig om et trossamfunds ansvar i forhold til behandling af personoplysninger foretaget i forbindelse med forkyndelsesvirksomhed fra dør til dør, som organiseres, koordineres og tilskyndes af dette trossamfund.

Domstolen fandt således, at forpligtelsen for enhver person til at overholde Unionens retsregler om beskyttelse af personoplysninger ikke kan anses for at gribe ind i de religiøse samfunds organisatoriske autonomi. Domstolen konkluderede i denne forbindelse, at artikel 2, litra d), i direktiv 95/46, sammenholdt med chartrets artikel 10, stk. 1, skal fortolkes således, at et trossamfund kan holdes ansvarligt, sammen med dets forkyndende medlemmer, for behandlingen af personoplysninger foretaget af sidstnævnte i forbindelse med forkyndelsesvirksomhed fra dør til dør, som organiseres, koordineres og tilskyndes af dette trossamfund, uden at det i denne forbindelse er

påkrævet, at trossamfundet har adgang til disse oplysninger, eller at det har udstedt skriftlige retningslinjer eller anvisninger til dets medlemmer vedrørende denne behandling.

Dom af 5. juni 2018 (Store Afdeling), Wirtschaftsakademie Schleswig Holstein (C-210/16, [EU:C:2018:388](#))

Den tyske databeskyttelsesmyndighed gav i sin egenskab af tilsynsmyndighed som omhandlet i artikel 28 i direktiv 95/46 en tysk uddannelsesvirksomhed, der udbød uddannelse via en fanside på det sociale netværk Facebook, et påbud om at deaktivere sin fanside. Ifølge nævnte myndighed underrettede hverken denne virksomhed eller Facebook nemlig brugerne af fansiden om, at Facebook indsamlede deres personoplysninger ved hjælp af cookies, og at nævnte virksomhed og Facebook efterfølgende behandlede disse data.

I denne sammenhæng præciserede Domstolen begrebet »den registeransvarlige« for behandlingen af personoplysninger. Domstolen antog i den henseende, at administratoren af en fanside på Facebook, såsom den i hovedsagen omhandlede virksomhed, bidrager til at afgøre, til hvilket formål og med hvilke hjælpemidler der foretages behandling af personoplysninger om brugerne af fansiden, ved at foretage indstillinger (afhængigt af bl.a. målgruppen samt målene for forvaltning af og reklame for sine aktiviteter). Af denne grund skulle administratoren ifølge Domstolen sammen med Facebook Ireland (det amerikanske selskab Facebooks datterselskab i EU) kvalificeres som registeransvarlig for denne behandling som omhandlet i artikel 2, litra d), i direktiv 95/46.

Dom af 29. juli 2019, Fashion ID (C-40/17, [EU:C:2019:629](#))

I denne sag havde Domstolen lejlighed til at præcisere begrebet »registeransvarlig« med hensyn til integrationen af en plug-in på et websted.

I den foreliggende sag havde Fashion ID, der er en tysk virksomhed, som sælger modetøj online, integreret det sociale modul »synes godt om« fra det sociale netværk Facebook på sit websted. Denne integration syntes at resultere i, at når en besøgende konsulterer Fashion ID's websted, overføres denne besøgendes personoplysninger til Facebook Ireland. Det lod til, at denne transmission fandt sted, uden at nævnte bruger var bevidst om dette, og uafhængigt af om den pågældende var medlem af det sociale netværk Facebook eller om vedkommende havde klikket på »synes godt om«-knappen fra Facebook.

Verbraucherzentrale NRW, der er en tysk almennyttig forbrugerbeskyttelsesorganisation, havde kritiseret Fashion ID for at have overført personoplysninger vedrørende webstedets besøgende til Facebook Ireland dels uden de besøgendes samtykke, dels i strid med de oplysningskrav, der er fastsat i

bestemmelserne om beskyttelse af personoplysninger. Tvisten blev indbragt for Oberlandesgericht Düsseldorf (den regionale appeldomstol i Düsseldorf, Tyskland), som anmodede Domstolen om en fortolkning af flere bestemmelser i direktiv 95/46.

Domstolen konstaterede indledningsvis, at operatøren for et websted, såsom Fashion ID, kan anses for at være den registeransvarlige som omhandlet i artikel 2, litra d), i direktiv 95/46. Dette ansvar begrænses imidlertid til den operation eller den række af operationer, der omfatter behandling af personoplysninger, for hvilken eller hvilke denne operatør rent faktisk fastlægger, til hvilket formål og på hvilken måde dette må finde sted, dvs. den i hovedsagen omhandlede indsamling og videregivelse ved transmission af personoplysninger. Ifølge Domstolen forekom det derimod umiddelbart udelukket, at Fashion ID fastlagde, til hvilke formål og med hvilke hjælpemidler, der efterfølgende foretoges behandlingsoperationer vedrørende personoplysninger af Facebook Ireland efter deres transmission til dette selskab, hvorfor Fashion ID ikke kunne anses for at være den registeransvarlige for disse operationer som omhandlet i nævnte direktivs artikel 2, litra d).

Domstolen fremhævede endvidere, at det er nødvendigt, at operatøren af et websted og udbyderen af et socialt modul, såsom Facebook Ireland, hver især forfølger en legitim interesse som omhandlet i artikel 7, litra f), i direktiv 95/46, for at disse operationer kan anses for begrundede med henvisning til dem.

Endelig præciserede Domstolen, at den registreredes samtykke, der er omhandlet i artikel 2, litra h), og artikel 7, litra a), i direktiv 95/46, skal være indhentet af en operatør af et websted alene vedrørende de operationer, der omfatter behandling af personoplysninger, for hvilke denne operatør fastlægger, til hvilket formål og på hvilken måde dette må finde sted. I en sådan situation påhviler den oplysningspligt, der er fastsat i dette direktivs artikel 10, ligeledes nævnte operatør, idet de informationer, som denne skal give den berørte person, imidlertid alene skal vedrøre den operation eller den række af operationer, der omfatter behandling af personoplysninger, for hvilke denne operatør fastlægger, til hvilket formål og på hvilken måde denne må finde sted.

Dom af 5. december 2023 (Store Afdeling), Nacionalinis visuomenės sveikatos centras (C-683/21, [EU:C:2023:949](#))

I denne sag (se ligeledes afsnit II.3 med overskriften »Begrebet »behandling af personoplysninger«») bemærkede Domstolen, at en enhed, der har givet en virksomhed til opgave at udvikle en IT-mobilapplikation, og som i denne forbindelse har deltaget i fastlæggelsen af formålene med og hjælpemidlerne til den behandling af personoplysninger, der foretages ved hjælp af denne applikation, kan anses for at være dataansvarlig⁴⁰. Denne betragtning kan ikke drages i tvivl af den omstændighed, at denne enhed ikke selv har foretaget behandling af oplysningerne, ikke udtrykkeligt har

⁴⁰ Som omhandlet i databeskyttelsesforordningens artikel 4, nr. 7).

givet samtykke til gennemførelsen af de konkrete aktiviteter i forbindelse med en sådan behandling eller til overladelsen af denne mobilapplikation til offentligheden og ikke har erhvervet mobilapplikationen, medmindre enheden før denne overladelse til offentligheden udtrykkeligt har gjort indsigelse mod denne og mod den behandling af personoplysninger, der er fulgt heraf.

6. Begrebet »fælles dataansvarlig«

Dom af 5. december 2023 (Store Afdeling), Nacionalinis visuomenės sveikatos centras (C-683/21, [EU:C:2023:949](#))

I denne sag (se ligeledes afsnit II.3 og II.5 med overskrifterne »Begrebet »behandling af personoplysninger« og »Begrebet »registeransvarlig«/»dataansvarlig«») bemærkede Domstolen, at kvalificering af to enheder som fælles dataansvarlige hverken forudsætter, at der foreligger en ordning mellem disse enheder om fastlæggelse af formålene med og hjælpemidlerne til behandling af personoplysningerne, eller at der foreligger en ordning, der fastlægger de vilkår, der regulerer det fælles dataansvar. I henhold til databeskyttelsesforordningen ⁴¹ skal de fælles dataansvarlige ganske vist ved hjælp af en ordning mellem dem på en gennemsigtig måde fastlægge deres respektive ansvar for overholdelse af forpligtelserne i henhold til forordningen. En sådan ordning er imidlertid ikke en forudsætning for, at to eller flere enheder kan kvalificeres som »fælles dataansvarlige«, men en forpligtelse, som databeskyttelsesforordningen pålægger de fælles dataansvarlige, når de først er blevet kvalificeret som sådanne, med henblik på at sikre overholdelsen af de krav i denne forordning, der påhviler dem. Kvalificeringen som fælles dataansvarlig følger således af den omstændighed alene, at flere enheder har deltaget i fastlæggelsen af formålene med og hjælpemidlerne til behandling.

Hvad angår de pågældende enheders fælles fastlæggelse af formålene med og hjælpemidlerne til behandling præciserede Domstolen, at disse enheders deltagelse heri kan antage forskellige former og følge af såvel deres fælles beslutning som af deres konvergerende beslutninger. I sidstnævnte tilfælde skal disse beslutninger imidlertid supplere hinanden på en sådan måde, at de har en mærkbar indvirkning på fastlæggelsen af formålene med og hjælpemidlerne til behandling.

⁴¹ Databeskyttelsesforordningens artikel 26, stk. 1, sammenholdt med 79. betragtning til forordningen.

7. Betingelser for lovligheden af en behandling af personoplysninger

Dom af 16. december 2008 (Store Afdeling), Huber (C-524/06, [EU:C:2008:724](#))

Bundesamt für Migration und Flüchtlinge (forbundskontoret for migration og flygtninge, Tyskland) administrerede et centralt register over udlændinge, hvori visse personoplysninger om udlændinge, som opholder sig på tysk område i en periode på højst tre måneder, registreres. Registret blev anvendt til statistiske formål og til brug for sikkerheds-, politi- og justitsmyndighedernes opfyldelse af deres opgaver på området for bekæmpelse og opklaring af handlinger, der er strafbare eller bringer den offentlige sikkerhed i fare.

Heinz Huber, som er østrigsk statsborger, bosatte sig i Tyskland i 1996 for dér at udøve sit erhverv som selvstændig forsikringsagent. Heinz Huber anmodede om at få slettet de oplysninger, der var registreret om ham i det pågældende register, idet han mente, at han på grund af registreringen af disse oplysninger blev udsat for forskelsbehandling, idet der ikke fandtes en tilsvarende database for tyske statsborgere.

Sagen blev forelagt for Oberverwaltungsgericht für das Land Nordrhein-Westfalen (appeldomstolen i forvaltningsretlige sager i Land Nordrhein-Westfalen, Tyskland), som i denne forbindelse forelagde Domstolen et spørgsmål om foreneligheden med EU-retten af den behandling af personoplysninger, som det pågældende register foretog.

Domstolen bemærkede først og fremmest, at en unionsborgers ret til ophold i en medlemsstat, hvor han ikke er statsborger, ikke er ubetinget, idet den kan være undergivet begrænsninger. Anvendelsen af et sådant register til brug for myndighederne med ansvar for forvaltningen af lovgivningen om opholdsret er således principielt lovlig og efter omstændighederne forenelig med forbuddet mod forskelsbehandling på grundlag af nationalitet i artikel 12, stk. 1, EF (nu artikel 18, første afsnit, TEUF). Et sådant register må imidlertid ikke indeholde andre oplysninger end dem, der er nødvendige til dette formål i henhold til direktivet om beskyttelse af personoplysninger.

Med hensyn til nødvendigheden af behandlingen som omhandlet i artikel 7, litra e), i direktiv 95/46 bemærkede Domstolen først og fremmest, at der var tale om et selvstændigt EU-retligt begreb, som skal fortolkes i fuld overensstemmelse med formålet med direktiv 95/46, som det er formuleret i dets artikel 1, stk. 1. Dernæst konstaterende den, at et system til behandling af personoplysninger er i overensstemmelse med EU-retten, hvis det udelukkende indeholder oplysninger, som er nødvendige for de nævnte myndigheders forvaltning af denne lovgivning, og hvis centraliseringen muliggør en mere effektiv forvaltning af denne lovgivning for så vidt angår opholdsret for unionsborgere, der ikke er statsborgere i denne medlemsstat.

Under alle omstændigheder kan opbevaring og behandling af navngivne personoplysninger inden for rammerne af et sådant register til statistisk brug ikke anses

for nødvendig i den forstand, hvori udtrykket er anvendt i artikel 7, litra e), i direktiv 95/46.

Med hensyn til spørgsmålet om anvendelse af oplysningerne i registret med henblik på kriminalitetsbekæmpelse bemærkede Domstolen endvidere bl.a., at dette mål tilsigter retsforfølgning af begåede forbrydelser og lovovertrædelser uafhængigt af gerningsmændenes nationalitet. Følgelig bør der for en medlemsstat ikke være forskel på dens egne statsborgere og unionsborgere, der ikke er statsborgere i den pågældende medlemsstat, men som opholder sig på dens område, hvad hensynet til kriminalitetsbekæmpelse angår. Forskelsbehandlingen af disse statsborgere og disse unionsborgere i medfør af den systematiske behandling, der kun foretages af personoplysninger vedrørende unionsborgere, der ikke er statsborgere i den pågældende medlemsstat, med henblik på kriminalitetsbekæmpelse, udgør derfor en forskelsbehandling omfattet af forbuddet i artikel 12, stk. 1, EF.

Dom af 19. oktober 2016, Breyer (C-582/14, [EU:C:2016:779](#))

I denne dom (se også afsnit II.2 med overskriften »Begrebet »personoplysninger«») tog Domstolen ligeledes stilling til spørgsmålet om, hvorvidt artikel 7, litra f), i direktiv 95/46 er til hinder for en bestemmelse i national ret, hvorefter udbyderen af online-medietjenester kun må indsamle og anvende personoplysninger om en bruger uden samtykke fra denne, i det omfang dette er nødvendigt for at kunne afregne og give den pågældende bruger adgang til konkret at benytte online-mediet, og hvorefter formålet om at sikre online-mediets generelle funktionsdygtighed ikke kan begrunde, at personoplysningerne anvendes, også efter at brugeren har afsluttet sin konkrete søgning på webstedet.

Domstolen fastslog, at artikel 7, litra f), i direktiv 95/46 var til hinder for den pågældende lovgivning. I henhold til denne bestemmelse er behandling af personoplysninger i henhold til denne bestemmelse lovlig, hvis den er nødvendig for, at den registeransvarlige eller den tredjemand eller de tredjemænd, til hvem oplysningerne videregives, kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder går forud herfor. I denne sag udelukkede den tyske lovgivning imidlertid kategorisk og generelt muligheden for behandling af visse kategorier af personoplysninger uden at tillade en afvejning af de i en konkret sag foreliggende modstående rettigheder og interesser. Dermed havde den på ulovlig vis begrænset rækkevidden af det princip, der er fastsat i artikel 7, litra f), i direktiv 95/46, idet den udelukkede, at formålet om at garantere online-mediernes generelle funktionsdygtighed kan være genstand for en afvejning i forhold til disse brugeres interesser eller grundlæggende rettigheder og frihedsrettigheder.

Dom af 27. september 2017, Puškár (C-73/16, [EU:C:2017:725](#))

I tvisten i hovedsagen havde Peter Puškár anlagt et søgsmål ved Najvyšší súd Slovenskej republiky (Den Slovakiske Republiks øverste domstol) med påstand om, at Finančné riaditeľstvo (finansdirektoratet), alle skattekontorer herunder og Kriminálny úrad finančnej správy (kontoret for bekæmpelse af økonomisk kriminalitet) blev pålagt ikke at opføre hans navn på en liste over personer, der af finansdirektoratet ansås for stråmænd, og som var oprettet af direktoratet i forbindelse med skatteopkrævning, og hvor ajourføringen blev varetaget af finansdirektoratet og kontoret for bekæmpelse af økonomisk kriminalitet (herefter »den omtvistede liste«). Peter Puškár havde endvidere nedlagt påstand om, at enhver nævnelse af ham skulle slettes fra disse lister og i finansforvaltningens EDB-systemer.

Under disse omstændigheder forelagde Najvyšší súd (øverste domstol, Den Slovakiske Republik) bl.a. Domstolen et spørgsmål om, hvorvidt retten til respekt for privatliv, familieliv, hjem og kommunikation, der er sikret ved chartrets artikel 7, og retten til beskyttelse af personoplysninger, der er fastlagt i chartrets artikel 8, kan fortolkes således, at en medlemsstat ikke må føre lister over personoplysninger med henblik på beskatning uden den registreredes samtykke, dvs. at en offentlig myndigheds indsamling af personoplysninger med henblik på forhindring af skattesvig i sig selv udgør en risiko.

Domstolen konkluderede, at artikel 7, litra e), i direktiv 95/46 ikke er til hinder for en medlemsstats myndigheders behandling af personoplysninger med henblik på skatteopkrævning og bekæmpelse af skattesvig, såsom den behandling, der var foretaget ved udarbejdelsen af den omtvistede liste i hovedsagen, uden de registreredes samtykke, forudsat, dels, at disse myndigheder er blevet pålagt opgaver i samfundets interesse af den nationale lovgivning som omhandlet i denne bestemmelse, at udarbejdelsen af denne liste og opførelsen af de registreredes navne på denne liste faktisk er egnet og nødvendig med henblik på opfyldelsen af de forfulgte mål, og at der foreligger tilstrækkelige holdepunkter for at antage, at de registrerede med rette er opført på denne liste, dels at alle de betingelser for en lovlig behandling af personoplysninger, som er fastsat ved direktiv 95/46, er opfyldt.

Domstolen bemærkede i denne forbindelse, at det tilkommer den nationale ret at efterprøve, om udarbejdelsen af den omtvistede liste er nødvendig for udførelsen af de i hovedsagen omhandlede opgaver i samfundets interesse, under hensyntagen til bl.a. det nøjagtige formål med udarbejdelsen af den omtvistede liste, de retsvirkninger, som de personer, der optræder på listen, er underlagt, og hvorvidt denne liste er offentlig eller ej. Endvidere tilkommer det, henset til proportionalitetsprincippet, den nationale ret at efterprøve, om udarbejdelsen af den omtvistede liste og opførelsen af de pågældende personers navne på denne er egnet til at opfylde de mål, der forfølges med udarbejdelsen, og om der ikke findes mindre indgribende foranstaltninger til at nå disse mål.

Domstolen konstaterede desuden, at den omstændighed, at en person er opført på den omtvistede liste, kan krænke visse af personens rettigheder. En opførelse på denne liste vil nemlig kunne skade hans omdømme og påvirke hans forhold til skattemyndighederne. Denne opførelse vil også kunne påvirke formodningen om denne persons uskyld, som er sikret ved chartrets artikel 48, stk. 1, og friheden til at oprette og drive egen virksomhed, som er sikret ved chartrets artikel 16, for de juridiske personer, som sættes i forbindelse med fysiske personer opført på den omtvistede liste. En sådan krænkelse kan således kun være hensigtsmæssig, hvis der foreligger tilstrækkelige holdepunkter for mistanken om, at den pågældende person proforma varetager ledelsesposter hos de juridiske personer, der sættes i forbindelse med ham, og dermed påvirker skatteopkrævningen og bekæmpelsen af skattesvig.

Domstolen fandt i øvrigt, at såfremt der i medfør af artikel 13 i direktiv 95/46 forelå grunde til at begrænse visse af de rettigheder, der er fastsat i dette direktivs artikel 6 og 10-12, såsom den registreredes ret til information, skulle en sådan begrænsning være nødvendig af hensyn til de interesser, der fremgår af den nævnte artikel 13, stk. 1, såsom bl.a. en væsentlig økonomisk eller finansiell interesse på skatteområdet, og være baseret på lovgivningsmæssige foranstaltninger.

Dom af 11 november 2020, Orange Romania (C-61/19, [EU:C:2020:901](#))

Orange România SA leverer mobiltelekommunikationstjenester på det rumænske marked. Den 28. marts 2018 pålagde Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (den nationale tilsynsmyndighed for behandling af personoplysninger, Rumænien, herefter »ANSPDCP«) Orange România en bøde for at have indsamlet og opbevaret genparter af kundernes identitetsbeviser uden udtrykkeligt samtykke fra disse.

Ifølge ANSPDCP indgik Orange România fra den 1. marts 2018 til den 26. marts 2018 aftaler om levering af mobiltelekommunikationstjenester, som indeholdt et vilkår om, at kunderne var blevet informeret om og havde givet deres samtykke til indsamling og opbevaring af en genpart af deres identitetsbevis med henblik på identifikation. Feltet vedrørende dette vilkår var blevet afkrydset af den dataansvarlige, inden aftalen blev underskrevet.

På denne baggrund anmodede Tribunalul București (retten i første instans i Bukarest, Rumænien) Domstolen om at præcisere de betingelser, hvorunder kunders samtykke til behandling af deres personoplysninger kan anses for gyldigt.

Domstolen bemærkede indledningsvis, at EU-retten ⁴² fastsætter en liste over de tilfælde, hvor behandling af personoplysninger kan anses for at være lovlig. Den

⁴² Artikel 7 i direktiv 95/46 og databeskyttelsesforordningens artikel 6.

registreredes samtykke skal navnlig være frivilligt, specifikt, informeret og utvetydigt⁴³. I denne forbindelse udgør tavshed, forudafkrydsede felter eller inaktivitet ikke et gyldigt samtykke.

Når den registreredes samtykke gives i en skriftlig erklæring, der også vedrører andre forhold, skal denne erklæring desuden forelægges i en letforståelig og lettilgængelig form og i et klart og enkelt sprog. For at sikre, at den registrerede reelt har et frit valg, må aftalevilkårene ikke vildlede den pågældende med hensyn til muligheden for at indgå aftalen, selv om denne nægter at give samtykke til behandlingen af sine personoplysninger.

Domstolen præciserede, at Orange România som den dataansvarlige skal kunne godtgøre, at behandlingen af personoplysningerne er lovlig, og dermed i det foreliggende tilfælde, at der forelå et gyldigt samtykke fra kunderne. Eftersom de pågældende kunder åbenbart ikke selv satte kryds i feltet vedrørende indsamling og opbevaring af genpart af deres identitetsbeviser, kunne den blotte omstændighed, at dette felt var blevet afkrydset, i denne forbindelse ikke godtgøre, at der forelå en bekræftende tilkendegivelse fra disse kunder om samtykke. Det tilkom den forelæggende ret at foretage den nødvendige efterprøvelse i denne henseende.

Ifølge Domstolen tilkom det ligeledes den forelæggende ret at vurdere, om de omhandlede aftalevilkår kunne vildlede de registrerede kunder med hensyn til muligheden for at indgå aftalen, selv om den pågældende nægtede at give samtykke til behandling af sine personoplysninger, i mangel af nærmere oplysninger om denne mulighed. Domstolen bemærkede desuden, at Orange România, såfremt en kunde nægtede at give samtykke til behandling af sine oplysninger, krævede, at kunden skriftligt erklærede, at vedkommende ikke gav samtykke til hverken indsamling eller opbevaring af en genpart af sit identitetsbevis. Domstolen var af den opfattelse, at et sådant yderligere krav uretmæssigt kunne påvirke det frie valg med hensyn til at modsætte sig denne indsamling og opbevaring. Det påhvilede under alle omstændigheder det nævnte selskab at godtgøre, at selskabets kunder ved en aktiv adfærd havde tilkendegivet deres samtykke til behandlingen af deres personoplysninger, og selskabet kunne ikke kræve, at de aktivt tilkendegav deres nægtelse heraf.

Domstolen konkluderede således, at en aftale om levering af telekommunikationstjenester, der indeholder et vilkår om, at den registrerede er blevet informeret om og har givet samtykke til indsamling og opbevaring af en genpart af vedkommendes identitetsbevis med henblik på identifikation af den pågældende, ikke kan bevise, at den registrerede har givet et gyldigt samtykke til denne indsamling og opbevaring, hvis feltet vedrørende dette vilkår er blevet afkrydset af den dataansvarlige inden underskrivelsen af aftalen, eller aftalevilkårene kan vildlede den registrerede med

⁴³ Artikel 2, litra h), i direktiv 95/46 og databeskyttelsesforordningens artikel 4, nr. 11).

hensyn til muligheden for at indgå den pågældende aftale, selv om vedkommende nægter at give samtykke til behandlingen af sine oplysninger, eller den dataansvarlige uretmæssigt påvirker det frie valg med hensyn til at modsætte sig denne indsamling og opbevaring ved at kræve, at den registrerede for at tilkendegive sin nægtelse af samtykke skal udfylde en supplerende formular om nægtelse.

Dom af 22. juni 2021 (Store Afdeling), Latvijas Republikas Saeima (Strafpoint) (C-439/19, [EU:C:2021:504](#))

I denne dom (se ligeledes afsnit II.3 med overskriften »Begrebet »behandling af personoplysninger«») fastslog Domstolen, at databeskyttelsesforordningen var til hinder for lovgivningen, der forpligtede Ceļu satiksmes drošības direkcija (direktoratet for færdselssikkerhed, Letland) (herefter »CSDD«) til at gøre oplysningerne vedrørende de strafpoint, som førere af motorkøretøjer var blevet pålagt, tilgængelige for offentligheden, uden at den person, der anmodede om aktindsigt, skulle godtgøre en særlig interesse i at få de nævnte oplysninger. Domstolen fastslog, at det, navnlig med henblik på det formål om at forbedre trafikikkerheden, som den lettiske regering havde anført, ikke var godtgjort, at det var nødvendigt at videregive personoplysninger vedrørende de strafpoint, der pålægges for færdselsforseelser. Ifølge Domstolen begrundede endvidere hverken retten til aktindsigt i officielle dokumenter eller retten til informationsfrihed en sådan lovgivning.

I denne sammenhæng bemærkede Domstolen, at den forbedring af trafikikkerheden, som tilsigtedes med den lettiske lovgivning, er et mål af almen interesse, der er anerkendt af Unionen, og at medlemsstaterne derfor kan kvalificere trafikikkerheden som en »opgave i samfundets interesse«⁴⁴. Det var imidlertid ikke godtgjort, at den lettiske ordning for videregivelse af personoplysninger vedrørende strafpoint var nødvendig for at sikre det tilsigtede mål. Dels rådede den lettiske lovgiver nemlig over en bred vifte af handlemuligheder, som havde givet den mulighed for nå dette mål, og som var mindre indgribende i de berørte personers grundlæggende rettigheder. Dels skulle der tages hensyn til, at oplysningerne om strafpoint var følsomme, og til, at videregivelsen af disse oplysninger til offentligheden kunne udgøre et særligt alvorligt indgreb i retten til respekt for privatlivet og til beskyttelse af personoplysninger, eftersom videregivelsen kunne medføre samfundets misbilligelse og føre til stigmatisering af den pågældende person.

Domstolen fastslog endvidere, at henset til følsomheden af disse oplysninger og alvoren af dette indgreb i disse to grundlæggende rettigheder, gik disse rettigheder forud for såvel offentlighedens interesse i at få aktindsigt i officielle dokumenter, såsom det nationale register over køretøjer og førere, som retten til informationsfrihed.

⁴⁴ Ifølge databeskyttelsesforordningens artikel 6, stk. 1, litra e), er behandling af personoplysninger lovlig, når den »er nødvendig af hensyn til udførelse af en opgave i samfundets interesse [...]«.

I øvrigt fastslog Domstolen af tilsvarende grunde, at databeskyttelsesforordningen ligeledes var til hinder for den lettiske lovgivning, for så vidt som den tillod CSDD at videregive oplysninger om strafpoint, som pålægges førere af motorkøretøjer for færdselsforseelser, til erhvervsdrivende, med henblik på at de sidstnævnte kunne videreanvende oplysningerne og videregive dem til offentligheden.

Endelig præciserede Domstolen, at princippet om EU-rettens forrang var til hinder for, at den forelæggende ret, som var forelagt et søgsmål til prøvelse af den lettiske lovgivning, som Domstolen havde erklæret uforenelig med EU-retten, besluttede at opretholde retsvirkningerne af denne lovgivning indtil afsigelsen af den endelige dom.

III. Behandling af personoplysninger som omhandlet i sektorspecifikke regler

1. Behandling af personoplysninger i den elektroniske kommunikationssektor

Dom af 2. oktober 2018 (Store Afdeling), Ministerio Fiscal (C-207/16, [EU:C:2018:788](#))

Denne sag omhandlede en spansk forundersøgelsesdomstols afslag på en anmodning, der var blevet indgivet i forbindelse med en efterforskning af et røveri, hvor der blev stjålet en tegnebog og en mobiltelefon. Nærmere bestemt havde kriminalpolitiet anmodet nævnte domstol om at få adgang til identifikationsoplysningerne for brugerne af de telefonnumre, der var blevet aktiveret fra den stjålne telefon i en periode på 12 dage fra det tidspunkt, hvor røveriet fandt sted. Afslaget havde været støttet på den begrundelse, at de faktiske omstændigheder, der lå til grund for den strafferetlige efterforskning, ikke kunne anses for at udgøre en »alvorlig« forbrydelse – hvilket ifølge spansk ret vil sige en forbrydelse, der straffes med mere end fem års fængsel – idet det nemlig kun ved denne type forbrydelse er muligt at få adgang til identifikationsoplysningerne.

