EUROPEISKA UNIONENS DOMSTOL
DIREKTORATET FÖR FORSKNING OCH DOKUMENTATION

Tematiskt faktablad

SKYDD AV PERSONUPPGIFTER

Rätten till skydd av personuppgifter är en grundläggande rättighet vars iakttagande är ett viktigt mål för Europeiska unionen.

Den har stadfästs i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad stadgan). I artikel 8 i stadgan föreskrivs följande:

”1. Var och en har rätt till skydd av de personuppgifter som rör honom eller henne.

2. Dessa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund. Var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem.

3. En oberoende myndighet ska kontrollera att dessa regler efterlevs.”

Denna grundläggande rättighet är dessutom nära knuten till rätten till respekt för privatlivet och familjelivet, vilken slås fast i artikel 7 i stadgan.

Rätten till skydd av personuppgifter har också stadfästs i artikel 16.1 i fördraget om Europeiska unionens funktionssätt (FEUF), som i detta hänseende har ersatt artikel 286 EG.

Vad gäller sekundärrätten, har Europeiska gemenskapen från mitten av 1990-talet antagit en rad rättsakter för att säkerställa skyddet av personuppgifter. Direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter,[1] som antogs med stöd av artikel 100a EG, utgjorde unionens viktigaste rättsakt på detta område. I direktivet fastställdes allmänna bestämmelser om när personuppgifter fick behandlas och om de berörda personernas rättigheter. I direktivet

[1] Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 1995, s. 31), konsoliderad version den 20 november 2003, upphävd från och med den 25 maj 2018 (se fotnot 5).

föreskrevs bland annat att nationella oberoende tillsynsmyndigheter skulle inrättas i medlemsstaterna.

Direktiv 2002/58/EG[2] har därefter kompletterat direktiv 95/46 genom att harmonisera medlemsstaternas bestämmelser om skyddet av rätten till personlig integritet, vad bland annat gäller behandlingen av personuppgifter inom sektorn för elektronisk kommunikation.[3] Det ska påpekas att unionslagstiftaren har för avsikt att göra en översyn av detta direktiv. Den 10 januari 2017 lade kommissionen fram ett förslag i syfte att ersätta direktivet med en förordning om integritet och elektronisk kommunikation.[4]

Inom området med frihet, säkerhet och rättvisa (tidigare artiklarna 30 och 31 FEU) reglerades (fram till maj 2018) skyddet av personuppgifter på områdena för straffrättsligt samarbete och polissamarbete i rambeslut 2008/977/RIF.[5]

År 2016 ändrade Europeiska unionen den övergripande rättsliga ramen på området. För detta ändamål antogs förordning (EU) 2016/679[6] om dataskydd (nedan kallad dataskyddsförordningen), som ersätter direktiv 95/46 och är direkt tillämplig sedan den 25 maj 2018, samt direktiv (EU) 2016/680[7] om skydd för nämnda uppgifter på straffrättens område, vilket ersätter rambeslut 2008/977/RIF och vilket medlemsstaterna skulle ha införlivat senast den 6 maj 2018.

Vad slutligen gäller skyddet av personuppgifter när gemenskapsinstitutionerna och gemenskapsorganen behandlar sådana uppgifter säkerställdes detta inledningsvis genom förordning (EG) nr 45/2001.[8] Denna förordning har bland annat utgjort grund för inrättandet år 2004 av Europeiska datatillsynsmannen. År 2018 antog Europeiska unionen en ny rättslig ram på området, bland annat genom att anta förordning (EU) 2018/1725,[9] genom vilken förordning nr 45/2001 och beslut nr 1247/2002/EG[10] upphävdes och vilken är tillämplig sedan den 11 december 2018. Den nya förordningen syftar till att i möjligaste mån anpassa reglerna på

---

2 Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 2002, s. 37), konsoliderad version den 19 december 2009.

3 Direktiv 2002/58 har ändrats genom Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG, (EUT L 105, 2006, s. 54). Detta direktiv har ogiltigförklarats av domstolen i dom av den 8 april 2014, Digital Rights Ireland och Seitlinger m.fl. (C-293/12 och C-594/12, EU:C:2014:238) av det skälet att den innebar ett allvarligt åsidosättande av rätten till respekt för privatlivet och av skyddet av personuppgifter (se avsnitt I.1, med rubriken ”Förenligheten av unionens sekundärrätt med rätten till skydd av personuppgifter”, i detta faktablad).

4 Förslag till Europaparlamentets och rådets förordning om respekt för privatlivet och skydd av personuppgifter i samband med elektronisk kommunikation och om upphävande av direktiv 2002/58/EG (förordning om integritet och elektronisk kommunikation), COM/2017/010 final - 2017/03 (COD).

5 Rådets rambeslut 2008/977/RIF av den 27 november 2008 om skydd av personuppgifter som behandlas inom ramen för polissamarbete och straffrättsligt samarbete (EUT L 350, 2008, s. 60), som upphävts från och med den 6 maj 2018 (se fotnot 6).

6 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (EUT L 119, 2016, s. 1)

7 Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 2016, s. 89).

8 Europaparlamentets och rådets förordning (EG) nr 45/2001 av den 18 december 2000 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter (EGT L 8, 2001, s. 1).

9 Europaparlamentets och rådets förordning (EU) 2018/1725 av den 23 oktober 2018 om skydd för fysiska personer med avseende på behandling av personuppgifter som utförs av unionens institutioner, organ och byråer och om det fria flödet av sådana uppgifter samt om upphävande av förordning (EG) nr 45/2001 och beslut nr 1247/2002/EG.

10 Europaparlamentets, rådets och kommissionens beslut nr 1247/2002/EG av den 1 juli 2002 om tjänsteföreskrifter och allmänna villkor för utövande av funktionen som europeisk datatillsynsman (EGT L 183, 2002, s. 1).

området till det system som införts genom dataskyddsförordningen, för att uppnå en konsekvent strategi i fråga om skydd av personuppgifter inom hela unionen.

INNEHÅLLSFÖRTECKNING

I. Den rätt till skydd av personuppgifter som erkänns i Europeiska unionens stadga om de grundläggande rättigheterna

1. Förenligheten av unionens sekundärrätt med rätten till skydd av personuppgifter

Dom av den 9 november 2010 (stora avdelningen), Volker und Markus Schecke och Eifert (C-92/09 och C-93/09, EU:C:2010:662)[11]

De nationella målen rörde tvister mellan jordbrukare och delstaten Hessen, angående offentliggörande på webbplatsen för Bundesanstalt für Landwirtschaft und Ernährung (den federala myndigheten för jordbruks- och livsmedelsfrågor) av personuppgifter rörande jordbrukarna i egenskap av mottagare av medel från Europeiska garantifonden för jordbruket (EGFJ) och Europeiska jordbruksfonden för landsbygdsutveckling (Ejflu). Jordbrukarna motsatte sig detta offentliggörande och gjorde därvid särskilt gällande att det inte var motiverat av ett överordnat allmänintresse. Delstaten Hessen ansåg emellertid att offentliggörandet av dessa uppgifter följde av förordningarna nr 1290/2005[12] och 259/2008[13], vilka reglerar finansieringen av den gemensamma jordbrukspolitiken och kräver offentliggörande av uppgifter som rör fysiska personer som mottar stöd från EGFJ och Ejflu.

Verwaltungsgericht Wiesbaden (Förvaltningsdomstolen i Wiesbaden, Tyskland) ställde mot denna bakgrund flera frågor till domstolen angående giltigheten av vissa bestämmelser i förordning nr 1290/2005 och förordning nr 259/2008, vilka kräver tillhandahållande av sådan information till allmänheten, särskilt via webbplatser som drivs av nationella organ.

Domstolen konstaterade, vad gäller avvägningen mellan den rätt till skydd av personuppgifter som erkänns i stadgan och kravet på öppenhet avseende EU-medel, att offentliggörande på en webbplats av namnen på mottagarna och de belopp som utbetalas till dem, med hänsyn till tredje parters fria tillgång till webbplatsen utgör ett ingrepp i de berörda stödmottagarnas rätt till respekt för privatlivet, i allmänhet, och i rätten till skydd av deras personuppgifter i synnerhet (punkterna 56–64).

För att vara motiverat ska ett sådant ingrepp vara föreskrivet i lag, vara förenligt med det väsentliga innehållet i nämnda rättigheter och, i enlighet med proportionalitetsprincipen, vara nödvändigt och faktiskt svara mot mål av allmänt intresse som erkänns av unionen. Undantag och begränsningar avseende dessa rättigheter måste således inskränkas till vad som är absolut

[11] En redogörelse för domen finns i årsrapporten för år 2010, s. 11.

[12] Rådets förordning (EG) nr 1290/2005 av den 21 juni 2005 om finansiering av den gemensamma jordbrukspolitiken, upphävd genom Europaparlamentets och rådets förordning (EU) nr 1306/2013 av den 17 december 2013 om finansiering, förvaltning och övervakning av den gemensamma jordbrukspolitiken (EUT L 347, 2013, s. 549).

[13] Kommissionens förordning (EG) nr 259/2008 av den 18 mars 2008 om tillämpningsföreskrifter för rådets förordning (EG) nr 1290/2005 när det gäller offentliggörande av uppgifter om stödmottagare från EGFJ och Ejflu (EUT L 76, 2008, s. 28), upphävd genom kommissionens genomförandeförordning (EU) nr 908/2014 av den 6 augusti 2014 om tillämpningsföreskrifter för Europaparlamentets och när det gäller utbetalningsställen och andra organ, finansiell förvaltning, avslutande av räkenskaper, bestämmelser om kontroller, garantier och insyn (EUT L 255, 2014, s. 59).

nödvändigt (punkt 65). I detta sammanhang har domstolen slagit fast att även om skattebetalarna i ett demokratiskt samhälle har rätt att informeras om hur offentliga medel används, kvarstår faktum att rådet och kommissionen var skyldiga att göra en lämplig avvägning mellan de olika intressena, vilket gjorde det nödvändigt att före antagandet av de omtvistade bestämmelserna kontrollera huruvida offentliggörandet av dessa uppgifter på en enda webbplats per medlemsstat inte gick utöver vad som var nödvändigt för att uppnå de berättigade mål som eftersträvas (punkterna 77, 79, 85 och 86).

Domstolen ogiltigförklarade således vissa bestämmelser i förordning nr 1290/2005 och förordning nr 259/2008 i dess helhet, i den del som det enligt denna lagstiftning – med avseende på fysiska personer som tar emot stöd från EGFJ och Ejflu – krävs att det ska offentliggöras personuppgifter beträffande samtliga stödmottagare, utan att det görs någon åtskillnad utifrån relevanta kriterier, såsom de perioder under vilka personerna tog emot stöd samt stödets frekvens, typ eller omfattning (punkt 92 samt punkt 1 i domslutet). Domstolen ansåg emellertid inte att verkningarna av de offentliggöranden av förteckningar över mottagare av stöd som de nationella myndigheterna gjort under den period som föregick dagen för avkunnandet av domen kunde ifrågasättas (punkt 94 samt punkt 2 i domslutet).

Dom av den 17 oktober 2013, Schwarz (C-291/12, EU:C:2013:670)

Michael Schwarz ansökte om pass hos staden Bochum (Tyskland), varvid han samtidigt förklarade att han vägrade lämna sina fingeravtryck i detta sammanhang. Stadt Bochum avslog hans ansökan. Michael Schwarz överklagade beslutet till Verwaltungsgericht Gelsenkirchen (Förvaltningsdomstolen i Gelsenkirchen, Tyskland) och yrkade att kommunen skulle föreläggas att utfärda ett pass till honom utan att registrera hans fingeravtryck. Michael Schwarz bestred vid den domstolen giltigheten av förordning (EG) nr 2252/2004[14] som införde en skyldighet att ta fingeravtryck på personer som ansöker om pass och gjorde bland annat gällande att förordningen var oförenlig med rätten till skydd av personuppgifter och rätten till privatliv.

I detta sammanhang vände sig Verwaltungsgericht Gelsenkirchen till EU-domstolen för att få klarhet i huruvida nämnda förordning, i den mån som den ålägger den som ansöker om pass att lämna fingeravtryck och föreskriver lagring av dem i passet, är giltig, särskilt mot bakgrund av stadgan.

Domstolen besvarade denna fråga jakande med motiveringen att även om de nationella myndigheternas lagring och registrering av fingeravtryck, vilket regleras genom artikel 1.2 i förordning nr 2252/2004, utgör ett ingrepp i rätten till respekt för privatlivet och skydd av personuppgifter, är detta ingrepp motiverat av syftet att förhindra att pass används i bedrägligt syfte.

För det första syftar en sådan begränsning, som föreskrivs i lag, till att uppnå ett mål av allmänintresse som erkänns av unionen, i den mån den är avsedd att bland annat hindra olaglig inresa av personer till unionens territorium (punkterna 35–38). Vidare är tagande och lagring av

14 Rådets förordning (EG) nr 2252/2004 av den 13 december 2004 om standarder för säkerhetsdetaljer och biometriska kännetecken i pass och resehandlingar som utfärdas av medlemsstaterna (EUT L 385, 2004, s. 1) i dess lydelse enligt Europaparlamentets och rådets förordning (EG) nr 444/2009 av den 6 maj 2009 (EUT L 142, 2009, s. 1).

fingeravtryck lämpliga åtgärder för att uppnå detta mål. Även om metoden att kontrollera identiteten med hjälp av fingeravtryck inte är helt tillförlitlig minskar den nämligen i hög grad risken för godtagande av obehöriga personer. Å andra sidan leder emellertid inte bristande samstämmighet mellan passinnehavarens fingeravtryck och uppgifterna i passet till att den berörda personen automatiskt vägras inresa till unionens territorium, utan leder endast till att det utförs en mer grundlig kontroll för att slutgiltigt fastställa personens identitet (punkterna 42–45).

Vad slutligen rör frågan huruvida en sådan behandling är nödvändig har domstolen inte uppmärksammats på några åtgärder som är tillräckligt effektiva, men som skulle innebära ett mindre omfattande intrång i de rättigheter som erkänns i artiklarna 7 och 8 i stadgan än vad som följer av en metod som bygger på att fingeravtryck tas (punkt 53). Artikel 1.2 i förordning nr 2252/2004 medför inte någon behandling av lagrade fingeravtryck som går utöver vad som är nödvändigt för att uppnå nämnda syfte. I förordningen föreskrivs nämligen uttryckligen att fingeravtrycken endast får användas för att kontrollera passets autenticitet och innehavarens identitet. Artikel 1.2 i förordningen innebär dessutom ett skydd mot risken att obehöriga personer tar del av uppgifter som innehåller fingeravtryck och föreskriver att fingeravtryck endast ska lagras i själva passet, som är innehavarens exklusiva egendom (punkterna 54–57, 60 och 63).

Dom av den 8 april 2014 (stora avdelningen), Digital Rights Ireland och Seitlinger m.fl. (förenade målen C-293/12 och C-594/12, EU:C:2014:238)[15]

Denna dom har sitt ursprung i frågor om giltigheten av direktiv 2006/24/EG om lagring av uppgifter, mot bakgrund av den grundläggande rätten till privatliv och skydd av personuppgifter, vilka ställts i nationella förfaranden vid en irländsk och en österrikisk domstol. Mål C-293/12 rörde en tvist vid High Court (Högsta domstolen, Irland) mellan bolaget Digital Rights och irländska myndigheter avseende lagenligheten av nationella åtgärder om lagring av uppgifter avseende elektronisk kommunikation. I mål C-594/12 hade Verfassungsgerichtshof (Författningsdomstolen, Österrike) mottagit flera konstitutionella överklaganden med yrkande om ogiltigförklaring av de nationella bestämmelser som införlivade direktiv 2006/24 med österrikisk rätt.

Genom begäran om förhandsavgörande ställde den irländska och den österrikiska domstolen frågor till EU-domstolen om giltigheten av direktiv 2006/24 mot bakgrund av artiklarna 7, 8 och 11 i stadgan. De hänskjutande domstolarna bad närmare bestämt domstolen att uttala sig om huruvida skyldigheten enligt direktivet för leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät att under en viss tid lagra uppgifter avseende en persons privatliv och vederbörandes kommunikationer och ge nationella behöriga myndigheter tillgång till dessa innebar ett omotiverat ingrepp i dessa grundläggande rättigheter. De berörda typerna av uppgifter är bland annat de som är nödvändiga för att spåra och identifiera en kommunikations källa, för att identifiera slutmålet för en kommunikation, för att identifiera en kommunikations datum, tidpunkt, varaktighet och typ, för att identifiera användarnas kommunikationsutrustning och för att identifiera lokaliseringen av mobil

15 En redogörelse för domen finns i årsrapporten för år 2014, s. 60.

kommunikationsutrustning. Bland dessa uppgifter ingår abonnentens eller den registrerade användarens namn och adress, det uppringande telefonnumret, det uppringda telefonnumret och IP-adressen för internettjänster. Dessa uppgifter gör det i synnerhet möjligt att få kännedom om med vilken person en abonnent eller registrerad användare har kommunicerat och på vilket sätt, hur länge kommunikationen varat och från vilken plats kommunikationen skett. Uppgifterna gör det dessutom möjligt att få kännedom om hur ofta abonnenten eller den registrerade användaren kommunicerat med vissa personer under en viss tidsperiod.

Domstolen slog inledningsvis fast att genom införandet av sådana skyldigheter för dessa leverantörer utgjorde bestämmelserna i direktiv 2006/24 ett synnerligen allvarligt ingrepp i den grundläggande rätten till respekt för privatlivet och skydd av personuppgifter som garanteras i artiklarna 7 och 8 i stadgan. I detta sammanhang fastställde visserligen domstolen att denna inskränkning skulle kunna motiveras av ett mål av allmänt intresse, såsom kampen mot organiserad brottslighet. Domstolen påpekade i detta avseende för det första att den lagring av uppgifter som krävs enligt direktivet inte var av sådant slag att den påverkade det väsentliga innehållet i den grundläggande rätten till privatliv och skyddet för personuppgifter, eftersom det inte var tillåtet att skaffa sig kännedom om själva innehållet i de elektroniska kommunikationerna och det föreskrivs att leverantörer av tjänster eller nätverk måste iaktta vissa principer för skydd av personuppgifter och datasäkerhet. För det andra konstaterade domstolen att lagring av uppgifter för eventuell vidarebefordran till behöriga nationella myndigheter verkligen motsvarade ett mål av allmänt intresse, nämligen kampen mot grov brottslighet och därmed att bidra till den allmänna säkerheten (punkterna 38–44).

Domstolen ansåg emellertid att unionslagstiftaren genom att anta datalagringsdirektivet hade överskridit de begränsningar som följer av iakttagandet av proportionalitetsprincipen. Följaktligen ogiltigförklarade domstolen direktivet med motiveringen att det långtgående och synnerligen allvarliga ingrepp i de grundläggande rättigheterna som direktivet innehöll inte var tillräckligt avgränsat för att se till att detta ingrepp är begränsat till vad som är absolut nödvändigt (punkt 65). Direktiv 2006/24 omfattade nämligen generellt samtliga personer, samtliga elektroniska kommunikationsmedel och samtliga trafikuppgifter utan att det gjordes några åtskillnader, begränsningar eller undantag utifrån syftet att bekämpa allvarliga brott (punkterna 57–59). I direktivet föreskrevs inte något objektivt kriterium för att säkerställa att behöriga nationella myndigheter endast har tillgång till uppgifterna och endast kan använda uppgifterna för att förebygga, upptäcka och lagföra brott som kan anses tillräckligt allvarliga för att motivera ett sådant intrång, materiella och formella villkor för tillträde eller användning. Inte heller föreskrevs några materiella eller processuella villkor för en sådan användning (punkterna 60–62). Vad slutligen beträffar hur länge uppgifterna får lagras ålades i direktivet en period av minst sex månader, utan att det gjordes någon åtskillnad mellan typen av uppgifter utifrån de personer som berördes eller den eventuella nyttan med uppgifterna i förhållande till det eftersträvade målet (punkterna 63 och 64).

När det gäller de krav som följer av artikel 8.3 i stadgan slog domstolen fast att direktiv 2006/24 inte föreskrev tillräckliga garantier för att säkerställa ett effektivt skydd mot missbruk och olaglig tillgång till och användning av uppgifterna och inte heller ett krav på lagring av uppgifter på unionens territorium.

Följaktligen säkerställde inte detta direktiv till fullo att kontrollen av efterlevnaden av kraven avseende skydd och säkerhet utförs av en oberoende myndighet, vilket uttryckligen krävs i stadgan (punkterna 66–68).

2. Iakttagande av rätten till skydd av personuppgifter vid genomförandet av unionsrätten

Dom av den 21 december 2016 (stora avdelningen), Tele2 Sverige (förenade målen C-203/15 och C-698/15, EU:C:2016:970)[16]

Till följd av domen Digital Rights Ireland och Seitlinger m.fl., genom vilken domstolen ogiltigförklarade direktiv 2006/24 (se ovan), anhängiggjordes två mål vid domstolen rörande den allmänna skyldigheten, som föreskrivs i Sverige och Förenade kungariket, för leverantörer av elektroniska kommunikationstjänster att lagra uppgifter rörande dessa kommunikationer, vars lagring krävdes enligt det ogiltigförklarade direktivet.

Dagen efter domen i Digital Rights Ireland och Seitlinger m.fl. anmälde teleoperatören Tele2 Sverige till Post- och telestyrelsen sitt beslut att inte längre lagra uppgifter och sin avsikt att radera uppgifter som redan hade registrerats (mål C-203/15). Svensk lag ålade nämligen leverantörer av elektroniska kommunikationstjänster att systematiskt och kontinuerligt, utan några undantag, lagra alla typer av trafikuppgifter och lokaliseringsuppgifter för alla abonnenter och registrerade användare vid all form av elektronisk kommunikation. I mål C-698/15 hade tre personer väckt talan mot det brittiska system för datalagring som tillät inrikesministern att ålägga offentliga teleoperatörer att lagra alla uppgifter som rör kommunikation under en period om högst tolv månader. Lagring av innehållet i kommunikationen var däremot undantagen.

Kammarrätten i Stockholm och Court of Appeal (England and Wales) (Civil Division) (Appellationsdomstolen för England och Wales, avdelningen för tvistemål och förvaltningsmål, Förenade kungariket), ombad EU-domstolen att uttala sig om tolkningen av artikel 15.1 i direktiv 2002/58 om integritet och elektronisk kommunikation, som gör det möjligt för medlemsstaterna att införa vissa undantag till den skyldighet som anges i nämnda direktiv, att säkerställa konfidentiell behandling av uppgifter inom elektronisk kommunikation och därmed förbundna trafikuppgifter.

I domen slog domstolen fast att artikel 15.1 i direktiv 2002/58, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan utgör hinder för en nationell lagstiftning, som den svenska, vilken i brottsbekämpande syfte föreskriver en generell och odifferentierad lagring av samtliga trafikuppgifter och lokaliseringsuppgifter avseende samtliga abonnenter och registrerade användare och samtliga elektroniska kommunikationsmedel. En sådan nationell lagstiftning överskrider enligt domstolen gränserna för vad som är strängt nödvändigt och kan inte anses motiverad i ett demokratiskt samhälle, såsom krävs enligt artikel 15.1 i direktiv 2002/58 jämförd med ovannämnda artiklar i stadgan (punkterna 99–105, 107 och 112 samt punkt 1 i domslutet).

16 En redogörelse för domen finns i årsrapporten för år 2016, s. 62.

Samma bestämmelse, jämförd med samma artiklar i stadgan utgör även hinder för en nationell lagstiftning som reglerar skydd och säkerhet för trafikuppgifter och lokaliseringsuppgifter och, i synnerhet, behöriga nationella myndigheters tillgång till lagrade uppgifter och som inte – inom ramen för brottsbekämpning – begränsar denna tillgång till enbart åtgärder som syftar till att bekämpa grov brottslighet, inte föreskriver att tillgången ska vara underkastad förhandskontroll av en domstol eller en oberoende förvaltningsmyndighet och inte kräver att uppgifterna ska lagras inom unionen (punkterna 118–122 och 125 samt punkt 2 i domslutet).

Domstolen slog emellertid fast att artikel 15.1 i direktiv 2002/58 inte utgör hinder för en nationell lagstiftning som gör det möjligt att som en preventiv åtgärd, i syfte att bekämpa allvarlig brottslighet, genomföra riktad lagring av sådana uppgifter, förutsatt att den är begränsad till vad som är absolut nödvändigt i fråga om kategorier av uppgifter, de kommunikationsmedel som påverkas, de berörda personerna och den föreskrivna lagringstiden. För att uppfylla dessa krav måste den nationella lagstiftningen för det första föreskriva tydliga och precisa bestämmelser som gör det möjligt att effektivt skydda uppgifterna mot risken för missbruk. Den måste särskilt precisera under vilka omständigheter och villkor en sådan lagringsåtgärd får vidtas i förebyggande syfte, vilket säkerställer att lagringen begränsas till vad som är strängt nödvändigt. Vad för det andra gäller de materiella villkor som en sådan nationell lagstiftning måste uppfylla för att säkerställa att den är begränsad till vad som är strängt nödvändigt, måste lagringen av uppgifterna alltid uppfylla objektiva kriterier, som fastställer ett samband mellan de uppgifter som ska lagras och det eftersträvade syftet. I synnerhet måste villkoren vara sådana att de klart avgränsar åtgärdens omfattning och följaktligen den berörda personkretsen. Vad gäller denna avgränsning ska den nationella lagstiftningen grunda sig på objektiva omständigheter som gör det möjligt att ta sikte på en personkrets vars uppgifter kan avslöja en, åtminstone indirekt, koppling till grov brottslighet, på ett eller annat sätt bidra till att bekämpa grov brottslighet eller förhindra en allvarlig risk för den allmänna säkerheten (punkterna 108–111).

II. Behandling av personuppgifter i den mening som avses i de allmänna bestämmelserna på detta område

1. Behandling av personuppgifter som inte omfattas av tillämpningsområdet för direktiv 95/46

Dom av den 30 maj 2006 (stora avdelningen), parlamentet/rådet (C-317/04 och C-318/04, EU:C:2006:346)

Efter terroristattackerna den 11 september 2001 har Förenta staterna utfärdat lagstiftning med bestämmelser om att lufttrafikföretag med trafik till, inom eller från Förenta staternas territorium är skyldiga att ge amerikanska myndigheter elektronisk tillgång till de uppgifter som återfinns i lufttrafikföretagens system för bokning och kontroll vid avgångar, kallade Passenger Name Records (PNR).

Eftersom kommissionen ansåg att dessa bestämmelser kunde strida mot EU-lagstiftningen och medlemsstaternas lagstiftning om uppgiftsskydd, inledde kommissionen förhandlingar med de

amerikanska myndigheterna. Efter förhandlingarna antog kommissionen den 14 maj 2004 beslut 2004/535/EG[17] i vilket det slogs fast att Förenta staternas tull- och gränsskyddsmyndighet (United States Bureau of Customs and Border Protection, nedan kallad CBP) garanterar en adekvat skyddsnivå för de PNR-uppgifter som överförs från gemenskapen (nedan kallat beslutet om adekvat skydd). Rådet antog därefter den 17 maj 2004 beslut 2004/496/EG[18] om ingående av ett avtal mellan Europeiska gemenskapen och Förenta staterna om behandling och överföring av PNR-uppgifter till CBP som genomförs av lufttrafikföretag som är etablerade i gemenskapens medlemsstater.

Europaparlamentet begärde att domstolen skulle ogiltigförklara de båda ovannämnda besluten och gjorde bland annat gällande att beslutet om adekvat skydd hade antagits utan behörighet *(ultra vires*), att artikel 95 EG (nu artikel 114 FEUF) inte kunde utgöra den korrekta rättsliga grunden för beslutet om godkännande av ingåendet av avtalet, och att det i båda fallen hade skett en kränkning av de grundläggande rättigheterna.