Domstolen erindrede først om, at offentlige myndigheders adgang til personoplysninger, der er lagret af udbydere af elektroniske kommunikationstjenester, inden for rammerne af en strafferetlig bevisoptagelse er omfattet af anvendelsesområdet for direktiv 2002/58, hvorpå den fastslog, at adgang til data med henblik på at identificere indehavere af SIM-kort, der er blevet aktiveret med en stjålet mobiltelefon, såsom efternavn, fornavn og eventuelt adresse på disse indehavere, udgør et indgreb i de grundlæggende rettigheder til respekt for privatliv og til databeskyttelse, der er fastsat i chartret, selv om der ikke foreligger omstændigheder, der gør det muligt at kvalificere dette indgreb som »alvorligt«, og uden at det har betydning, om de

videregivne oplysninger er følsomme oplysninger, eller om det nævnte indgreb har medført eventuelle ubehageligheder for de berørte. Domstolen fremhævede imidlertid, at dette indgreb ikke er så alvorligt, at denne adgang skal begrænses til forebyggelse, efterforskning, afsløring og retsforfølgning af straffelovsovertrædelser med henblik på bekæmpelse af grov kriminalitet. Selv om der i direktiv 2002/58 foretages en udtømmende opregning af de formål, som kan begrunde en national lovgivning, der regulerer offentlige myndigheders adgang til de pågældende oplysninger, og som således fraviger princippet om fortrolighed i forbindelse med elektronisk kommunikation, idet denne adgang faktisk og præcist skal opfylde et af disse mål, bemærkede Domstolen nemlig hvad angår formålet om forebyggelse, efterforskning, afsløring og retsforfølgning af straffelovsovertrædelser, at ordlyden af direktiv 2002/58 ikke begrænser dette formål til kun at omfatte bekæmpelse af alvorlige forbrydelser, men tager sigte på »straffesager« generelt.

I denne forbindelse præciserede Domstolen, at selv om den ganske vist i dommen i sagen Tele2 Sverige og Watson m.fl.⁴⁵ havde fastslået, at det kun er bekæmpelse af grov kriminalitet, der kan begrunde offentlige myndigheders adgang til personoplysninger, der er lagret af udbydere af elektroniske kommunikationstjenester, og som tilsammen gør det muligt at drage præcise slutninger vedrørende privatlivet for de personer, hvis data er omhandlet, var en sådan fortolkning begrundet med den omstændighed, at det formål, der forfølges med en lovgivning, der regulerer denne adgang, skal stå i forhold til alvoren af det indgreb i de omhandlede grundlæggende rettigheder, som denne adgang indebærer. I overensstemmelse med proportionalitetsprincippet er et alvorligt indgreb således kun begrundet på dette område, hvis det har til formål at bekæmpe kriminalitet, der på samme måde kan kvalificeres som »grov«. Når indgrebet ikke er alvorligt, kan nævnte adgang begrundes med henblik på forebyggelse, efterforskning, afsløring og retsforfølgning af »straffelovsovertrædelser« generelt.

Hvad angår den pågældende sag fastslog Domstolen, at adgangen til de data alene, som den omhandlede anmodning omfattede, ikke kunne kvalificeres som et »alvorligt« indgreb i de grundlæggende rettigheder for de personer, hvis data var omhandlet, eftersom disse data ikke gjorde det muligt at drage præcise slutninger vedrørende deres privatliv. Domstolen fastslog herefter, at det indgreb, som en adgang til sådanne data indebærer, kan være begrundet i formålet om forebyggelse, efterforskning, afsløring og retsforfølgning af »straffelovsovertrædelser« generelt, uden at det er nødvendigt, at disse forbrydelser kvalificeres som »alvorlige«.

⁴⁵ Domstolens dom af 21.12.2016, Tele2 Sverige og Watson m.fl. (C-203/15 og C-698/15, [EU:C:2016:970](#)).

Domme af 6. oktober 2020 (Store Afdeling), *Privacy International* (C-623/17, [EU:C:2020:790](#)) og *La Quadrature du Net m.fl.* (C-511/18, C-512/18 og C-520/18, [EU:C:2020:791](#))

Retspraksis om lagring af og adgang til personoplysninger inden for området for elektronisk kommunikation, navnlig dommen i sagen *Tele2 Sverige og Watson m.fl.*, hvori Domstolen bl.a. fastslog, at medlemsstaterne ikke kan pålægge udbydere af elektroniske kommunikationstjenester en forpligtelse til at foretage generel og udifferentieret lagring af trafik- og lokaliseringsdata, har givet anledning til betænkeligheder hos visse stater, som har udtrykt bekymring for, at de er blevet frataget et instrument, som efter deres opfattelse er nødvendigt for at beskytte den nationale sikkerhed og for at bekæmpe kriminalitet.

Det var på denne baggrund, at Investigatory Powers Tribunal (domstol for efterforskningsbeføjelser, Det Forenede Kongerige) (*Privacy International*, sag C-623/17), Conseil d'État (øverste domstol i forvaltningsretlige sager, Frankrig) (*La Quadrature du Net m.fl.*, forenede sager C-511/18 og C-512/18) og Cour constitutionnelle (forfatningsdomstol, Belgien) (*Ordre des barreaux francophones et germanophone m.fl.*, sag C-520/18) var blevet forelagt tvister vedrørende lovligheden af de lovgivninger, som visse af disse medlemsstater havde vedtaget inden for disse områder, og som navnlig foreskrev en forpligtelse for udbydere af elektroniske kommunikationstjenester til at foretage overføring til en offentlig myndighed eller generel og udifferentieret lagring af brugernes trafik- og lokaliseringsdata.

Med to domme afsagt i Store Afdeling den 6. oktober 2020 fastslog Domstolen først, at nationale lovgivninger, der pålægger udbydere af elektroniske kommunikationstjenester at lagre trafik- og lokaliseringsdata eller at overføre disse data til de nationale sikkerheds- og efterretningstjenester med henblik på dette formål, er omfattet af anvendelsesområdet for direktiv 2002/58.

Domstolen bemærkede derefter, at direktiv 2002/58 ⁴⁶ ikke tillader, at en fravigelse af den principielle forpligtelse til at sikre fortroligheden af elektronisk kommunikation og de dermed forbundne data og af forbuddet mod lagring af disse data bliver hovedreglen. Dette indebærer, at dette direktiv kun tillader medlemsstaterne, bl.a. af hensyn til den nationale sikkerhed, at vedtage lovgivningsmæssige foranstaltninger, der har til formål at begrænse rækkevidden af de rettigheder og forpligtelser, der er fastsat i dette direktiv, herunder forpligtelsen til at sikre fortroligheden af kommunikation og af trafikdata ⁴⁷, såfremt dette sker i overensstemmelse med EU-rettens generelle principper, som bl.a. omfatter proportionalitetsprincippet og de grundlæggende rettigheder, der er sikret ved chartret ⁴⁸.

⁴⁶ Artikel 15, stk. 1 og 3, i direktiv 2002/58.

⁴⁷ Artikel 5, stk. 1, i direktiv 2002/58.

⁴⁸ Navnlig chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1.

I denne forbindelse fastslog Domstolen i Privacy International-sagen for det første, at direktiv 2002/58, sammenholdt med chartret, er til hinder for en national lovgivning, der med henblik på at beskytte den nationale sikkerhed pålægger udbydere af elektroniske kommunikationstjenester at foretage generel og udifferentieret overføring af trafik- og lokaliseringsdata til sikkerheds- og efterretningstjenesterne. I de forenede sager La Quadrature du Net m.fl. og i sagen Ordre des barreaux francophones et germanophone m.fl. var Domstolen for det andet af den opfattelse, at dette samme direktiv er til hinder for lovgivningsmæssige foranstaltninger, der pålægger udbydere af elektroniske kommunikationstjenester i forebyggende øjemed at foretage generel og udifferentieret lagring af trafik- og lokaliseringsdata.

Disse forpligtelser til at foretage generel og udifferentieret overføring og lagring af sådanne data udgjorde nemlig særligt alvorlige indgreb i de grundlæggende rettigheder, der er sikret ved chartret, uden at den adfærd, som de personer, hvis data var berørt, havde udvist, havde nogen forbindelse med det formål, der forfulgtes med den omhandlede lovgivning. På samme måde fortolkede Domstolen artikel 23, stk. 1, i den generelle forordning om databeskyttelse, sammenholdt med chartret, således, at denne bestemmelse er til hinder for en national lovgivning, der pålægger udbydere af adgang til offentlige onlinekommunikationstjenester og udbydere af hostingtjenester at foretage generel og udifferentieret lagring navnlig af de personoplysninger, der er forbundet med brugen af disse tjenester.

Domstolen var til gengæld af den opfattelse, at i de situationer, hvor den pågældende medlemsstat står over for en alvorlig trussel mod den nationale sikkerhed, der må anses for at være reel og aktuel eller forudsigelig, er direktiv 2002/58, sammenholdt med chartret, ikke til hinder for at pålægge udbydere af elektroniske kommunikationstjenester et påbud om at foretage generel og udifferentieret lagring af trafik- og lokaliseringsdata. I denne forbindelse præciserede Domstolen, at den afgørelse, som fastsætter dette påbud for en periode, der er tidsmæssigt begrænset til det strengt nødvendige, skal kunne 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. Under disse samme omstændigheder er det nævnte direktiv heller ikke til hinder for, at der bliver foretaget automatiseret analyse af data, herunder navnlig trafik- og lokaliseringsdata, der vedrører samtlige brugere af elektroniske kommunikationsmidler.

Domstolen tilføjede, at direktiv 2002/58, sammenholdt med chartret, ikke er til hinder for lovgivningsmæssige foranstaltninger, der gør det muligt i en periode, der er tidsmæssigt begrænset til det strengt nødvendige, at foretage målrettet lagring af trafik- 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. Dette direktiv er endvidere ikke til hinder for sådanne foranstaltninger, der foreskriver generel og udifferentieret lagring af de IP-adresser, der er tildelt kilden til en

kommunikation, for så vidt som lagringsperioden er begrænset til det strengt nødvendige, og heller ikke for sådanne foranstaltninger, som foreskriver en sådan lagring af data, der vedrører den civile identitet på brugerne af de elektroniske kommunikationsmidler, idet medlemsstaterne i dette sidstnævnte tilfælde ikke har pligt til at begrænse lagringen tidsmæssigt. Det nævnte direktiv er desuden ikke til hinder for en lovgivningsmæssig foranstaltning, der gør det muligt at foretage hurtig lagring af de data, som tjenesteudbydere råder over, når der opstår situationer, hvori det er nødvendigt at lagre de nævnte data ud over de lovbestemte frister for datalagring med henblik på at opklare alvorlige strafbare handlinger eller angreb mod den nationale sikkerhed, i de tilfælde, hvor disse strafbare handlinger eller disse angreb allerede har kunnet konstateres, eller hvor der foreligger rimelig grund til at mistænke, at der er begået sådanne strafbare handlinger eller angreb.

Domstolen fastslog endvidere, at direktiv 2002/58, sammenholdt med chartret, ikke er til hinder for en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester at gøre brug af indsamling i realtid af bl.a. trafik- og lokaliseringsdata, når denne indsamling er begrænset til personer, med hensyn til hvilke der foreligger rimelig grund til at mistænke, at de på den ene eller den anden måde er involveret i terrorvirksomhed, og er underlagt en forudgående prøvelse, der skal foretages af enten en domstol eller en uafhængig administrativ enhed, der træffer bindende afgørelser, for at sikre, at en sådan indsamling i realtid kun er tilladt inden for rammerne af, hvad der er strengt nødvendigt. I et hastende tilfælde skal denne prøvelse foretages hurtigst muligt.

Endelig behandlede Domstolen spørgsmålet om, hvorvidt det er muligt at opretholde de tidsmæssige virkninger af en national lovgivning, der er fundet uforenelig med EU-retten. Domstolen fastslog i denne henseende, at en national ret ikke kan anvende en bestemmelse i den nationale lovgivning, som giver den bemyndigelse til tidsmæssigt at begrænse virkningerne af en afgørelse om ulovlighed, som det i medfør af denne lovgivning påhviler denne ret at træffe, med hensyn til en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester at foretage en generel og udifferentieret lagring af trafik- og lokaliseringsdata, som er fundet uforenelig med direktiv 2002/58, sammenholdt med chartret.

Med henblik på at give den nationale ret et hensigtsmæssigt svar bemærkede Domstolen på denne baggrund, at antagelsen og bedømmelsen af beviser, der er opnået ved hjælp af en lagring, som er uforenelig med EU-retten, inden for rammerne af en straffesag, der er indledt mod personer, som er mistænkt for at have begået kriminelle handlinger, på EU-rettens nuværende udviklingstrin alene henhører under national ret. Domstolen præciserede imidlertid, at direktiv 2002/58, som fortolket i lyset af effektivitetsprincippet, kræver, at den nationale ret i straffesager ser bort fra de beviser, der er opnået ved hjælp af en generel og udifferentieret lagring af trafik- og lokaliseringsdata, som er uforenelig med EU-retten, inden for rammerne af en sådan

straffesag, hvis de personer, som er mistænkt for at have begået kriminelle handlinger, ikke er i stand til effektivt at udtale sig om disse beviser.

Dom af 2. marts 2021, Prokuratuur (Betingelser for adgang til oplysninger om elektronisk kommunikation) (C-746/18, [EU:C:2021:152](#))

Der var i Estland blevet indledt en straffesag mod H.K. for tyveri, brug af en anden persons bankkort og voldshandlinger mod personer, der deltog i en retssag. H.K. blev af en ret i første instans idømt en frihedsstraf på to år for disse lovovertrædelser. Denne afgørelse blev derefter stadfæstet i appelinstanten. De politirapporter, der lå til grund for konstateringen af disse lovovertrædelser, var bl.a. blevet udfærdiget på grundlag af personoplysninger, som var blevet genereret i forbindelse med leveringen af elektroniske kommunikationstjenester. Riigikohus (øverste domstol, Estland), ved hvilken H.K. iværksatte kassationsappel, var i tvivl om, hvorvidt de betingelser, hvorunder efterforskningsmyndigheden havde fået adgang til disse data, var i overensstemmelse med EU-retten ⁴⁹.

Tvivlen vedrørte for det første spørgsmålet om, hvorvidt varigheden af den periode, i hvilken efterforskningsmyndigheden havde haft adgang til dataene, var et kriterium, der gav mulighed for at bedømme alvoren af det indgreb i de pågældende personers grundlæggende rettigheder, som denne adgang udgjorde. Når denne periode er meget kort, eller mængden af indsamlede data er meget begrænset, var den forelæggende ret således i tvivl om, hvorvidt formålet om generel bekæmpelse af kriminalitet og ikke blot bekæmpelse af grov kriminalitet kunne begrunde et sådant indgreb. For det andet var den forelæggende ret i tvivl om, hvorvidt den estiske anklagemyndighed, henset til de forskellige opgaver, som denne var tillagt ved den nationale lovgivning, udgjorde en »uafhængig« administrativ myndighed som omhandlet i dommen i sagen Tele2 Sverige og Watson m.fl. ⁵⁰, der kunne give efterforskningsmyndigheden adgang til de omhandlede data.

Med sin dom, afsagt i Store Afdeling, fastslog Domstolen, at direktiv 2002/58, sammenholdt med chartret, er til hinder for en national lovgivning, der giver offentlige myndigheder adgang til trafikdata eller lokaliseringsdata, som 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, og som kan gøre det muligt at drage præcise slutninger om den pågældendes privatliv, med henblik på at foretage forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager, uden at denne adgang er begrænset til de procedurer, der har til formål at bekæmpe grov kriminalitet eller at forebygge alvorlige trusler mod den offentlige sikkerhed. Ifølge Domstolen er varigheden af den periode, for hvilken der er anmodet om adgang til disse data, og mængden eller arten af de data, der

⁴⁹ Nærmere bestemt artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1.

⁵⁰ Domstolens dom af 21.12.2016, Tele2 Sverige og Watson m.fl. (C-203/15 og C-698/15, [EU:C:2016:970](#), præmis 120).

er tilgængelige i en sådan periode, uden betydning i denne henseende. Domstolen bemærkede desuden, at samme direktiv i lyset af chartret, er til hinder for en national lovgivning, der tillægger anklagemyndigheden beføjelse til at give en offentlig myndighed adgang til trafikdata og lokaliseringsdata i forbindelse med en strafferetlig efterforskning.

Hvad angår det med den omhandlede lovgivning forfulgte formål om forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager var Domstolen af den opfattelse, at det i overensstemmelse med proportionalitetsprincippet kun er bekæmpelse af grov kriminalitet eller forebyggelse af alvorlige trusler mod den offentlige sikkerhed, der kan begrunde offentlige myndigheders adgang til en samling af trafikdata eller lokaliseringsdata, som kan gøre det muligt at drage præcise slutninger vedrørende de berørte personers privatliv, uden at andre faktorer vedrørende forholdsmæssigheden af en anmodning om adgang, såsom varigheden af den periode, for hvilken der anmodes om adgang til sådanne data, kan føre til, at formålet om forebyggelse, efterforskning, afsløring og retsforfølgning i straffesager i almindelighed kan begrunde en sådan adgang.

Hvad angår den beføjelse, som anklagemyndigheden var tillagt, til at give en offentlig myndighed adgang til trafikdata og lokaliseringsdata med henblik på at lede en strafferetlig efterforskning, bemærkede Domstolen, at det tilkommer national ret at fastsætte de betingelser, hvorunder udbydere af elektroniske kommunikationstjenester skal give de kompetente nationale myndigheder adgang til de data, som de råder over. For at opfylde kravet om proportionalitet skal en sådan lovgivning imidlertid 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 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.

Domstolen bemærkede, at det med henblik på i praksis at sikre fuld iagttagelse af disse betingelser er afgørende, at de kompetente nationale myndigheders adgang til de lagrede data er undergivet en forudgående kontrol, der foretages af enten en domstol eller en uafhængig administrativ enhed, og at denne domstols eller enheds afgørelse skal træffes på grundlag af en begrundet anmodning, som navnlig fremsættes af disse myndigheder inden for rammerne af procedurer med henblik på forebyggelse, afsløring eller strafferetlig forfølgning. I et behørigt begrundet hastende tilfælde skal denne prøvelse foretages hurtigst muligt.

I denne henseende præciserede Domstolen, at den forudgående kontrol bl.a. kræver, at den domstol eller enhed, der har til opgave at foretage denne kontrol, har alle de beføjelser og frembyder alle de garantier, der er nødvendige for at sikre en afvejning af de forskellige berørte interesser og rettigheder. Hvad nærmere bestemt angår en

strafferetlig efterforskning kræver en sådan kontrol, at denne domstol eller denne enhed er i stand til at sikre en rimelig ligevægt mellem dels de interesser, der er forbundet med, hvad der er nødvendigt af hensyn til efterforskningen i forbindelse med bekæmpelsen af kriminalitet, dels den grundlæggende ret til respekt for privatlivet og beskyttelsen af personoplysninger for så vidt angår de personer, hvis oplysninger er berørt af adgangen. Når denne kontrol ikke foretages af en domstol, men af en uafhængig administrativ enhed, skal denne have en status, der gør det muligt for den at udføre sine opgaver på en objektiv og upartisk måde og i denne forbindelse at handle uden udefrakommende indflydelse.

Domstolen bemærkede, at det heraf følger, at det krav om uafhængighed, som den myndighed, der har til opgave at udføre den forudgående kontrol, skal opfylde, indebærer, at denne myndighed skal være udenforstående i forhold til den myndighed, der anmoder om adgang til dataene, således at den førstnævnte myndighed er i stand til at foretage denne kontrol på en objektiv og upartisk måde uden nogen form for udefrakommende indflydelse. Navnlig inden for det strafferetlige område indebærer kravet om uafhængighed, at den myndighed, der har til opgave at foretage denne forudgående kontrol, for det første ikke er involveret i den pågældende strafferetlige efterforskning og for det andet er neutral i forhold til parterne i straffesagen. Dette er ikke tilfældet for en anklagemyndighed, der leder efterforskningen, og som i givet fald udøver påtalekompetencen, således som det var tilfældet for den estiske anklagemyndighed. Det fulgte heraf, at anklagemyndigheden ikke var i stand til at foretage den ovenfor nævnte forudgående kontrol.

Dom af 5. april 2022 (Store Afdeling), Commissioner of An Garda Síochána m.fl. (C-140/20, [EU:C:2022:258](#))

I denne sag blev anmodningen om præjudiciel afgørelse indgivet af Supreme Court (øverste domstol, Irland) i forbindelse med en civil sag anlagt af en person, der var blevet idømt livsvarigt fængsel for et drab begået i Irland. Den pågældende gjorde gældende, at visse bestemmelser i den nationale lov om lagring af data genereret i forbindelse med elektronisk kommunikation var i strid med EU-retten. Trafikdata og lokaliseringsdata vedrørende den sigtedes telefonopkald var i henhold til denne lov blevet lagret af udbydere af elektroniske kommunikationstjenester og gjort tilgængelige for politimyndighederne. Den forelæggende rets tvivl vedrørte bl.a. spørgsmålet, om en ordning for generel og udifferentieret lagring af disse data i forbindelse med bekæmpelse af grov kriminalitet er forenelig med direktiv 2002/58, sammenholdt med chartret.

Domstolen bekræftede ved sin dom, der blev afsagt af Store Afdeling, den retspraksis, der følger af dommen i sagen *La Quadrature du Net m.fl.*⁵¹, idet den præciserede

⁵¹ 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](#)).

rækkevidden af denne og bemærkede, at generel og udifferentieret lagring af trafikdata og lokaliseringsdata vedrørende elektronisk kommunikation ikke er tilladt med henblik på bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den offentlige sikkerhed. Domstolen bekræftede ligeledes den retspraksis, der følger af dommen i sagen Prokuratuur (Betingelser for adgang til oplysninger om elektronisk kommunikation)⁵², bl.a. hvad angår forpligtelsen til at undergive de kompetente nationale myndigheders adgang til de lagrede data en forudgående kontrol, der skal foretages af enten en domstol eller en uafhængig administrativ enhed, i forhold til en politiembedsmand.

Domstolen fastslog for det første, at direktiv 2002/58, sammenholdt med chartret, er til hinder for lovgivningsmæssige foranstaltninger, 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. Når der henses til dels de afskrækkende virkninger for udøvelsen af de grundlæggende rettigheder⁵³, som denne lagring kan have, dels alvoren af det indgreb, som den indebærer, skal en sådan lagring nemlig udgøre undtagelsen og ikke reglen i det system, der er indført ved dette direktiv, således at disse data ikke kan gøres til genstand for en systematisk og løbende lagring. Kriminalitet, selv særlig grov kriminalitet, kan ikke sidestilles med en trussel mod den nationale sikkerhed, for så vidt som der ved en sådan sidestilling ville kunne blive indført en mellemkategori mellem den nationale sikkerhed og den offentlige sikkerhed, med henblik på at anvende de krav, der gælder for førstnævnte, på sidstnævnte.

Derimod er direktiv 2002/58, sammenholdt med chartret, ikke til hinder for lovgivningsmæssige foranstaltninger, 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. Domstolen tilføjede, at en sådan lagringsforanstaltning rettet mod steder eller infrastrukturer, der regelmæssigt besøges af et meget stort antal personer, eller strategiske steder, såsom lufthavne, banegårde, havne eller vejafgiftsområder, kan gøre det muligt for de kompetente myndigheder at indhente oplysninger om tilstedeværelsen på disse steder eller i disse geografiske områder af de personer, som dér har brugt et elektronisk kommunikationsmiddel, og heraf drage konklusioner om disses tilstedeværelse og aktivitet på disse steder eller i disse geografiske områder med henblik på bekæmpelse af grov kriminalitet. Under alle omstændigheder kan eventuelle vanskeligheder ved at opstille de præcise tilfælde og betingelser, hvorunder der kan ske en målrettet lagring, ikke begrunde, at

⁵² Dom af 2.3.2021, Prokuratuur (Betingelser for adgang til oplysninger om elektronisk kommunikation) (C-746/18, [EU:C:2021:152](#)).

⁵³ Sikret ved chartrets artikel 7-11.

medlemsstaterne foreskriver generel og udifferentieret lagring af trafikdata og lokaliseringsdata.

Det nævnte direktiv, sammenholdt med chartret, er heller ikke til hinder for lovgivningsmæssige foranstaltninger, der med samme formål for øje 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, og de data, der vedrører identiteten på brugerne af elektroniske kommunikationsmidler. Hvad sidstnævnte aspekt angår præciserede Domstolen nærmere bestemt, at hverken direktiv 2002/58 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 påkommende tilfælde at give de kompetente nationale myndigheder adgang til disse oplysninger.

Det samme gælder for lovgivningsmæssige foranstaltninger, der ligeledes med henblik på bekæmpelse af grov kriminalitet og forebyggelse af alvorlige trusler mod den nationale sikkerhed gør det muligt ved en afgørelse fra den kompetente myndighed, som er underlagt en effektiv domstolsprøvelse, at påbyde udbydere af elektroniske kommunikationstjenester i en begrænset periode at foretage hurtig lagring («quick freeze») af de trafikdata og lokaliseringsdata, som disse tjenesteudbydere råder over. Det er nemlig kun bekæmpelsen af grov kriminalitet og a fortiori beskyttelsen af den nationale sikkerhed, der kan begrunde en sådan lagring, på den betingelse, at denne foranstaltning og adgangen til de lagrede data holder sig inden for grænserne af det strengt nødvendige. Domstolen bemærkede, at en sådan foranstaltning vedrørende hurtig lagring kan 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.

Herefter bemærkede Domstolen imidlertid, at alle de ovennævnte lovgivningsmæssige foranstaltninger ved klare og præcise regler skal sikre, 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. De forskellige foranstaltninger til lagring af trafikdata og lokaliseringsdata kan, efter den nationale lovgivers valg og inden for grænserne af det strengt nødvendige, finde anvendelse samtidig.

Domstolen bemærkede desuden, at såfremt der med henblik på bekæmpelse af grov kriminalitet blev givet adgang til sådanne data, som er blevet lagret generelt og udifferentieret for at håndtere en alvorlig trussel mod den nationale sikkerhed, ville det

være i strid med det hierarki af mål af almen interesse, der kan begrunde vedtagelse af en foranstaltning i henhold til direktiv 2002/58. Det ville nemlig indebære, at adgang ville kunne begrundes i et mål af mindre betydning end det, der har begrundet lagringen, nemlig beskyttelse af den nationale sikkerhed, med risiko for, at forbuddet mod at foretage en generel og udifferentieret lagring med henblik på bekæmpelse af grov kriminalitet herved ville blive berøvet sin effektive virkning.

For det andet fastslog Domstolen, at direktiv 2002/58, sammenholdt med chartret, er til hinder for en national lovgivning, hvorefter den centraliserede behandling af anmodninger om adgang til data lagret af udbydere af elektroniske kommunikationstjenester, der indgives af politiet i forbindelse med efterforskning og retsforfølgning af alvorlige strafbare handlinger, påhviler en politiembedsmand, også selv om vedkommende bistås af en enhed oprettet inden for politiet, der ved udførelsen af sine opgaver har en vis uafhængighed, og hvis afgørelser efterfølgende kan underkastes domstolsprøvelse. På den ene side opfylder en sådan embedsmand nemlig ikke de krav om uafhængighed og upartiskhed, der gælder for en administrativ myndighed, der foretager den forudgående kontrol af anmodninger om adgang fra de kompetente nationale myndigheder, for så vidt som vedkommende ikke er udenforstående i forhold til disse myndigheder. Selv om en sådan embedsmands afgørelse kan underkastes en efterfølgende kontrol, kan denne kontrol på den anden side ikke træde i stedet for en uafhængig og, undtagen i behørigt begrundede hastetilfælde, forudgående kontrol.

Endelig bekræftede Domstolen for det tredje sin praksis, hvorefter EU-retten er til hinder for, at en national ret tidsmæssigt begrænser virkningerne af en ugyldighedserklæring, som det i henhold til national ret påhviler denne ret at afsige med hensyn til en national lovgivning, der pålægger udbydere af elektroniske kommunikationstjenester at foretage en generel og udifferentieret lagring af trafikdata og lokaliseringsdata, på grund af denne lovgivnings uforenelighed med direktiv 2002/58. Domstolen bemærkede imidlertid, at spørgsmålet om antageligheden af beviser, der er fremskaffet ved hjælp af en sådan lagring, i overensstemmelse med princippet om medlemsstaternes procesautonomi henhører under national ret, dog under overholdelse af navnlig ækvivalensprincippet og effektivitetsprincippet.

Dom af 20. september 2022 (Store Afdeling), VD og SR (C-339/20 og C-397/20, [EU:C:2022:703](#))

Efter en undersøgelse afviklet af Autorité des marchés financiers (AMF) (finansstilsynsmyndigheden, Frankrig) blev der indledt straffesager i forhold til VD og SR, som var to fysiske personer, der blev tiltalt for insiderhandel, hæleri i forbindelse med insiderhandel, medvirken, korruption og hvidvask. Som led i undersøgelsen anvendte AMF personoplysninger fra telefonsamtaler gennemført af VD og SR, som var indhentet i henhold til den franske code des postes et des communications électroniques (lov om postvæsen og elektronisk kommunikation), i forbindelse med leveringen af elektroniske kommunikationstjenester.