När det gäller beslutet om adekvat skydd prövade domstolen inledningsvis huruvida kommissionen med giltighet kunde anta sitt beslut på grundval av direktiv 95/46/EG. I detta sammanhang konstaterade domstolen att det följde av beslutet om adekvat skydd att överföringen av PNR-uppgifter till CBP utgör en behandling som rör allmän säkerhet och statens verksamhet på straffrättens område. Enligt domstolen är det visserligen riktigt att PNR-uppgifterna initialt insamlades av lufttrafikföretagen inom ramen för en verksamhet som omfattas av unionsrätten, det vill säga försäljning av en flygbiljett som ger rätt till en tjänst. Däremot hade den uppgiftsbehandling som beaktats i beslutet om adekvat skydd en helt annan karaktär. Beslutet om adekvat skydd avsåg nämligen inte en uppgiftsbehandling som är nödvändig för tillhandahållandet av en tjänst, utan en behandling som anses vara nödvändig för att säkerställa allmän säkerhet och för att tillgodose repressiva syften (punkterna 56 och 57).

I detta avseende påpekade domstolen att den omständigheten att PNR-uppgifterna hade samlats in av privata operatörer för kommersiella syften och att det var dessa operatörer som skötte överföringen av uppgifterna till en tredje stat inte utgjorde hinder för att överföringen ansågs som en uppgiftsbehandling som föll utanför direktivets tillämpningsområde. Denna överföring skedde nämligen inom en ram som inrättats av statsmakterna och som avsåg allmän säkerhet. Följaktligen konstaterade domstolen att beslutet om adekvat skydd inte omfattades av direktivet, eftersom det rörde sig om en behandling av personuppgifter som är undantagen från dess tillämpningsområde. Följaktligen ogiltigförklarade domstolen beslutet om adekvat skydd (punkterna 58 och 59).

När det gäller rådets beslut fann domstolen att artikel 95 EG, jämförd med artikel 25 i direktiv 95/46, inte kan ge gemenskapen behörighet att ingå avtalet i fråga med Förenta staterna. Avtalet avsåg nämligen samma överföring av uppgifter som beslutet om adekvat skydd och avser således sådan uppgiftsbehandling som är undantagen från direktivets tillämpningsområde.

17 Kommissionens beslut 2004/535/EG av den 14 maj 2004 om adekvat skydd av personuppgifter som finns i Passenger Name Record för flygpassagerare som överförs till Förenta staternas tull- och gränsskyddsmyndighet (EUT L 235, 2004. s. 11).

18 Rådets beslut 2004/496/EG av den 17 maj 2004 om ingående av ett avtal mellan Europeiska gemenskapen och Amerikas förenta stater om lufttrafikföretags behandling och överföring av passageraruppgifter till Bureau of Customs and Border Protection inom Förenta staternas Department of Homeland Security (EUT L 183, 2004, s. 83 och rättelse i EUT L 255, 2005, s. 168).

Domstolen ogiltigförklarade följaktligen rådets beslut om att godkänna ingåendet av avtalet (punkterna 67–69).

Dom av den 11 december 2014, Ryneš (C-212/13, EU:C:2014:2428)

Som svar på upprepade angrepp hade František Ryneš installerat en övervakningskamera på sitt hus. Efter ytterligare ett angrepp på hans hus hade inspelningar från den kameran gjort det möjligt att identifiera två misstänkta, mot vilka straffrättsliga förfaranden inletts. Lagligheten av behandlingen av de uppgifter som registrerats av övervakningskameran hade ifrågasatts av en av de misstänkta vid den tjeckiska myndigheten för personuppgiftsskydd, vilken slog fast att František Ryneš hade åsidosatt reglerna om skydd av personuppgifter och ålade honom böter.

František Ryneš överklagade ett avgörande från Městský soud v Praze (Stadsdomstolen i Prag, Tjeckien) – genom vilket den domstolen hade fastställt myndighetens beslut – till Nejvyšší správní soud (Högsta förvaltningsdomstolen), vilken frågade EU-domstolen huruvida den registrering som utfördes av František Ryneš, i syfte att skydda sitt liv, sin hälsa och sin egendom utgjorde behandling av uppgifter som inte omfattas av direktiv 95/46, på grund av att registreringen hade utförts av en fysisk person uteslutande för personliga ändamål eller för hemmabruk, i den mening som avses i artikel 3.2 andra strecksatsen i detta direktiv.

Domstolen slog fast att kameraövervakningsutrustning som används för visuell inspelning av människor som lagras kontinuerligt på en hårddisk och som installerats i en bostad för att skydda husägarnas egendom, hälsa och liv – där denna kamerautrustning även övervakar ett område dit allmänheten har tillträde – inte ska anses utgöra behandling av personuppgifter som ett led i verksamhet av rent privat natur eller som har samband med hans hushåll (punkt 35 och domslutet).

I detta hänseende erinrade domstolen om att skyddet av den grundläggande rätten till respekt för privatlivet som stadgas i artikel 7 i stadgan kräver att undantag från och begränsningar av detta skydd ska inskränkas till vad som är strängt nödvändigt. Eftersom bestämmelserna i direktiv 95/46 reglerar behandling av personuppgifter som kan innebära intrång i de grundläggande friheterna och då särskilt i rätten till privatliv, måste bestämmelserna i fråga med nödvändighet tolkas mot bakgrund av de grundläggande rättigheterna i den nämnda stadgan. Undantaget i artikel 3.2 andra strecksatsen i direktivet ska därför tolkas strikt (punkterna 27–29). Dessutom undantar bestämmelsens ordalydelse behandling av personuppgifter som enbart sker som ett led i verksamhet av privat natur eller som har samband med personens hushåll från tillämpningsområdet för direktiv 95/46. I den mån videoövervakning, även delvis, omfattar ett område dit allmänheten har tillträde och därmed går utanför uppgiftshanterarens privata sfär kan denna verksamhet inte anses vara ”av rent privat natur” eller ha ”samband med hans hushåll” i den mening som avses i nämnda bestämmelse (punkterna 30, 31 och 33).

2. Begreppet personuppgifter

Dom av den 19 oktober 2016, Breyer (C-582/14, EU:C:2016:779)[19]

Patrick Breyer väckte talan vid tysk allmän domstol och yrkade att Förbundsrepubliken Tyskland skulle förbjudas att lagra eller låta tredje parter lagra datorbehandlade uppgifter som överförs efter varje besök på webbplatser som drivs av tyska federala myndigheter. I syfte att avvärja attacker och möjliggöra lagföring av ”pirater” registrerade nämligen de tyska federala myndigheternas leverantör av kommunikationstjänster på internet uppgifter bestående av en ”dynamisk” IP-adress – en IP-adress som ändras vid varje ny uppkoppling mot internet – liksom datum och tid för besöket på webbplatsen. Till skillnad från statiska IP-adresser, gjorde de dynamiska IP-adresserna inte det möjligt att skapa en koppling, genom handlingar tillgängliga för allmänheten, mellan en viss dator och den fysiska anslutning till nätverket som internetleverantören använde. De registrerade uppgifterna i sig gjorde det inte möjligt för leverantören av kommunikationstjänster på internet att identifiera användaren. Å andra sidan hade internetleverantören tillgång till ytterligare uppgifter som i kombination med IP-adressen gjorde det möjligt att identifiera användaren.

Mot denna bakgrund beslutade Bundesgerichtshof (Federala högsta domstolen, Tyskland), dit målet överklagats, att fråga EU-domstolen om en IP-adress, som registrerats av en leverantör av kommunikationstjänster på internet i samband med tillgången till dess webbplats, är en personuppgift.

Domstolen påpekade inledningsvis att för att en uppgift ska kunna kvalificeras som ”personuppgift” i den mening som avses i artikel 2 a i direktiv 95/46 krävs det inte att det är en enda person som innehar alla upplysningar som är nödvändiga för att identifiera den berörda personen. Den omständigheten att de ytterligare upplysningar som är nödvändiga för att identifiera en användare av en webbplats inte innehas av leverantören av elektroniska informations- eller kommunikationstjänster, utan av användarens internetleverantör, utesluter således inte att de dynamiska IP-adresser som leverantören av elektroniska informations- eller kommunikationstjänster har registrerat utgör personuppgifter i den mening som avses i artikel 2 a i direktiv 95/46 för denne (punkterna 43 och 44).

Följaktligen slog domstolen fast att en dynamisk IP-adress som en leverantör av elektroniska informations- eller kommunikationstjänster registrerar i samband med att en person besöker en webbplats som nämnda leverantör gör tillgänglig för allmänheten utgör en personuppgift i den mening som avses i artikel 2 a i direktiv 95/46 i förhållande till leverantören, när denne förfogar över lagliga medel som gör det möjligt för vederbörande att identifiera den registrerade med hjälp av de ytterligare upplysningar som den registrerades internetleverantör förfogar över (punkt 49 samt punkt 1 i domslutet).

19 En redogörelse för domen finns i årsrapporten för år 2016, s. 61.

Dom av den 20 december 2017, Nowak (C-434/16, EU:C:2017:994)

Peter Nowak var revisorspraktikant och hade misslyckats på ett prov som anordnats av det irländska institutet för auktoriserade revisorer. Peter Nowak hade med stöd av section 4 i dataskyddslagen gett in en ansökan om tillgång till samtliga personuppgifter som rörde honom, vilka innehades av institutet för auktoriserade revisorer. Institutet lämnade ut vissa dokument till Peter Nowak, men lämnade inte ut hans prov med motiveringen att uppgifterna i provet inte utgjorde personuppgifter rörande honom i den mening som avses i dataskyddslagen.

Eftersom dataskyddskommissionären av samma skäl inte heller hade beviljat hans ansökan om tillgång till handlingar vände sig Peter Nowak till nationell domstol. Supreme Court (Högsta domstolen, Irland), vid vilken Peter Nowak anhängiggjort ett överklagande, ställde frågor till EU-domstolen för att få klarhet i huruvida artikel 2 a i direktiv 95/46 ska tolkas så, att under sådana omständigheter som de som är aktuella i det nationella målet utgör de skriftliga svar som en examinand lämnat på ett prov för yrkesexamen och examinatorns eventuella anteckningar angående nämnda svar personuppgifter rörande examinanden, i den mening som avses i den bestämmelsen.

För det första påpekade domstolen att för att en uppgift ska kunna kvalificeras som ”personuppgift”, i den mening som avses i artikel 2 a i direktiv 95/46, krävs det inte att det är en enda person som innehar alla upplysningar som är nödvändiga för att identifiera den registrerade. Det förhåller sig dessutom så, att i det fallet att examinatorn inte känner till examinandens identitet vid rättningen av de svar som vederbörande har lämnat på ett prov, har den organisation som anordnar provet, i förevarande fall det irländska institutet för auktoriserade revisorer, tillgång till de uppgifter som krävs för att det utan svårighet eller tvivel ska vara möjligt att identifiera examinanden utifrån personens identifieringsnummer, vilket är angivet på provet eller på provets omslag, och sålunda knyta svaren till examinanden.

För det andra slog domstolen fast att de skriftliga svar som en kandidat till en yrkesexamen lämnar utgör upplysningar som avser honom. Svarens innehåll avspeglar nämligen examinandens kunskapsnivå och kompetens inom ett visst område samt, i förekommande fall, vederbörandes tankeprocesser, omdöme och förmåga till kritiskt tänkande. Syftet med insamlandet av nämnda svar är dessutom att utvärdera examinandens yrkeskvalifikationer och lämplighet att utöva det aktuella yrket. Användningen av dessa upplysningar, vilken bland annat tar sig uttryck i examinandens godkända eller icke godkända resultat på det aktuella provet, är vidare ägnad att påverka personens rättigheter och intressen, eftersom den kan avgöra eller inverka på vederbörandes möjligheter att få tillträde till det önskade yrket eller den önskade anställningen. Konstaterandet att de skriftliga svar som lämnas av en examinand på ett prov för en yrkesexamen utgör upplysningar som på grund av sitt innehåll, syfte eller verkan avser personen i fråga gäller för övrigt även i samma utsträckning när det är fråga om ett så kallat open book-prov (punkterna 31 och 36–40).

När det för det tredje gäller examinatorns anteckningar avseende examinandens svar, slog domstolen fast att de, liksom svaren som sökanden lämnat vid provet, utgör upplysningar rörande examinanden, eftersom de återger examinatorns uppfattning eller bedömning av examinandens individuella prestationer vid provet, och i synnerhet av dennes kunskaper och färdigheter inom det berörda området. Dessutom har dessa anteckningar just till syfte att

dokumentera examinatorns bedömning av examinandens prestationer och är ägnade att ha verkningar för den personen (punkterna 42 och 43).

För det fjärde slog domstolen fast att de skriftliga svar som en examinand lämnat på ett prov för yrkesexamen och examinatorns eventuella anteckningar angående svaren således kan vara föremål för en kontroll, bland annat av deras riktighet och behovet av att de lagras, i den mening som avses i artikel 6.1 d och e i direktiv 95/46, och kan vara föremål för rättelse eller utplåning enligt artikel 12 b i samma direktiv. Det faktum att examinanden med stöd av artikel 12 a i direktivet ges rätt till tillgång till svaren och anteckningarna tjänar den målsättning med direktivet som består i att garantera skyddet för examinandens privatliv med avseende på behandlingen av hans eller hennes personuppgifter, oberoende av huruvida examinanden även har en sådan rätt till tillgång enligt den nationella lagstiftning som är tillämplig på provförfarandet. Domstolen konstaterar för det första att rätten till tillgång respektive att erhålla rättelse i artikel 12 a respektive b i direktiv 95/46 inte omfattar frågorna i provet, vilka i sig inte utgör personuppgifter avseende examinanden (punkterna 56 och 58).

Mot denna bakgrund slog domstolen fast att under sådana omständigheter som de som är aktuella i det nationella målet utgör de skriftliga svar som en examinand lämnat på ett prov för yrkesexamen och examinatorns eventuella anteckningar angående dessa svar personuppgifter, i den mening som avses i artikel 2 a i direktiv 95/46 (punkt 62 samt punkt 1 i domslutet).

3. Begreppet ”behandling av personuppgifter”

Dom av den 6 november 2003 (stora avdelningen), Lindqvist (C-101/01, EU:C:2003:596)

Bodil Lindqvist var frivilligarbetare i en församling inom Svenska kyrkan och hade på sin hemdator skapat webbplatser och där publicerat personuppgifter rörande flera personer som, i likhet med henne, arbetade på frivillig basis inom församlingen. Bodil Lindqvist förpliktades att betala böter på grund av att hon hade använt sig av personuppgifter inom ramen för en automatiserad behandling utan att dessförinnan göra en skriftlig anmälan till Datainspektionen, vilka hon utan tillstånd hade överfört till tredjeländer, och på grund av att hon hade behandlat känsliga personuppgifter.

Bodil Lindqvist överklagade detta beslut till Göta hovrätt (Sverige), vilken hänsköt frågor till EU-domstolen för att särskilt få klarhet i huruvida Bodil Lindqvist hade genomfört en ”behandling av personuppgifter som helt eller delvis företas på automatisk väg”, i den mening som avses i direktiv 95/46.

Domstolen slog fast att omnämnandet av olika personer – vilka identifieras med namn eller på annat sätt, till exempel med telefonnummer eller med uppgifter om deras arbetsförhållanden och fritidsintressen – på en webbsida utgör en ”behandling av personuppgifter som helt eller delvis företas på automatisk väg”, i den mening som avses detta direktiv (punkt 27 samt punkt 1 i domslutet). En sådan behandling av personuppgifter som genomförs vid utövandet av ideell eller religiös verksamhet omfattas nämligen inte av något av undantagen från direktivets tillämpningsområde, eftersom den inte ingår i den kategori av verksamhet som rör allmän säkerhet eller i den kategori som uteslutande är av rent privat natur eller som har samband med

hans hushåll, vilka faller utanför direktivets tillämpningsområde (punkterna 38 och 43–48 samt punkt 2 i domslutet).

Dom av den 13 maj 2014 (stora avdelningen), Google Spain och Google (C-131/12, EU:C:2014:317)

År 2010 lämnade en spansk medborgare in ett klagomål vid Agencia Española de Protección de Datos (den spanska dataskyddsmyndigheten (AEPD) mot La Vanguardia Ediciones SL, som ger ut en dagstidning med stor spridning i Spanien, och mot Google Spain och Google. Denna person gjorde gällande att när en Internetanvändare sökte på dennes namn i Googles sökmotor visades, i förteckningen över sökresultat, länkar till två sidor från dagstidningen La Vanguardia, daterade 1998, där det bland annat tillkännagavs en försäljning av fast egendom på offentlig auktion till följd av en utmätning för återbetalning av denna persons skulder. Genom klagomålet begärde vederbörande att La Vanguardia skulle förpliktas att antingen ta bort eller ändra dessa sidor eller att använda vissa verktyg som gjorts tillgängliga av sökmotorerna för att skydda uppgifterna. Personen begärde också att Google Spain eller Google skulle föreläggas att ta bort eller dölja personuppgifterna så att de inte längre skulle ingå bland sökresultaten och i länkarna till La Vanguardia.

AEPD avslog det klagomål som riktats mot La Vanguardia med motiveringen att informationen i fråga hade offentliggjorts i laga ordning av utgivaren, men biföll klagomålet när det gäller Google Spain och Google och förelade dessa två bolag att vidta nödvändiga åtgärder för att avlägsna uppgifterna från sina index och göra det omöjligt att i framtiden få tillgång till dem. Efter att bolagen överklagat beslutet till Audiencia Nacional (Nationella domstolen, Spanien) i syfte att AEPD:s beslut skulle ogiltigförklaras ställde den spanska domstolen en rad frågor till EU-domstolen.

Domstolen hade således tillfälle att klargöra begreppet ”behandling av personuppgifter” på internet i enlighet med direktiv 95/46.

Domstolen slog fast att en sökmotors verksamhet – som består i att lokalisera information som har publicerats eller lagts ut på internet av tredje män, indexera den på automatisk väg, lagra den tillfälligt och slutligen ställa den till förfogande för internetanvändare enligt en viss prioriteringsordning – ska anses utgöra behandling av personuppgifter när informationen innehåller personuppgifter (punkt 1 i domslutet). Domstolen erinrade dessutom om att de transaktioner som omfattas av direktivet ska anses utgöra behandling även om åtgärderna endast avser information som redan publicerats i media. Ett generellt undantag från tillämpningen av direktivet i ett sådant fall skulle innebära att detta till stor del förlorade sin verkan (punkterna 29 och 30).

Dom av den 10 juli 2018 (stora avdelningen), Jehovan todistajat (C-25/17, EU:C:2018:551)[20]

Den finska dataskyddsmyndigheten antog ett beslut som förbjöd samfundet Jehovas vittnen att samla in eller behandla personuppgifter inom ramen för medlemmarnas predikoarbete genom

[20] En redogörelse för domen finns i årsrapporten för år 2018, s. 87 och 88.

dörrknackning om inte de rättsliga villkoren för behandling av sådana uppgifter i den finska lagstiftningen hade iakttagits. Medlemmar av detta samfund insamlar nämligen, i samband med sitt predikoarbete genom dörrknackning, uppgifter om personer som de har mött och som inte är kända för dem eller för detta samfund. Uppgifterna har formen av minnesanteckningar och samlas in för att kunna återfinnas vid ett eventuellt senare besök, utan att de berörda personerna samtyckt därtill eller informeras därom. Härvidlag har samfundet Jehovas vittnen fastställt riktlinjer om hur man bör göra sådana anteckningar. Dessa riktlinjer har publicerats i åtminstone en av samfundets tidskrifter rörande predikoarbete.

Domstolen fann att den insamling av personuppgifter som medlemmarna i ett religiöst samfund ägnar sig åt inom ramen för sitt predikoarbete genom dörrknackning och senare behandling av dessa uppgifter inte omfattas av undantaget i tillämpningsområdet för direktiv 95/46, eftersom den varken utgör behandling av personuppgifter som genomförs som ett led i sådan verksamhet som avses i artikel 3.2 första strecksatsen i detta direktiv, eller behandling av personuppgifter som utförs av en fysisk person som ett led i verksamhet av rent privat natur eller som har samband med dennes hushåll, i den mening som avses i artikel 3.2 andra strecksatsen i nämnda direktiv (punkt 51 samt punkt 1 i domslutet).

Dom av den 14 februari 2019, Buivids (C-345/17, EU:C:2019:122)

Domstolen tolkade i detta mål dels tillämpningsområdet för direktiv 95/46, dels begreppet ”behandling av personuppgifter som sker uteslutande för journalistiska ändamål” i artikel 9 i detta direktiv.

Denna dom meddelades efter det att Lettlands högsta domstol begärt förhandsavgörande i ett mål mellan Sergejs Buivids (nedan kallad klaganden) och den lettiska myndigheten Datainspektionen angående den förstnämndes överklagande av denna myndighets beslut i vilket denna funnit att klaganden hade brutit mot den nationella lagstiftningen om skydd av personuppgifter genom att på en webbplats offentliggöra ett videoklipp som han själv spelat in då han i den nationella polisens lokaler till poliser lämnade en redogörelse i ett ärende rörande administrativa sanktionsåtgärder. Efter det att hans överklagande hade avslagits i två lägre domstolar, lämnade klaganden in ett överklagande till Högsta domstolen. Han åberopade i den domstolen sin rätt till yttrandefrihet och gjorde gällande att det aktuella videoklippet visade medlemmar ur den nationella polisstyrkan, vilka är offentliga tjänstemän, i en för allmänheten tillgänglig lokal och att bestämmelserna i lagen om skydd av personuppgifter därför inte var tillämpliga på dessa personer.

Vad för det första gäller tillämpningsområdet för direktiv 95/46 konstaterade domstolen dels att bilderna av de poliser som spelats in i det aktuella videoklippet utgör personuppgifter, dels att videoinspelningen av dessa personer, lagrad på minneskortet i den av klaganden använda kameran, utgör behandling av personuppgifter. Domstolen tillade att offentliggörandet av en videoinspelning på vilken förekommer personuppgifter, på en webbplats för videoklipp där användarna kan titta på och dela dessa, utgör en behandling av dessa uppgifter som helt eller delvis företas på automatisk väg. Domstolen framhöll vidare att nämnda inspelning och dess offentliggörande inte omfattas av de föreskrivna undantagen från tillämpningsområdet för direktiv 95/46, avseende bland annat behandling av personuppgifter inom ramen för verksamhet som inte omfattas av detta direktivs tillämpningsområde och behandling som ett led

i verksamhet av rent privat natur eller i samband med en persons hushåll. Domstolen fann följaktligen att en inspelning av ett videoklipp som visar poliser på en polisstation i samband med att en person lämnar en redogörelse i ett ärende, samt offentliggörande av videoklippet på en webbplats för videoklipp där användarna kan ladda upp, titta på och dela dessa, omfattas av direktivets tillämpningsområde (punkterna 31, 32, 35, 39, 42 och 43 samt punkt 1 i domslutet).

Vad för det andra gäller innebörden av begreppet ”behandling av personuppgifter uteslutande för journalistiska ändamål” erinrade domstolen först om att uttrycket ”journalistiska ändamål” ska ges en vid tolkning på så sätt att de undantag och avvikelser som föreskrivs i artikel 9 i direktiv 95/46 är tillämpliga på alla personer som är journalistiskt verksamma. Domstolen ansåg i enlighet härmed att den omständigheten att klaganden inte är journalist till yrket inte utesluter att inspelningen av det aktuella videoklippet och offentliggörandet av detsamma kan anses utgöra ”behandling av personuppgifter uteslutande för journalistiska ändamål”. Domstolen betonade vidare att de undantag och avvikelser som föreskrivs i artikel 9 i direktiv 95/46 endast ska tillämpas i den mån de visar sig vara nödvändiga för att förena två grundläggande rättigheter, nämligen skyddet för privatlivet och yttrandefriheten. Domstolen preciserade i detta sammanhang att det inte kan uteslutas att inspelningen och offentliggörandet av det aktuella videoklippet – som skett utan att de poliser som figurerar i videoklippet underrättats om inspelningen och om vilka syften som inspelningen har – utgör ett ingrepp i den grundläggande rättigheten till skydd för privatlivet för dessa personer. Domstolen fann följaktligen att inspelningen av det aktuella videoklippet och offentliggörandet av detta på en webbplats för videoklipp – kan utgöra behandling av personuppgifter uteslutande för journalistiska ändamål, såvitt det framgår av videoklippet att det enda syftet med att spela in och offentliggöra videoklippet varit att sprida information, åsikter eller idéer till allmänheten, vilket det ankommer på den hänskjutande domstolen att pröva (punkterna 51, 52, 55, 63 och 67 samt punkt 2 i domslutet).

Dom av den 22 juni 2021 (stora avdelningen), Latvijas Republikas Saeima (Prickning) (C-439/19, EU:C:2021:504)

Den fysiska personen B prickades för en eller flera överträdelser av trafikregler. Ceļu satiksmes drošības direkcija (styrelsen för säkerhet i vägtrafiken, Lettland) (nedan kallad trafiksäkerhetsstyrelsen) förde in information om prickningen i det nationella fordons- och förarregistret.

Enligt den lettiska vägtrafiklagstiftningen[21] ska registrets information om prickning av förare vid överträdelser av trafikregler vara tillgänglig för allmänheten och lämnas ut av trafiksäkerhetsstyrelsen till den som begär det, utan att den som begär ut informationen behöver visa att vederbörande har ett särskilt intresse av att få tillgång till dessa uppgifter, vilket även gäller ekonomiska aktörer som begär ut information för vidareutnyttjande. B ifrågasatte om denna lagstiftning var rättsenlig. Han väckte därför talan vid Latvijas Republikas Satversmes tiesa (Författningsdomstolen, Lettland) och yrkade att det skulle fastställas huruvida lagstiftningen var förenlig med rätten till respekt för privatlivet.

[21] Artikel 14[1].2 i Ceļu satiksmes likums (vägtrafiklagen) av den 1 oktober 1997 (Latvijas Vēstnesis, 1997, nr 274/276).

Författningsdomstolen fann att den vid bedömningen av denna grundlagsskyddade rättighet var skyldig att ta hänsyn till dataskyddsförordningen. Den begärde sålunda att EU-domstolen skulle klargöra innebörden av ett antal bestämmelser i dataskyddsförordningen i syfte att fastställa huruvida den lettiska vägtrafiklagstiftningen var förenlig med nämnda förordning.

EU-domstolen (stora avdelningen) slog i sin dom fast att behandling av personuppgifter avseende prickning vid överträdelser av trafikregler utgör en ”behandling av personuppgifter som rör fällande domar i brottmål samt lagöverträdelser som innefattar brott”,[22] som enligt dataskyddsförordningen ska ges ett utökat skydd på grund av att det rör sig om särskilt känsliga uppgifter (punkterna 10, 46, 74 och 94 samt punkt 1 i domslutet).

EU-domstolen konstaterade, i detta sammanhang, inledningsvis att informationen om prickning vid överträdelser av trafikregler utgör personuppgifter och att trafiksäkerhetsstyrelsens utlämnande av dessa till utomstående utgör en behandling som ingår i dataskyddsförordningens materiella tillämpningsområde. Detta tillämpningsområde är nämligen mycket vittgående och nämnda behandling är inte hänförlig till något av undantagen från förordningens tillämplighet (punkterna 60, 61 och 72).

För det första omfattas behandlingen inte av det undantag som innebär att dataskyddsförordningen inte är tillämplig på en behandling som utförs som ett led i en verksamhet som inte omfattas av unionsrätten.[23] Det undantaget ska anses ha som enda syfte att från förordningens tillämpningsområde utesluta behandling av personuppgifter som utförs av statliga myndigheter som ett led i verksamhet som syftar till att upprätthålla nationell säkerhet eller en verksamhet som kan placeras i samma kategori. Denna verksamhet omfattar bland annat verksamhet som syftar till att skydda statens grundfunktioner och samhällets grundläggande intressen. Verksamhet som rör vägtrafiksäkerhet bedrivs emellertid inte i detta syfte och kan följaktligen inte placeras i kategorin verksamhet som syftar till att upprätthålla nationell säkerhet (punkterna 62 och 66–68).