For så vidt som de respektive sigtelser var støttet på trafikdata fremlagt af AMF, anlagde VD og SR begge sag for cour d'appel de Paris (appeldomstolen i Paris, Frankrig), hvorved de bl.a. fremsatte et anbringende, der vedrørte en tilsidesættelse af artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartrets artikel 7, 8 og 11 samt artikel 52, stk. 1. Nærmere bestemt anfægtede VD og SR med støtte i retspraksis efter dommen i sagen Tele2 Sverige og Watson m.fl.⁵⁴ den omstændighed, at AMF med henblik på indsamlingen af de nævnte data støttede sig på de omhandlede nationale bestemmelser, selv om disse bestemmelser efter deres opfattelse for det første var uforenelige med EU-retten, for så vidt som de foreskrev en generel og udifferentieret lagring af forbindelsesdata, og for det andet ikke fastsatte nogen begrænsning for AMF's efterforskeres beføjelse til at indhente de lagrede data.

Ved to domme afsagt den 20. december 2018 og den 7. marts 2019 besluttede cour d'appel de Paris (appeldomstolen i Paris) ikke at give VD og SR medhold i deres søgsmål. Den ret, der behandlede sagens realitet, lagde for at forkaste ovennævnte anbringende navnlig vægt på den omstændighed, at forordningen om markedsmisbrug⁵⁵ gør det muligt for de kompetente myndigheder, i det omfang det er tilladt i national ret, at få udleveret eksisterende fortegnelser og trafikdata, som operatørerne af elektroniske kommunikationstjenester råder over, når der er grundlag for en mistanke om overtrædelse af forbuddet mod insiderhandel, og når sådanne fortegnelser kan være relevante for undersøgelsen af overtrædelsen.

VD og SR iværksatte herefter appel til prøvelse af disse domme ved Cour de cassation (kassationsdomstol, Frankrig), der var den forelæggende ret i disse sager.

I denne sammenhæng nærede den forelæggende ret tvivl om, hvorvidt artikel 15, stk. 1, i direktiv 2002/58, sammenholdt med chartret, kunne forenes med de krav, som fremgår af artikel 12, stk. 2, litra a) og d), i direktivet om »markedsmisbrug«⁵⁶ og artikel 23, stk. 2, litra g) og h), i forordningen om markedsmisbrug. Denne tvivl udsprang af de i hovedsagerne omhandlede retsfor skrifter, som i forebyggende øjemed pålagde operatørerne af elektroniske kommunikationstjenester en pligt til generel og udifferentieret lagring af trafikdata i et år fra den dato, hvor de var blevet registreret, med henblik på bekæmpelsen af overtrædelser i form af markedsmisbrug, hvilket omfattede insiderhandel. Såfremt Domstolen måtte fastslå, at den i hovedsagerne omhandlede lovgivning om lagring af forbindelsesdata var uforenelig med EU-retten, forelagde den forelæggende ret spørgsmålet om den midlertidige opretholdelse af virkningerne af denne lovgivning med henblik på at undgå retlig usikkerhed og tillade, at tidligere indsamlede og lagrede data blev anvendt til afsløring og efterforskning af insiderhandel.

⁵⁴ Domstolens dom af 21.12.2016, Tele2 Sverige og Watson m.fl. (C-203/15 og C-698/15, [EU:C:2016:970](#)).

⁵⁵ Europa-Parlamentets og Rådets forordning (EU) nr. 596/2014 af 16.4.2014 om markedsmisbrug (forordningen om markedsmisbrug) og om ophævelse af Europa-Parlamentets og Rådets direktiv 2003/6/EF og Kommissionens direktiv 2003/124/EF, 2003/125/EF og 2004/72/EF (EUT 2014, L 173, s. 1).

⁵⁶ Europa-Parlamentets og Rådets direktiv 2003/6/EF af 28.1.2003 om insiderhandel og kursmanipulation (markedsmisbrug) (EFT 2003, L 96, s. 16).

Med sin dom fastslog Domstolen, sat i Store Afdeling, at en generel og udifferentieret lagring af trafikdata i et år fra den dato, hvor de var blevet registreret af operatørerne af elektroniske kommunikationstjenester, ikke er tilladt i forebyggende øjemed med henblik på bekæmpelsen af overtrædelser i form af markedsmisbrug. Den bekræftede endvidere sin praksis om, at EU-retten er til hinder for, at en national retsinstans tidsmæssigt begrænser virkningerne af en ugyldighedserklæring, som det i henhold til national ret påhviler den at træffe i forhold til nationale retsfor skrifter, der er uforenelige med EU-retten.

Domstolen bemærkede indledningsvis, at der ved fortolkningen af en EU-retlig bestemmelse ikke blot 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.

Hvad angår ordlyden af de bestemmelser, der var omhandlet i de præjudicielle spørgsmål, fastslog Domstolen, at hvor artikel 12, stk. 2, litra d), i direktivet om »markedsmisbrug« vedrørte AMF's beføjelse til »at kræve oplysninger om foreliggende telefonsamtaler og foreliggende datatrafik«, henviste artikel 23, stk. 2, litra g) og h), i forordningen om markedsmisbrug til denne myndigheds mulighed for dels at få udleveret »fortegnelse over datatrafik hos investeringsselskaber, kreditinstitutter eller finansieringsinstitutter«, dels, »såfremt det er tilladt i henhold til national ret, at få udleveret fortegnelser over datatrafik hos en telekommunikationsoperatør«. Ifølge Domstolen fremgår det utvetydigt af disse bestemmelsers ordlyd, at de blot fastsætter rammer for AMF's beføjelse til at »kræve« eller endda at »få udleveret« disse operatørers data, hvilket svarer til en adgang til disse data. Desuden antyder henvisningen til »foreliggende« fortegnelser »hos« de nævnte operatører, at EU-lovgiver ikke har ønsket at regulere den nationale lovgivers mulighed for at indføre en pligt til lagring af sådanne fortegnelser. Ifølge Domstolen understøttes denne fortolkning i øvrigt af såvel den sammenhæng, hvori de nævnte bestemmelser indgår, som af de mål, der forfølges med den lovgivning, som disse bestemmelser er en del af.

Hvad angår den sammenhæng, hvori de af de præjudicielle spørgsmål omhandlede bestemmelser indgik, bemærkede Domstolen, at selv om det følger af ordlyden af de relevante bestemmelser i direktivet om »markedsmisbrug« og forordningen om markedsmisbrug⁵⁷, at EU-lovgiver tilsigtede at pålægge medlemsstaterne at træffe de nødvendige foranstaltninger, med henblik på at de kompetente myndigheder på det finansielle område har en række passende værktøjer, kompetencer og midler samt de nødvendige tilsyns- og undersøgelsesbeføjelser til at sikre deres opgavers effektivitet, tager disse bestemmelser hverken stilling til medlemsstaternes eventuelle mulighed for med henblik herpå at pålægge operatørerne af elektroniske kommunikationstjenester en pligt til generel og udifferentieret lagring af trafikdata eller til de betingelser,

⁵⁷ Henholdsvis artikel 12, stk. 1, i direktivet om »markedsmisbrug« og artikel 23, stk. 3, i forordningen om markedsmisbrug, sammenholdt med 62. betragtning hertil.

hvorunder de nævnte operatører skal lagre disse data med henblik på den eventuelle udlevering heraf til de kompetente myndigheder.

Hvad angår de mål, der forfølges med den omhandlede lovgivning, bemærkede Domstolen, at det fremgår af såvel direktivet om »markedsmisbrug« som af forordningen om markedsmisbrug⁵⁸, at disse instrumenter har til formål at sikre EU-finansmarkedernes integritet og forbedre investorernes tillid til disse markeder, en tillid, som bl.a. afhænger af, at de stilles lige, og at de er beskyttet mod ulovlig anvendelse af intern viden. Formålet med det forbud mod insiderhandel, der er fastsat i nævnte instrumenter⁵⁹, er således at sikre, at medkontrahenterne stilles lige i en børstransaktion, hvorved man undgår, at en person, som er i besiddelse af intern viden og dermed befinder sig i en fordelagtig stilling i forhold til andre investorer, profiterer heraf til skade for den, som ikke er i besiddelse af den interne viden. Selv om det fremgår af forordningen om markedsmisbrug⁶⁰, at fortegnelser over forbindelsesdata udgør yderst vigtigt – og undertiden det eneste – bevismateriale, der kan afsløre og bevise insiderhandel og markedsmanipulation, følger det ikke desto mindre heraf, at denne forordning kun sigter til fortegnelser, der »opbevares« af operatører af elektroniske kommunikationstjenester, samt til beføjelsen for den myndighed, der er kompetent på det finansielle område, til at »kræve« at få udleveret »eksisterende« data hos disse operatører. Det fremgår således på ingen måde af denne retsakt, at EU-lovgiver herved tilsigtede at indrømme medlemsstaterne en beføjelse til at pålægge operatørerne af elektroniske kommunikationstjenester en generel pligt til lagring af data. Det følger heraf, at hverken direktivet om »markedsmisbrug« eller forordningen om markedsmisbrug kan udgøre et retsgrundlag for en generel pligt til lagring af fortegnelser over trafikdata, som opbevares af operatører af elektroniske kommunikationstjenester, med henblik på at den myndighed, der er kompetent på det finansielle område, kan udøve sine beføjelser i henhold til disse retsakter.

Dernæst bemærkede Domstolen, at direktiv 2002/58 udgør referenceretsakten for så vidt angår lagring og, mere generelt, behandling af personoplysninger i den elektroniske kommunikationssektor, således at den af Domstolen anlagte fortolkning i forhold til dette direktiv ligeledes gælder for fortegnelser over trafikdata, som operatører af elektroniske kommunikationstjenester råder over, og som de myndigheder, der er kompetente på det finansielle område som omhandlet i direktivet om »markedsmisbrug« og forordningen om markedsmisbrug⁶¹, kan kræve udleveret fra disse. Vurderingen af lovligheden af behandlingen af de fortegnelser, som operatørerne af elektroniske kommunikationstjenester råder over⁶², skal følgelig foretages i lyset af

⁵⁸ Henholdsvis 2. og 12. betragtning til direktivet om »markedsmisbrug« og artikel 1 i forordningen om markedsmisbrug, sammenholdt med 2. og 24. betragtning hertil.

⁵⁹ Artikel 2, stk. 1, i direktivet om »markedsmisbrug« og artikel 8, stk. 1, i forordningen om markedsmisbrug.

⁶⁰ 62. betragtning til forordningen om markedsmisbrug.

⁶¹ Henholdsvis artikel 11 i direktivet om »markedsmisbrug« og artikel 22 i forordningen om markedsmisbrug.

⁶² Som omhandlet i artikel 12, stk. 2, litra d), i direktivet om »markedsmisbrug« og artikel 23, stk. 2, litra g) og h), i forordningen om markedsmisbrug.

de betingelser, der er fastsat i direktiv 2002/58, samt fortolkningen af dette direktiv i Domstolens praksis.

Domstolen fastslog således, at direktivet om »markedsmisbrug« og forordningen om markedsmisbrug, sammenholdt med direktiv 2002/58, og i lyset af chartret, er til hinder for retsfor skrifter, der med henblik på bekæmpelse af overtrædelser i form af markedsmisbrug, hvilket omfatter insiderhandel, i forebyggende øjemed foreskriver midlertidig, men generel og udifferentieret lagring af trafikdata i et år fra den dato, hvor de er blevet registreret af operatørerne af elektroniske kommunikationstjenester.

Endelig bekræftede Domstolen sin praksis, hvorefter EU-retten er til hinder for, at en national retsinstans tidsmæssigt begrænser virkningerne af en ugyldighedserklæring, som det i henhold til national ret påhviler den at træffe i forhold til nationale retsfor skrifter, der for det første pålægger operatører af elektroniske kommunikationstjenester at foretage en generel og udifferentieret lagring af trafikdata og for det andet giver mulighed for at udlevere disse data til den kompetente myndighed på det finansielle område uden forudgående tilladelse fra en domstol eller fra en uafhængig administrativ myndighed, eftersom disse bestemmelser er uforenelige med direktiv 2002/58, sammenholdt med chartret. Domstolen bemærkede imidlertid, at spørgsmålet om antageligheden af beviser, der er fremskaffet ved hjælp af en sådan lagring, i overensstemmelse med princippet om medlemsstaternes procesautonomi henhører under national ret, dog under overholdelse af navnlig ækvivalensprincippet og effektivitetsprincippet. Sidstnævnte pålægger den nationale ret at se bort fra de oplysninger og de beviser, der er opnået ved hjælp af en generel og udifferentieret lagring, som er uforenelig med EU-retten, hvis de berørte personer ikke er i stand til effektivt at udtale sig om disse oplysninger og disse beviser, som henhører under et område, der ligger uden for rettens sagkundskab, og som kan have afgørende indflydelse på vurderingen af de faktiske omstændigheder.

Dom af 30. april 2024 (plenum), La Quadrature du Net m.fl. (Personoplysninger og bekæmpelse af immaterialretskrænkelser) (C-470/21, [EU:C:2024:370](#))

Efter en anmodning om præjudiciel afgørelse fra Conseil d'État (øverste domstol i forvaltningsretlige sager, Frankrig) udbyggede Domstolen (plenum) sin praksis vedrørende direktiv 2002/58 med præciseringer vedrørende for det første de betingelser, hvorunder generel lagring af IP-adresser foretaget af udbydere af elektroniske kommunikationstjenester kan anses for ikke at medføre et alvorligt indgreb i den ret til respekt for privatlivet, beskyttelse af personoplysninger og ytringsfrihed, som er sikret ved chartret ⁶³, og for det andet muligheden for en offentlig myndighed for at få adgang til visse personoplysninger, der er lagret under overholdelse af disse betingelser,

⁶³ Chartrets artikel 7, 8 og 11

i forbindelse med bekæmpelse af krænkelse af intellektuelle ejendomsrettigheder begået online.

I det foreliggende tilfælde havde fire foreninger indgivet en anmodning om ophævelse af dekretet om automatiseret behandling af personoplysninger til Premier ministre (premierministeren, Frankrig) ⁶⁴. Anmodningen blev ikke besvaret, og disse foreninger anlagde derfor sag ved Conseil d'État (øverste domstol i forvaltningsretlige sager) med påstand om annullation af denne afgørelse om stiltiende afslag. Ifølge sagsøgerne var dette dekret og de bestemmelser, der udgjorde retsgrundlaget for det ⁶⁵, i strid med EU-retten.

Efter fransk lovgivning kan Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (den høje myndighed for spredning af værker og beskyttelse af rettigheder på internettet (Hadopi)), for at kunne identificere de ansvarlige for krænkelse af ophavsrettigheder eller beslægtede rettigheder, der begås online, få adgang til visse data, som udbydere af elektroniske kommunikationstjenester har pligt til at lagre. Disse data vedrører en berørt persons identitet knyttet til den pågældendes IP-adresse, som forudgående er blevet indsamlet af rettighedsorganisationer. Når først indehaveren af den IP-adresse, der er blevet brugt til aktiviteter, som medfører en sådan krænkelse, er identificeret, følger Hadopi proceduren med såkaldte »gradvise foranstaltninger«. Myndigheden har konkret beføjelse til at sende to henstillinger, der ligner advarsler, til denne person og, hvis aktiviteternes fortsættes, en skrivelse med meddelelse til den pågældende om, at vedkommendes aktiviteter kan give anledning til strafferetlig forfølgning. Endelig kan myndigheden indbringe sagen for anklagemyndigheden med henblik på retsforfølgning af personen ⁶⁶.

På denne baggrund anmodede Conseil d'État (øverste domstol i forvaltningsretlige sager) Domstolen om at fortolke direktiv 2002/58 ⁶⁷.

Hvad angår lagringen af identitetsdata og de hertil knyttede IP-adresser fremhævede Domstolen for det første, at ikke enhver generel og udifferentieret lagring af IP-adresser nødvendigvis udgør et alvorligt indgreb i retten til respekt for privatlivet, beskyttelse af personoplysninger og ytringsfrihed som sikret ved chartret.

Forpligtelsen til at foretage en sådan lagring kan være begrundet i formålet om at bekæmpe strafbare handlinger i almindelighed, når det faktisk er udelukket, at denne

⁶⁴ Décret no 2010-236 du 5 mars 2010, relatif au traitement automatisé de données à caractère personnel autorisé par l'article L. 331-29 du code de la propriété intellectuelle dénommé »Système de gestion des mesures pour la protection des œuvres sur internet« (dekret 2010-236 af 5.3.2010 om den automatiserede behandling af personoplysninger, der er tilladt i medfør af artikel L. 331-29 i lov om intellektuel ejendomsret og benævnt »System til håndtering af foranstaltninger til beskyttelse af værker på internettet«) (JORF nr. 56 af 7.3.2010, tekst nr. 19), som ændret ved décret no 2017-924, du 6 mai 2017, relatif à la gestion des droits d'auteur et des droits voisins par un organisme de gestion de droits et modifiant le code de la propriété intellectuelle (dekret 2017-924 af 6.5.2017 om forvaltning af ophavsret og beslægtede rettigheder gennem en forvaltningsorganisation og om ændring af lov om intellektuel ejendomsret) (JORF nr. 109 af 10.5.2017, tekst nr. 176).

⁶⁵ Bl.a. artikel L. 331-21, stk. 3-5, i lov om intellektuel ejendomsret.

⁶⁶ Med virkning fra den 1.1.2022 blev Hadopi lagt sammen med Conseil supérieur de l'audiovisuel (øverste råd for audiovisuelle anliggender (CSA)), der er en anden uafhængig offentlig myndighed, til Autorité de régulation de la communication audiovisuelle et numérique (tilsynsmyndighed for audiovisuel og digital kommunikation (ARCOM)). Proceduren med gradvise foranstaltninger er dog i det væsentlige forblevet uændret.

⁶⁷ Artikel 15, stk. 1, i direktiv 2002/58.

lagring kan medføre alvorlige indgreb i den berørte persons privatliv som følge af muligheden for at drage præcise slutninger om vedkommende, bl.a. ved at koble disse IP-adresser sammen med en række trafik- eller lokaliseringsdata.

En medlemsstat, der påtænker at pålægge udbyderne af elektroniske kommunikationstjenester en sådan forpligtelse, skal derfor sikre, at måden, hvorpå disse data lagres, udelukker, at der kan drages præcise slutninger om de pågældende personers privatliv.

Domstolen præciserede, at lagringsmåden med dette for øje skal vedrøre selve strukturen af lagringen, som i det væsentlige skal være tilrettelagt således, at det sikres, at de forskellige kategorier af lagrede data faktisk er hermetisk adskilte. De nationale regler vedrørende denne lagringsmåde skal således sikre, at hver kategori af data, herunder identitetsdataene og IP-adresserne, opbevares fuldstændig adskilt fra de øvrige kategorier af lagrede data, og at denne adskillelse faktisk er hermetisk tæt, ved hjælp af et sikkert og pålideligt IT-system. Desuden må disse regler, for så vidt som de giver mulighed for at koble de lagrede IP-adresser sammen med den berørte persons identitet med henblik på bekæmpelse af strafbare handlinger, kun tillade en sådan sammenkobling ved anvendelse af en effektiv teknisk fremgangsmåde, der ikke skader effektiviteten af den hermetiske adskillelse af disse datakategorier. Pålideligheden af denne adskillelse skal kontrolleres regelmæssigt af en udenforstående offentlig myndighed. For så vidt som den gældende nationale lovgivning fastsætter sådanne strenge krav, kan det indgreb, der følger af denne lagring af IP-adresser, ikke kvalificeres som »alvorligt«.

Domstolen konkluderede følgelig, at såfremt der findes lovbestemmelser, som garanterer, at ingen kombination af data vil kunne gøre det muligt at drage præcise slutninger om privatlivet for den person, hvis data er blevet lagret, er direktiv 2002/58, sammenholdt med chartret, ikke til hinder for, at en medlemsstat indfører en forpligtelse til generel og udifferentieret lagring af IP-adresser i et tidsrum, der ikke overstiger det strengt nødvendige, med henblik på bekæmpelse af strafbare handlinger i almindelighed.

For det andet fastslog Domstolen med hensyn til adgangen til identitetsdata knyttet til IP-adresser, at direktiv 2002/58, sammenholdt med chartret, principielt ikke er til hinder for en national lovgivning, der tillader, at en offentlig myndighed får adgang til disse data, som er lagret af udbyderne af elektroniske kommunikationstjenester særskilt og på en sådan måde, at dataene er hermetisk adskilte, alene med det formål, at denne myndighed kan identificere indehaverne af disse adresser, der mistænkes for at være ansvarlige for krænkelse af ophavsrettigheder og beslægtede rettigheder på internettet, og træffe foranstaltninger over for dem. I et sådant tilfælde skal den nationale lovgivning forbyde de embedsmænd, der har en sådan adgang, for det første at udbrede oplysninger i nogen som helst form om indholdet af de filer, som disse indehavere har konsulteret, undtagen med henblik på indbringelse af sagen for anklagemyndigheden, for det andet at foretage sporing af nogen art af indehavernes

søgemønstre og for det tredje at anvende disse IP-adresser til andre formål end at træffe disse foranstaltninger.

I denne forbindelse bemærkede Domstolen bl.a., at selv om ytringsfriheden og fortroligheden af personoplysninger er yderst vigtige hensyn, er disse grundlæggende rettigheder dog ikke absolutte. I forbindelse med en afvejning af de omhandlede rettigheder og interesser må disse til tider vige for andre grundlæggende rettigheder og tvingende almene hensyn, såsom beskyttelsen af den offentlige orden og forebyggelsen af strafbare handlinger eller beskyttelsen af andres rettigheder og friheder. Dette er navnlig tilfældet, når den afgørende vægt, der tillægges disse yderst vigtige hensyn, kan hindre effektiviteten af en strafferetlig efterforskning, bl.a. ved at gøre det umuligt eller uforholdsmæssigt vanskeligt faktisk at identificere gerningsmanden til en strafbar handling og pålægge vedkommende en sanktion.

I samme forbindelse henviste Domstolen ligeledes til sin praksis om, at hvad angår bekæmpelsen af strafbare handlinger, der krænker ophavsrettigheder eller beslægtede rettigheder, og som begås online, synes det forhold, at adgang til IP-adresserne kan udgøre det eneste efterforskningsmiddel, der gør det muligt at identificere den pågældende person, at godtgøre, at lagring af og adgang til disse adresser er strengt nødvendig for virkeliggørelsen af det formål, der forfølges, og dermed opfylder proportionalitetskravet. Ikke at tillade en sådan adgang ville i øvrigt indebære en reel risiko for systemisk straffrihed for strafbare handlinger, der begås online, eller som internettets særlige kendetegn gør det lettere at begå eller forberede. Eksistensen af en sådan risiko er en relevant omstændighed, når det i forbindelse med en afvejning af de forskellige foreliggende rettigheder og interesser bedømmes, om et indgreb i retten til respekt for privatlivet, beskyttelse af personoplysninger og ytringsfrihed er en forholdsmæssig foranstaltning i forhold til formålet om at bekæmpe strafbare handlinger.

For det tredje fastslog Domstolen med hensyn til spørgsmålet om, hvorvidt den offentlige myndigheds adgang til identitetsdata knyttet til en IP-adresse skal underkastes en forudgående kontrol foretaget af en domstol eller en uafhængig administrativ enhed, at kravet om en sådan kontrol gælder, når adgangen i medfør af en national lovgivning medfører risiko for et alvorligt indgreb i den berørte persons grundlæggende rettigheder i den forstand, at den kan gøre det muligt for den offentlige myndighed at drage præcise slutninger om denne persons privatliv og efter omstændighederne fastlægge en detaljeret profil af vedkommende. Omvendt skal dette krav om en forudgående kontrol ikke finde anvendelse, når indgrebet i de grundlæggende rettigheder ikke kan kvalificeres som alvorligt.

I denne henseende præciserede Domstolen, at såfremt der er indført en lagringsordning, der sikrer, at de forskellige kategorier af lagrede data faktisk er hermetisk adskilte, er den offentlige myndigheds adgang til identitetsdata knyttet til IP-adresser principielt ikke underlagt kravet om en forudgående kontrol. En sådan adgang

alene med det formål at identificere indehaveren af en IP-adresse udgør nemlig som hovedregel ikke et alvorligt indgreb i ovennævnte rettigheder.

Domstolen udelukkede imidlertid ikke, at der i atypiske situationer kan være risiko for, at den offentlige myndighed i forbindelse med en procedure som den i hovedsagen omhandlede med gradvise foranstaltninger kan drage præcise slutninger om den berørte persons privatliv, bl.a. når denne person gentagne gange, eller i stor målestok, beskæftiger sig med aktiviteter, der krænker ophavsrettigheder eller beslægtede rettigheder i peer-to-peer-netværk i forbindelse med bestemte typer beskyttede værker, som afslører – eventuelt følsomme – oplysninger om vedkommendes privatliv.

I det foreliggende tilfælde kunne en indehaver af en IP-adresse være særligt udsat for en sådan risiko på tidspunktet for den offentlige myndigheds afgørelse om en eventuel indbringelse af sagen for anklagemyndigheden med henblik på retsforfølgning af den pågældende. Voldsomheden af indgrebet i retten til respekt for privatlivet kan nemlig stige, efterhånden som proceduren med gradvise foranstaltninger, der forløber i trin, når igennem de forskellige faser, som den består af. Den kompetente myndigheds adgang til det sæt af data, der vedrører den berørte person, og som er kumuleret i de forskellige faser af denne procedure, kan gøre det muligt at drage præcise slutninger om vedkommendes privatliv. Følgelig skal den nationale lovgivning fastsætte krav om en forudgående kontrol, der skal foretages, inden den offentlige myndighed kan sammenkoble identitetsdata og et sådant sæt af data, og inden en eventuel fremsendelse af skrivelsen med meddelelse om, at personen beskæftiger sig med aktiviteter, der kan give anledning til strafferetlig forfølgning. Kontrollen skal i øvrigt sikre effektiviteten af proceduren med gradvise foranstaltninger ved navnlig at gøre det muligt at identificere tilfælde af eventuelle gentagelser af den omhandlede overtrædelse. Med henblik herpå skal denne procedure tilrettelægges og struktureres på en sådan måde, at en persons identitetsdata, der er knyttet til IP-adresser, som forudgående er indsamlet på internettet, ikke af de personer i den kompetente offentlige myndighed, der har til opgave at undersøge de faktiske omstændigheder, automatisk kan sammenkobles med de oplysninger, som denne myndighed allerede råder over, og som kan gøre det muligt at drage præcise slutninger om denne persons privatliv.

Hvad endvidere angår genstanden for den forudgående kontrol bemærkede Domstolen, at i de tilfælde, hvor den berørte person mistænkes for at have begået en overtrædelse, der hører under strafbare handlinger i almindelighed, skal den domstol eller uafhængige administrative enhed, der skal foretage kontrollen, nægte adgang, når denne ville gøre det muligt for den offentlige myndighed at drage præcise slutninger om personens privatliv. Derimod skal selv adgang, der gør det muligt at drage sådanne præcise slutninger, tillades i de tilfælde, hvor den berørte person mistænkes for at have begået strafbare handlinger, som den pågældende medlemsstat anser for at være til skade for en grundlæggende samfundsinteresse og derfor hører under de alvorlige former for kriminalitet.

Domstolen præciserede ligeledes, at en forudgående kontrol i intet tilfælde kan være fuldstændig automatiseret, for hvad angår en strafferetlig efterforskning kræver en sådan kontrol en afvejning af på den ene side de legitime interesser, der er forbundet med bekæmpelse af kriminalitet, og på den anden side respekten for privatlivet og beskyttelsen af personoplysninger. En sådan afvejning kræver en fysisk persons medvirken, idet denne er så meget desto mere nødvendig, som automatikken i og det store omfang af den omhandlede databehandling indebærer risici for privatlivet.

Domstolen konkluderede således, at muligheden for de personer i den offentlige myndighed, der har til opgave at undersøge de faktiske omstændigheder, for at koble en persons identitetsdata, der er knyttet til en IP-adresse, sammen med de filer med oplysninger, der gør det muligt at få kendskab til titlen på de beskyttede værker, hvis tilrådsstilling på internettet har begrundet rettighedsorganisationernes indsamling af IP-adresserne, i tilfælde af samme persons gentagelse af en aktivitet, der krænker ophavsrettigheder eller beslægtede rettigheder, skal være undergivet en kontrol ved en domstol eller en uafhængig administrativ enhed. Denne kontrol må ikke være fuldstændig automatiseret, og den skal foretages forud for en sådan sammenkobling af data, der i sådanne tilfælde kan gøre det muligt at drage præcise slutninger om privatlivet for denne person, hvis IP-adresse er blevet anvendt til aktiviteter, der kan krænke ophavsrettigheder eller beslægtede rettigheder.

For det fjerde og sidste bemærkede Domstolen, at det databehandlingssystem, som den offentlige myndighed anvender, med jævne mellemrum skal kontrolleres af et uafhængigt organ, der er udenforstående i forhold til denne myndighed. Denne kontrol tager sigte på at efterprøve systemets integritet, herunder de effektive garantier mod risikoen for uberettiget eller ulovlig adgang til og anvendelse af disse data, samt systemets effektivitet og pålidelighed med hensyn til at afsløre eventuelle overtrædelser.

I denne forbindelse bemærkede Domstolen, at den automatiserede behandling af personoplysninger foretaget af den offentlige myndighed på grundlag af oplysninger om krænkelser af immaterialretligheder konstateret af rettighedsorganisationer i det foreliggende tilfælde kunne medføre et vist antal falsk positive tilfælde og især risiko for, at et potentielt meget stort antal oplysninger blev misbrugt af tredjemand til uberettigede eller ulovlige formål, hvilket forklarer behovet for en sådan kontrol. Domstolen tilføjede desuden, at denne behandling skal overholde de særlige regler om beskyttelse af personoplysninger, der er fastsat i direktiv 2016/680. Selv om den offentlige myndighed i den foreliggende sag ikke havde selvstændige beslutningsbeføjelser i forbindelse med proceduren med såkaldte gradvise foranstaltninger, skulle den nemlig kvalificeres som en »offentlig myndighed«, der er involveret i forebyggelse og afsløring af strafbare handlinger, og den hørte dermed under dette direktivs anvendelsesområde. Personer, der er involveret i en sådan procedure, skal således være omfattet af en række sammenhængende materielle og processuelle garantier som foreskrevet ved direktiv 2016/680, idet det tilkom den forelæggende ret at efterprøve, om sådanne garantier var fastsat i national ret.

2. Behandling af personoplysninger i straffesager

Dom af 12. maj 2021 (Store Afdeling), Bundesrepublik Deutschland (Efterlysningsblad (rødt hjørne) fra INTERPOL) (C-505/19, [EU:C:2021:376](#))

Efter anmodning fra USA og på grundlag af en arrestordre udstedt af dette lands myndigheder offentliggjorde Den Internationale Kriminalpolitiorganisation (herefter »INTERPOL«) i 2012 et efterlysningsblad (rødt hjørne) vedrørende WS, der er tysk statsborger, med henblik på en eventuel udlevering af ham. Når en person, der er genstand for et sådant efterlysningsblad, lokaliseres i en medlemsstat i INTERPOL, skal denne medlemsstat principielt foretage en midlertidig anholdelse af personen eller overvåge eller begrænse dennes rejser.

Ifølge den forelæggende ret var der imidlertid allerede før offentliggørelsen af dette efterlysningsblad (rødt hjørne) blevet indledt en undersøgelsesprocedure vedrørende de samme strafbare handlinger som dem, der lå til grund for efterlysningsbladet, mod WS i Tyskland. Denne procedure blev endeligt afsluttet i 2010, efter at WS havde betalt et pengebeløb i overensstemmelse med en særlig bilæggelsesprocedure, som er fastsat i tysk strafferet. Efterfølgende meddelte Bundeskriminalamt (forbundskriminalpoliti, Tyskland) INTERPOL, at det som følge af denne tidligere procedure var af den opfattelse, at princippet *ne bis in idem* fandt anvendelse i den foreliggende sag. Dette princip, der er fastsat i såvel artikel 54 i konventionen om gennemførelse af Schengenaftalen ⁶⁸ som chartrets artikel 50, forbyder bl.a., at en person, over for hvem der er afsagt endelig dom, retsforfølges på ny for den samme lovovertrædelse.

I 2017 anlagde WS sag mod Forbundsrepublikken Tyskland ved Verwaltungsgericht Wiesbaden (forvaltningsdomstolen i Wiesbaden, Tyskland) med påstand om, at denne medlemsstat tilpligtedes at træffe de foranstaltninger, der var nødvendige for at trække det nævnte efterlysningsblad (rødt hjørne) tilbage. I denne henseende påberåbte WS sig, ud over en tilsidesættelse af princippet *ne bis in idem*, en tilsidesættelse af sin ved artikel 21 TEUF sikrede ret til fri bevægelighed, for så vidt som han ikke kunne rejse til en stat, der er part i Schengenaftalen, eller til en medlemsstat uden at risikere at blive anholdt. Han var ligeledes af den opfattelse, at som følge af disse tilsidesættelser var behandlingen af hans personoplysninger, der var indeholdt i efterlysningsbladet (rødt hjørne), i strid med direktiv 2016/680 om beskyttelse af personoplysninger i straffesager ⁶⁹.

⁶⁸ Konventionen om gennemførelse af Schengenaftalen af 14.6.1985 mellem regeringerne for staterne i Den Økonomiske Union Benelux, Forbundsrepublikken Tyskland og Den Franske Republik om gradvis ophævelse af kontrollen ved de fælles grænser (EFT 2000, L 239, s. 19) (herefter »gennemførelseskonventionen«).

⁶⁹ Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27.4.2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller

Det var i denne sammenhæng, at Verwaltungsgericht Wiesbaden (forvaltningsdomstolen i Wiesbaden) besluttede at forelægge Domstolen et spørgsmål om anvendelsen af princippet *ne bis in idem* og nærmere bestemt om muligheden for at foretage en midlertidig anholdelse af en person, der er genstand for et efterlysningsblad (rødt hjørne), i en situation som den omhandlede. Såfremt det nævnte princip fandt anvendelse, ønskede den forelæggende ret endvidere oplyst, hvilke konsekvenser dette har for medlemsstaternes behandling af de personoplysninger, som er indeholdt i et sådant efterlysningsblad.

I sin dom afsagt af Store Afdeling fastslog Domstolen bl.a., at bestemmelserne i direktiv 2016/680, sammenholdt med gennemførelseskonventionens artikel 54 og chartrets artikel 50, skal fortolkes således, at de ikke er til hinder for en behandling af de personoplysninger, som er indeholdt i et efterlysningsblad (rødt hjørne) udsendt af INTERPOL, så længe det ikke ved en sådan retsafgørelse er blevet godtgjort, at princippet *ne bis in idem* finder anvendelse for så vidt angår de strafbare handlinger, hvorpå dette efterlysningsblad er støttet, og forudsat at en sådan behandling opfylder de i direktivet fastsatte betingelser.

Hvad angår spørgsmålet om de personoplysninger, der er indeholdt i et efterlysningsblad (rødt hjørne) fra INTERPOL, anførte Domstolen, at enhver aktivitet, som disse oplysninger gøres til genstand for, såsom registreringen heraf i en medlemsstats efterlysningsdatabaser, udgør »behandling«, der er omfattet af direktiv 2016/680⁷⁰. Endvidere fastslog Domstolen dels, at denne behandling forfølger et legitimt formål, dels at den ikke kan anses for ulovlig med den begrundelse alene, at princippet *ne bis in idem* kan finde anvendelse på de strafbare handlinger, hvorpå efterlysningsbladet (rødt hjørne) er støttet⁷¹. Denne behandling foretaget af medlemsstaternes myndigheder kan i øvrigt vise sig at være nødvendig netop med henblik på at kontrollere, om det nævnte princip finder anvendelse.

Under disse omstændigheder fastslog Domstolen ligeledes, at direktiv 2016/680, sammenholdt med gennemførelseskonventionens artikel 54 og chartrets artikel 50, ikke er til hinder for behandling af de personoplysninger, der er indeholdt i et efterlysningsblad (rødt hjørne), så længe det ikke ved en endelig retsafgørelse er blevet fastslået, at princippet *ne bis in idem* finder anvendelse i den foreliggende sag. En sådan behandling skal imidlertid opfylde de betingelser, der er fastsat i dette direktiv. I denne henseende skal den bl.a. være nødvendig for, at en kompetent national myndighed kan udføre en opgave med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner⁷².

Når princippet *ne bis in idem* derimod finder anvendelse, er det ikke længere nødvendigt at registrere de personoplysninger, der er indeholdt i et efterlysningsblad

fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (EUT 2016, L 119, s. 89).

⁷⁰ Jf. artikel 2, stk. 1, og artikel 3, nr. 2), i direktiv 2016/680.

⁷¹ Jf. artikel 4, stk. 1, litra b), og artikel 8, stk. 1, i direktiv 2016/680.

⁷² Jf. artikel 1, stk. 1, og artikel 8, stk. 1, i direktiv 2016/680.

(rødt hjørne) fra INTERPOL, i medlemsstaternes efterlysningsdatabaser, eftersom den pågældende person ikke længere kan gøres til genstand for strafforfølgning for de strafbare handlinger, der er omfattet af det nævnte efterlysningsblad, og følgelig ikke længere kan anholdes på grundlag af disse handlinger. Det følger heraf, at den pågældende person skal kunne anmode om sletning af vedkommendes oplysninger. Hvis denne registrering imidlertid opretholdes, skal den ledsages af en angivelse af, at den pågældende person på grund af princippet *ne bis in idem* ikke længere kan retsforfølges i en medlemsstat eller i en stat, der er part i Schengenaftalen, for de samme strafbare handlinger.

Dom af 21. juni 2022 (Store Afdeling), Ligue des droits humains (C-817/19, [EU:C:2022:491](#))

I denne sag (se ligeledes afsnit I.1 med overskriften »Den afledte EU-rets overensstemmelse med retten til beskyttelse af personoplysninger«) foretog Domstolen, efter at have fastslået gyldigheden af PNR-direktivet, nogle præciseringer angående fortolkningen af visse af direktivets bestemmelser ⁷³.

Den bemærkede for det første, at direktivet udtømmende opregner de formål, der forfølges med behandlingen af PNR-oplysninger. Dette direktiv er derfor til hinder for en national lovgivning, der tillader behandling af PNR-oplysninger til andre formål end bekæmpelse af terrorhandling og grov kriminalitet. En national lovgivning, der desuden anerkender efterretnings- og sikkerhedstjenesternes overvågning af de omhandlede aktiviteter som formål med behandlingen af PNR-oplysninger, kan således udgøre en tilsidesættelse af den udtømmende karakter af denne opregning. Det system, der er indført ved PNR-direktivet, må heller ikke anvendes med henblik på at forbedre grænsekontrollen og bekæmpe ulovlig indvandring. Det følger ligeledes heraf, at PNR-oplysninger ikke må opbevares i en enkelt database, der kan konsulteres med henblik på både PNR-direktivets formål og andre formål.

Domstolen belyste for det andet begrebet uafhængig national myndighed, der er kompetent til at kontrollere, om betingelserne for videregivelse af PNR-oplysninger med henblik på efterfølgende vurdering er opfyldt, og til at godkende en sådan videregivelse. Navnlig kan den myndighed, der er oprettet som passageroplysningsenhed, ikke kvalificeres som en sådan uafhængig myndighed, da den ikke er udenforstående i forhold til den myndighed, der anmoder om adgang til oplysningerne. Da passageroplysningsenhedens personale kan være udstationeret fra de myndigheder, der kan anmode om en sådan adgang, synes den nemlig nødvendigvis at være knyttet til disse myndigheder. PNR-direktivet er derfor til hinder for en national lovgivning, hvorefter den myndighed, der er oprettet som passageroplysningsenhed, ligeledes har egenskab af kompetent national myndighed med bemyndigelse til at godkende

⁷³ Navnlig direktivets artikel 2 (»Anvendelse af [direktivet] på flyvninger inden for EU«), artikel 6 (»Behandling af PNR-oplysninger«) og artikel 12 (»Dataopbevaringsperiode og anonymisering«).

videregivelsen af PNR-oplysningerne ved udløbet af seks månedersperioden efter videregivelsen af disse oplysninger til passageroplysningsenheden.

For det tredje fastslog Domstolen med hensyn til dataopbevaringsperioden for PNR-oplysninger, at PNR-direktivets artikel 12, sammenholdt med chartrets artikel 7 og 8 samt artikel 52, stk. 1, er til hinder for en national lovgivning, som fastsætter en generel opbevaringsperiode for PNR-oplysninger på fem år, der finder anvendelse uden forskel på alle flypassagerer.

Ifølge Domstolen synes opbevaring af PNR-oplysninger, efter udløbet af den indledende opbevaringsperiode på seks måneder, nemlig ikke at være begrænset til det strengt nødvendige for så vidt angår de flypassagerer, for hvilke hverken den forudgående vurdering, de eventuelle kontroller, der er foretaget i løbet af den indledende opbevaringsperiode på seks måneder, eller nogen anden omstændighed har afsløret, at der foreligger objektive forhold – såsom at PNR-oplysningerne vedrørende de pågældende passagerer har givet et hit, der er blevet kontrolleret i forbindelse med den forudgående vurdering – som kan godtgøre en risiko i forbindelse med terrorhandlinger eller grov kriminalitet, der har en – i det mindste indirekte – objektiv forbindelse med disse passagerers flyrejse. Derimod fandt Domstolen, at opbevaring af PNR-oplysninger vedrørende samtlige flypassagerer, som er omfattet af det system, der er indført ved dette direktiv, i den indledende periode på seks måneder, principielt ikke synes at gå ud over grænserne for det strengt nødvendige.

For det fjerde udtalte Domstolen sig om en eventuel anvendelse af PNR-direktivet på andre transportformer, der befordrer passagerer i EU, med henblik på bekæmpelse af terrorhandlinger og grov kriminalitet. PNR-direktivet, sammenholdt med artikel 3, stk. 2, TEU, artikel 67, stk. 2, TEUF og chartrets artikel 45, er til hinder for et system for videregivelse og behandling af PNR-oplysninger for samtlige transportere med andre midler inden for EU, når den pågældende medlemsstat ikke står over for en reel og aktuel eller forudsigelig terrortrussel. I en sådan situation skal anvendelsen af det system, der er indført ved PNR-direktivet, ligesom for flyvninger inden for EU, begrænses til at omfatte PNR-oplysninger for transportere vedrørende bl.a. bestemte flyforbindelser eller rejseruter eller bestemte banegårde eller havne, for hvilke der foreligger oplysninger, der kan begrunde denne anvendelse. Det tilkommer den pågældende medlemsstat at udvælge de transportere, for hvilke sådanne oplysninger foreligger, og regelmæssigt foretage en ny vurdering af denne anvendelse i lyset af udviklingen i de forhold, der har begrundet valget af disse transportere.

IV. Videregivelse af personoplysninger til tredjelande

Dom af 6. november 2003 (Store Afdeling), Lindqvist (C-101/01, [EU:C:2003:596](#))

I denne sag (se ligeledes afsnit II.3 med overskriften »Begrebet »behandling af personoplysninger«») ønskede den forelæggende ret nærmere bestemt oplyst, om Bodil Lindqvist havde videregivet oplysninger til tredjelande i henhold til nævnte direktiv.

Domstolen fastslog, at der ikke foreligger en »videregivelse til et tredjeland af personoplysninger« i den forstand, hvori udtrykket er anvendt i artikel 25 i direktiv 95/46, når en person, der befinder sig i en medlemsstat, lægger personoplysninger ud på en internetside, der er lagret hos en fysisk eller juridisk person, som er internetvært for det websted, hvor den pågældende side kan konsulteres, og som er etableret i samme medlemsstat eller i en anden medlemsstat, hvorved personoplysningerne bliver tilgængelige for alle, der kobler sig på internettet, herunder personer i et tredjeland.

Når henses dels til internettets udviklingstrin på tidspunktet for udarbejdelsen af direktiv 95/46, dels til de manglende kriterier for anvendelsen af internettet i kapitel IV, som omfatter nævnte artikel 25, der har til formål at sikre medlemsstaternes kontrol med videregivelse af personoplysninger til tredjelande, og at hindre videregivelse, når disse ikke sikrer et tilstrækkeligt beskyttelsesniveau, kan det ikke formodes, at fællesskabslovgiver havde tilsigtet, at begrebet »videregivelse til et tredjeland af personoplysninger« fremtidigt skulle omfatte en sådan situation, hvor der lægges oplysninger ud på en internetside, selv om disse således er blevet gjort tilgængelige for personer i tredjelande, der har de tekniske muligheder for at få adgang hertil.

Dom af 6. oktober 2015 (Store Afdeling), Schrems (C-362/14, [EU:C:2015:650](#))

Maximillian Schrems, der er østrigsk statsborger og bruger af det sociale netværk Facebook, havde indgivet en klage til Data Protection Commissioner (den tilsynsførende for databeskyttelse, Irland) med den begrundelse, at Facebook Ireland videregav sine brugeres personoplysninger til USA og lagrede dem på servere beliggende i dette land, hvor de var genstand for en behandling. Maximillian Schrems anførte, at den gældende lovgivning og praksis i USA ikke sikrede en tilstrækkelig beskyttelse af de personoplysninger, der videregives til landet, mod de offentlige myndigheders overvågningsvirksomhed. Data Protection Commissioner afviste at behandle klagen med bl.a. den begrundelse, at Kommissionen i sin beslutning 2000/520/EF⁷⁴ fandt, at

⁷⁴ Kommissionens beslutning 2000/520/EF af 26.7.2000 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af safe harbor-principperne til beskyttelse af privatlivets fred og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium (EFT 2000, L 215, s. 7).

USA inden for rammerne af den såkaldte safe harbor-ordning⁷⁵ sikrede et tilstrækkeligt beskyttelsesniveau for videregivne personoplysninger.

High Court (appeldomstol, Irland) indgav i denne forbindelse en anmodning til Domstolen om fortolkning af artikel 25, stk. 6, i direktiv 95/46, hvorefter Kommissionen kan fastslå, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau i forbindelse med de videregivne oplysninger, og nærmere bestemt en anmodning om klarlæggelse af gyldigheden af beslutning 2000/520, som Kommissionen havde vedtaget på grundlag af artikel 25, stk. 6, i direktiv 95/46.

Domstolen erklærede Kommissionens beslutning ugyldig i det hele, idet den først og fremmest fremhævede, at vedtagelse af beslutningen krævede, at Kommissionen behørigt konstaterer, at det pågældende tredjeland faktisk sikrer et beskyttelsesniveau for de grundlæggende rettigheder, som i det væsentlige svarer til det niveau, der er sikret i Unionens retsorden. Da Kommissionen imidlertid ikke har konstateret dette i beslutning 2000/520, tilsidesætter beslutningens artikel 1 de krav, der er fastsat i artikel 25, stk. 6, i direktiv 95/46, sammenholdt med chartret, og er følgelig ugyldig. Safe harbor-principperne finder nemlig udelukkende anvendelse på de selvcertificerede amerikanske foretagender, der modtager personoplysninger fra Unionen, uden at der stilles krav om, at de amerikanske offentlige myndigheder undergives overholdelse af de nævnte principper. Endvidere åbner beslutning 2000/520 op for, at der foretages indgreb i de grundlæggende rettigheder hos de personer, hvis personoplysninger bliver eller kan blive videregivet fra Unionen til USA, uden at beslutningen indeholder nogen konstateringer om, hvorvidt der i USA foreligger regler af statslig karakter, hvorved det tilsigtes at begrænse de eventuelle indgreb i disse rettigheder, og uden at det af beslutningen fremgår, at der foreligger en effektiv domstolsbeskyttelse mod indgreb af denne art.

Domstolen erklærede desuden artikel 3 i beslutning 2000/520 for ugyldig, da den berører de nationale tilsynsmyndigheder de beføjelser, som de er tillagt i medfør af artikel 28 i direktiv 95/46, i det tilfælde, hvor en person anfører nogle forhold, der kan rejse tvivl om, hvorvidt en afgørelse fra Kommissionen, hvorved det er blevet konstateret, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau, er forenelig med beskyttelsen af privatlivet og personers frihedsrettigheder og grundlæggende rettigheder. Domstolen konkluderede, at ugyldigheden af artikel 1 og 3 i beslutning 2000/520 berørte gyldigheden af denne beslutning i det hele.

Med hensyn til umuligheden af at begrunde et sådant indgreb bemærkede Domstolen først, at en EU-lovgivning, som indebærer et indgreb i de ved chartrets artikel 7 og 8 sikrede grundlæggende rettigheder, skal fastsætte klare og præcise regler, som regulerer rækkevidden og anvendelsen af en foranstaltning og opstiller en række mindstekrav, således at de personer, hvis personoplysninger er berørt, råder over

⁷⁵ Safe harbor-ordningen indeholder en række principper vedrørende beskyttelsen af personoplysninger, som de amerikanske virksomheder kan vælge at tilslutte sig.

tilstrækkelige garantier, der gør det muligt effektivt at beskytte deres oplysninger mod risikoen for misbrug og mod ulovlig adgang til og anvendelse af disse oplysninger. Behovet for at råde over sådanne garantier er så meget desto større, når personoplysningerne undergives automatisk databehandling, og der eksisterer en betydelig risiko for ulovlig adgang til disse oplysninger.

Desuden kræver beskyttelsen af den grundlæggende ret til respekt for privatlivet på EU-plan særligt, at undtagelserne fra og begrænsningerne af beskyttelsen af personoplysninger holdes inden for det strengt nødvendige. En lovgivning, der på generel vis tillader opbevaring af samtlige personoplysninger fra samtlige de personer, hvis oplysninger er blevet videregivet fra Unionen, uden at der bliver foretaget nogen form for differentiering, begrænsning eller undtagelse under hensyn til det forfulgte mål, og uden at der bliver fastsat noget objektivt kriterium, som gør det muligt at afgrænse de offentlige myndigheders adgang til oplysningerne og deres senere anvendelse heraf med henblik på veldefinerede formål, der er strengt begrænsede, og som kan begrunde det indgreb, som såvel adgangen til disse oplysninger som anvendelsen heraf indebærer, er således ikke begrænset til det strengt nødvendige. En lovgivning, der på generel vis gør det muligt for de offentlige myndigheder at få adgang til indholdet af elektronisk kommunikation, udgør navnlig et indgreb i det væsentlige indhold af den grundlæggende ret til respekt for privatlivet. Tilsvarende opfylder en lovgivning, der ikke fastsætter nogen mulighed for retssubjektet til at gøre brug af retsmidler med henblik på at få adgang til personoplysninger, som vedrører den pågældende, eller til at få sådanne oplysninger berigtiget eller slettet, ikke det væsentligste indhold af den grundlæggende ret til en effektiv domstolsbeskyttelse, således som denne er sikret ved chartrets artikel 47.

Udtalelse 1/15 (PNR-aftalen mellem EU og Canada), af 26. juli 2017 (Store Afdeling)
([EU:C:2017:592](#))

Den 26. juli 2017 udtalte Domstolen sig for første gang om foreneligheden af et udkast til en international aftale med Den Europæiske Unions charter om grundlæggende rettigheder, særlig med bestemmelserne om respekt for privatliv og beskyttelse af personoplysninger.

EU og Canada har forhandlet om en aftale om overførsel af passagerlisteoplysninger (PNR-aftale), der blev undertegnet i 2014. Rådet havde anmodet Europa-Parlamentet om at godkende aftalen, og Europa-Parlamentet besluttede at indbringe spørgsmålet for Domstolen med henblik på at få klarlagt, om aftalen var i overensstemmelse med EU-retten.

Den påtænkte aftale gør det muligt systematisk og fortsat at overføre PNR-oplysningerne for samtlige flypassagerer til en canadisk myndighed, som kan bruge og opbevare dem, og den muliggør endvidere en eventuel efterfølgende overførsel heraf til andre myndigheder og andre tredjelande med henblik på bekæmpelse af terrorisme og

grov grænseoverskridende kriminalitet. Med henblik herpå fastsætter aftalen bl.a. en opbevaringsperiode på fem år for oplysningerne, ligesom der stilles særlige krav til PNR-oplysningernes sikkerhed og integritet som f.eks. umiddelbar maskering af følsomme oplysninger, og aftalen fastsætter ligeledes rettigheder til adgang til oplysningerne, til berigtigelse og sletning og muligheden for at indgive en administrativ klage og for domstolsprøvelse.

De PNR-oplysninger, der er omfattet af den påtænkte aftale, omfatter foruden flypassagerernes navn og kontaktoplysninger, navnlig oplysninger, som er nødvendige for reservationen, såsom de planlagte rejsedatoer, rejseruten, billetoplysninger, grupperne af personer registreret under samme reservationsnummer, oplysninger om betaling eller debitering, bagageoplysninger og generelle bemærkninger om passagererne.

Domstolen fastslog i sin udtalelse, at PNR-aftalen ikke kunne indgås i dens aktuelle form, fordi flere af dens bestemmelser var uforenelige med Den Europæiske Unions grundlæggende rettigheder.

For det første konstaterede Domstolen, at såvel overførslen af PNR-oplysninger fra Unionen til den kompetente canadiske myndighed som de rammer, som Unionen havde forhandlet på plads med Canada vedrørende den opbevaring og brug af disse oplysninger samt den eventuelle efterfølgende overførsel heraf til andre canadiske myndigheder, Europol, Eurojust, medlemsstaternes retslige myndigheder eller politimyndigheder eller andre tredjelandes myndigheder, udgjorde indgreb i den ved chartrets artikel 7 sikrede ret. Disse transaktioner indebærer ligeledes et indgreb i den grundlæggende ret til beskyttelse af personoplysninger, som er sikret ved chartrets artikel 8, eftersom de udgør en behandling af personoplysninger.

Domstolen påpegede endvidere, at selv om visse af PNR-oplysningerne isoleret set ikke syntes at kunne afsløre vigtige oplysninger om de pågældende personers privatliv, forholdt det sig ikke desto mindre således, at oplysningerne samlet set bl.a. kunne afsløre den fuldstændige rejserute, rejsevanerne, eksisterende forhold mellem to eller flere personer og oplysninger om flypassagerernes økonomiske situation, madvaner eller helbredstilstand, og de kunne sågar give følsomme oplysninger om disse passagerer som defineret i den påtænkte aftales artikel 2, litra e) (oplysninger om racemæssig eller etnisk oprindelse, politiske holdninger, religiøs overbevisning osv.).

Domstolen fastslog i denne forbindelse, at selv om de pågældende indgreb under disse omstændigheder kunne begrundes i et mål af almen interesse (beskyttelse af den offentlige sikkerhed i forbindelse med bekæmpelse af terrorhandlinger og grov grænseoverskridende kriminalitet), var flere af aftalens bestemmelser ikke begrænset til det strengt nødvendige, og de fastsatte ikke klare og præcise regler.

Domstolen bemærkede navnlig, at en overførsel af følsomme oplysninger til Canada kræver en præcis og særlig solid begrundelse, der er udledt af andre hensyn end beskyttelse af den offentlige sikkerhed mod terrorisme og grov grænseoverskridende

kriminalitet, henset til risikoen for en behandling, der er i strid med princippet om ikke-forskelsbehandling. I det foreliggende tilfælde forelå en sådan begrundelse ikke. Domstolen fastslog, at bestemmelserne i aftalen om overførsel af følsomme oplysninger til Canada samt om behandling og opbevaring af disse oplysninger var uforenelige med de grundlæggende rettigheder.

For det andet var Domstolen af den opfattelse, at den fortsatte opbevaring af PNR-oplysningerne for samtlige flypassagerer efter disses afgang fra Canada, der var fastsat i den påtænkte aftale, ikke var begrænset til det strengt nødvendige. Hvad således angik de flypassagerer, med hensyn til hvilke der ikke var blevet konstateret en risiko for terrorisme eller grov grænseoverskridende kriminalitet fra deres ankomst til Canada frem til deres udrejse fra dette land, syntes der efter deres udrejse ikke at foreligge nogen forbindelse, selv indirekte, mellem deres PNR-oplysninger og det med den påtænkte aftale forfulgte formål, som kunne begrunde en opbevaring af disse oplysninger. Når det derimod fastslås, at der foreligger objektive forhold, som gør det muligt at antage, at visse af flypassagererne selv efter deres afgang fra Canada ville kunne frembyde en risiko i forbindelse med bekæmpelsen af terrorisme og grov, grænseoverskridende kriminalitet, syntes det tilladeligt at opbevare deres PNR-oplysninger ud over deres ophold i Canada og endog i en periode på fem år.

For det tredje fastslog Domstolen, at den grundlæggende ret til respekt for privatlivets fred, der er fastsat i chartrets artikel 7, indebærer, at den berørte person skal kunne have sikkerhed for, at den pågældendes personoplysninger behandles korrekt og lovligt. Personen skal have ret til indsigt i de oplysninger om vedkommende selv, som gøres til genstand for behandling, for at kunne foretage den nødvendige efterprøvelse heraf.

Domstolen fremhævede i denne forbindelse, at det er vigtigt, at flypassagererne i den påtænkte aftale underrettes om overførslen af deres PNR-oplysninger til det pågældende tredjeland og om brugen af disse oplysninger, så snart denne underretning ikke kan skade de i den påtænkte aftale omhandlede offentlige myndigheders efterforskning. En sådan underretning er nemlig de facto nødvendig for at gøre det muligt for flypassagererne at udøve deres ret til at anmode om indsigt i PNR-oplysninger, der vedrører dem, og til i givet fald at anmode om berigtigelse af disse samt til i overensstemmelse med chartrets artikel 47, stk. 1, at have adgang til effektive retsmidler for en domstol.

Hvor der foreligger objektive forhold, der begrundet en brug af passagerlisteoplysningerne med henblik på bekæmpelse af terrorisme og grov grænseoverskridende kriminalitet og forudsætter en forudgående tilladelse fra en retslig myndighed eller en uafhængig administrativ myndighed, er en individuel underretning af flypassagererne således nødvendig. Det samme gælder i de tilfælde, hvor flypassagerernes passagerlisteoplysninger videregives til andre offentlige myndigheder eller til privatpersoner. En sådan underretning skal imidlertid først finde sted, når den ikke kan skade de i den påtænkte aftale omhandlede offentlige myndigheders efterforskning.