För det andra utgör utlämnandet av personuppgifter om prickning vid överträdelser av trafikregler inte heller en sådan behandling som omfattas av det undantag som innebär att dataskyddsförordningen inte är tillämplig på behandling av personuppgifter som utförs av de behöriga myndigheterna inom det straffrättsliga området.[24] Domstolen konstaterade nämligen att trafiksäkerhetsstyrelsen inte kan betraktas som en sådan ”behörig myndighet”[25] när den lämnar ut den aktuella informationen (punkterna 69–71).

Vid fastställandet av huruvida utlämnandet av personuppgifter om överträdelser av trafikregler, såsom information om prickning, utgör en behandling av personuppgifter avseende ”lagöverträdelser som innefattar brott”,[26] för vilka ett utökat skydd gäller, konstaterade domstolen – bland annat med stöd av tillkomsthistorien vid antagandet av

---

22 Artikel 10 i dataskyddsförordningen.
23 Artikel 2.2 a i dataskyddsförordningen.
24 Artikel 2.2 d i dataskyddsförordningen.
25 Artikel 3.7 i Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 2016, s. 89).
26 Artikel 10 i dataskyddsförordningen.

dataskyddsförordningen – att detta begrepp uteslutande hänför sig till brott. Den omständigheten att överträdelser av trafikregler i den lettiska rättsordningen kvalificeras som förvaltningsrättsliga överträdelser är dock inte avgörande för bedömningen av huruvida överträdelser av trafikregler omfattas av begreppet ”brott”, eftersom det rör sig om ett självständigt unionsrättsligt begrepp som ska ges en självständig och enhetlig tolkning inom hela unionen. Efter det att domstolen erinrat om de tre relevanta kriterierna för att fastställa huruvida en överträdelse är straffrättslig till sin karaktär – nämligen den rättsliga kvalificeringen av överträdelsen enligt nationell rätt, överträdelsens art och strängheten i den sanktion som åläggs – slog den fast att de överträdelser av trafikreglerna som var aktuella i målet omfattades av begreppet ”lagöverträdelser som innefattar brott” i den mening som avses i dataskyddsförordningen. När det gäller de två första kriterierna konstaterade domstolen att även om överträdelserna inte kvalificeras som ”straffrättsliga” enligt nationell rätt kan en sådan karaktär följa av överträdelsens art och framför allt av det repressiva syftet med den sanktion som överträdelsen kan medföra. I det aktuella fallet hade prickningen av den som bryter mot trafikregler, precis som de andra sanktioner som detta kunde leda till, bland annat ett repressivt syfte. Vad gäller det tredje kriteriet påpekade domstolen att prickning endast sker för de överträdelser av trafikreglerna som är av en viss allvarlighetsgrad och att sådana överträdelser följaktligen kan leda till sanktioner av en viss stränghetsgrad. Dessutom är prickning i allmänhet något som tillkommer utöver den sanktion som påförs, och kumuleringen av dessa prickar får rättsliga följder som till och med kan innebära körförbud (punkterna 77, 80, 85, 87–90 och 93).

4. Begreppet ”register med personuppgifter”

Dom av den 10 juli 2018 (stora avdelningen), Jehovan todistajat (C-25/17, EU:C:2018:551)

Domstolen preciserade i denna dom (se även avsnitt II.3, med rubriken ”Begreppet ’behandling av personuppgifter’”) begreppet register i artikel 2 c i direktiv 95/46.

Domstolen erinrade först om att detta direktiv endast är tillämpligt på manuell behandling av personuppgifter om de uppgifter som behandlas ingår i eller kommer att ingå i ett register. Den slog därefter fast att detta begrepp omfattar en samling av personuppgifter som samlats in inom ramen för predikoarbete genom dörrknackning, som innefattar namn, adress och ytterligare information om de besökta personerna, när dessa uppgifter är strukturerade efter bestämda kriterier på ett sådant sätt att uppgifterna i praktiken med lätthet kan tas fram för senare användning. För att omfattas av detta begrepp behöver en sådan samling av uppgifter inte innehålla register, särskilda förteckningar eller andra arrangemang för sökning (punkt 62 samt punkt 2 i domslutet).

5. Begreppet personuppgiftsansvarig

Dom av den 10 juli 2018 (stora avdelningen), Jehovan todistajat (C-25/17, EU:C:2018:551)

Domstolen prövade i denna dom (se även avsnitt II.3, med rubriken ”Begreppet ’behandling av personuppgifter’” och avsnitt II.4, med rubriken ”Begreppet ’register med personuppgifter’”) ett religiöst samfunds ansvar för behandling av personuppgifter som sker inom ramen för

predikoarbete genom dörrknackning som organiseras, samordnas och uppmuntras av detta samfund.

Domstolen ansåg att den skyldighet som åligger var och en att följa unionsrättens bestämmelser om skydd av personuppgifter inte kan anses utgöra ett intrång i de organisatoriska befogenheterna för nämnda religiösa samfund. Den slog i detta sammanhang fast att artikel 2 d i direktiv 95/46, jämförd med artikel 10.1 i stadgan, ska tolkas så, att ett religiöst samfund, tillsammans med dess medlemmar som ägnar sig åt predikoarbete, kan anses ansvarigt för behandlingen av personuppgifter som samlats in av dessa medlemmar inom ramen för predikoarbete genom dörrknackning, vilket organiseras, samordnas och uppmuntras av detta samfund, och att det härför inte krävs att nämnda samfund har tillgång till dessa uppgifter eller att det har fastställts att samfundet gett sina medlemmar skriftliga riktlinjer eller instruktioner avseende sådan behandling (punkterna 74 och 75 samt punkt 3 i domslutet).

Dom av den 5 juni 2018 (stora avdelningen), Wirtschaftsakademie Schleswig Holstein (C-210/16, EU:C:2018:388)[27]

Den tyska dataskyddsmyndigheten hade i sin egenskap av tillsynsmyndighet, i den mening som avses i artikel 28 i direktiv 95/46, ålagt ett bolag som var specialiserat på utbildning och som erbjöd utbildning genom en fanpage på det sociala nätverket Facebook att avaktivera sin fanpage. Enligt denna myndighet informerade nämligen varken detta bolag eller Facebook besökarna på denna fanpage om att denna sida samlade in personuppgifter om besökarna med hjälp av kakor, eller om att de därefter behandlade dessa uppgifter.

Domstolen preciserade i detta sammanhang begreppet ”personuppgiftsansvarig”. Domstolen ansåg att administratören av en fanpage på Facebook, såsom det bolag som var aktuellt i det nationella målet, genom sin konfiguration, särskilt mot bakgrund av dess målgrupp och syften avseende administrationen eller marknadsföringen av dess verksamhet, medverkar till att fastställa ändamålen och medlen för behandlingen av personuppgifter från besökarna på nämnda fanpage. På grund av detta ska denna administratör enligt domstolen betraktas som personuppgiftsansvarig i unionen, tillsammans med Facebook Ireland, med avseende på denna behandling, i den mening som avses i artikel 2 d i direktiv 95/46 (punkt 39).

Dom av den 29 juli 2019, Fashion ID (C-40/17, EU:C:2019:629)

Domstolen hade i detta mål tillfälle att utveckla begreppet ”personuppgiftsansvarig” med avseende på integreringen av ett insticksprogram på en webbsida.

Fashion ID, ett företag som säljer modekläder på nätet, hade på sin webbplats integrerat det sociala insticksprogrammet ”Gilla” från det sociala nätverket Facebook. Integreringen förefaller ha fått till följd att när en besökare är inne på Fashion ID:s webbplats översänds personuppgifter rörande honom eller henne till Facebook Ireland. Det verkar som om denna överföring görs

[27] En redogörelse för domen finns i årsrapporten för år 2018, s. 86 och 87.

utan besökarens vetskap och oavsett om han eller hon är medlem i det sociala nätverket Facebook eller har klickat på Facebooks ”Gilla”–knapp.

Verbraucherzentrale NRW, en allmännyttig konsumentskyddsorganisation, gjorde gällande att Fashion ID hade översänt sina webbplatsbesökares personuppgifter till Facebook Ireland, dels utan deras samtycke, dels i strid med informationsplikten som följer av bestämmelserna om skydd av personuppgifter. Oberlandesgericht Düsseldorf (Düsseldorfs regionala överdomstol, Tyskland), vid vilken tvisten var anhängig, begärde att EU-domstolen skulle tolka flera olika bestämmelser i direktiv 95/46 .

Domstolen konstaterade först att en sådan webbplatsoperatör som Fashion ID kan anses vara en sådan personuppgiftsansvarig person som avses i artikel 2 d i direktiv 95/46. Detta ansvar är dock begränsat till den behandling eller den gemensamma behandling av personuppgifter som den faktiskt bestämmer ändamålen och medlen för, nämligen insamlingen och utlämnandet genom översändande av personuppgifterna i fråga. Det framstod däremot, enligt domstolen, vid första anblicken som uteslutet att Fashion ID fastställer ändamålen och medlen för de senare åtgärder avseende behandling av personuppgifter som utförs av Facebook Ireland efter det att uppgifterna har utlämnats till den senare, varför Fashion ID inte kunde anses vara ansvarig för dessa åtgärder i den mening som avses i artikel 2 d (punkterna 76 och 85 samt punkt 2 i domslutet).

Domstolen framhöll vidare att både webbplatsoperatören och det företag som tillhandahåller det sociala insticksprogrammet, såsom Facebook Ireland, ska ha ett berättigat intresse av att utföra behandlingarna i den mening som avses i artikel 7 f i direktiv 95/46, för att dessa behandlingar ska vara tillåtna (punkt 97 samt punkt 3 i domslutet).

Domstolen preciserade slutligen att det samtycke som enligt artiklarna 2 h och 7 a i direktiv 95/46 ska inhämtas av webbplatsoperatören enbart omfattar den behandling av personuppgifter som webbplatsoperatören faktiskt bestämmer ändamålen och medlen för. Den informationsplikt som föreskrivs i artikel 10 i detta direktiv åligger i en sådan situation även den nämnda webbplatsoperatören, varvid de uppgifter som webbplatsoperatören ska ge till den registrerade enbart omfattar den behandling eller den gemensamma behandling av personuppgifter som operatören faktiskt bestämmer ändamålen och medlen för (punkt 106 samt punkt 4 i domslutet).

Dom av den 9 juli 2020, Land Hessen, C-272/19, EU:C:2020:535)

En medborgare som gjort en framställning till utskottet för framställningar vid delstaten Hessens lantdag (Tyskland) begärde hos detta utskott att få tillgång till de personuppgifter som rörde honom, vilka utskottet registrerat i samband med behandlingen av hans framställning. Till stöd för sin begäran åberopade medborgaren dataskyddsförordningen, i vilken det föreskrivs att en berörd person har rätt att från den personuppgiftsansvarige få tillgång till de personuppgifter som rör honom eller henne.

Talmannen i delstaten Hessens lantdag avslog denna begäran med motiveringen att förfarandet för framställningar är ett parlamentariskt uppdrag och att detta parlament inte omfattas av tillämpningsområdet för dataskyddsförordningen.

Den aktuella medborgaren överklagade beslutet till Verwaltungsgericht Wiesbaden (Förvaltningsdomstolen i Wiesbaden, Tyskland) som konstaterade att tysk rätt inte gav någon rätt till tillgång till personuppgifter inom ramen för en sådan framställning som den aktuella. En rätt till tillgång till sådana uppgifter skulle emellertid kunna följa av dataskyddsförordningen, varför Verwaltungsgericht Wiesbaden (Förvaltningsdomstolen i Wiesbaden) ställde frågor till EU-domstolen härom. Den hänskjutande domstolen var dessutom osäker på huruvida den uppfyllde kraven på oavhängighet och således huruvida den skulle anses vara en domstol som har rätt att hänskjuta tolkningsfrågor till EU-domstolen, och ställde därför frågor till EU-domstolen på denna punkt.

Domstolen svarade i sin dom att eftersom ett framställningsutskott vid ett delstatsparlament i en medlemsstat ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter, ska detta utskott anses som ”personuppgiftsansvarig” i den mening som avses i dataskyddsförordningen.[28] Detta utskotts behandling av personuppgifter omfattas således av denna förordning, bland annat av den bestämmelse som ger de berörda personerna en rätt att få tillgång till de personuppgifter som rör dem. [29]

Domstolen konstaterade bland annat att verksamheten i delstaten Hesses framställningsutskott inte omfattas av något undantag i dataskyddsförordningen. Den medgav att denna verksamhet är av offentlig karaktär och är specifik för denna delstat, då utskottet indirekt bidrar till den parlamentariska verksamheten, men påpekade att denna verksamhet även den är av både politisk och administrativ art. Det framgick vidare inte av de uppgifter som domstolen hade tillgång till att denna verksamhet i förevarande fall motsvarade något av de undantag som föreskrivs i dataskyddsförordningen (punkterna 71–74 samt domslutet).

6. Villkor som ska vara uppfyllda för att behandling av personuppgifter ska vara tillåten

Dom av den 16 december 2008 (stora avdelningen), Huber (C-524/06, EU:C:2008:724)[30]

Den federala myndigheten för migration och flyktingar (Bundesamt für Migration und Flüchtlinge, Tyskland) driver ett centralt register över utlänningar som sammanför vissa personuppgifter avseende utlänningar som vistas i Tyskland för en period som är längre än tre månader. Registret används för statistiska ändamål och av säkerhetstjänsten och polisen samt av domstolarna när de utövar sina befogenheter att inleda utredningar och efterforskningar med avseende på kriminella gärningar eller gärningar som äventyrar den allmänna säkerheten.

Heinz Huber är österrikisk medborgare och flyttade till Tyskland 1996 för att arbeta som oberoende försäkringsagent. Heinz Huber anser att behandlingen av uppgifterna om honom i registret i fråga är diskriminerande, eftersom det inte finns någon sådan databas över tyska medborgare, och begärde därför att de aktuella uppgifterna skulle strykas ur registret.

28 Artikel 4 led 7 i dataskyddsförordningen.
29 Artikel 15 i dataskyddsförordningen.
30 En redogörelse för domen finns i årsrapporten för år 2008, s. 45.