Dom af 16. juli 2020 (Store Afdeling), Facebook Ireland og Schrems (C-311/18, [EU:C:2020:559](#))

Databeskyttelsesforordningen bestemmer, at overførsel af personoplysninger til et tredjeland principielt kun må finde sted, hvis det pågældende tredjeland sikrer et tilstrækkeligt beskyttelsesniveau for disse oplysninger. Ifølge denne forordning kan Kommissionen fastslå, at et tredjeland sikrer et tilstrækkeligt beskyttelsesniveau på grundlag af dets nationale lovgivning eller dets internationale forpligtelser ⁷⁶. Hvis der ikke er vedtaget en sådan afgørelse om tilstrækkeligheden af beskyttelsesniveauet, må en overførsel af personoplysninger kun foretages, hvis dataeksportøren, som er etableret i Unionen, giver de fornødne garantier, der bl.a. kan følge af standardbestemmelser om databeskyttelse vedtaget af Kommissionen, og hvis de registrerede har rettigheder, som kan håndhæves, og adgang til effektive retsmidler ⁷⁷. Databeskyttelsesforordningen fastsætter desuden præcist, på hvilke betingelser en sådan overførsel må finde sted i mangel af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet eller fornødne garantier ⁷⁸.

Maximillian Schrems, der er østrigsk statsborger med bopæl i Østrig, har været bruger af Facebook siden 2008. Ligesom for andre brugere, der har bopæl i Unionen, overfører Facebook Ireland personoplysningerne vedrørende Maximillian Schrems helt eller delvist til servere, der tilhører Facebook Inc., og som befinder sig i USA, hvor de er genstand for en behandling. Maximillian Schrems indgav en klage til den irske tilsynsmyndighed, som i det væsentlige gik ud på at få forbudt disse overførsler. Han gjorde gældende, at USA's lovgivning og praksis ikke giver en tilstrækkelig beskyttelse mod de offentlige myndigheders adgang til de oplysninger, der overføres til USA. Denne klage blev afslået bl.a. med den begrundelse, at Kommissionen i beslutning 2000/520 ⁷⁹ havde fastslået, at USA sikrede et tilstrækkeligt beskyttelsesniveau. Ved dom af 6. oktober 2015 kendte Domstolen, som havde fået forelagt et præjudicielt spørgsmål af High Court (ret i første instans, Irland), denne beslutning ugyldig (herefter »Schrems I-dommen«) ⁸⁰.

Efter Schrems I-dommen og den irske rets efterfølgende annulation af afgørelsen om afslag på Maximillian Schrems' klage opfordrede den irske tilsynsmyndighed Maximillian Schrems til at omformulere sin klage i lyset af, at Domstolen havde kendt beslutning 2000/520 ugyldig. Maximillian Schrems fastholdt i sin omformulerede klage, at USA ikke sikrer en tilstrækkelig beskyttelse af de oplysninger, som overføres til dette land. Han anmodede om, at de overførsler af hans personoplysninger fra EU til USA, som Facebook Ireland på daværende tidspunkt foretog på grundlag af

⁷⁶ Databeskyttelsesforordningens artikel 45.

⁷⁷ Databeskyttelsesforordningens artikel 46, stk. 1, og artikel 46, stk. 2, litra c).

⁷⁸ Databeskyttelsesforordningens artikel 49.

⁷⁹ Kommissionens beslutning af 26.7.2000 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af safe harbor-principperne til beskyttelse af privatlivets fred og de dertil hørende hyppige spørgsmål fra det amerikanske handelsministerium (EFT 2000, L 215, s. 7).

⁸⁰ Domstolens dom af 6.10.2015, Schrems, C-362/14, [EU:C:2015:650](#).

standardbestemmelserne om beskyttelse i bilaget til afgørelse 2010/87/EU⁸¹, fremadrettet skulle suspenderes eller forbydes. Den irske tilsynsmyndighed fandt, at behandlingen af Maximillian Schrems klage bl.a. afhang af gyldigheden af afgørelse 2010/87, hvorfor denne myndighed indledte en sag ved High Court (ret i første instans), med henblik på at denne ret skulle indgive en anmodning om præjudiciel afgørelse til Domstolen. Efter indledningen af denne sag vedtog Kommissionen afgørelse (EU) 2016/1250 om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af EU's og USA's værn om privatlivets fred⁸².

Den forelæggende ret anmodede med sin anmodning om præjudiciel afgørelse Domstolen om at tage stilling til, hvorvidt databeskyttelsesforordningen finder anvendelse på overførsler af personoplysninger på grundlag af standardbestemmelserne om databeskyttelse i afgørelse 2010/87, til, hvilket beskyttelsesniveau der kræves af denne forordning i forbindelse med en sådan overførsel, og til, hvilke forpligtelser der i denne forbindelse påhviler tilsynsmyndighederne. Derudover rejste High Court (ret i første instans) spørgsmålet om gyldigheden af såvel afgørelse 2010/87 som afgørelse 2016/1250.

Domstolen fastslog med denne dom, at undersøgelsen af afgørelse 2010/87 i lyset af chartret intet havde frembragt, der kunne påvirke gyldigheden af denne afgørelse. Derimod erklærede Domstolen afgørelse 2016/1250 ugyldig.

Domstolen fastslog først og fremmest, at EU-retten og navnlig databeskyttelsesforordningen finder anvendelse på en overførsel af personoplysninger, der foretages til forretningsmæssige formål af en erhvervsdrivende, der er etableret i en medlemsstat, til en anden erhvervsdrivende, der er etableret i et tredjeland, selv om disse oplysninger under eller efter overførslen kan blive behandlet af det pågældende tredjeland's myndigheder af hensyn til den offentlige sikkerhed, forsvaret og statens sikkerhed. Domstolen præciserede, at denne type behandling af oplysninger foretaget af et tredjeland's myndigheder ikke kan udelukke en sådan overførsel fra anvendelsesområdet for databeskyttelsesforordningen.

Med hensyn til det beskyttelsesniveau, som kræves i forbindelse med en sådan overførsel, fastslog Domstolen, at de krav, som i denne henseende er fastsat ved databeskyttelsesforordningens bestemmelser, og som vedrører fornødne garantier, rettigheder, som kan håndhæves, og effektive retsmidler, skal fortolkes således, at personer, hvis oplysninger overføres til et tredjeland på grundlag af standardbestemmelser om databeskyttelse, skal være omfattet af et beskyttelsesniveau, der i det væsentlige svarer til det niveau, der er sikret i Unionen ved denne forordning, sammenholdt med chartret. Domstolen præciserede i denne sammenhæng, at der ved

⁸¹ Kommissionens afgørelse af 5.2.2010 om standardkontraktbestemmelser for videregivelse af personoplysninger til registerførere etableret i tredjelande i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF (EUT 2010, L 39, s. 5), som ændret ved Kommissionens gennemførelsesafgørelse (EU) 2016/2297 af 16.12.2016 (EUT 2016, L 344, s. 100).

⁸² Kommissionens gennemførelsesafgørelse (EU) 2016/1250 af 12.7.2016 i henhold til Europa-Parlamentets og Rådets direktiv 95/46/EF om tilstrækkeligheden af den beskyttelse, der opnås ved hjælp af EU's og USA's værn om privatlivets fred (EUT 2016, L 207, s. 1).

vurderingen af dette beskyttelsesniveau skal tages hensyn til både de kontraktvilkår, som er aftalt mellem dataeksportøren, der er etableret i Unionen, og modtageren af overførslen, der er etableret i det pågældende tredjeland, og – for så vidt angår en eventuel adgang for dette tredjelands offentlige myndigheder til de således overførte personoplysninger – til de relevante forhold i dettes retssystem.

Hvad angår tilsynsmyndighedernes forpligtelser i forbindelse med en sådan overførsel fastslog Domstolen, at medmindre der foreligger en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, som er gyldigt vedtaget af Kommissionen, har disse myndigheder bl.a. pligt til at suspendere eller forbyde en overførsel af personoplysninger til et tredjeland, såfremt de – i lyset af de omstændigheder, der kendetegner denne overførsel – finder, at standardbestemmelserne om databeskyttelse ikke er overholdt eller ikke kan overholdes i dette land, og at det ikke er muligt ved andre midler at sikre den beskyttelse af de overførte oplysninger, som kræves efter EU-retten, hvis dataeksportøren, som er etableret i Unionen, ikke selv har suspenderet overførslen eller bragt den til ophør.

Domstolen undersøgte herefter gyldigheden af afgørelse 2010/87. Ifølge Domstolen rejser den omstændighed alene, at standardbestemmelserne om databeskyttelse i denne afgørelse som følge af deres kontraktlige karakter ikke er bindende for myndighederne i det tredjeland, som oplysningerne kan blive overført til, ikke tvivl om gyldigheden af denne afgørelse. Domstolen præciserede, at gyldigheden af afgørelsen derimod afhænger af, om den omfatter effektive mekanismer, som i praksis gør det muligt at sikre, at det i EU-retten krævede beskyttelsesniveau overholdes, og at overførslerne af personoplysninger på grundlag af sådanne bestemmelser suspenderes eller forbydes, hvis disse bestemmelser overtrædes, eller hvis det er umuligt at overholde dem. Domstolen konstaterede, at afgørelse 2010/87 fastsætter sådanne mekanismer. I denne henseende fremhævede Domstolen navnlig, at denne afgørelse indfører en pligt for dataeksportøren og modtageren af overførslen til forudgående at undersøge, om dette beskyttelsesniveau er overholdt i det pågældende tredjeland, og forpligter modtageren af overførslen til at underrette dataeksportøren, såfremt den pågældende ikke er i stand til at overholde standardbestemmelserne om beskyttelse, hvorefter det påhviler dataeksportøren at suspendere dataoverførslen og/eller ophæve kontrakten med modtageren.

Domstolen undersøgte endelig gyldigheden af afgørelse 2016/1250 i lyset af de krav, der følger af databeskyttelsesforordningen, sammenholdt med chartrets bestemmelser om respekt for privatlivet og familielivet, beskyttelsen af personoplysninger og retten til en effektiv domstolsbeskyttelse. I denne henseende fremhævede Domstolen, at denne afgørelse, ligesom beslutning 2000/520, giver forrang til kravene vedrørende den nationale sikkerhed, den offentlige interesse og overholdelsen af den amerikanske lovgivning og således åbner op for, at der gøres indgreb i de grundlæggende rettigheder for de personer, hvis personoplysninger bliver overført til dette tredjeland. Ifølge Domstolen er de begrænsninger af beskyttelsen af personoplysninger, som følger af

USA's nationale bestemmelser om de amerikanske offentlige myndigheders adgang til og brug af sådanne oplysninger, der overføres fra Unionen til dette tredjeland, og som Kommissionen vurderede i afgørelse 2016/1250, ikke afgrænset på en sådan måde, at de lever op til krav, som i det væsentlige svarer til dem, der er foreskrevet i EU-retten ved proportionalitetsprincippet, for så vidt som de overvågningsprogrammer, der er baseret på disse bestemmelser, ikke er begrænset til det strengt nødvendige. På grundlag af konstateringerne i denne afgørelse fremhævede Domstolen, at for så vidt angår visse overvågningsprogrammer lader disse bestemmelser på ingen måde fremgå, at der er begrænsninger af beføjelsen i medfør af disse til at gennemføre overvågningsprogrammerne, og heller ikke, at der er garantier for ikke-amerikanske personer, som potentielt kan være omfattet af dem. Domstolen tilføjede, at selv om de samme bestemmelser fastsætter krav, som de amerikanske myndigheder skal overholde ved gennemførelsen af de pågældende overvågningsprogrammer, giver de ikke de registrerede rettigheder, som kan håndhæves over for de amerikanske myndigheder ved domstolene.

Med hensyn til kravet om domstolsbeskyttelse fastslog Domstolen, at i modsætning til hvad Kommissionen konstaterede i afgørelse 2016/1250, tilvejebringer den ombudsmandsmekanisme, som er omhandlet i denne afgørelse, ikke et retsmiddel for et organ, som giver de registrerede garantier, der i det væsentlige svarer til dem, der kræves i EU-retten, således at det sikres, både at den ombudsmand, som er oprettet ved denne mekanisme, er uafhængig, og at der findes bestemmelser, som giver denne ombudsmand beføjelse til at træffe bindende afgørelser i forhold til de amerikanske efterretningstjenester. Af samtlige disse grunde fastslog Domstolen, at afgørelse 2016/1250 var ugyldig.

V. Beskyttelse af personoplysninger på internettet

1. Ret til at gøre indsigelse mod behandling af personoplysninger (»retten til at blive glemt«)

Dom af 13. maj 2014 (Store Afdeling), Google Spain og Google (C-131/12, [EU:C:2014:317](#))

I denne dom (se ligeledes afsnit II.1 med overskriften »Den generelle lovgivnings anvendelsesområde« og afsnit II.3 med overskriften »Begrebet »behandling af personoplysninger«») præciserede Domstolen rækkevidden af retten til indsiget og indsigelsesretten i forbindelse med behandlingen af personoplysninger på internettet, der er fastsat i direktiv 95/46.

Da Domstolen udtalte sig om omfanget af en internetsøgemaskineudbyders ansvar, fastslog den hovedsageligt, at en søgemaskineudbyder med henblik på at overholde de rettigheder, der er fastsat i artikel 12, litra b), og artikel 14, første afsnit, litra a), i direktiv

95/46, og for så vidt som de i disse artikler fastsatte betingelser faktisk er opfyldt, under visse omstændigheder er forpligtet til fra den resultatliste, der vises efter en søgning på en persons navn, at fjerne link til websteder, som er offentliggjort af tredjemand, og som indeholder oplysninger vedrørende denne person. Domstolen præciserede, at der kan foreligge en sådan forpligtelse, også i det tilfælde, hvor dette navn eller disse oplysninger ikke forudgående eller samtidig slettes fra disse websteder, og i givet fald selv når offentliggørelsen på disse sider i sig selv er lovlig.

Hvad angår endvidere spørgsmålet, om direktivet giver den berørte person ret til at kræve, at link til websteder slettes fra en sådan resultatliste, med den begrundelse, at personen ønsker, at oplysningerne på listen om dennes person »glemmes« efter et vist tidsrum, bemærkede Domstolen først og fremmest, at selv en behandling af korrekte oplysninger, der oprindeligt var lovlig, med tiden kan blive uforenelig med direktivet, når disse oplysninger ikke længere er nødvendige af hensyn til de formål, hvortil de er blevet indsamlet, eller i forbindelse med hvilke de er blevet behandlet. Det er bl.a. tilfældet, når de forekommer utilstrækkelige, irrelevante eller ikke længere relevante eller omfatter for meget i forhold til formålet, og henset til den tid, der er gået. Såfremt det efter en anmodning fra den berørte person konstateres, at inklusionen af sådanne link på listen på nuværende tidspunkt er uforenelig med direktivet, skal de omhandlede oplysninger og link på nævnte resultatliste slettes. Med henblik på konstateringen af, om den berørte person har ret til, at oplysningen vedrørende personen ikke længere knyttes til personens navn på en resultatliste, er det herved ikke et krav, at inklusionen af den pågældende oplysning på resultatlisten skader den berørte person.

Endelig præciserede Domstolen, at disse rettigheder, da den berørte person, henset til den pågældendes grundlæggende rettigheder i medfør af chartrets artikel 7 og 8, kan anmode om, at den pågældende oplysning ikke længere stilles til rådighed for den brede offentlighed ved sin inklusion på en sådan resultatliste, i princippet går forud for ikke blot søgemaskineudbyderens økonomiske interesse, men også for offentlighedens interesse i at finde nævnte oplysning ved en søgning på denne persons navn. Dette er imidlertid ikke tilfældet, såfremt det af særlige grunde, såsom den rolle, som nævnte person har i det offentlige liv, fremgår, at indgrebet i personens grundlæggende rettigheder er begrundet i offentlighedens vægtige interesse i at have adgang til den pågældende oplysning via inklusionen på resultatlisten.

2. Behandling af personoplysninger og intellektuelle ejendomsrettigheder

Dom af 29. januar 2008 (Store Afdeling), Promusicae (C-275/06, [EU:C:2008:54](#))

Promusicae, en spansk sammenslutning, der arbejder uden vinding for øje, og hvis medlemmer er producenter og udgivere af musikoptagelser samt af audiovisuelle optagelser, havde anlagt et søgsmål ved de spanske domstole med påstand om, at

Telefónica de España SAU (et erhvervsdrivende selskab, hvis virksomhed navnlig består i at levere ydelser vedrørende adgang til internettet) blev pålagt at afsløre identiteten og den fysiske adresse på nogle personer, som selskabet leverede en ydelse vedrørende adgang til internettet til, og hvis »IP-adresser« såvel som datoen og tidspunktet for tilslutningen var kendt. Ifølge Promusicae anvendte disse personer programmet for udveksling af arkiver (benævnt »peer to peer« eller »P2P«) (et transparent middel til deling af indhold, der er uafhængigt, decentraliseret og forsynet med avancerede søge- og downloadingfunktioner), og gav via deres fælles filer i deres computere adgang til fonogrammer, som medlemmerne af Promusicae har udnyttelsesrettighederne til. Promusicae havde derfor krævet at få meddelt disse oplysninger med henblik på at kunne anlægge en civil retssag mod de pågældende.

Under disse omstændigheder forelagde Juzgado de lo Mercantil nº 5 de Madrid (handelsret nr. 5 i Madrid, Spanien) Domstolen spørgsmålet, om det i henhold til EU-lovgivningen påhviler medlemsstaterne at fastsætte pligten til at videregive personoplysninger under en civil retssag med det formål at sikre en effektiv beskyttelse af ophavsretten.

Ifølge Domstolen rejste den pågældende anmodning om præjudiciel afgørelse spørgsmålet om, hvorledes man opnår den nødvendige forening af de krav, der er forbundet med forskellige grundlæggende rettigheder, nemlig dels beskyttelsen af privatlivets fred, dels beskyttelsen af ejendomsretten og adgang til effektive retsmidler.

Domstolen konkluderede i denne forbindelse, at direktiv 2000/31/EF om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked (»direktivet om elektronisk handel«)⁸³, direktiv 2001/29/EF om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet⁸⁴, direktiv 2004/48/EF om håndhævelsen af intellektuelle ejendomsrettigheder⁸⁵ og direktiv 2002/58 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (direktiv om databeskyttelse inden for elektronisk kommunikation) ikke i en situation som den i hovedsagen omhandlede pålægger medlemsstaterne at fastsætte pligten til at videregive personoplysninger med henblik på at sikre den effektive beskyttelse af ophavsretten under en civil retssag. EU-retten kræver imidlertid, at medlemsstaterne under gennemførelsen af de ovennævnte direktiver påser, at de lægger en fortolkning af disse direktiver til grund, som gør det muligt at sikre den rette afvejning af de forskellige grundlæggende rettigheder, der er beskyttet af Fællesskabets retsorden. Herefter påhviler det under gennemførelsen af de ovennævnte direktiver ikke blot myndighederne og domstolene i medlemsstaterne at fortolke deres nationale ret på en måde, der er forenelig med de nævnte direktiver, men

⁸³ Europa-Parlamentets og Rådets direktiv 2000/31/EF af 8.6.2000 om visse retlige aspekter af informationssamfundstjenester, navnlig elektronisk handel, i det indre marked (»direktivet om elektronisk handel«) (EFT 2000, L 178, s. 1).

⁸⁴ Europa-Parlamentets og Rådets direktiv 2001/29/EF af 22.5.2001 om harmonisering af visse aspekter af ophavsret og beslægtede rettigheder i informationssamfundet (EFT 2001, L 167, s. 10).

⁸⁵ Europa-Parlamentets og Rådets direktiv 2004/48/EF af 29.4.2004 om håndhævelsen af intellektuelle ejendomsrettigheder (EUT 2004, L 157, s. 45, berigtiget i EUT 2004, L 195, s. 16).

også at sikre, at de ikke lægger en fortolkning heraf til grund, som kommer i konflikt med disse grundlæggende rettigheder eller med andre almindelige fællesskabsretlige principper, såsom proportionalitetsprincippet.

Dom af 19. april 2012, Bonnier Audio m.fl. (C-461/10, [EU:C:2012:219](#))

Högsta domstolen (øverste domstol, Sverige) havde forelagt Domstolen en anmodning om en præjudiciel afgørelse med henblik på en fortolkning af direktiv 2002/58 og 2004/48 i forbindelse med en tvist mellem på den ene side Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB og Storyside AB (herefter samlet »Bonnier Audio m.fl.«) og på den anden side Perfect Communication Sweden AB (herefter »ePhone«) vedrørende ePhones anfægtelse af en anmodning om påbud om at tilvejebringe oplysninger, som Bonnier Audio m.fl. havde indgivet.

I denne sag var Bonnier Audio m.fl. forlag, der bl.a. har eneret til at fremstille 27 nærmere angivne bøger i lydbogsformat, til at udgive eksemplarer af værkerne samt til at stille værkerne til rådighed for almenheden. De var af den opfattelse, at der var sket en krænkelse af deres eneret, idet disse 27 værker uden indehavernes samtykke var blevet gjort tilgængelige for almenheden via en FTP-server (»file transfer protocol«), der gjorde det muligt at dele filer og overføre data mellem computere via internettet. De havde således anlagt sag ved de svenske domstole med påstand om, at der udstedtes påbud med henblik på at få oplyst navn og adresse på den person, der benyttede den IP-adresse, som angiveligt blev anvendt til at overføre de omhandlede filer.

I denne forbindelse forelagde Högsta domstolen (øverste domstol), for hvilken der var iværksat en kassationsappel, Domstolen et spørgsmål om, hvorvidt EU-retten var til hinder for anvendelsen af en national bestemmelse, der er indført i henhold til artikel 8 i direktiv 2004/48, og som indebærer, at en internetudbyder i et civilt søgsmål med det formål at kunne identificere en bestemt abonnent tilpligtes at give indehaverne af ophavsretten eller den, til hvem retten er overgået, oplysninger om den abonnent, der har fået tildelt en bestemt IP-adresse af internetudbyderen, hvorfra den pågældende krænkelse var foretaget. Det var forudsat, at sagsøgeren havde godtgjort, at der var konkrete indicier for, at der forelå en krænkelse af visse ophavsrettigheder, og at foranstaltningen stod i rimeligt forhold hertil.

Domstolen bemærkede først og fremmest, at artikel 8, stk. 3, i direktiv 2004/48, sammenholdt med artikel 15, stk. 1, i direktiv 2002/58, ikke er til hinder for, at medlemsstaterne fastsætter en forpligtelse til overførsel af personoplysninger til privatpersoner med henblik på at retsforfølge krænkelse af ophavsretten ved de civile domstole, men omvendt heller ikke tvinger dem til at fastsætte en sådan forpligtelse. Myndighederne og domstolene i medlemsstaterne skal imidlertid ikke blot fortolke deres nationale ret på en måde, der er forenelig med disse direktiver, men også sikre, at de ikke lægger en fortolkning heraf til grund, som kommer i konflikt med disse

grundlæggende rettigheder eller med andre almindelige EU-retlige principper, såsom proportionalitetsprincippet.

Domstolen konstaterede i denne forbindelse, at der i henhold til den pågældende nationale lovgivning bl.a. stilles krav om, at der for, at der kunne udstedes et påbud om udlevering af de pågældende oplysninger skulle foreligge konkrete indicier for, at der var sket en krænkelse af en intellektuel ejendomsrettighed til et værk, at oplysningerne kunne formodes at fremme undersøgelsen af overtrædelsen eller krænkelsen af en ophavsret, og at begrundelsen for påbuddet skulle have en interesse, der kunne opveje ulemperne eller den skade, som den kunne indebære for den person, der rammes af den, eller for en anden eventuel modstående interesse.

Domstolen konkluderede derfor, at direktiv 2002/58 og 2004/48 ikke er til hinder for en national lovgivning som den i hovedsagen omhandlede, for så vidt som denne lovgivning gør det muligt for den nationale retsinstans, til hvilken der indgives anmodning om udstedelse af et påbud om at videregive personoplysninger af en person, der har søgsmålskompetence, på grundlag af omstændighederne i den konkrete sag og under hensyntagen til de krav, der følger af proportionalitetsprincippet, at afveje de pågældende modstridende interesser mod hinanden.

3. Fjernelse af personoplysninger

Dom af 24. september 2019 (Store Afdeling), GC m.fl. (Fjernelse af følsomme oplysninger) (C-136/17, [EU:C:2019:773](#))

I denne dom præciserede Domstolen i Store Afdeling de forpligtelser, som påhviler en søgemaskineudbyder i forbindelse med en anmodning om fjernelse af følsomme personoplysninger.

Google havde afvist at efterkomme fire personers anmodninger om at fjerne links til forskellige websider, navnlig presseartikler, som var offentliggjort af tredjemænd, fra den resultatliste, som søgemaskinen viser efter en søgning på deres respektive navne. Som svar på disse fire personers klager afviste Commission nationale de l'informatique et des libertés (CNIL) (den nationale kommission for databehandling og frihedsrettigheder, Frankrig) at pålægge Google at fjerne de omhandlede links. Sagen blev indbragt for Conseil d'État (øverste domstol i forvaltningsretlige sager, Frankrig), som anmodede Domstolen om at præcisere de forpligtelser, der påhviler søgemaskineudbyderen ved behandlingen af en anmodning om fjernelse i henhold til direktiv 95/46.

For det første bemærkede Domstolen, at behandlingen af personoplysninger om racemæssig eller etnisk baggrund, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold og oplysninger om helbredsforhold og seksuelle

forhold, med forbehold af visse undtagelser og fravigelser, er forbudt ⁸⁶. Behandlingen af oplysninger vedrørende lovovertrædelser, straffedomme eller sikkerhedsforanstaltninger må i princippet kun foretages under kontrol af en offentlig myndighed, eller hvis der gælder tilstrækkelige, specifikke garantier i medfør af den nationale lovgivning ⁸⁷.

Domstolen fastslog, at forbuddet og restriktionerne vedrørende behandlingen af disse særlige kategorier af personoplysninger finder anvendelse på søgemaskineudbyderen i lighed med enhver anden registeransvarlig. Formålet med disse forbud og restriktioner består i at sikre en øget beskyttelse mod sådanne behandlinger, der som følge af disse oplysningers særligt følsomme karakter kan udgøre et særligt alvorligt indgreb i de grundlæggende rettigheder til respekt for privatliv og beskyttelse af personoplysninger.

Søgemaskineudbyderen er imidlertid ikke ansvarlig for den omstændighed, at personoplysninger forekommer på en webside, som en tredjemand har offentliggjort, men for henvisningen til denne side. Under disse omstændigheder finder forbuddet og restriktionerne vedrørende behandlingen af følsomme personoplysninger kun anvendelse på denne udbyder på grund af denne visning af links og dermed ved hjælp af en efterprøvelse under de kompetente nationale myndigheders kontrol på grundlag af en anmodning om fjernelse af links fremsat af den registrerede.

For det andet fastslog Domstolen, at søgemaskineudbyderen med forbehold af de i direktivet fastsatte undtagelser i princippet er forpligtet til at efterkomme en anmodning om fjernelse af links til følsomme personoplysninger, når udbyderen forelægges en sådan anmodning. Hvad angår disse undtagelser kan udbydere bl.a. afvise at efterkomme en sådan anmodning, hvis udbyderen konstaterer, at de pågældende links fører til oplysninger, som klart er offentliggjort af den registrerede ⁸⁸, forudsat at visningen af disse links opfylder de øvrige lovlighedsbetingelser for en behandling af personoplysninger, og medmindre den registrerede har ret til at gøre indsigelse mod denne visning af grunde, der vedrører dennes særlige situation ⁸⁹.

Under alle omstændigheder skal søgemaskineudbyderen, når denne forelægges en anmodning om fjernelse af et link til en webside, hvor følsomme personoplysninger offentliggøres, prøve, om medtagelsen af dette link på resultatlisten, som vises efter en søgning på den registreredes navn, er strengt nødvendig for at beskytte informationsfriheden for de internetbrugere, som potentielt kunne være interesserede i at få adgang til denne webside ved en sådan søgning. I denne henseende har Domstolen fremhævet, at selv om retten til respekt for privatlivet og retten til beskyttelse af personoplysninger generelt vejer tungest i forhold til internetbrugernes informationsfrihed, kan denne afvejning dog i særlige tilfælde afhænge af den pågældende oplysnings art, og hvor følsom den er for den registreredes privatliv, samt

⁸⁶ Artikel 8, stk. 1, i direktiv 95/46 og artikel 9, stk. 1, i forordning 2016/679.

⁸⁷ Artikel 8, stk. 5, i direktiv 95/46 og artikel 10 i forordning 2016/679.

⁸⁸ Artikel 8, stk. 2, litra e), i direktiv 95/46 og artikel 9, stk. 2, litra e), i forordning 2016/679.

⁸⁹ Artikel 14, første afsnit, litra a), i direktiv 95/46 og artikel 21, stk. 1, i forordning 2016/679.

offentlighedens interesse i at råde over denne oplysning, hvilket bl.a. kan variere, alt efter hvilken rolle denne person har i det offentlige liv.

For det tredje fastslog Domstolen, at det tilkommer en søgemaskineudbyder inden for rammerne af en anmodning om fjernelse af links vedrørende oplysninger om en retslig procedure i en straffesag mod den registrerede, som vedrører et tidligere trin i denne procedure, og som ikke længere svarer til den aktuelle situation, under hensyntagen til alle sagens omstændigheder at vurdere, om denne person har ret til, at de pågældende oplysninger på det nuværende stadium ikke længere er knyttet til vedkommendes navn på en resultatliste, som vises efter en søgning på dette navn. Selv om dette ikke er tilfældet på grund af den omstændighed, at medtagelsen af det pågældende link viser sig at være strengt nødvendigt for at forene den registreredes ret til respekt for privatlivets fred og ret til beskyttelse af personoplysninger med potentielt interesserede internetbrugeres informationsfrihed, er udbyderen imidlertid forpligtet til senest i forbindelse med anmodningen om fjernelse at tilpasse resultatlisten på en sådan måde, at det samlede image, der følger heraf for internetbrugeren, afspejler den aktuelle retslige situation, hvilket bl.a. indebærer, at links til websider, der indeholder oplysninger herom, vises øverst på denne liste.

Dom af 24. september 2019, Google (Territorial rækkevidde af retten til at få fjernet links) (C-507/17, [EU:C:2019:772](#))

Commission nationale de l'informatique et des libertés (CNIL) (den nationale kommission for databehandling og frihedsrettigheder) (Frankrig) havde udstedt et pålæg til Google om, at selskabet, når det efterkommer en anmodning om fjernelse, skal foretage fjernelsen af links til websider, der indeholder personoplysninger vedrørende den registrerede, fra den resultatliste, der vises efter en søgning på den registreredes navn, på alle selskabets søgemaskines domæneendelser. Efter at Google havde nægtet at efterkomme dette pålæg, udstedte CNIL en bøde til dette selskab på 100 000 EUR. Google anlagde sag ved Conseil d'État (øverste domstol i forvaltningsretlige sager, Frankrig), som anmodede Domstolen om at præcisere den territoriale rækkevidde af forpligtelsen for en søgemaskineudbyder til at gennemføre retten til at få slettet links i henhold til direktiv 95/46.

Domstolen bemærkede indledningsvis, at fysiske personer på grundlag af EU-retten har mulighed for at gøre deres ret til at få fjernet links gældende over for en søgemaskineudbyder, der råder over et eller flere etableringssteder på Unionens område, uafhængigt af hvorvidt behandlingen af personoplysninger (i den foreliggende sag links til websider indeholdende personoplysninger vedrørende den person, der gjorde denne ret gældende) finder sted inden for Unionen ⁹⁰.

⁹⁰ Artikel 4, stk. 1, litra a), i direktiv 95/46 og artikel 3, stk. 1, i forordning 2016/679.

Domstolen fastslog for så vidt angår rækkevidden af retten til at få fjernet links, at søgemaskineudbyderen ikke er forpligtet til at fjerne links på alle udgaver af denne udbyders søgemaskiner, men på de udgaver, der svarer til alle medlemsstaterne. Domstolen bemærkede i denne henseende, at selv om en universel fjernelse af links, henset til internettets og søgemaskinernes karakteristika efter sin karakter fuldt ud ville opfylde EU-lovgivers formål om at sikre et højt niveau for beskyttelse af personoplysninger i hele Unionen, fremgår det på ingen måde af EU-retten ⁹¹, at EU-lovgiver med henblik på at sikre gennemførelsen af et sådant formål har valgt at tillægge retten til at få fjernet links en rækkevidde, der går ud over medlemsstaternes område. Navnlig gælder det, at selv om EU-retten har indført samarbejdsmekanismer for medlemsstaternes tilsynsmyndigheder for at nå til en fælles afgørelse på grundlag af en afvejning mellem dels beskyttelsen af privatlivets fred og personoplysninger, dels interessen for offentligheden i de forskellige medlemsstater i at have adgang til oplysninger, er sådanne mekanismer for nuværende ikke foreskrevet for så vidt angår rækkevidden af en ret til at få fjernet links uden for Unionen.

På EU-rettens nuværende udviklingstrin påhviler det en søgemaskineudbyder at foretage den fjernelse af links, der er anmodet om, for de udgaver af søgemaskinen, der svarer til medlemsstaterne, og ikke kun for den ene udgave af søgemaskinen, der svarer til den medlemsstat, hvor den person, der får fjernet links, er bosiddende, bl.a. for at sikre et ensartet og højt niveau for beskyttelse i hele Unionen. Det påhviler i øvrigt en sådan udbyder om nødvendigt at træffe tilstrækkeligt effektive foranstaltninger for at hindre eller i det mindste i høj grad afholde internetbrugerne i Unionen fra at have adgang til de links, der er genstand for fjernelsen, efter omstændighederne via en udgave af søgemaskinen, der svarer til et tredjeland, og det tilkommer den nationale retsinstans at efterprøve, om de af udbyderen iværksatte foranstaltninger opfylder dette krav.

Endelig fremhævede Domstolen, at selv om EU-retten ikke kræver, at søgemaskineudbyderen skal fjerne links på alle udgaver af udbyderens søgemaskine, forbyder den det heller ikke. Derfor er en medlemsstats tilsynsmyndighed eller retsinstans fortsat kompetent til at foretage en afvejning ud fra de nationale standarder for beskyttelse af grundlæggende rettigheder mellem på den ene side den registreredes ret til respekt for sit privatliv og beskyttelsen af vedkommendes personoplysninger, og på den anden side retten til informationsfrihed, og til efter denne afvejning i givet fald at pålægge udbyderen af denne søgemaskine at fjerne links i alle udgaver af denne søgemaskine.

⁹¹ Artikel 12, litra b), og artikel 14, første afsnit, litra a), i direktiv 95/46 og artikel 17, stk. 1, i forordning 2016/679.

Dom af 8. december 2022 (Store Afdeling), Google (Fjernelse af links til et angiveligt urigtigt indhold) (C-460/20, [EU:C:2022:962](#))

Sagsøgerne i hovedsagen – dvs. TU, der har tillidsposter og er indehaver af andele i forskellige selskaber, og RE, som var TU's samlever, og som indtil maj 2015 var prokurist i et af disse selskaber – var genstand for tre artikler offentliggjort på en internetside i 2015 af Google LLC (herefter »Google«), udbyderen af dette websted. Disse artikler, hvoraf en var illustreret ved fire fotografier, der repræsenterede sagsøgerne, og som antydede, at sagsøgerne levede et luksuriøst liv, indeholdt en kritisk beskrivelse af investeringsmodellen i flere af deres selskaber. Adgangen til disse artikler var mulig ved at indtaste sagsøgernes for- og efternavne både separat og i sammenhæng med bestemte firmanavne i den søgemaskine, der drives af Google. Listen over søgeresultater henviste til disse artikler via et link og til fotografier i form af miniaturebilleder (»thumbnails«).

Sagsøgerne i hovedsagen anmodede Google, som dataansvarlig for den behandling af personoplysninger, der foretages af selskabets søgemaskine, dels om at fjerne links til de omhandlede artikler fra listen over søgeresultater med den begrundelse, at disse indeholder en lang række urigtige udsagn og meninger, der antager karakter af bagvaskelse, dels om at fjerne miniaturebillederne fra listen over søgeresultater. Google afslog at efterkomme denne anmodning.

Da sagsøgerne hverken fik medhold i første instans eller i appelinstansen, iværksatte de revisionsappel ved Bundesgerichtshof (forbundsdomstol, Tyskland), inden for rammerne af hvilken Bundesgerichtshof forelagde Domstolen en anmodning om præjudiciel afgørelse vedrørende fortolkningen af databeskyttelsesforordningen og direktiv 95/46⁹².

I dommen, der blev afsagt af Store Afdeling, udviklede Domstolen sin praksis angående de betingelser, der gælder for anmodninger om fjernelse af links rettet til en søgemaskineudbyder på grundlag af reglerne om beskyttelse af personoplysninger. Domstolen undersøgte for det første omfanget af de forpligtelser og det ansvar, der påhviler en søgemaskineudbyder i forbindelse med behandlingen af en anmodning om fjernelse af links på grundlag af angiveligt urigtige oplysninger i det indhold, der er linket til, og for det andet den bevisbyrde, der påhviler den registrerede for så vidt angår denne urigtighed. Domstolen udtalte sig desuden om nødvendigheden af med henblik på behandlingen af en anmodning om sletning af fotografier, der vises i form af miniaturebilleder på listen over resultaterne af en billedsøgning, at tage hensyn til den oprindelige sammenhæng for offentliggørelsen af disse fotografier på internettet.

For det første fastslog Domstolen, at i forbindelse med afvejningen mellem på den ene side retten til respekt for privatlivet og retten til beskyttelse af personoplysninger og på

⁹² Henholdsvis databeskyttelsesforordningens artikel 17, stk. 3, litra a), og artikel 12, litra b), og artikel 14, første afsnit, litra a), i direktiv 95/46.

den anden side retten til ytrings- og informationsfrihed⁹³ med henblik på behandlingen af en anmodning til en søgemaskineudbyder om fjernelse af links, som tilsigter at få et link fra listen over søgeresultater, der fører til et indhold, der indeholder angiveligt urigtige oplysninger, slettet, er denne fjernelse af links betinget af, at spørgsmålet om rigtigheden af det indhold, der linkes til, er blevet afgjort i det mindste foreløbigt i et søgsmål anlagt af den person, der har indgivet anmodningen, mod udbyderen af indholdet.

Med henblik på at undersøge, under hvilke omstændigheder en søgemaskineudbyder er forpligtet til at efterkomme en anmodning om fjernelse og dermed at fjerne linket til et websted, hvor der forekommer de angivelser, som den registrerede finder urigtige, fra den resultatliste, som vises efter en søgning på denne persons navn, bemærkede Domstolen indledningsvis bl.a. følgende:

- For så vidt som søgemaskinens aktivitet i forhold til webstedsudgiveres aktivitet i væsentligt større og yderligere grad kan påvirke de grundlæggende rettigheder til privatlivets fred og beskyttelse af personoplysninger, skal søgemaskineudbyderen i sin egenskab af den person, som afgør formålet med aktiviteten og hjælpemidlerne hertil, inden for rammerne af sit ansvar, sine kompetencer og sine muligheder sikre, at den opfylder kravene i databeskyttelsesforordningen, med henblik på at de garantier, som direktiv 95/46 og databeskyttelsesforordningen fastsætter, kan udfolde deres fulde virkning, og at en effektiv og fuldstændig beskyttelse af de berørte personer faktisk kan gennemføres.
- Når søgemaskineudbyderen har modtaget en anmodning om fjernelse af links, skal denne prøve, om medtagelsen af et link til det pågældende websted på resultatlisten er nødvendig for, at de internetbrugere, som potentielt kunne være interesserede i at få adgang til dette websted ved en sådan søgning, kan udøve deres ret til informationsfrihed, som er beskyttet af retten til ytrings- og informationsfrihed.
- Databeskyttelsesforordningen fastsætter udtrykkeligt kravet om en afvejning mellem på den ene side den grundlæggende ret til respekt for privatlivet og den grundlæggende ret til beskyttelse af personoplysninger og på den anden side den grundlæggende ret til informationsfrihed.

Indledningsvis fastslog Domstolen, at selv om retten til respekt for privatlivet og retten til beskyttelse af personoplysninger for den registrerede generelt vejer tungest i forhold til internetbrugernes legitime interesse i at få adgang til de pågældende oplysninger, kan denne afvejning dog under relevante omstændigheder i hvert enkelt tilfælde afhænge af den pågældende oplysningens art, og hvor følsom den er for den registreredes privatliv, samt offentlighedens interesse i at råde over denne oplysning, hvilket bl.a. kan variere, alt efter hvilken rolle denne person har i det offentlige liv.

⁹³ Grundlæggende rettigheder, der er sikret ved henholdsvis chartrets artikel 7, 8 og 11.

Spørgsmålet om, hvorvidt det indhold, der er linket til, er rigtigt eller ej, udgør ligeledes et relevant forhold i forbindelse med denne vurdering. Under visse omstændigheder har internetbrugernes ret til information og indholdsleverandørens ytringsfrihed således forrang for retten til beskyttelse af privatlivets fred og beskyttelsen af personoplysninger, navnlig når den registrerede spiller en rolle i det offentlige liv. Dette forhold er dog under alle omstændigheder omvendt, når i det mindste en del af de oplysninger, der er omfattet af anmodningen om fjernelse af links, og som ikke er uvæsentlig i forhold til indholdet som helhed, viser sig at være urigtige. I et sådant tilfælde kan retten til information og retten til at blive informeret nemlig ikke tages i betragtning, da de ikke kan omfatte retten til at udbrede sådanne oplysninger og have adgang til dem.

Hvad dernæst på den ene side angår forpligtelsen til at fastslå, om oplysningerne i det indhold, der er linket til, er korrekte eller ej, præciserede Domstolen, at den person, der anmoder om at få fjernet links som følge af, at sådanne oplysninger er urigtige, skal godtgøre, at de oplysninger, der fremgår af det nævnte indhold, eller i det mindste en del af disse oplysninger, som ikke er uvæsentlig i forhold til indholdet som helhed, er åbenbart urigtige. For at undgå at pålægge denne person en urimelig byrde, der kan skade den effektive virkning af retten til at få fjernet links, påhviler det imidlertid alene denne person at fremlægge beviser, som det, henset til omstændighederne i den konkrete sag, med rimelighed kan kræves af denne person at finde frem til. Denne person er i princippet ikke forpligtet til allerede under den administrative procedure til støtte for sin anmodning om fjernelse af links at fremlægge en retsafgørelse, der er truffet over for udgiveren af det omhandlede websted, selv i form af en afgørelse om foreløbige forholdsregler.

Hvad på den anden side angår søgemaskineudbyderens forpligtelser og ansvar fremhævede Domstolen, at søgemaskineudbyderen med henblik på at efterprøve, om et indhold fortsat kan medtages på listen over søgeresultater foretaget via dennes søgemaskine efter en anmodning om fjernelse af links, skal basere sig på alle de foreliggende rettigheder og interesser samt på samtlige omstændigheder i den foreliggende sag. Denne udbyder kan således ikke pålægges en forpligtelse til at undersøge de faktiske omstændigheder og med henblik herpå at organisere en kontradiktorisk korrespondance med indholdsleverandøren for at opnå manglende oplysninger vedrørende rigtigheden af det indhold, der linkes til. En forpligtelse til at bidrage til at fastslå, om det pågældende indhold er korrekt eller ej, ville pålægge nævnte udbyder en byrde, der går ud over, hvad der med rimelighed kan forventes af udbyderen, henset til dennes ansvar, kompetencer og muligheder. Denne løsning indebærer en alvorlig risiko for, at indhold, der imødekommer almenhedens legitime og vægtige informationsbehov, fjernes, og at det således bliver vanskeligt at finde det på internettet. Der foreligger således en reel risiko for en afskrækkende virkning på udøvelsen af ytrings- og informationsfriheden, hvis en sådan udbyder næsten systematisk foretager en sådan fjernelse af links med henblik på at undgå at skulle bære

byrden ved undersøgelsen af de relevante faktiske omstændigheder for at fastslå, om det indhold, der linkes til, er rigtigt.

Når den person, der har indgivet en anmodning om fjernelse af links, fremlægger beviser, som godtgør, at oplysningerne i det indhold, der er linket til, eller i det mindste en del af disse oplysninger, som ikke er uvæsentlig i forhold til indholdet som helhed, er åbenbart urigtige, er søgemaskineudbyderen følgelig forpligtet til at efterkomme denne anmodning om fjernelse af links. Det samme gør sig gældende, når denne person forelægger en retsafgørelse, der er truffet i forhold til udgiveren af webstedet, og som er baseret på en konstatering af, at oplysningerne i det indhold, der linkes til, som ikke er uvæsentlige i forhold til indholdet som helhed, i det mindste ved første øjekast er urigtige. Hvis den urigtige karakter af sådanne oplysninger ikke fremgår på åbenbar vis af de beviser, som den registrerede har fremlagt, er søgemaskineudbyderen derimod ikke forpligtet til at efterkomme en sådan anmodning om fjernelse af links, hvis der ikke foreligger en sådan retsafgørelse. Når de omhandlede oplysninger kan bidrage til en debat af almen interesse, skal retten til ytrings- og informationsfrihed, henset til samtlige øvrige omstændigheder i den foreliggende sag, tillægges særlig relevans.

Endelig tilføjede Domstolen, at når søgemaskineudbyderen ikke tager en anmodning om fjernelse af links til følge, skal den registrerede kunne indbringe dette for tilsynsmyndigheden eller for en retsinstans, med henblik på at denne foretager de nødvendige undersøgelser og følgelig pålægger den registeransvarlige at træffe de påkrævede foranstaltninger. I denne henseende tilkommer det således navnlig de retslige myndigheder at sikre afvejningen af de konkurrerende interesser, idet disse er bedst i stand til at foretage en kompleks og tilbundsgående afvejning, som tager hensyn til alle de kriterier og forhold, der er fastsat i den relevante praksis.

For det andet fastslog Domstolen, at der i forbindelse med afvejningen af de ovennævnte grundlæggende rettigheder med henblik på behandlingen af en anmodning om at slette fotografier, der vises som miniaturebilleder af en fysisk person, fra resultaterne af en billedsøgning, der er foretaget på grundlag af denne persons navn, skal tages hensyn til disse fotografiers informative værdi uafhængigt af sammenhængen for deres offentliggørelse på det websted, hvorfra de stammer. Der skal imidlertid tages hensyn til alle de tekstelementer, som direkte ledsager visningen af disse fotografier i søgeresultaterne, og som vil kunne kaste lys over deres informative værdi.

For at nå til denne konklusion fremhævede Domstolen, at billedsøgninger, der foretages via en søgemaskine på internettet på en persons navn, er underlagt de samme principper som dem, der finder anvendelse på søgning på websteder og de oplysninger, der forekommer på disse. Domstolen fastslog, at visningen efter en søgning på et navn af fotografier i form af miniaturebilleder af den registrerede kan udgøre et særligt vigtigt indgreb i denne persons ret til beskyttelse af privatlivets fred og retten til beskyttelse af den registreredes personoplysninger.

Når en søgemaskineudbyder modtager en anmodning om fjernelse, som tilsigter at fjerne resultater fra en billedsøgning baseret på en persons navn, der består af miniaturebilleder af fotografier af denne person, skal søgemaskineudbyderen prøve, om visningen af de omhandlede fotografier er nødvendig for, at de internetbrugere, som potentielt kunne være interesserede i at få adgang til disse fotografier ved en sådan søgning, kan udøve deres ret til informationsfrihed.

For så vidt som søgemaskinen viser den berørte persons fotografier uden for den sammenhæng, hvori de er offentliggjort på det websted, der er linket til, oftest med henblik på at illustrere de tekstmæssige elementer, som denne side indeholder, skal det imidlertid afgøres, om denne sammenhæng ikke desto mindre skal tages i betragtning ved den afvejning af de konkurrerende rettigheder og interesser, der skal foretages. I denne forbindelse afhænger spørgsmålet om, hvorvidt denne vurdering ligeledes skal omfatte indholdet fra det websted, som indeholder det fotografi, der i form af et miniaturebillede heraf er søgt slettet fra visningen, af genstanden for og arten af den omhandlede behandling.

Hvad for det første angår genstanden for den omhandlede behandling bemærkede Domstolen, at offentliggørelsen af fotografier som ikke-verbalt kommunikationsmiddel kan have en stærkere indvirkning på internetbrugerne end offentliggørelsen af tekster. Fotografierne er nemlig som sådan et vigtigt middel til at tiltrække internetbrugernes opmærksomhed og kan give anledning til en interesse i at få adgang til de artikler, som de illustrerer. Navnlig på grund af den omstændighed, at fotografierne ofte kan fortolkes på flere måder, kan visningen som miniaturebilleder på listen over søgeresultater medføre et særligt alvorligt indgreb i den registreredes ret til beskyttelse af sit image, hvilket der skal tages hensyn til i forbindelse med afvejningen af de konkurrerende rettigheder og interesser. Der skal derfor foretages en særskilt afvejning alt efter om der er tale om dels artikler forsynet med fotografier, der er offentliggjort af webstedsudgiveren, og som – når de indgår i deres oprindelige sammenhæng – illustrerer de oplysninger, der gives i disse artikler, og de heri udtrykte meningstilkendegivelser, dels fotografier, der vises i form af miniaturebilleder på en søgemaskineudbyders resultatliste, uden for den sammenhæng, hvori de oprindeligt blev offentliggjort på webstedet.

Domstolen bemærkede i denne henseende, at ikke blot er der ikke nødvendigvis sammenfald mellem det grundlag, der berettiger offentliggørelsen af en personoplysning på internettet, og det grundlag, der finder anvendelse på søgemaskiners aktivitet, men resultatet af den omhandlede rettigheds- og interesseafvejning, der skal foretages, kan – selv når dette er tilfældet – være forskelligt, alt efter om der er tale om behandlingen foretaget af søgemaskineudbyderen eller behandlingen foretaget af webstedsudgiveren. For det første kan de legitime interesser, der berettiger disse behandlinger, være forskellige, og de konsekvenser, som nævnte behandlinger har for den berørte person, navnlig for den pågældendes privatliv, og for det andet er de ikke nødvendigvis de samme.

Hvad for det andet angår arten af den behandling, der foretages af søgemaskineudbyderen, fastslog Domstolen, at søgemaskineudbyderen ved at identificere fotografier af fysiske personer, der er offentliggjort på internettet, og ved at vise dem særskilt i resultaterne af en billedsøgning i form af miniaturebilleder, kan tilbyde en tjeneste, der indebærer en behandling af personoplysninger, som er selvstændig og adskilt fra den behandling, som udgiveren af det websted, hvorfra fotografierne er hentet, foretager, og fra den behandling, som denne udbyder også er ansvarlig for, i forbindelse med linket til denne side.

Følgelig er det nødvendigt at foretage en selvstændig vurdering af søgemaskineudbyderens aktivitet, der består i at vise resultater af en billedsøgning i form af miniaturebilleder, eftersom den yderligere krænkelse af de grundlæggende rettigheder, der følger af en sådan aktivitet, kan være særlig intensiv som følge af, at alle oplysninger om den registrerede, der befinder sig på internettet, sammenlægges i forbindelse med en søgning på navn. I forbindelse med denne selvstændige vurdering skal der tages hensyn til den omstændighed, at visning på internettet af fotografier i form af miniaturebilleder i sig selv udgør det resultat, som internetbrugeren ønsker at opnå, uafhængigt af internetbrugers senere beslutning om at få adgang til det oprindelige websted.

Domstolen bemærkede imidlertid, at en sådan specifik afvejning, som tager hensyn til den selvstændige karakter af den behandling, som søgemaskineudbyderen foretager, ikke berører den eventuelle relevans af tekstelementer, der direkte kan ledsage visning af et fotografi på listen over søgeresultater, idet sådanne oplysninger kan kaste lys over fotografiets informative værdi for offentligheden og dermed påvirke afvejningen af de foreliggende rettigheder og interesser.

4. Samtykke fra brugeren af et internetwebsted til lagring af oplysninger

Dom af 1. oktober 2019 (Store Afdeling), Planet49 (C-673/17, [EU:C:2019:801](#))

Ved denne dom fastslog Domstolen, at samtykke til lagring af oplysninger eller til adgang til oplysninger via cookies, der er installeret på brugeren af et internetwebstedes terminaludstyr, ikke er gyldigt afgivet, når tilladelsen følger af et forudafkrydset felt, og dette uafhængigt af om de omhandlede oplysninger udgør personoplysninger eller ej. Domstolen præciserede desuden, at tjenesteudbyderen skal give brugeren af et internetwebsted oplysninger om cookiernes funktionsvarighed og om, hvorvidt tredjemand har mulighed for at få adgang til disse cookies eller ej.

Twisten i hovedsagen vedrørte Planet49's afholdelse af en salgsfremmende konkurrence på internetwebstedet [www.dein-macbook.de](#). For at deltage skulle internetbrugere angive deres navn og adresse på en internetside med afkrydsningsfelter. Det felt, der gav tilladelse til installationen af cookies, var forudafkrydset. Bundesgerichtshof (forbundsdomstol, Tyskland), som skulle behandle en sag, som den tyske

forbundssammenslutning af forbrugerforeninger havde anlagt, var i tvivl om, hvorvidt indhentelse af samtykke fra brugerne ved hjælp af det forudafkrydsede felt var gyldigt, og om omfanget af den oplysningspligt, der påhvilede tjenesteudbyderen.

Anmodningen om præjudiciel afgørelse vedrørte i det væsentlige fortolkningen af begrebet samtykke, som er omhandlet i direktiv 2002/58⁹⁴, sammenholdt med direktiv 95/46⁹⁵ og med databeskyttelsesforordningen⁹⁶.

Domstolen bemærkede for det første, at artikel 2, litra h), i direktiv 95/46, som artikel 2, litra f), i direktiv 2002/58 henviser til, definerer samtykket som »enhver frivillig, specifik og informeret viljetilkendegivelse, hvorved den registrerede indvilliger i, at personoplysninger, der vedrører den pågældende selv, gøres til genstand for behandling«. Den anførte, at kravet om en viljes-»tilkendegivelse« fra den registreredes side tydeligt pegede på en aktiv og ikke passiv adfærd. Et samtykke givet ved hjælp af et forudafkrydset felt indebærer imidlertid ikke en aktiv adfærd fra brugeren af et internetwebsteds side. Tilblivelseshistorien for artikel 5, stk. 3, i direktiv 2002/58, som siden ændringen ved direktiv 2009/136 har fastsat, at brugeren skal have »givet sit samtykke« til placeringen af cookies, synes desuden at indikere, at det ikke længere på forhånd kan formodes, at brugeren giver samtykke, og at dette skal følge af en aktiv adfærd fra dennes side. Endelig er et aktivt samtykke nu fastsat ved databeskyttelsesforordningen⁹⁷, hvis artikel 4, nr. 11), kræver en viljestilkendegivelse, der tager form af bl.a. en »klar bekræftelse«, og hvis 32. betragtning udtrykkeligt udelukker, at der foreligger et samtykke i tilfælde af »[t]avshed, forudafkrydsede felter eller inaktivitet«.

Domstolen udtalte derfor, at samtykket ikke er gyldigt afgivet, når lagring af oplysninger eller adgang til oplysninger, som allerede er lagret på brugeren af et internetwebsteds terminaludstyr, tillades ved et forudafkrydset felt, som brugeren skal vælge fra for at nægte at give sit samtykke. Den tilføjede, at det forhold, at en bruger trykker på knappen for at deltage i den omhandlede konkurrence, ikke kan være tilstrækkeligt for at lægge til grund, at denne gyldigt har givet sit samtykke til placering af cookies.

For det andet konstaterede Domstolen, at artikel 5, stk. 3, i direktivet 2002/58 har til formål at beskytte brugeren mod indgreb i dennes privatsfære, uanset om dette indgreb vedrører personoplysninger eller ej. Det følger heraf, at begrebet samtykke ikke skal fortolkes forskelligt, alt efter om de lagrede eller konsulterede oplysninger på brugeren af et internetwebsteds terminaludstyr udgør personoplysninger eller ej.

For det tredje anførte Domstolen, at artikel 5, stk. 3, i direktiv 2002/58 kræver, at brugeren har givet sit samtykke efter at have modtaget klare og fyldestgørende oplysninger, bl.a. om formålet med behandlingen. Klare og fyldestgørende oplysninger

⁹⁴ Artikel 2, litra f), og artikel 5, stk. 3, i direktiv 2002/58, som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25.11.2009 (EUT 2009, L 337, s. 11).

⁹⁵ Artikel 2, litra h), i direktiv 95/46.

⁹⁶ Artikel 6, stk. 1, litra a), i forordning 2016/679.

⁹⁷ Ibidem.

indebærer, at brugeren er i stand til uden besvær at bestemme følgerne af det eventuelle samtykke og at sikre, at dette samtykke gives med fuldt kendskab til følgerne. I denne henseende udtalte Domstolen, at oplysninger om cookiernes funktionsvarighed og om tredjemands mulighed for at få adgang til disse cookies indgår blandt de klare og fyldestgørende oplysninger, som tjenesteudbyderen skal give til brugeren af et internetwebsted.

5. Behandling af personoplysninger på sociale onlinenetværk

Dom af 4. juli 2023 (Store Afdeling), Meta Platforms m.fl. (Almindelige betingelser for anvendelse af et socialt netværk) (C-252/21, [EU:C:2023:537](#))

Virksomheden Meta Platforms er ejer af det sociale onlinenetværk »Facebook«, som er gratis for private brugere. Den økonomiske model for det sociale onlinenetværk er baseret på onlinereklamefinansiering, som er tilpasset den individuelle bruger. En sådan reklametype er gjort teknisk mulig ved den automatiske oprettelse af detaljerede profiler for brugerne af netværket og af de onlinetjenester, som Meta-koncernen tilbyder. For at kunne anvende det nævnte sociale netværk, skal brugerne således, når de opretter en profil, acceptere de af Meta Platforms fastsatte almindelige betingelser, som henviser til den af selskabet fastlagte datapolitik og politik om cookies. I henhold til sidstnævnte indsamler Meta Platforms – ud over de oplysninger, som disse brugere giver direkte ved oprettelsen af deres profil – ligeledes oplysninger vedrørende de nævnte brugernes aktiviteter inden for og uden for det sociale netværk og tilknytter dem til de pågældende brugeres Facebook-konti. Hvad angår de sidstnævnte oplysninger, der også benævnes »off Facebook-oplysningerne«, er der dels tale om oplysninger om besøg på tredjeparters websteder, dels oplysninger om brug af andre onlinetjenester, der tilhører Meta-koncernen (herunder Instagram og WhatsApp). Disse oplysningers samlede indhold gør det muligt at drage detaljerede konklusioner vedrørende brugernes præferencer og interesser.