Mot denna bakgrund beslutade Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Högsta förvaltningsdomstolen i delstaten Nordrhein-Westfalen, Tyskland), vid vilken målet anhängiggjorts, att fråga EU-domstolen huruvida den behandling av personuppgifter som hade gjorts i registret i fråga var förenlig med unionsrätten.

Domstolen erinrade inledningsvis om att en unionsmedborgares uppehållsrätt i en medlemsstat där han inte är medborgare inte är ovillkorlig, utan kan vara föremål för begränsningar. Användningen av ett sådant register i syfte att utgöra stöd för de myndigheter som ansvarar för tillämpningen av bestämmelserna om uppehållsrätt är således i princip tillåten och, med beaktande av registrets natur, förenlig med förbudet mot diskriminering på grund av nationalitet som stadgas i artikel 12.1 EG (numera artikel 18 första stycket FEUF). Ett sådant register får emellertid endast innehålla uppgifter som är nödvändiga för detta ändamål i den mening som avses i direktivet om skydd av personuppgifter (punkterna 54, 58 och 59).

När det gäller frågan huruvida behandlingen är nödvändig i den mening som avses i artikel 7 e i direktiv 95/46 erinrade domstolen inledningsvis om att det rör sig om ett självständigt unionsrättsligt begrepp som ska tolkas på ett sätt som fullt ut svarar mot syftet med direktiv 95/46 såsom detta slagits fast i artikel 1.1 i direktivet. Domstolen konstaterade därefter att ett system för behandling av personuppgifter är förenligt med unionsrätten om det endast innehåller uppgifter som är nödvändiga för nämnda myndigheters tillämpning av denna lagstiftning och om dess centraliserade karaktär möjliggör en mer effektiv tillämpning av denna lagstiftning med avseende på uppehållsrätten för unionsmedborgare som inte är medborgare i den berörda medlemsstaten.

Lagring och behandling av personuppgifter avseende identifierade personer i ett sådant register för statistiska ändamål kan under inga omständigheter anses vara nödvändig i den mening som avses i artikel 7 e i direktiv 95/46 (punkterna 52, 66 och 68).

När det gäller frågan om användningen av uppgifterna i registret, för ändamål som rör brottsbekämpning noterade domstolen särskilt att detta syfte avser beivrande av brott och överträdelser oberoende av gärningsmännens nationalitet. Av detta följer att en medlemsstat, med avseende på syftet att bekämpa kriminalitet, inte får särbehandla sina egna medborgare i förhållande till unionsmedborgare som inte är medborgare i medlemsstaten men som uppehåller sig på dess territorium. Skillnaden i behandling av de egna medborgarna jämfört med unionsmedborgare som följer av att endast personuppgifter avseende unionsmedborgare som inte är medborgare i den berörda medlemsstaten behandlas systematiskt i syfte att bekämpa kriminalitet utgör därmed diskriminering vilken är förbjuden enligt artikel 12.1 EG (punkterna 78–80).

Dom av den 24 november 2011, ASNEF och FECEMD (C-468/10 och C-469/10, EU:C:2011:777)

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) och Federación de Comercio Electrónico y Marketing Directo (FECEMD) hade väckt förvaltningsrättslig talan vid Tribunal Supremo (Högsta domstolen, Spanien) mot flera olika artiklar i kungligt dekret 1720/2007, som innehöll tillämpningsbestämmelser för den organiska lagen 15/1999 som införlivade direktiv 95/46.

ASNEF och FECEMD gjorde särskilt gällande att det i spansk rätt, för att personuppgifter ska få behandlas utan den registrerades samtycke, föreskrivs ytterligare ett villkor som inte återfinns i direktiv 95/46, nämligen att uppgifterna ska finnas i ”källor tillgängliga för allmänheten”, vilka anges i artikel 3 j i den organiska lagen 15/1999. De gjorde i detta sammanhang gällande att denna lag och kungligt dekret 1720/2007 begränsade tillämpningsområdet för artikel 7 f i direktiv 95/46 som för att personuppgifter ska få behandlas utan den registrerades samtycke föreskriver ett villkor som endast rör det berättigade intresse som eftersträvas av den personuppgiftsansvarige eller av den eller de tredje män till vilka uppgifterna har lämnats ut.

I detta hänseende påpekade domstolen inledningsvis att artikel 7 i direktiv 95/46 innehåller en uttömmande uppräkning av de situationer där en behandling av personuppgifter kan anses vara tillåten utan den registrerades samtycke. Medlemsstaterna får följaktligen inte, med stöd av artikel 5 i direktivet, införa ytterligare principer för tillåtligheten av behandlingen av personuppgifter utöver dem som nämns i artikel 7 i direktivet eller föreskriva ytterligare villkor som påverkar räckvidden av de principer som föreskrivs i artikel 7. Artikel 5 tillåter nämligen endast medlemsstaterna att, inom de begränsningar som bestämmelserna i kapitel II i direktivet innebär, och således artikel 7, precisera på vilka villkor behandling av personuppgifter är tillåten (punkterna 30, 32 och 33).

Medlemsstaterna får särskilt föreskriva vägledande principer för den nödvändiga avvägning mellan de motstående rättigheterna och intressena som ska göras enligt artikel 7 f i direktivet. De får även beakta det faktum att allvaret i kränkningen av den registrerades grundläggande rättigheter som nämnda behandling innebär kan variera beroende på om uppgifterna i fråga redan finns i källor tillgängliga för allmänheten (punkterna 44 och 46).

Domstolen slog emellertid fast att om en nationell lagstiftning, för vissa kategorier av personuppgifter, utesluter behandling genom att för dessa kategorier ange det slutliga resultatet av en avvägning mellan de motstående rättigheterna och intressena, utan att tillåta ett annat resultat med anledning av de särskilda omständigheterna i ett enskilt fall, rör det sig inte om en precision i den mening som avses i artikel 5 i direktiv 95/46. Följaktligen slog domstolen fast att artikel 7 f i direktiv 95/46 utgör hinder för att en medlemsstat kategoriskt och generellt utesluter möjligheten att behandla vissa typer av personuppgifter, utan att tillåta en avvägning mellan de motstående rättigheterna och intressena i det enskilda fallet (punkterna 47 och 48).

Dom av den 19 oktober 2016, Breyer (C-582/14, EU:C:2016:779)

I denna dom (se även avsnitt II.2, med rubriken ”Begreppet personuppgifter”) uttalade sig domstolen också om frågan huruvida artikel 7 f i direktiv 95/46 utgör hinder för en nationell bestämmelse enligt vilken en leverantör av elektroniska informations- eller kommunikationstjänster endast får samla in och använda personuppgifter avseende en användare utan dennes samtycke i den mån det krävs för att möjliggöra och fakturera den aktuella användarens konkreta användning av tjänsten, och enligt vilken syftet att säkerställa den elektroniska informations- eller kommunikationstjänstens allmänna funktion inte kan rättfärdiga en användning av dessa uppgifter efter det att den aktuella sessionen har avslutats.

Domstolen slog fast att artikel 7 f i direktiv 95/46 utgör hinder för lagstiftningen i fråga. Enligt denna bestämmelse är behandling av personuppgifter i den mening som avses i denna

bestämmelse tillåten om det är nödvändigt för ändamål som rör berättigade intressen hos den personuppgiftsansvarige eller hos den eller de tredje män till vilka uppgifterna har lämnats ut, utom när sådana intressen uppvägs av den registrerades intressen eller dennes grundläggande fri- och rättigheter. I detta fall hade nämligen den tyska lagstiftningen kategoriskt och generellt uteslutit möjligheten att behandla vissa typer av personuppgifter, utan att tillåta en avvägning mellan de motstående rättigheterna och intressena i det enskilda fallet. Därigenom hade den tyska lagstiftaren olagligen minskat räckvidden av denna princip som föreskrivs i artikel 7 f i direktiv 95/46 genom att utesluta att målet att säkerställa elektroniska informations- eller kommunikationstjänsters allmänna kapacitet kan vägas mot användarnas grundläggande fri- och rättigheter (punkterna 62–64 samt punkt 2 i domslutet).

Dom av den 4 maj 2017, Rīgas satiksme (C-13/16, EU:C:2017:336)

Denna fråga har uppkommit i en tvist mellan den nationella polismyndigheten och Rīgas satiksme, vilket är ett trådbussbolag i staden Riga (Lettland), rörande en begäran om utlämnande av uppgifter om den som gjort sig skyldig till en olycka. Vid en trafikolycka hade en taxichaufför stannat sin bil vid vägkanten. Passageraren i baksätet på taxin öppnade taxibilens dörr samtidigt som en trådbuss tillhörande Rīgas satiksme passerade taxibilen. Dörren slog i och skadade trådbussen. I syfte att väcka en civilrättslig talan bad Rīgas satiksme bland annat den nationella polisen om uppgifter som identifierade den person som vållat olyckan. Polisen vägrade att lämna ut passagerarens identifikationsnummer och adress och handlingar rörande förklaringar av de personer som var inblandade i olyckan på grund av att handlingar i akten i ett administrativt förfarande endast får lämnas till parterna i detta förfarande, och, vad gäller identifikationsnummer och adress, lagen om skydd av personuppgifter förbjuder tillhandahållande av sådana uppgifter avseende enskilda.

Mot denna bakgrund beslutade Augstākās tiesas Administratīvo lietu departaments (Högsta domstolen, avdelningen för förvaltningsrätt, Lettland) att vilandeförklara målet och fråga domstolen huruvida artikel 7 f i direktiv 95/46 ska tolkas så, att den innebär en skyldighet att lämna ut personuppgifter till tredje man i syfte att göra det möjligt för vederbörande att väcka skadeståndstalan vid allmän domstol med anledning av en skada som orsakats av den person vars personuppgifter är skyddade, och huruvida det faktum att nämnda person är minderårig kan ha betydelse för tolkningen av bestämmelsen.

Domstolen slog fast att artikel 7 f i direktiv 95/46 ska tolkas så, att den inte innebär en skyldighet att lämna ut personuppgifter till tredje man i syfte att göra det möjligt för vederbörande att väcka skadeståndstalan vid allmän domstol i anledning av en skada som orsakats av den person vars personuppgifter är skyddade. Denna bestämmelse utgör emellertid inte hinder för ett sådant utlämnande, för det fall att det skulle ske med stöd av nationell rätt och med iakttagande av de villkor som föreskrivs i den bestämmelsen (punkterna 27 och 34 samt domslutet).

I detta sammanhang påpekade domstolen att det – med förbehåll för den nationella domstolens kontroll i detta avseende – inte, under sådana omständigheter som de som är aktuella i det nationella målet, förefaller vara motiverat att med hänvisning till att den person som orsakat skadan är minderårig vägra att till en part som lidit skada lämna ut personuppgifter som är nödvändiga för att väcka skadeståndstalan mot nämnda person eller, i förekommande fall, mot vederbörandes vårdnadshavare (punkt 33).

Dom av den 27 september 2017, Puškár (C-73/16, EU:C:2017:725)

I målet vid den nationella domstolen hade Peter Puškár väckt talan vid Najvyšší súd Slovenskej republiky (Republiken Slovakiens högsta domstol) och yrkat att Finančné riaditel'stvo (finansdirektoratet) och alla skattekontor underordnade Kriminálny úrad finančnej správy (kontoret för bekämpning av ekonomisk brottslighet) skulle förpliktas att inte föra upp hans namn på förteckningen över personer som av finansdirektoratet betraktas som bulvaner, vilken upprättats av finansdirektoratet i samband med skatteuppbörd och som uppdateras av finansdirektoratet och de skattekontor som arbetar med bekämpning av ekonomisk brottslighet (nedan kallad den omtvistade förteckningen). Sökanden begärde dessutom att alla uppgifter rörande honom skulle strykas från dessa förteckningar och från finansförvaltningens it-system.

Mot denna bakgrund beslutade Najvyšší súd Slovenskej republiky (Republiken Slovakiens högsta domstol) att till domstolen bland annat ställa frågan huruvida rätten till respekt för privatliv och familjeliv, bostad och kommunikationer enligt artikel 7 och rätten till skydd av personuppgifter enligt artikel 8 i stadgan kunde tolkas så, att en medlemsstat inte utan den berörda personens samtycke får upprätta förteckningar med personuppgifter som ska användas i samband med uppbörd av skatt, med den följden att en offentlig myndighets insamling av personuppgifter i syfte att förhindra skatteundandragande i sig utgör en risk.

Domstolen slog fast att artikel 7 e i direktiv 95/46 ska tolkas på så sätt att den inte utgör hinder för att myndigheterna i en medlemsstat behandlar personuppgifter för att använda dem i samband med uppbörd av skatt och bekämpning av skatteundandragande, på det sätt som skett genom upprättandet av den omtvistade förteckningen i det nationella målet, utan samtycke av de berörda personerna, under vissa förutsättningar. En första förutsättning är att dessa myndigheter genom nationell lagstiftning anförtrotts arbetsuppgifter av allmänt intresse i den mening som avses i denna bestämmelse, att åtgärden att upprätta denna förteckning och att på denna uppföra namnen på de berörda personerna faktiskt är ägnad att och nödvändig för att uppnå de eftersträvade målen och att det finns tillräckliga skäl för att anta att de berörda personerna på goda grunder förekommer i denna förteckning. En andra förutsättning är att samtliga de villkor för att denna behandling av personuppgifter ska vara laglig som uppställs i direktiv 95/46 är uppfyllda (punkt 117 samt punkt 3 i domslutet).

I detta hänseende påpekade domstolen att det ankommer på den hänskjutande domstolen att bedöma om upprättandet av den omtvistade förteckningen är nödvändigt för att kunna utföra de uppgifter av allmänt intresse som är aktuella i det nationella målet, med beaktande bland annat av det exakta syftet med att upprätta den omtvistade förteckningen, de rättsliga verkningar den medför för de personer som förekommer i förteckningen och huruvida förteckningen är offentlig eller inte. Med beaktande av proportionalitetsprincipen ankommer det även på den hänskjutande domstolen att pröva om åtgärden att upprätta den omtvistade förteckningen och att på denna uppföra namnet på de berörda personerna är ägnad att uppfylla de ändamål för vilka detta gjorts och om det inte är möjligt att uppnå dessa ändamål genom mindre ingripande åtgärder (punkterna 111–113).

Domstolen konstaterade dessutom att det förhållandet att en person är uppförd på den omtvistade förteckningen kan inkräkta på vissa av hans eller hennes rättigheter. Att föras upp på denna förteckning kan nämligen skada personens anseende och påverka hans eller hennes relationer med skattemyndigheterna. Att förekomma i förteckningen kan även påverka

presumtionen för denna persons oskuld, som föreskrivs i artikel 48.1 i stadgan, och näringsfriheten enligt artikel 16 i stadgan för de juridiska personer som förbinds med de fysiska personer som uppförts på den omtvistade förteckningen. Ett sådant ingrepp kan således bara vara rimligt om det finns tillräckliga skäl att misstänka att den berörda personen på ett fiktivt sätt innehar ledningsfunktioner inom de juridiska personer som vederbörande sätts i samband med och således påverkar skatteuppbörden och bekämpningen av skatteundandragande negativt (punkt 114).

Domstolen slog dessutom fast att om det finns skäl för att, enligt artikel 13 i direktiv 95/46, begränsa vissa av de rättigheter som föreskrivs i artiklarna 6 och 10–12 i detsamma, såsom den berörda personens rätt till information, ska en sådan begränsning vara nödvändig för att säkerställa ett intresse som anges i artikel 13.1, såsom bland annat ett viktigt ekonomiskt eller finansiellt intresse inom skatteområdet, och vara grundad på lag (punkt 116).

Dom av den 11 november 2020, Orange România (C-61/19, EU:C:2020:901)

Orange România SA tillhandahåller tjänster för mobil telekommunikation på den rumänska marknaden. Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (Nationella tillsynsmyndigheten för behandling av personuppgifter, Rumänien) (nedan kallad ANSPDCP) beslutade den 28 mars 2018 att påföra Orange România böter för att ha samlat in och lagrat kopior av sina kunders identitetshandlingar utan att ha inhämtat ett uttryckligt samtycke från kunderna.

Enligt ANSPDCP hade Orange România under perioden från den 1 till den 26 mars 2018 ingått avtal om tillhandahållande av tjänster för mobil telekommunikation vilka innehöll en klausul om att kunderna fått information om och samtyckte till att en kopia av deras identitetshandlingar samlades in och lagrades för identifieringsändamål. Rutan avseende denna klausul kryssades i av den personuppgiftsansvarige innan avtalet undertecknades.

Mot denna bakgrund beslutade Tribunalul București (Förstainstansdomstolen i Bukarest) att be EU-domstolen att precisera vilka villkor som måste vara uppfyllda för att kunderna ska anses ha lämnat ett giltigt samtycke till behandlingen av personuppgifterna.

EU-domstolen erinrade först om att det i unionsrätten[31] finns en förteckning över de fall då en behandling av personuppgifter kan anses vara laglig. Det krävs närmare bestämt att den berörda personen har avgett en frivillig, specifik, informerad och otvetydig viljeyttring.[32] Giltigt samtycke föreligger inte i fall av tystnad, på förhand ikryssade rutor eller inaktivitet (punkterna 34, 36, 37 och 39).

Om den registrerades samtycke lämnas i en skriftlig förklaring som också rör andra frågor, gäller dessutom att denna förklaring ska läggas fram i en begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. För att ge den berörda personen genuin eller fri valmöjlighet får avtalsvillkoren inte vilseleda de registrerade om möjligheten att ingå avtalet även

[31] Artikel 7 i direktiv 95/46 och artikel 6 i dataskyddsförordningen.
[32] Artikel 2 h i direktiv 95/46 och artikel 4 led 11 i dataskyddsförordningen.

om vederbörande vägrar att samtycka till behandling av sina personuppgifter (punkterna 34, 36, 37, 39 och 41).

Domstolen preciserade att Orange România, såsom personuppgiftsansvarig, måste kunna visa att behandlingen av personuppgifterna är laglig, och följaktligen att det finns ett giltigt samtycke från dess kunder. Eftersom de berörda kunderna inte själva verkade ha kryssat i rutan avseende insamlingen och lagringen av en kopia av deras identitetshandlingar kunde inte enbart det förhållandet att rutan kryssats i anses styrka att dessa kunder genom en bekräftande viljeyttring lämnat sitt samtycke. Det ankom på den hänskjutande domstolen att göra nödvändiga kontroller i detta avseende (punkterna 42 och 46).

Enligt EU-domstolen ålåg det även den hänskjutande domstolen att bedöma huruvida de aktuella avtalsvillkoren kunde vilseleda den registrerade om möjligheten att ingå avtalet även för det fall vederbörande skulle vägra att samtycka till behandlingen av sina personuppgifter, i avsaknad av preciseringar om denna möjlighet. EU-domstolen konstaterade vidare att Orange România, om en kund vägrade att lämna sitt samtycke till behandling av uppgifter om honom eller henne, krävde att kunden skriftligen angav att han eller hon inte samtyckte till vare sig insamling eller lagring av en kopia av vederbörandes identitetshandling. Enligt domstolen påverkar ett sådant ytterligare krav nämligen på ett otillbörligt sätt möjligheten att fritt motsätta sig sådan insamling och lagring. Det ålåg under alla omständigheter det nämnda bolaget att styrka att dess kunder – genom ett aktivt agerande – uppenbart har gett uttryck för sitt samtycke till behandling av deras personuppgifter, och bolaget kunde inte kräva att kunderna aktivt gav uttryck för sin vägran (punkterna 49–51).

Domstolen fann följaktligen att ett avtal om tillhandahållande av telekommunikationstjänster som innehåller en klausul enligt vilken den berörda personen har informerats om och samtyckt till insamling och lagring av en kopia av sin identitetshandling för att vederbörande ska kunna identifieras, inte är av sådan art att det styrker att personen i fråga lämnat ett giltigt samtycke till denna insamling och denna lagring, när den ruta som avser denna klausul kryssats i av den personuppgiftsansvarige innan avtalet undertecknades, när villkoren i detta avtal kan vilseleda den registrerade om möjligheten att ingå avtalet även om han eller hon vägrar att ge sitt samtycke till behandling av sina personuppgifter, eller när den personuppgiftsansvarige på ett otillbörligt sätt påverkar möjligheten att fritt motsätta sig sådan insamling och lagring genom att kräva att den berörda personen, för att vägra att ge sitt samtycke till denna behandling, fyller i ytterligare ett formulär för att ge uttryck för denna vägran (punkt 52 och domslutet).

Dom av den 12 maj 2021 (stora avdelningen), Bundesrepublik Deutschland (Rött meddelande från Interpol) (C-505/19, EU:C:2021:376)

År 2012 offentliggjorde Internationella kriminalpolisorganisationen (nedan kallad Interpol), på begäran av Förenta staterna och på grundval av en arresteringsorder som utfärdats av myndigheterna i det landet, ett rött meddelande avseende WS, en tysk medborgare, i syfte att eventuellt utlämna honom till Förenta staterna. När en person som är föremål för ett sådant meddelande lokaliseras i en stat som är medlem av Interpol ska staten i princip besluta om tillfälligt omhändertagande av den eftersökta personen eller övervakning eller begränsning av hans eller hennes rörelsefrihet.

Enligt den hänskjutande domstolen hade en utredning mot WS avseende samma gärningar som de som detta röda meddelande grundades på emellertid inletts i Tyskland redan innan meddelandet offentliggjordes. Det förfarandet avslutades genom ett lagakraftägande beslut år 2010 efter det att WS hade betalat ett visst penningbelopp, i enlighet med ett särskilt förfarande för uppgörelse som tillämpas i tysk straffrätt. Därefter informerade Bundeskriminalamt (den federala kriminalpolisen, Tyskland) Interpol om att den ansåg att principen *ne bis in idem*, på grund av detta tidigare förfarande, var tillämplig i förevarande fall. Denna princip, som stadgas såväl i artikel 54 i konventionen om tillämpning av Schengenavtalet[33] som i artikel 50 i stadgan, innebär bland annat förbud mot att en person beträffande vilken fråga om ansvar redan har prövats genom lagakraftägande avgörande åtalas på nytt för samma brott.

År 2017 väckte WS talan vid Verwaltungsgericht Wiesbaden (Förvaltningsdomstolen i Wiesbaden, Tyskland) mot Förbundsrepubliken Tyskland. WS yrkade att denna medlemsstat skulle föreläggas att vidta nödvändiga åtgärder för att utverka att det röda meddelandet drogs tillbaka. WS gjorde i detta avseende gällande, förutom att principen *ne bis in idem* hade åsidosatts, att hans rätt till fri rörlighet, som garanteras i artikel 21 FEUF, hade åsidosatts, eftersom han inte kunde bege sig till en stat som var part i Schengenavtalet eller till en medlemsstat utan att riskera att gripas. Han ansåg även att behandlingen av hans personuppgifter, som finns i det röda meddelandet, på grund av dessa åsidosättanden stred mot direktiv 2016/680 om skydd av personuppgifter på det straffrättsliga området.[34]

Det var mot denna bakgrund som Tribunal administratif de Wiesbaden (Förvaltningsdomstolen i Wiesbaden) beslutade att ställa frågor till EU-domstolen om tillämpningen av principen *ne bis in idem*, närmare bestämt möjligheten att tillfälligt omhänderta en person som avses med ett rött meddelande i en sådan situation som var aktuell i det målet. För det fall denna princip var tillämplig önskade den hänskjutande domstolen dessutom få klarhet i vilka konsekvenser det får för medlemsstaternas behandling av de personuppgifter som ingår i ett sådant meddelande.

Domstolen (stora avdelningen) slog i sin dom bland annat fast att bestämmelserna i direktiv 2016/680, jämförda med artikel 54 i tillämpningskonventionen och artikel 50 i stadgan, ska tolkas på så sätt att de inte utgör hinder för behandling av personuppgifter som finns i ett rött meddelande som utfärdats av Interpol, så länge det inte har fastställts, genom ett rättsligt avgörande, att principen *ne bis in idem* är tillämplig med avseende på den gärning som detta meddelande grundas på. Detta förutsätter att en sådan behandling uppfyller de villkor som föreskrivs i detta direktiv (punkt 121 samt punkt 2 i domslutet).

Vad gäller frågan om de personuppgifter som finns i ett rött meddelande från Interpol konstaterade domstolen att varje åtgärd som vidtas med dessa uppgifter, såsom att de införs i en medlemsstats dataregister, utgör en ”behandling” som omfattas av direktiv 2016/680.[35] Domstolen ansåg vidare dels att man med denna behandling eftersträvar ett berättigat ändamål, dels att behandlingen inte kan anses olaglig av det enda skälet att *principen ne bis in*

---

33 Konventionen om tillämpning av Schengenavtalet av den 14 juni 1985 mellan regeringarna i Beneluxstaterna, Förbundsrepubliken Tyskland och Franska republiken om gradvis avskaffande av kontroller vid de gemensamma gränserna (EGT L 239, 2000, s. 19) (nedan kallad tillämpningskonventionen),

34 Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 2016, s. 89).

35 Se artikel 2.1 och artikel 3.2 i direktiv 2016/680.

idem skulle kunna vara tillämplig med avseende på den gärning som det röda meddelandet grundas på.[36] En sådan behandling, som medlemsstaternas myndigheter utför, kan för övrigt visa sig vara nödvändig för att kontrollera om nämnda princip är tillämplig (punkterna 111, 114, 116, 117 och 119).

Under dessa omständigheter fann domstolen att direktiv 2016/680, jämfört med artikel 54 i tillämpningskonventionen och artikel 50 i stadgan, inte utgör hinder för behandling av personuppgifter som finns i ett rött meddelande, så länge det inte har fastställts genom ett lagakraftägande rättsligt avgörande att principen *ne bis in idem* är tillämplig i det aktuella fallet. En sådan behandling ska emellertid uppfylla de villkor som föreskrivs i detta direktiv. Behandlingen måste därför bland annat vara nödvändig för att utföra en uppgift som utförs av en behörig nationell myndighet i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder[37] (punkt 121 samt punkt 2 i domslutet).

Om principen *ne bis in idem* är tillämplig, är det däremot inte längre nödvändigt att införa personuppgifter som finns i ett rött meddelande från Interpol i medlemsstaternas dataregister, eftersom den aktuella personen inte längre kan bli föremål för ett straffrättsligt förfarande för den gärning som omfattas av nämnda meddelande och därmed inte längre kan gripas för samma gärning. Av detta följer att den registrerade måste kunna begära att hans eller hennes uppgifter raderas. Om registreringen av dessa uppgifter upprätthålls ska den emellertid åtföljas av en upplysning om att den aktuella personen inte längre kan åtalas i en medlemsstat eller i en avtalsslutande stat för samma gärning på grund av principen *ne bis in idem* (punkt 120).

Dom av den 22 juni 2021 (stora avdelningen), Latvijas Republikas Saeima (Prickning) (C-439/19, EU:C:2021:504)

Domstolen slog i denna dom (se även avsnittet II.3 med rubriken ”Begreppet ’behandling av personuppgifter’”) fast att dataskyddsförordningen utgör hinder för den lettiska lagstiftning som gör det obligatoriskt för Ceļu satiksmes drošības direkcija (Trafiksäkerhetsmyndigheten, Lettland) (nedan kallad trafiksäkerhetsmyndigheten) att tillhandahålla allmänheten information om prickning av förare vid överträdelser av trafikregler, utan att den som begär ut informationen behöver visa att vederbörande har ett särskilt intresse av att få tillgång till dessa uppgifter. Domstolen konstaterade vidare att det inte var styrkt att det var nödvändigt – bland annat med hänsyn till det av den lettiska regeringen åberopade målet att förbättra trafiksäkerheten – att lämna ut personuppgifter om prickning vid överträdelser av trafikregler till allmänheten. Vidare fann domstolen att varken allmänhetens rätt att ta del av allmänna handlingar eller rätten till informationsfrihet motiverade en sådan lagstiftning (punkterna 113 och 120–122 samt punkt 2 i domslutet).