Ved afgørelse af 6. februar 2019 pålagde Bundeskartellamt (forbundskonkurrencemyndighed, Tyskland) Meta Platforms et forbud dels mod i de dagældende almindelige betingelser at gøre de tysk bosiddende brugeres anvendelse af det sociale netværk Facebook betinget af behandlingen af deres off Facebook-oplysninger, dels mod uden brugernes samtykke at behandle disse oplysninger. Forbundskonkurrencemyndigheden pålagde desuden Meta Platforms at tilpasse deres almindelige betingelser, således at det klart fremgår heraf, at de nævnte oplysninger hverken indsamles, tilknyttes brugernes Facebook-konti eller anvendes uden den pågældende brugers samtykke. Endelig fremhævede denne myndighed, at et sådant samtykke ikke er gyldigt, når det er en betingelse for anvendelsen af det sociale netværk. Forbundskonkurrencemyndigheden begrundede sin afgørelse med, at behandlingen af

de pågældende oplysninger, som ikke var i overensstemmelse med databeskyttelsesforordningen, udgjorde misbrug af Meta Platforms' dominerende stilling på markedet for sociale onlinenetværk.

Meta Platforms anlagde søgsmål til prøvelse af denne afgørelse ved Oberlandesgericht Düsseldorf (den regionale ret i første instans i Düsseldorf, Tyskland). Da denne bl.a. nærede tvivl om fortolkningen og anvendelsen af visse bestemmelser i databeskyttelsesforordningen, forelagde den Domstolen en anmodning om en præjudiciel afgørelse.

I sin dom klarlagde Domstolen en operatør af sociale netværks mulighed for at behandle sine brugeres »følsomme« personoplysninger, betingelserne for lovlig behandling af personoplysninger foretaget af en sådan operatør samt gyldigheden af et samtykke, som af disse brugere afgives med henblik på en sådan behandling til en virksomhed, der har en dominerende stilling på det nationale marked for sociale onlinenetværk.

Hvad angår behandlingen af særlige kategorier af personoplysninger ⁹⁸ fastslog Domstolen, at såfremt en bruger af et socialt onlinenetværk besøger websteder eller anvender applikationer i forbindelse med en eller flere af disse kategorier og eventuelt indtaster oplysninger heri ved at registrere sig eller foretage onlinebestillinger, skal den behandling af personoplysninger, som operatøren af dette sociale onlinenetværk foretager ⁹⁹, anses for at udgøre »behandling af særlige kategorier af personoplysninger« som omhandlet i databeskyttelsesforordningens artikel 9, stk. 1, når denne behandling af oplysninger kan afsløre oplysninger, der er omfattet af en af disse kategorier, uanset om oplysningerne vedrører en bruger af dette netværk eller enhver anden fysisk person. En sådan behandling af oplysninger er principielt forbudt med visse undtagelser ¹⁰⁰.

I sidstnævnte henseende præciserede Domstolen, at når en bruger af et socialt onlinenetværk besøger websteder eller anvender applikationer i forbindelse med en eller flere af de nævnte kategorier, kan vedkommende ikke anses for tydeligvis at have offentliggjort ¹⁰¹ de oplysninger om dette besøg, som operatøren af det sociale onlinenetværk har indsamlet gennem cookies eller lignende lagringsteknologier. Når brugeren indtaster oplysninger på sådanne websteder eller applikationer eller trykker

⁹⁸ Jf. databeskyttelsesforordningens artikel 9, stk. 1. Denne bestemmelse foreskriver, at »[b]ehandling af personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering er forbudt«.

⁹⁹ Denne behandling består i indsamling af oplysninger fra besøg på disse websteder eller anvendelse af disse applikationer samt de af brugeren indtastede oplysninger gennem grænseflader, cookies eller lignende lagringsteknologier, sammenstilling af samtlige disse oplysninger med brugerens konto på den pågældendes sociale netværk og operatørens anvendelse af nævnte oplysninger.

¹⁰⁰ Som fastsat i databeskyttelsesforordningens artikel 9, stk. 2. Følgende fremgår af denne bestemmelse: »Stk. 1 finder ikke anvendelse, hvis et af følgende forhold gør sig gældende:

a) Den registrerede har givet udtrykkeligt samtykke til behandling af sådanne personoplysninger til et eller flere specifikke formål, medmindre det i EU-retten eller medlemsstaternes nationale ret er fastsat, at det i stk. 1 omhandlede forbud ikke kan hæves ved den registreredes samtykke. [...]
e) Behandling vedrører personoplysninger, som tydeligvis er offentliggjort af den registrerede.
f) Behandling er nødvendig, for at retskrav kan fastlægges, gøres gældende eller forsvares, eller når domstole handler i deres egenskab af domstol. [...]

¹⁰¹ Som omhandlet i databeskyttelsesforordningens artikel 9, stk. 2, litra e).

på valgknapper på disse websteder og applikationer, såsom knapperne »synes godt om«, »del«, eller på knapper, som giver brugeren mulighed for at identificere sig på disse websteder eller i disse applikationer ved anvendelse af de loginoplysninger, der er tilknyttet brugerens konto på det sociale netværk, telefonnummer eller e-mailadresse, kan en sådan bruger kun anses for tydeligvis at have offentliggjort de således indtastede oplysninger eller oplysninger fra tryk på disse knapper, når vedkommende udtrykkeligt på forhånd har tilkendegivet sit valg, eventuelt på grundlag af en personlig tilpasning, der er foretaget med fuldt kendskab til sagen, om at gøre oplysningerne om den pågældende offentligt tilgængelige for et ubegrænset antal personer.

Hvad mere generelt angår betingelserne for lovligheden af en behandling af personoplysninger bemærkede Domstolen, af en databehandling i henhold til databeskyttelsesforordningen er lovlig, såfremt og i det omfang den registrerede har givet samtykke til et eller flere specifikke formål ¹⁰². Når der ikke foreligger et sådant samtykke, eller når samtykket ikke er blevet givet frivilligt, specifikt, informeret og utvetydigt, er en sådan behandling alligevel begrundet, hvis den opfylder et af kravene om nødvendighed ¹⁰³, der skal fortolkes indskrænkende. Den behandling af personoplysninger om sine brugere, som foretages af en operatør af et socialt onlinenetværk, kan imidlertid kun anses for at være nødvendig af hensyn til opfyldelse af en kontrakt, som brugerne er part i, såfremt denne behandling er objektivt uundværlig for at gennemføre et formål, som er en integrerende del af den kontraktlige ydelse til de nævnte brugere, således at kontraktens hovedformål ikke vil kunne opfyldes uden den pågældende behandling.

Ifølge Domstolen kan den omhandlede behandling af oplysninger desuden kun anses for nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, på betingelse af at nævnte operatør har oplyst de brugere, hos hvem oplysningerne er blevet indsamlet, om den legitime interesse, som forfølges med behandlingen heraf, at behandlingen foretages inden for rammerne af, hvad der er strengt nødvendigt for at gennemføre denne legitime interesse, og at det fremgår af en afvejning af de modstridende interesser, henset til samtlige relevante omstændigheder, at brugernes interesser og grundlæggende rettigheder og frihedsrettigheder ikke går forud for den dataansvarliges eller tredjemands nævnte legitime interesse. Domstolen fastslog imidlertid bl.a., at de nævnte brugeres interesser og grundlæggende rettigheder i mangel af deres samtykke går forud for denne operatørs interesse i den personlige tilpasning af reklamer, hvorved operatøren finansierer sin virksomhed.

Endelig præciserede Domstolen, at den omhandlede behandling af oplysninger er begrundet, når den faktisk er nødvendig for at overholde en retlig forpligtelse, som

¹⁰² I henhold til databeskyttelsesforordningens artikel 6, stk. 1, første afsnit, litra a).

¹⁰³ Nævnt i databeskyttelsesforordningens artikel 6, stk. 1, første afsnit, litra b)-f). I henhold til disse bestemmelser er behandling kun lovlig, hvis og i det omfang behandlingen bl.a. er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i [databeskyttelsesforordningens artikel 6, stk. 1, første afsnit, litra b)], overholdelse af en retlig forpligtelse, som påhviler den dataansvarlige [databeskyttelsesforordningens artikel 6, stk. 1, første afsnit, litra c)], eller er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse [databeskyttelsesforordningens artikel 6, stk. 1, første afsnit, litra f)].

påhviler den dataansvarlige i henhold til EU-retten eller lovgivningen i den pågældende medlemsstat, når dette retsgrundlag opfylder et formål i samfundets interesse og står i rimeligt forhold til det legitime mål, der forfølges, og behandlingen foretages inden for rammerne af, hvad der er strengt nødvendigt.

Hvad angår gyldigheden af de berørte brugeres samtykke til behandling af deres oplysninger i henhold til databeskyttelsesforordningen fastslog Domstolen, at den omstændighed, at en operatør af et socialt onlinenetværk har en dominerende stilling på markedet for sociale onlinenetværk, ikke som sådan er til hinder for, at brugerne af et sådant netværk gyldigt kan give samtykke til denne operatørs behandling af deres personoplysninger. Henset til, at en sådan stilling kan påvirke disse brugeres frie valg og skabe en klar uligevægt mellem disse og den nævnte operatør, udgør den imidlertid et vigtigt element med henblik på at afgøre, om et samtykke rent faktisk er afgivet gyldigt, og navnlig frivilligt, hvilket det påhviler samme operatør at påvise ¹⁰⁴.

Brugerne af det pågældende sociale netværk skal således som led i den kontraktlige proces frit kunne vælge individuelt at afvise at give samtykke til særlige behandlinger af oplysninger, som ikke er nødvendige med henblik på opfyldelsen af kontrakten, uden at de imidlertid forpligtes til at give fuldt afkald på at anvende den tjeneste, som operatøren af det sociale onlinenetværk udbyder, hvilket indebærer, at nævnte brugere, i givet fald mod passende vederlag, kan tilbydes et tilsvarende alternativ, som ikke ledsages af sådanne behandlinger af oplysninger. Desuden skal der kunne gives særskilt samtykke til behandlingen af off Facebook-oplysninger.

VI. Nationale tilsynsmyndigheder

1. Rækkevidden af kravet om uafhængighed

Dom af 9 marts 2010 (Store Afdeling, Kommissionen mod Tyskland (C-518/07, [EU:C:2010:125](#))

Kommissionen havde med sin stævning nedlagt påstand om, at det blev fastslået, at Forbundsrepublikken Tyskland havde tilsidesat sine forpligtelser i henhold til artikel 28, stk. 1, andet afsnit, i direktiv 95/46 ved at underlægge de nationale tilsynsmyndigheder, der er kompetente med hensyn til behandling af personoplysninger uden for den offentlige sektor i de forskellige delstater, et statsligt tilsyn og således foretage en ukorrekt gennemførelse af kravet om »fuld uafhængighed« for de myndigheder, der skal sikre beskyttelsen af disse oplysninger.

Forbundsrepublikken Tyskland var af den opfattelse, at artikel 28, stk. 1, andet afsnit, i direktiv 95/46 kræver en funktionel uafhængighed for tilsynsmyndighederne i den

¹⁰⁴ I henhold til databeskyttelsesforordningens artikel 7, stk. 1.

forstand, at disse myndigheder skal være uafhængige af den ikke-offentlige sektor, der er underlagt deres kontrol, og at de ikke må udsættes for ydre påvirkning. Ifølge Forbundsrepublikken Tyskland udgjorde det statslige tilsyn, der blev udøvet i de tyske delstater, imidlertid ikke en sådan ydre påvirkning, men en intern overvågningsmekanisme af administrationen, der blev gennemført af myndigheder, der henhører under det samme administrative apparat som tilsynsmyndighederne, og som ligesom sidstnævnte er forpligtet til at opfylde formålene med direktiv 95/46.

Domstolen fastslog, at garantien for de nationale tilsynsmyndigheders uafhængighed som omhandlet i direktiv 95/46 har til formål at sikre et effektivt og pålideligt tilsyn med overholdelsen af reglerne om beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger og skal fortolkes i lyset af dette formål.

Tilsynsmyndighedernes uafhængighed er ikke etableret med henblik på at give disse myndigheder og deres ansatte en særlig status, men med henblik på at styrke beskyttelsen af personer og organer, der måtte blive berørt af deres afgørelser. Det følger heraf, at når tilsynsmyndighederne udøver deres funktioner, skal de handle objektivt og upartisk.

Domstolen anførte, at de tilsynsmyndigheder, der er kompetente med hensyn til behandling af personoplysninger uden for den offentlige sektor, skal være uafhængige, således at de har mulighed for at udøve deres funktioner uden ydre påvirkning. Denne uafhængighed udelukker ikke alene enhver påvirkning, der bliver udøvet af de kontrollerede organer, men også ethvert påbud og enhver anden ydre påvirkning – hvad enten denne er direkte eller indirekte – der kan skabe tvivl om udførelsen af de nævnte myndigheders opgave, der består i at skabe en ligevægt mellem beskyttelsen af retten til privatlivets fred og den frie udveksling af personoplysninger. Den blotte risiko for, at den tilsynsførende myndighed kan påvirke tilsynsmyndighedernes beslutninger politisk, er tilstrækkelig til at hindre, at sidstnævnte kan udøve deres opgaver uafhængigt. Det kan for det første medføre en »forudgående lydighed« fra disse myndigheders side over for det statslige tilsyns beslutningspraksis. For det andet kræver den rolle som vogter af retten til privatlivets fred, som tilsynsmyndighederne har påtaget sig, at deres beslutninger og således myndighederne selv står uden for enhver mistanke om partiskhed. Ifølge Domstolen var det statslige tilsyn ikke foreneligt med kravet om uafhængighed.

Dom af 16 oktober 2012 (Store Afdeling), Kommissionen mod Østrig (C-614/10, [EU:C:2012:631](#))

Europa-Kommissionen havde med sin stævning nedlagt påstand om, at Domstolen fastslog, at Republikken Østrig havde tilsidesat sine forpligtelser i henhold til artikel 28, stk. 1, andet afsnit, i direktiv 95/46, idet den ikke havde vedtaget alle de nødvendige bestemmelser, med henblik på at den i Østrig gældende lovgivning opfyldte kriteriet om uafhængighed vedrørende Datenschutzkommission (databeskyttelseskommission), der var nedsat som tilsynsmyndighed for beskyttelse af personoplysninger.

Domstolen fastslog, at Østrig havde begået traktatbrud, idet Domstolen i det væsentlige var af den opfattelse, at en medlemsstat, der har indført retsfor skrifter, hvorefter det administrerende medlem af den pågældende myndighed er en statstjenestemand, som er undergivet et tjenstligt tilsyn, hvis kontor er integreret i den nationale regerings tjenestegrene, og fra hvem statschefen har en ubetinget ret til at blive informeret om alle aspekter ved forvaltningen af den pågældende myndighed, ikke opfylder kriteriet om tilsynsmyndighedens uafhængighed i direktiv 95/46.

Domstolen fremhævede først og fremmest, at ordene »i fuld uafhængighed« i artikel 28, stk. 1, andet afsnit, i direktiv 95/46 indebærer, at tilsynsmyndighederne skal være uafhængige, således at de har mulighed for at udøve deres funktioner uden udefrakommende påvirkning. I denne henseende er den omstændighed, at en sådan myndighed har en funktionel uafhængighed, idet dens medlemmer er uafhængige og ikke bundet af nogen instrukser i udøvelsen af deres hverv, ikke i sig selv tilstrækkelig til at sikre tilsynsmyndigheden mod enhver udefrakommende påvirkning. Den uafhængighed, som kræves i denne forbindelse, har imidlertid til formål at udelukke ikke alene direkte indflydelse i form af instrukser, men også enhver form for indirekte indflydelse, der vil kunne påvirke tilsynsmyndighedens afgørelser. Henset til den rolle som vogter af retten til privatlivets fred, som disse myndigheder varetager, skal deres beslutninger, og således også myndighederne selv, stå uden for enhver mistanke om partiskhed.

Domstolen præciserede, at en national tilsynsmyndighed ikke har brug for en selvstændig budgetpost i lighed med den, som er fastsat ved artikel 43, stk. 3, i forordning nr. 45/2001, for at kunne opfylde uafhængighedskriteriet i direktiv 95/46. Medlemsstaterne er dog ikke forpligtet til i deres nationale lovgivning at overtage lignende bestemmelser som dem, der er indeholdt i kapitel V i forordning nr. 45/2001, for at sikre deres tilsynsmyndighed(s/ers) fulde uafhængighed, og kan dermed bestemme, at tilsynsmyndigheden i budgetmæssig henseende henhører under et bestemt ministerområde. Imidlertid må tildeling af udstyr og personale mæssige ressourcer, som er nødvendige for en sådan myndighed, ikke forhindre den i at udøve sine funktioner »i fuld uafhængighed«, som omhandlet i artikel 28, stk. 1, andet afsnit, i direktiv 95/46.

Dom af 8. april 2014 (Store Afdeling), Kommissionen mod Ungarn (C-288/12, [EU:C:2014:237](#))

I denne sag havde Kommissionen nedlagt påstand om, at Domstolen fastslog, at Ungarn havde tilsidesat sine forpligtelser i henhold til direktiv 95/46, idet Ungarn havde bragt mandatet for tilsynsmyndigheden for beskyttelse af personoplysninger til ophør før tid.

Domstolen fastslog, at en medlemsstat, der bringer mandatet for tilsynsmyndigheden for beskyttelse af personoplysninger til ophør før tid, tilsidesætter sine forpligtelser i henhold til direktiv 95/46.

Ifølge Domstolen udelukker den uafhængighed, som de tilsynsmyndigheder, der er kompetente med hensyn til behandling af nævnte oplysninger, skal have, bl.a. ethvert påbud og enhver anden ydre påvirkning – uanset formen, og hvad enten denne er direkte eller indirekte – der kan påvirke deres afgørelser, og som således kan skabe tvivl om udførelsen af de nævnte myndigheders opgave, der består i at skabe en ligevægt mellem beskyttelsen af retten til privatlivets fred og den frie udveksling af personoplysninger.

Domstolen fremhævede endvidere, at funktionel uafhængighed ikke i sig selv er tilstrækkelig til at sikre myndighederne mod enhver udefrakommende påvirkning, idet den blotte risiko for, at det statslige tilsyn kan påvirke tilsynsmyndighedernes beslutninger politisk, er tilstrækkeligt til at hindre, at sidstnævnte kan udøve deres opgaver uafhængigt. Hvis en medlemsstat kunne bringe en tilsynsmyndigheds mandat til ophør før dets oprindeligt fastsatte udløb, uden at de regler og garantier, der er blevet opstillet med henblik herpå ved den gældende lovgivning, overholdes, ville truslen om et sådant ophør før tid, som en sådan myndighed ville blive udsat for i den periode, hvori den udøver sit mandat, kunne føre til en form for lydighed fra dennes side i forhold til den politiske magt, der er uforenelig med det nævnte krav om uafhængighed. I en sådan situation ville tilsynsmyndigheden heller ikke kunne anses for under alle omstændigheder at handle uden for enhver mistanke om partiskhed.

2. Fastlæggelse af den ret, der finder anvendelse, og den kompetente tilsynsmyndighed

Dom af 1. oktober 2015, Weltimmo (C-230/14, [EU:C:2015:639](#))

Nemzeti Adatvédelmi és Információszabadság Hatóság (national myndighed til beskyttelse af oplysninger og informationsfriheden, Ungarn) havde pålagt selskabet Weltimmo, der er registreret i Slovakiet, og som administrerer websteder med annoncer for ejendomme beliggende i Ungarn, en bøde med den begrundelse, at selskabet ikke havde slettet personoplysningerne for annoncørerne på disse websteder, selv om de havde anmodet herom, og havde videregivet disse oplysninger til inkassofirmaer med henblik på at opnå betaling af ubetalte fakturaer. Ifølge den ungarske tilsynsmyndighed havde selskabet Weltimmo dermed overtrådt den ungarske lov til gennemførelse af direktiv 95/46.

Der blev iværksat en kassationsappel ved Kúria (øverste domstol, Ungarn), som gav udtryk for tvivl om fastlæggelsen af den ret, der finder anvendelse, og de beføjelser, som den ungarske tilsynsmyndighed har i henhold til artikel 4, stk. 1, og artikel 28 i direktiv 95/46. Den forelagde derfor Domstolen flere præjudicielle spørgsmål.

Med hensyn til den gældende nationale ret fastslog Domstolen, at artikel 4, stk. 1, litra a), i direktiv 95/46 gør det muligt at anvende en anden medlemsstats lovgivning om beskyttelse af personoplysninger end den medlemsstat, hvor den registeransvarlige er registreret, for så vidt som denne via en permanent struktur på denne medlemsstats område udøver en, selv minimal, faktisk og reel aktivitet, som led i hvilken denne behandling foretages. Med henblik på at afgøre, om dette er tilfældet, kunne den forelæggende ret bl.a. tage hensyn til den omstændighed dels, at den registeransvarliges aktivitet, som led i hvilken behandlingen finder sted, består i administration af websteder med ejendomsannoncer, der vedrører ejendomme på denne medlemsstats område, og som er udformet på denne medlemsstats sprog, hvorfor webstederne hovedsagelig eller fuldt ud er rettet mod denne medlemsstat. Dels kunne den forelæggende ret ligeledes tage hensyn til den omstændighed, at den registeransvarlige har en repræsentant i den nævnte medlemsstat, som skal inddrive de krav, der er opstået som følge af denne aktivitet, og repræsentere den registeransvarlige i forbindelse med de administrative og retslige procedurer vedrørende behandlingen af de berørte oplysninger. Domstolen præciserede derimod, at det ingen relevans har, hvilket statsborgerskab de personer, der er berørt af denne behandling af personoplysninger, har.

Med hensyn til den kompetence og de beføjelser, som den tilsynsmyndighed, der har modtaget en klage, har i henhold til artikel 28, stk. 4, i direktiv 95/46, fastslog Domstolen, at denne myndighed kan undersøge klagerne, uafhængigt af hvilken ret der finder anvendelse, og inden det er afklaret, hvilken national ret der finder anvendelse på den omhandlede behandling. Såfremt tilsynsmyndigheden når til den konklusion, at en anden medlemsstats ret finder anvendelse, kan den imidlertid ikke pålægge sanktioner uden for området for den medlemsstat, som den henhører under. I en sådan situation tilkommer det tilsynsmyndigheden, idet den udøver den forpligtelse til samarbejde, der er fastsat i direktivets artikel 28, stk. 6, at anmode tilsynsmyndigheden i den anden medlemsstat om at fastslå en eventuel overtrædelse af denne ret og pålægge sanktioner, hvis der deri er hjemmel til det, i givet fald med støtte i de oplysninger, som den førstnævnte tilsynsmyndighed har overført til tilsynsmyndigheden i den anden medlemsstat.

3. De nationale tilsynsmyndigheders beføjelser

Dom af 6. oktober 2015 (Store Afdeling), Schrems (C-362/14, [EU:C:2015:650](#))

I denne sag (se ligeledes afsnit IV med overskriften »Videregivelse af personoplysninger til tredjelande«) fastslog Domstolen navnlig, at de nationale tilsynsmyndigheder har kompetence til at kontrollere videregivelse af personoplysninger til tredjelande.

Domstolen fastslog i denne forbindelse først og fremmest, at de nationale tilsynsmyndigheder råder over en bred vifte af beføjelser, og disse beføjelser, der er opregnet på ikke-udtømmende vis i artikel 28, stk. 3, i direktiv 95/46, udgør lige så mange beføjelser, der er nødvendige til varetagelsen af deres opgaver. De nævnte myndigheder er således bl.a. tillagt beføjelser til at iværksætte undersøgelser, såsom beføjelsen til at indsamle alle de oplysninger, der er nødvendige for at varetage deres tilsynsopgaver, beføjelser til at gribe effektivt ind, såsom beføjelsen til midlertidigt eller definitivt at forbyde en behandling af oplysninger, eller beføjelse til at indbringe sager for retsinstanser.

Hvad angår beføjelsen til at kontrollere videregivelsen af personoplysninger til tredjelande fastslog Domstolen, at det ganske vist fremgår af artikel 28, stk. 1 og 6, i direktiv 95/46, at de nationale tilsynsmyndigheders beføjelser vedrører den behandling af personoplysninger, der foretages på den medlemsstats område, som disse myndigheder henhører under, således at de ikke råder over nogen beføjelser på grundlag af denne artikel 28 i forhold til den behandling af sådanne oplysninger, der foretages på et tredjelandets område.

Den transaktion, der består i at overføre personoplysninger fra en medlemsstat til et tredjeland, udgør imidlertid som sådan en behandling af personoplysninger foretaget på en medlemsstats område. Da de nationale tilsynsmyndigheder i overensstemmelse med chartrets artikel 8, stk. 3, og artikel 28 i direktiv 95/46 har til opgave at påse overholdelsen af de EU-retlige regler om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger, er hver af disse følgelig blevet tillagt beføjelse til at undersøge, om en videregivelse af disse oplysninger fra den medlemsstat, som myndigheden henhører under, til et tredjeland overholder de ved direktivet fastsatte krav.

Dom af 5. juni 2018 (Store Afdeling), Wirtschaftsakademie Schleswig Holstein (C-210/16, [EU:C:2018:388](#))

I denne dom (se ligeledes afsnit II.5 med overskriften »Begrebet »registeransvarlig«/»dataansvarlig««), der bl.a. vedrørte fortolkningen af artikel 4 og 28 i direktiv 95/46, udtalte Domstolen sig om omfanget af de beføjelser, som tilsynsmyndighederne råder over i forhold til en behandling af personoplysninger, som indebærer deltagelse af flere aktører.

Domstolen fastslog således, at i tilfælde, hvor et selskab, som er etableret uden for Den Europæiske Union (såsom det amerikanske selskab Facebook), har flere virksomheder eller organer i forskellige medlemsstater, er tilsynsmyndigheden i en medlemsstat kompetent til at udøve de beføjelser, der tillægges den i overensstemmelse med direktivets artikel 28, stk. 3, over for en af dette selskabs virksomheder eller organer, der er beliggende på denne medlemsstats område (i det omhandlede tilfælde Facebook Germany), selv om denne virksomhed eller dette organ ifølge koncernens interne

opgavefordeling udelukkende har til opgave at sælge annonceplads og varetage øvrige marketingforanstaltninger på denne medlemsstats område, og eneansvaret for indsamling og behandling af personoplysninger på hele EU's område tilkommer en virksomhed eller et organ, som er beliggende i en anden medlemsstat (i det omhandlede tilfælde Facebook Ireland).

Domstolen præciserede desuden, at når tilsynsmyndigheden i en medlemsstat vil udøve sine beføjelser i artikel 28, stk. 3, i direktiv 95/46 til at gribe ind over for et organ, som er beliggende på denne medlemsstats område, på grund af en tilsidesættelse af bestemmelserne om beskyttelse af personoplysninger begået af en registeransvarlig tredjemand, som er etableret i en anden medlemsstat (i det omhandlede tilfælde Facebook Ireland), er denne tilsynsmyndighed kompetent til – uafhængigt af tilsynsmyndigheden i sidstnævnte medlemsstat (Irland) – at prøve lovligheden af en sådan databehandling og kan udøve sine beføjelser til at gribe ind over for et organ, som er beliggende på dens område, uden på forhånd at have anmodet tilsynsmyndigheden i den anden medlemsstat om at gribe ind.

Dom af 15 juni 2021 (Store Afdeling), Facebook Ireland m.fl. (C-645/19, [EU:C:2021:483](#))

Den 11. september 2015 anlagde formanden for den belgiske kommission for beskyttelse af privatlivets fred (herefter »CBPL«) et søgsmål med påstand om forbud mod Facebook Ireland, Facebook Inc. og Facebook Belgium ved Nederlandstalige rechtbank van eerste aanleg Brussel (den nederlandsksprogede ret i første instans i Bruxelles, Belgien) med det formål at standse Facebooks angivelige tilsidesættelse af lovgivningen om databeskyttelse. Denne tilsidesættelse bestod bl.a. i indsamling og anvendelse af oplysninger om de belgiske internetbrugeres adfærd, uanset om de er indehavere af en Facebook-konto, ved hjælp af forskellige teknologier, såsom cookies, sociale plug-ins¹⁰⁵ eller pixels.

Den 16. februar 2018 erklærede denne retsinstans sig kompetent til at træffe afgørelse om dette søgsmål og fastslog med hensyn til realiteten, at det sociale netværk Facebook ikke i tilstrækkelig grad havde oplyst de belgiske internetbrugere om indsamlingen og brugen af de pågældende oplysninger. I øvrigt blev det af internetbrugerne afgivne samtykke til indsamling og behandling af de nævnte oplysninger anset for ugyldigt.

Den 2. marts 2018 iværksatte Facebook Ireland, Facebook Inc. og Facebook Belgium appel til prøvelse af denne dom ved hof van beroep te Brussel (appeldomstolen i Bruxelles, Belgien), der er den forelæggende ret i den foreliggende sag. Den belgiske databeskyttelsesmyndighed (herefter »databeskyttelsesmyndigheden«) optrådte ved denne ret som retssuccessor for CBPL's formand. Den forelæggende ret erklærede sig alene kompetent til at træffe afgørelse om den af Facebook Belgium iværksatte appel.

¹⁰⁵ F.eks. knapperne »Synes godt om« eller »Del«.

Den forelæggende ret var i tvivl om betydningen af anvendelsen af den »one-stop-shop«-mekanisme, der er fastsat i databeskyttelsesforordningen ¹⁰⁶, på databeskyttelsesmyndighedens kompetencer og ønskede nærmere bestemt oplyst, om databeskyttelsesmyndigheden for så vidt angår de faktiske omstændigheder, der lå efter ikrafttrædelsen af databeskyttelsesforordningen, dvs. den 25. maj 2018, kunne anlægge sag mod Facebook Belgium, eftersom Facebook Ireland var blevet identificeret som dataansvarlig for de pågældende oplysninger. Fra denne dato og navnlig i medfør af princippet om »one-stop-shop«, der er fastsat i databeskyttelsesforordningen, er det således alene den irske databeskyttelseskommissær, der er kompetent til at anlægge et søgsmål med påstand om forbud, som er undergivet de irske retters efterprøvelse.

Domstolen (Store Afdeling) præciserede i sin dom de nationale tilsynsmyndigheders beføjelser inden for rammerne af databeskyttelsesforordningen. Den fastslog bl.a., at denne forordning på visse betingelser tillader en tilsynsmyndighed i en medlemsstat at udøve sin beføjelse til at indbringe alle angivelige overtrædelser af databeskyttelsesforordningen for en retsinstans i denne medlemsstat og at indlede eller deltage i retssager for så vidt angår en grænseoverskridende behandling af oplysninger ¹⁰⁷, selv om den ikke er den ledende tilsynsmyndighed for denne behandling.

For det første præciserede Domstolen de betingelser, hvorunder en national tilsynsmyndighed, der ikke er ledende tilsynsmyndighed for så vidt angår en grænseoverskridende behandling, skal udøve sin beføjelse til at indbringe alle angivelige overtrædelser af databeskyttelsesforordningen for en retsinstans i en medlemsstat og om nødvendigt indlede eller deltage i retssager med henblik på at sikre anvendelsen af denne forordning. Dels skal databeskyttelsesforordningen tillægge denne tilsynsmyndighed en kompetence til at vedtage en afgørelse, hvorved det fastslås, at denne behandling tilsidesætter de regler, der er fastsat i denne forordning, dels skal denne beføjelse udøves under overholdelse af de procedurer for samarbejde og sammenhæng, der er fastsat i denne forordning ¹⁰⁸.

For så vidt angår grænseoverskridende behandlinger fastsætter databeskyttelsesforordningen således »one-stop-shop«-mekanismen ¹⁰⁹, der er baseret på en kompetencefordeling mellem en »ledende tilsynsmyndighed« og de øvrige berørte nationale tilsynsmyndigheder. Denne mekanisme kræver et tæt, loyalt og effektivt samarbejde mellem disse myndigheder med henblik på at sikre en sammenhængende og ensartet beskyttelse af personoplysninger og således sikre dens effektive virkning. Databeskyttelsesforordningen fastsætter i denne forbindelse den ledende tilsynsmyndigheds principielle kompetence til at vedtage en afgørelse, hvorved det

¹⁰⁶ Databeskyttelsesforordningens artikel 56, stk. 1, har følgende ordlyd: »Uden at det berører artikel 55, er tilsynsmyndigheden for den dataansvarliges eller databehandlerens hovedvirksomhed eller eneste etablering kompetent til at fungere som ledende tilsynsmyndighed for den grænseoverskridende behandling, der foretages af denne dataansvarlige eller databehandler.«

¹⁰⁷ Som omhandlet i databeskyttelsesforordningens artikel 4, nr. 23).

¹⁰⁸ Fastsat i databeskyttelsesforordningens artikel 56 og 60.

¹⁰⁹ Databeskyttelsesforordningens artikel 56, stk. 1.

fastslås, at en grænseoverskridende behandling tilsidesætter de regler, der er fastsat i denne forordning ¹¹⁰, mens de øvrige berørte tilsynsmyndigheders kompetence til at vedtage en sådan afgørelse, selv midlertidigt, udgør undtagelsen ¹¹¹. Dog kan den ledende tilsynsmyndighed ikke ved udøvelsen af sine beføjelser se bort fra en nødvendig dialog og et loyalt og effektivt samarbejde med de andre berørte tilsynsmyndigheder. Af denne grund kan den ledende tilsynsmyndighed ikke se bort fra de øvrige berørte tilsynsmyndigheders synspunkter, og alle relevante og begrundede indsigelser fra en af disse sidstnævnte myndigheder bevirker, at vedtagelsen af udkastet til den ledende tilsynsmyndigheds afgørelse blokeres – i det mindste midlertidigt.

Domstolen præciserede i øvrigt, at den omstændighed, at en medlemsstats tilsynsmyndighed, som ikke er den ledende tilsynsmyndighed for så vidt angår en grænseoverskridende behandling af oplysninger, kun kan udøve beføjelsen til at indbringe alle angivelige overtrædelser af databeskyttelsesforordningen for en retsinstans i denne medlemsstat og til at indlede eller deltage i retssager under overholdelse af reglerne om fordeling af beslutningskompetencen mellem den ledende tilsynsmyndighed og de øvrige tilsynsmyndigheder ¹¹², er i overensstemmelse med chartrets artikel 7, 8 og 47, der sikrer den berørte persons ret til beskyttelse af personoplysninger og dennes ret til effektive retsmidler.

For det andet fastslog Domstolen, at det, for at en medlemsstats tilsynsmyndighed, som ikke er den ledende tilsynsmyndighed, kan gøre brug af beføjelsen til at indlede eller deltage i retssager i forbindelse med grænseoverskridende behandling af personoplysninger ¹¹³, ikke kræves, at den dataansvarlige eller databehandleren for den grænseoverskridende behandling af personoplysninger, som dette søgsmål omhandler, har en hovedvirksomhed eller en anden etablering på denne medlemsstats område. Udøvelsen af denne beføjelse skal imidlertid henhøre under databeskyttelsesforordningens territoriale anvendelsesområde ¹¹⁴, hvilket forudsætter, at den dataansvarlige eller databehandleren for den grænseoverskridende behandling er etableret i Unionen.

For det tredje fastslog Domstolen, at i forbindelse med grænseoverskridende behandling af personoplysninger kan en medlemsstats tilsynsmyndighed, som ikke er den ledende tilsynsmyndighed, gøre brug af beføjelsen til at indbringe alle angivelige overtrædelser af databeskyttelsesforordningen for en retsinstans i denne medlemsstat og om nødvendigt til at indlede eller deltage i retssager, både med hensyn til den dataansvarliges hovedvirksomhed, der ligger i den medlemsstat, som henhører under denne myndighed, og med hensyn til en anden af den ansvarliges etableringer, for så

¹¹⁰ Databeskyttelsesforordningens artikel 60, stk. 7.

¹¹¹ Databeskyttelsesforordningens artikel 56, stk. 2, og artikel 66 fastsætter undtagelserne til princippet om den ledende tilsynsmyndigheds beslutningskompetence.

¹¹² Fastsat i databeskyttelsesforordningens artikel 55 og 56, sammenholdt med databeskyttelsesforordningens artikel 60.

¹¹³ I henhold til databeskyttelsesforordningens artikel 58, stk. 5.

¹¹⁴ Databeskyttelsesforordningens artikel 3, stk. 1, fastsætter, at denne forordning finder anvendelse på behandling af personoplysninger, som foretages »som led i aktiviteter, der udføres for en dataansvarlig eller en databehandler, som er etableret i Unionen, uanset om behandlingen finder sted i Unionen eller ej«.

vidt som søgsmålet omhandler en behandling af oplysninger, der er foretaget inden for rammerne af denne etablerings aktiviteter, og nævnte myndighed er kompetent til at udøve denne beføjelse.

Domstolen præciserede imidlertid, at udøvelsen af denne beføjelse forudsætter, at databeskyttelsesforordningen finder anvendelse. Da de aktiviteter, som den af Facebook-koncernens etableringer, der er beliggende i Belgien, udøver, i den foreliggende sag var uløseligt forbundet med den i hovedsagen omhandlede behandling af personoplysninger, som Facebook Ireland er ansvarlig for på Unionens område, er denne behandling foretaget »som led i aktiviteter, der udføres for en dataansvarlig«, og dermed omfattet af databeskyttelsesforordningens anvendelsesområde.

For det fjerde fastslog Domstolen, at når en tilsynsmyndighed i en medlemsstat, som ikke er den »ledende tilsynsmyndighed« har anlagt et søgsmål om grænseoverskridende behandling af personoplysninger inden datoen for databeskyttelsesforordningens ikrafttræden, kan dette søgsmål, set fra et EU-retligt synspunkt, opretholdes på grundlag af bestemmelserne i direktiv 95/46, som fortsat finder anvendelse for så vidt angår overtrædelser af de regler, som det fastsætter, der er begået indtil datoen for dette direktivs ophævelse. Dette søgsmål kan desuden anlægges af denne myndighed for overtrædelser, der er begået efter datoen for databeskyttelsesforordningens ikrafttræden, for så vidt som det er i en af de situationer, hvor denne forordning undtagelsesvis tillægger denne samme tilsynsmyndighed en kompetence til at vedtage en afgørelse, hvori det fastslås, at den omhandlede behandling af oplysninger tilsidesætter de regler, der er fastsat i denne forordning, under overholdelse af de procedurer for samarbejde og sammenhæng, sidstnævnte forordning fastsætter.

Endelig og for det femte anerkendte Domstolen den direkte virkning af databeskyttelsesforordningens bestemmelse, ifølge hvilken hver medlemsstat fastsætter ved lov, at dens tilsynsmyndighed har beføjelse til at indbringe overtrædelser af denne forordning for de judicielle myndigheder og om nødvendigt at indlede eller deltage i retssager. En sådan myndighed kan følgelig påberåbe sig denne bestemmelse for at anlægge eller genoptage en sag mod private, selv om den ikke specifikt er blevet gennemført i den pågældende medlemsstats lovgivning.

Dom af 16. januar 2024 (Store Afdeling), Österreichische Datenschutzbehörde (C-33/22, [EU:C:2024:46](#))

I denne sag (se ligeledes afsnit II.1 med overskriften »Den generelle lovgivnings anvendelsesområde«) bemærkede Domstolen, at databeskyttelsesforordningens bestemmelser om de nationale tilsynsmyndigheders kompetence og om retten til klage ¹¹⁵ ikke kræver, at der vedtages nationale gennemførelsesforanstaltninger, og at de er tilstrækkeligt klare, præcise og ubetingede til at have direkte virkning. Det følger

¹¹⁵ Jf. henholdsvis artikel 55, stk. 1, og artikel 77, stk. 1, i databeskyttelsesforordningen.

heraf, at selv om databeskyttelsesforordningen indrømmer medlemsstaterne en skønsmargen med hensyn til antallet af tilsynsmyndigheder, der skal oprettes ¹¹⁶, fastsætter den derimod rækkevidden af den kompetence, som disse myndigheder skal tillægges med henblik på at kontrollere anvendelsen af databeskyttelsesforordningen. I det tilfælde, hvor en medlemsstat har valgt at etablere en enkelt national tilsynsmyndighed, har denne således nødvendigvis alle de beføjelser, der er fastsat i denne forordning. Den modsatte fortolkning ville indebære, at disse bestemmelser mister deres effektive virkning, og risikerer at svække den effektive virkning af alle andre bestemmelser i databeskyttelsesforordningen, der kan have betydning for en klage.

Hvad angår den omstændighed, at nationale forfatningsbestemmelser udelukker muligheden for, at en tilsynsmyndighed, der henhører under den udøvende magt, kan føre tilsyn med, hvorledes et organ, der henhører under den lovgivende magt, anvender databeskyttelsesforordningen, fremhævede Domstolen, at det netop er under overholdelse af medlemsstaternes forfatningsmæssige struktur, at databeskyttelsesforordningen begrænser sig til at kræve, at medlemsstaterne opretter mindst én tilsynsmyndighed, samtidig med at de gives mulighed for at oprette flere. Denne forordning indrømmer således hver medlemsstat en skønsmargen, der gør det muligt for den at oprette så mange tilsynsmyndigheder, som det måtte være nødvendigt navnlig af hensyn til de krav, der følger af medlemsstatens forfatningsmæssige struktur.

Påberåbelsen af nationale bestemmelser må desuden ikke være til skade for EU-rettens enhed og effektivitet. De virkninger, der er knyttet til princippet om EU-rettens forrang, er nemlig bindende for alle organer i en medlemsstat, uden at de interne bestemmelser, herunder bl.a. forfatningsbestemmelser, kan være til hinder herfor.

Når en medlemsstat har valgt at oprette en enkelt tilsynsmyndighed, kan den således ikke påberåbe sig bestemmelser i national ret, selv hvis der er tale om forfatningsbestemmelser, med henblik på at undtage behandlinger af personoplysninger, der er omfattet af databeskyttelsesforordningens anvendelsesområde, fra denne myndigheds tilsyn.

4. Betingelser for pålæggelse af administrative bøder

Dom af 5. december 2023 (Store Afdeling), Nacionalinis visuomenės sveikatos centras (C-683/21, [EU:C:2023:949](#))

I denne sag (se ligeledes afsnit II.3, II.5 og II.6 med overskrifterne »Begrebet »behandling af personoplysninger««, »Begrebet »registeransvarlig«/»dataansvarlig«« og »Begrebet »fælles dataansvarlig««) fastslog Domstolen, at en administrativ bøde kun kan pålægges

¹¹⁶ Navnlig i databeskyttelsesforordningens artikel 51, stk. 1.

en dataansvarlig i henhold til databeskyttelsesforordningens artikel 83, hvis det godtgøres, at den pågældende forsætligt eller uagtsomt har begået en overtrædelse af reglerne i denne forordning ¹¹⁷.

I denne henseende præciserede Domstolen, at EU-lovgiver ikke har overladt medlemsstaterne en skønsmargen med hensyn til de materielle betingelser, som en tilsynsmyndighed skal overholde, når den beslutter at pålægge en dataansvarlig en administrativ bøde i henhold til denne bestemmelse. Det forhold, at databeskyttelsesforordningen giver medlemsstaterne mulighed for at fastsætte undtagelser for offentlige myndigheder og organer, der er etableret i den pågældende medlemsstat ¹¹⁸, og krav vedrørende den procedure, som tilsynsmyndighederne skal følge ved pålæggelse af en administrativ bøde ¹¹⁹, betyder på ingen måde, at medlemsstaterne også kan fastsætte sådanne materielle betingelser.

Med hensyn til disse betingelser bemærkede Domstolen, at det blandt de forhold, der er opregnet i databeskyttelsesforordningen, på baggrund af hvilke tilsynsmyndigheden pålægger den dataansvarlige en administrativ bøde, nævnes, at der tages hensyn til, »hvorvidt overtrædelsen blev begået forsætligt eller uagtsomt« ¹²⁰. Derimod henvises der i ingen af disse forhold til en eventuel mulighed for at drage den dataansvarlige til ansvar, hvis denne ikke har handlet culpøst. Det er således kun overtrædelser af databeskyttelsesforordningens bestemmelser, der er begået forsætligt eller uagtsomt af den dataansvarlige, der kan føre til, at denne pålægges en administrativ bøde i henhold til forordningens artikel 83.

Domstolen tilføjede, at denne fortolkning understøttes af den almindelige opbygning af og formålet med databeskyttelsesforordningen. I denne forbindelse præciserede den, at den omstændighed, at der findes en sanktionsordning i henhold til databeskyttelsesforordningen, der – når de særlige omstændigheder i den enkelte sag begrundet det – gør det muligt at pålægge en administrativ bøde, skaber et incitament for de dataansvarlige og databehandlerne til at overholde denne forordning, og at de administrative bøder på grund af deres afskrækkende virkning bidrager til at styrke beskyttelsen af de registrerede. EU-lovgiver har imidlertid ikke fundet det nødvendigt at fastsætte pålæggelse af administrative bøder, når der ikke foreligger skyld. Henset til den omstændighed, at databeskyttelsesforordningen tager sigte på et beskyttelsesniveau, der både er tilsvarende og ensartet, og at den med henblik herpå skal anvendes på en ensartet måde i hele EU, ville det være i strid med dette formål at give medlemsstaterne mulighed for at fastsætte en sådan ordning for pålæggelse af en bøde.

¹¹⁷ En overtrædelse som omhandlet i artikel 83, stk. 4-6.

¹¹⁸ I henhold til databeskyttelsesforordningen artikel 83, stk. 7, der fastsætter, at »[...] hver medlemsstat [kan] fastsætte regler om, hvorvidt og i hvilket omfang administrative bøder må pålægges offentlige myndigheder og organer, der er etableret i den pågældende medlemsstat«.

¹¹⁹ I henhold til databeskyttelsesforordningens artikel 83, stk. 8, sammenholdt med 129. betragtning til forordningen.

¹²⁰ Databeskyttelsesforordningens artikel 83, stk. 2, litra b).

Domstolen fastslog desuden, at en sådan bøde kan pålægges en dataansvarlig med hensyn til aktiviteter til behandling af personoplysninger, der er gennemført af en databehandler på den dataansvarliges vegne, medmindre databehandleren i forbindelse med disse aktiviteter har behandlet oplysningerne til egne formål eller har behandlet dem på en måde, der er uforenelig med rammerne eller de nærmere regler for behandlingen, således som fastsat af den dataansvarlige, eller på en sådan måde, at det ikke med rimelighed kan antages, at den dataansvarlige har givet sit samtykke hertil. I et sådant tilfælde skal databehandleren anses for at være ansvarlig for en sådan behandling.

Dom af 5. december 2023 (Store Afdeling), Deutsche Wohnen (C-807/21, [EU:C:2023:950](#))

Deutsche Wohnen SE (herefter »DW«) er et ejendomsselskab, der indirekte gennem aktier i forskellige selskaber ejer talrige bolig- og erhvervsenheder. Selskabet behandler i forbindelse med sine forretningsaktiviteter personoplysninger om lejerne af disse enheder.

I forbindelse med to kontroller foretaget i 2017 og 2019 konstaterede Berliner Beauftragte für den Datenschutz (tilsynsmyndigheden i Berlin, Tyskland) en række overtrædelser af databeskyttelsesforordningen begået af DW. Ved afgørelse af 30. oktober 2019 pålagde denne tilsynsmyndighed DW administrative bøder for disse overtrædelser.

DW anlagde sag til prøvelse af denne afgørelse ved Landgericht Berlin (den regionale ret i første instans i Berlin, Tyskland), der henlagde sagen. Denne ret anførte, at i henhold til tysk lovgivning¹²¹ kan en administrativ forseelse kun fastslås i forhold til en fysisk person og ikke i forhold til en juridisk person. Såfremt en juridisk person pålægges et ansvar, kan denne person desuden alene tilregnes handlinger, der er begået af medlemmer af dens organer eller af dens repræsentanter. Staatsanwaltschaft Berlin (anklagemyndigheden i Berlin, Tyskland) iværksatte appel til prøvelse af denne afgørelse ved Kammergericht Berlin (den regionale appeldomstol i Berlin, Tyskland). I forbindelse hermed anmodede denne appeldomstol Domstolen om en præjudiciel afgørelse vedrørende fortolkningen af databeskyttelsesforordningen.

Domstolen (Store Afdeling) udtalte sig i sin dom om betingelserne for pålæggelse af administrative bøder i henhold til databeskyttelsesforordningen. For det første undersøgte den spørgsmålet om, hvorvidt medlemsstaterne kan betinge pålæggelse af en administrativ bøde over for en juridisk person af, at overtrædelser af denne forordning forudgående er tilregnet en identificeret fysisk person. For det andet behandlede den også, i lighed med dommen i sagen Nacionalinis visuomenės sveikatos

¹²¹ Gesetz über Ordnungswidrigkeiten (lov om administrative forseelser) af 24.5.1968 (BGBl. 1968 I, s. 481), som affattet ved bekendtgørelse af 19.2.1987 (BGBl. 1987 I, s. 602), og som ændret ved lov af 19.6.2020 (BGBl. 2020 I, s. 1350).

centras, spørgsmålet om, hvorvidt den overtrædelse af databeskyttelsesforordningens bestemmelser, der sanktioneres, skal være begået forsætligt eller uagtsomt.

Hvad angår muligheden for at pålægge en juridisk person en administrativ bøde i henhold til databeskyttelsesforordningen anførte Domstolen indledningsvis, at de principper, forbud og forpligtelser, der er fastsat i databeskyttelsesforordningen, især er rettet mod de »dataansvarlige«, hvis ansvar omfatter enhver behandling af personoplysninger, der foretages af de dataansvarlige eller på de dataansvarliges vegne. Det er dette ansvar, der i tilfælde af overtrædelse af databeskyttelsesforordningens bestemmelser udgør grundlaget for at pålægge den dataansvarlige en administrativ bøde i henhold til forordningens artikel 83. Imidlertid har EU-lovgiver med henblik på fastlæggelse af et sådant ansvar ikke foretaget en sondring mellem fysiske og juridiske personer, idet dette ansvar er underlagt den ene betingelse, at de fysiske eller juridiske personer alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger ¹²². Følgelig er enhver person, der opfylder denne betingelse, principielt bl.a. ansvarlig for enhver overtrædelse af databeskyttelsesforordningen, som er begået af den pågældende selv eller på dennes vegne. Dette indebærer for det første, at juridiske personer ikke alene er ansvarlige for overtrædelser begået af deres repræsentanter, direktører eller forvaltere, men ligeledes af enhver anden person, der handler inden for rammerne af disse juridiske personers forretningsaktivitet og på deres vegne. For det andet skal de administrative bøder, der er fastsat i databeskyttelsesforordningen, i tilfælde af sådanne overtrædelser kunne pålægges juridiske personer direkte, når disse kan kvalificeres som ansvarlige for behandlingen.

Dernæst bemærkede Domstolen, at der ikke er nogen bestemmelse i databeskyttelsesforordningen, der gør det muligt at antage, at muligheden for at pålægge en juridisk person en administrativ bøde som dataansvarlig er betinget af en forudgående konstatering af, at denne overtrædelse er blevet begået af en identificeret fysisk person. Desuden har EU-lovgiver ikke overladt medlemsstaterne en skønsmargen i denne henseende. Det forhold, at databeskyttelsesforordningen giver medlemsstaterne mulighed for at fastsætte krav vedrørende den procedure, som tilsynsmyndighederne skal følge ved pålæggelse af en administrativ bøde ¹²³, betyder på ingen måde, at de også kan fastsætte yderligere materielle betingelser ud over dem, der er fastsat i databeskyttelsesforordningen.

Domstolen præciserede i denne forbindelse, at det ville være i strid med formålet med databeskyttelsesforordningen, såfremt medlemsstaterne ensidigt og som forudsætning for at kunne pålægge en dataansvarlig, der er en juridisk person, en administrativ bøde i henhold til forordningens artikel 83, kunne kræve, at den pågældende overtrædelse forudgående er tilregnet eller kan tilregnes en identificeret fysisk person. Desuden ville

¹²² Ifølge databeskyttelsesforordningens artikel 4, nr. 7).

¹²³ Således som det fremgår af databeskyttelsesforordningens artikel 58, stk. 4, og artikel 83, stk. 8, sammenholdt med 129. betragtning til forordningen.

et sådant yderligere krav endelig risikere at svække effektiviteten og den afskrækkende virkning af de administrative bøder, der pålægges juridiske personer i deres egenskab af dataansvarlige.

Endelig fremhævede Domstolen, at begrebet »virksomhed« som omhandlet i artikel 101 TEUF og 102 TEUF ¹²⁴ ikke har betydning for spørgsmålet om, hvorvidt og på hvilke betingelser en administrativ bøde kan pålægges en dataansvarlig, der er en juridisk person, men kun er relevant ved fastsættelsen af størrelsen af en sådan bøde.

Domstolen konkluderede således, at databeskyttelsesforordningen ¹²⁵ er til hinder for en national lovgivning, hvorefter en administrativ bøde kun kan pålægges en juridisk person i dennes egenskab af dataansvarlig for en overtrædelse af denne forordning ¹²⁶, for så vidt som denne overtrædelse forudgående er blevet tilregnet en identificeret fysisk person.

Hvad angår spørgsmålet om, hvorvidt medlemsstaterne kan fastsætte pålæggelse af en administrativ bøde, selv når den overtrædelse, der sanktioneres, ikke er blevet begået forsætligt eller uagtsomt, bemærkede Domstolen indledningsvis, at de materielle betingelser, som en tilsynsmyndighed skal overholde, når den pålægger en dataansvarlig en sådan bøde, udelukkende hører under EU-retten, og at medlemsstaterne ikke er overladt en skønsmargen i denne henseende. Idet den fulgte den samme argumentation som i dommen i sagen *Nacionalinis visuomenės sveikatos*, fastslog Domstolen, at en administrativ bøde i henhold til databeskyttelsesforordningens artikel 83 kun kan pålægges, hvis det godtgøres, at den dataansvarlige, som både er en juridisk person og en virksomhed, forsætligt eller uagtsomt har begået en overtrædelse af forordningens bestemmelser.

5. Forholdet mellem nationale tilsynsmyndigheders beføjelser og andre nationale myndigheders beføjelser

Dom af 4. juli 2023 (Store Afdeling), Meta Platforms m.fl. (Almindelige betingelser for anvendelse af et socialt netværk) (C-252/21, [EU:C:2023:537](#))

I denne sag (se ligeledes afsnit V.5 med overskriften »Behandling af personoplysninger på sociale onlinenetværk«) bemærkede Domstolen, idet den tog stilling til en konkurrencemyndigheds kompetence til at konstatere, at behandling af personoplysninger ikke er forenelig med databeskyttelsesforordningen, fastslog Domstolen, at en sådan myndighed, forudsat at den overholder sin forpligtelse til loyalt

¹²⁴ Hvilket begreb der henvises til i 150. betragtning til databeskyttelsesforordningen.

¹²⁵ Databeskyttelsesforordningens artikel 58, stk. 2, litra i), og artikel 83, stk. 1-6.

¹²⁶ En overtrædelse som omhandlet i databeskyttelsesforordningen artikel 83, stk. 4-6.

samarbejde¹²⁷ med tilsynsmyndighederne for databeskyttelse, som led i undersøgelsen af en virksomheds misbrug af dominerende stilling¹²⁸ kan fastslå, at denne virksomheds almindelige brugerbetingelser vedrørende behandlingen af personoplysninger og gennemførelsen heraf ikke er i overensstemmelse med denne forordning, når denne konstatering er nødvendig for at påvise et sådant misbrug. Når en konkurrencemyndighed i forbindelse med konstateringen af misbrug af en dominerende stilling konstaterer en overtrædelse af databeskyttelsesforordningen, erstatter den imidlertid ikke tilsynsmyndighederne.

Når konkurrencemyndighederne under udøvelsen af deres kompetencer skal undersøge, om en virksomheds adfærd er i overensstemmelse med bestemmelserne i databeskyttelsesforordningen, skal de således, henset til princippet om loyalt samarbejde, rådføre sig med og samarbejde loyalt med de berørte nationale tilsynsmyndigheder eller med den ledende tilsynsmyndighed. Alle disse myndigheder har således pligt til at respektere hinandens respektive beføjelser og kompetencer, således at forpligtelserne i henhold til databeskyttelsesforordningen og formålene med denne forordning overholdes, og den effektive virkning heraf sikres. Det følger heraf, at når en national konkurrencemyndighed som led i en undersøgelse med henblik på konstatering af en virksomheds misbrug af dominerende stilling finder det nødvendigt at undersøge, om denne virksomheds adfærd er lovlig i lyset af databeskyttelsesforordningens bestemmelser, skal nævnte myndighed efterprøve, om denne adfærd eller en tilsvarende adfærd allerede har været genstand for en afgørelse fra den kompetente nationale tilsynsmyndighed, den ledende tilsynsmyndighed eller endda Domstolen. Såfremt dette er tilfældet, kan den nationale konkurrencemyndighed ikke afvige herfra, alt imens den frit kan drage sine egne konklusioner ud fra anvendelsen af konkurrenceretten.

Når den nationale konkurrencemyndighed nærer tvivl om rækkevidden af den vurdering, som den kompetente nationale tilsynsmyndighed eller den ledende tilsynsmyndighed har foretaget, når den pågældende adfærd eller en tilsvarende adfærd samtidig undersøges af disse myndigheder, eller når konkurrencemyndigheden, såfremt de sidstnævnte myndigheder ikke har foretaget en sådan undersøgelse, finder, at en virksomheds adfærd er i strid med databeskyttelsesforordningens bestemmelser, skal denne konkurrencemyndighed høre disse myndigheder og anmode om deres samarbejde for at fjerne tvivlen eller for at afgøre, om der er grundlag for at afvente den pågældende tilsynsmyndigheds vedtagelse af en afgørelse, inden den foretager sin egen vurdering. Såfremt den adspurgte tilsynsmyndighed ikke gør indsigelse eller svarer inden for en rimelig frist, kan konkurrencemyndigheden fortsætte sin egen undersøgelse.

¹²⁷ Fastsat i artikel 4, stk. 3, TEU.

¹²⁸ Som omhandlet i artikel 102 TEUF.



DEN EUROPÆISKE UNIONS
DOMSTOL

Direktoratet for Forskning og Dokumentation

Juli 2024