Domstolen framhöll i detta sammanhang att den förbättrade trafiksäkerhet som eftersträvades genom den lettiska lagstiftningen var ett mål av allmänintresse som erkänns av unionen och att medlemsstaterna således kan beteckna trafiksäkerheten som en ”uppgift av allmänt intresse”.[38]

---

[36] Se artikel 4.1 b och artikel 8.1 i direktiv 2016/680.
[37] Se artikel 1.1 och artikel 8.1 i direktiv 2016/680.
[38] Enligt artikel 6.1 e i dataskyddsförordningen är behandlingen av personuppgifter laglig om den är ”nödvändig för att fullgöra en uppgift av allmänt intresse”.

Det var dock inte styrkt att de lettiska reglerna om utlämnande av personuppgifter om prickning vid överträdelser av trafikregler var nödvändiga för att det eftersträvade målet skulle uppnås. För det första förfogade den lettiska lagstiftaren nämligen över många olika handlingsmöjligheter som skulle ha gjort det möjligt att uppnå detta mål genom andra medel som i mindre utsträckning inskränker de berörda personernas grundläggande rättigheter. För det andra skulle hänsyn tas till hur känsliga uppgifterna om prickning är och till det faktum att utlämnandet av dessa till allmänheten kan utgöra ett allvarligt ingrepp i rätten till respekt för privatlivet och rätten till skydd för personuppgifter, eftersom det kan leda till avståndstagande från samhällets sida och medföra en stigmatisering av den berörda personen (se punkterna 109–113).

Dessutom fann domstolen att det, med beaktande av hur känsliga dessa uppgifter är och av hur allvarligt ingreppet i dessa två grundläggande rättigheter är, ska anses att dessa rättigheter väger tyngre än såväl allmänhetens intresse av att få tillgång till allmänna handlingar – såsom det nationella fordons- och förarregistret – som rätten till informationsfrihet (punkterna 120 och 121).

För det tredje, och av samma skäl, fann domstolen att dataskyddsförordningen även utgjorde hinder för den lettiska lagstiftningen i den mån denna tillät trafiksäkerhetsmyndigheten att lämna ut information om prickning av förare vid överträdelser av trafikregler till ekonomiska aktörer för att dessa skulle kunna vidareutnyttja uppgifterna och lämna ut dem till allmänheten (punkt 126 samt punkt 3 i domslutet).

Slutligen preciserade domstolen att principen om unionsrättens företräde utgjorde hinder för att den hänskjutande domstolen, som hade att pröva ett mål där invändningar hade riktats mot lettisk lagstiftning som av EU-domstolen bedömts vara oförenlig med unionsrätten, beslutade att verkningarna av denna lagstiftning skulle bestå till dess att den hänskjutande domstolen slutligt avgjorde målet (punkt 137 samt punkt 4 i domslutet).

III. Behandling av personuppgifter i den mening som avses i direktiv 2002/58

Dom av den 2 oktober 2018 (stora avdelningen), Ministerio Fiscal (C-207/16, EU:C:2018:788)[39]

Det nationella målet handlade om en spansk undersökningsdomstols avslag av en ansökan som ingetts inom ramen för en utredning av ett rån av en plånbok och en mobiltelefon. Närmare bestämt hade polisen begärt att domstolen avseende en period på tolv dagar räknat från dagen för rånet skulle bevilja polisen tillgång till identifikationsuppgifter om användare av telefonnummer som aktiverats från den stulna mobiltelefonen. Denna begäran avslogs med motiveringen att omständigheterna i brottsutredningen inte utgjorde ett ”allvarligt” brott – det vill säga, enligt spansk lag ett brott som kan bestraffas med fängelse i mer än fem år – eftersom tillgång till identifikationsuppgifter endast är möjlig för denna typ av brott.

39 En redogörelse för domen finns i årsrapporten för år 2018, s. 88 och 89.

Domstolen konstaterade att myndigheters tillgång, inom ramen för en brottsutredning, till personuppgifter som lagrats av leverantörer av elektroniska kommunikationstjänster omfattas av tillämpningsområdet för direktiv 2002/58. Därefter erinrade domstolen om att myndigheters tillgång till identitetsuppgifter för innehavare av SIM-kort som aktiverats med en stulen mobiltelefon, såsom för- och efternamn och eventuellt adress, utgör ett ingrepp i dessa personers grundläggande rättigheter enligt stadgan till respekt för privatlivet och till skydd av personuppgifter, även i avsaknad av omständigheter som kan kvalificera detta ingrepp som ”allvarligt” och oavsett om upplysningarna om de berördas privatliv är av känslig art och om de berörda har fått utstå olägenheter på grund av ingreppet. Emellertid betonade domstolen att detta ingrepp inte var så allvarligt att denna tillgång i samband med förebyggande, utredning, upptäckt och lagföring av brott måste begränsas till kampen mot allvarlig brottslighet. Direktiv 2002/58 innehåller en uttömmande lista på syften som kan motivera nationella bestämmelser om myndigheters tillgång till de aktuella uppgifterna och därmed göra undantag från principen om konfidentialitet vid elektronisk kommunikation. Tillgången till sådana uppgifter måste därför vara faktiskt och strikt begränsad till de fall då tillgång krävs för ett av dessa syften. Domstolen påpekade emellertid att vad gäller syftet att förebygga brott begränsar ordalydelsen i direktiv 2002/58 inte detta syfte till kampen mot allvarlig brottslighet, utan hänvisar till ”brott” i allmänhet (punkterna 38, 42 och 59–63 samt domslutet).

Härvidlag förtydligade domstolen att även om den i domen Tele2 Sverige och Watson m.fl.[40] slog fast att endast kampen mot allvarlig brottslighet kan motivera att myndigheterna får tillgång till personuppgifter som lagras av leverantörer av kommunikationstjänster, uppgifter som sammantagna kan göra det möjligt att dra mycket precisa slutsatser om privatlivet för de personer vilkas uppgifter har lagrats, var denna tolkning motiverad av att syftet med en lagstiftning som reglerar denna tillgång måste stå i proportion till hur allvarligt ingrepp i de grundläggande rättigheterna i fråga åtgärden innebär. I enlighet med proportionalitetsprincipen kan ett allvarligt ingrepp i samband med förebyggande, utredning, upptäckt och lagföring av brott således endast motiveras av syftet att bekämpa brottslighet, vilken då också måste kvalificeras som ”allvarlig”. När det ingrepp som en sådan tillgång innebär däremot inte är allvarligt, kan det emellertid motiveras av syftet att förebygga, utreda, upptäcka och lagföra ”brott” i allmänhet (punkterna 54–57).

I det aktuella fallet fann domstolen att tillgång till endast de uppgifter som avses med begäran i fråga inte kunde anses som ett ”allvarligt” ingrepp i de grundläggande rättigheterna för de personer som uppgifterna avser, eftersom dessa uppgifter inte gör det möjligt att dra några mer precisa slutsatser om dessa personers privatliv. Av detta drog domstolen slutsatsen att det ingrepp som tillgång till sådana uppgifter innebär kan vara motiverat av syftet att förebygga, utreda, upptäcka och lagföra ”brott” i allmänhet, utan att dessa brott behöver kvalificeras som ”allvarliga” (punkterna 61 och 62).

Domar av den 6 oktober 2020 (stora avdelningen), Privacy International (C-623/17, EU:C:2020:790) och La Quadrature du Net m.fl. (C-511/18, C-512/18 och C-520/18, EU:C:2020:791)[41]

40 Domstolens dom av den 21 december 2016, Tele2 Sverige och Watson m.fl. (C-203/15 och C-698/15, EU:C:2016:970).

41 En redogörelse för domarna finns i årsrapporten för år 2020, s. 29–32.

Rättspraxis i fråga om lagring och tillgång till personuppgifter på området för elektroniska kommunikationer har föranlett farhågor hos vissa medlemsstater, vilka är oroliga för att ha blivit berövade ett instrument som de anser sig behöva för att skydda den nationella säkerheten och bekämpa brott. Detta gäller särskilt domen Tele2 Sverige och Watson m.fl., i vilken domstolen bland annat ansåg att medlemsstaterna inte fick ålägga leverantörer av elektroniska kommunikationstjänster en skyldighet att på ett generellt och odifferentierat sätt lagra trafik- och lokaliseringsuppgifter.

Det var mot denna bakgrund som talan avseende lagenligheten av vissa medlemsstaters lagstiftning på dessa områden – i vilken det föreskrevs en skyldighet för leverantörer av elektroniska kommunikationstjänster att överföra användarnas trafik- och lokaliseringsuppgifter till en myndighet eller att på ett generellt och odifferentierat sätt lagra sådana uppgifter – väcktes vid Investigatory Powers Tribunal (Domstolen för utredningsbefogenheter, Förenade kungariket) (Privacy International, C-623/17), Conseil d'État (Högsta förvaltningsdomstolen, Frankrike) (La Quadrature du Net m.fl., förenade målen C-511/18 och C-512/18) respektive Cour constitutionnelle (Författningsdomstolen, Belgien) (Ordre des barreaux francophones et germanophone m.fl., C-520/18).

EU-domstolen (stora avdelningen) fann i två domar meddelade den 6 oktober 2020 att direktiv 2002/58 är tillämpligt på nationell lagstiftning som ålägger leverantörer av elektroniska kommunikationstjänster att lagra trafik- och lokaliseringsuppgifter eller att överföra sådana uppgifter till nationella säkerhets- och underrättelsetjänster i detta syfte (punkt 49 samt punkt 1 i domslutet i domen Privacy International och punkt 104 i domen La Quadrature du Net m.fl.).

Domstolen erinrade därefter om att direktiv 2002/58[42] inte tillåter att undantag från den principiella skyldigheten att garantera konfidentialitet för elektroniska kommunikationer och därmed förbundna uppgifter samt undantag från förbudet att lagra dessa uppgifter blir huvudregeln. Detta medför att det enligt direktivet endast är tillåtet för medlemsstaterna att, bland annat för ändamålet att skydda nationell säkerhet, anta lagstiftning som begränsar omfattningen av de rättigheter och skyldigheter som föreskrivs i direktivet, i synnerhet skyldigheten att garantera konfidentialiteten för kommunikationer och trafikuppgifter[43], under förutsättning att de allmänna principerna i unionsrätten iakttas, däribland proportionalitetsprincipen och de grundläggande rättigheter som garanteras i stadgan[44] (punkterna 59 och 60 i domen Privacy International och punkterna 111 och 113 i domen La Quadrature du Net m.fl.).

I detta sammanhang fann domstolen för det första, i målet Privacy International, att direktiv 2002/58, tolkat mot bakgrund av stadgan, utgör hinder för en nationell lagstiftning som ålägger leverantörer av elektroniska kommunikationstjänster att på ett generellt och odifferentierat sätt överföra trafik- och lokaliseringsuppgifter till säkerhets- och underrättelsetjänsterna i syfte att skydda nationell säkerhet. Domstolen fann för det andra, i de förenade målen La Quadrature du Net m.fl. och Ordre des barreaux francophones et germanophone m.fl., att nämnda direktiv

42 Artikel 15.1 och 15.3 i direktiv 2002/58.
43 Artikel 5.1 i direktiv 2002/58.
44 Särskilt artiklarna 7, 8, 11 och 52.1 i stadgan.

utgör hinder för lagstiftning vilken ålägger leverantörer av elektroniska kommunikationstjänster generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter i förebyggande syfte.

Skyldigheterna att överföra och på ett generaliserat och odifferentierat sätt lagra sådana uppgifter utgör nämligen synnerligen allvarliga ingrepp i de grundläggande rättigheter som garanteras i stadgan, utan att det finns något samband mellan de personer vilkas uppgifter berörs och det mål som eftersträvas med den aktuella lagstiftningen. På motsvarande sätt fann domstolen att artikel 23.1 i dataskyddsförordningen, mot bakgrund av stadgan, skulle tolkas så, att den utgör hinder för en nationell lagstiftning enligt vilken leverantörer som tillhandahåller allmänheten tillgång till internetkommunikationstjänster och värdtjänstleverantörer är skyldiga att generellt och odifferentierat lagra bland annat personuppgifter förbundna med dessa tjänster (punkterna 71 och 82 samt punkt 2 i domslutet i domen Privacy International och punkterna 146, 168, 174, 177 och 212 samt punkterna 1 och 3 i domslutet i domen La Quadrature du Net m.fl.).

Domstolen ansåg däremot att i situationer där den aktuella medlemsstaten står inför ett allvarligt hot mot nationell säkerhet beträffande vilket det är visat att hotet är verkligt och aktuellt eller förutsebart, utgör direktiv 2002/58, jämfört med stadgan, inte hinder för att leverantörer av elektroniska kommunikationstjänster åläggs att på ett generellt och odifferentierat sätt lagra trafik- och lokaliseringsuppgifter. Domstolen preciserade i detta sammanhang att beslutet om åläggande av nämnda lagringsskyldighet måste kunna bli föremål för effektiv kontroll antingen av en domstol eller av en oberoende myndighet, vars avgörande har bindande verkan, i syfte att kontrollera om någon av dessa situationer föreligger och att föreskrivna villkor och garantier iakttas, varvid åläggandet endast får meddelas för en period som tidsmässigt är begränsad till vad som är strängt nödvändigt. Direktivet utgör inte, på samma villkor, hinder för automatiserad analys av uppgifter, bland annat trafik- och lokaliseringsuppgifter, från samtliga användare av elektroniska kommunikationsmedel (punkterna 137–139 och 177–179 samt punkterna 1 och 2 i domslutet i domen La Quadrature du Net m.fl.).

Domstolen tillade att direktiv 2002/58, jämfört med stadgan, inte utgör hinder mot en riktad lagring av trafik- och lokaliseringsuppgifter vilken, på grundval av objektiva och icke-diskriminerande faktorer, är avgränsad genom de kategorier av personer som berörs eller genom ett geografiskt kriterium, för en period som är tidsmässigt begränsad till vad som är strängt nödvändigt. Direktivet utgör inte heller hinder för åtgärder som föreskriver en generell och odifferentierad lagring av IP-adresser som tilldelats en kommunikationskälla, under förutsättning att lagringen är tidsmässigt begränsad till vad som är strängt nödvändigt. Direktivet utgör inte heller hinder för åtgärder som föreskriver lagring av uppgifter om den fysiska identiteten hos användare av elektroniska kommunikationsmedel, och medlemsstaterna är inte skyldiga att begränsa den tid under vilken dessa uppgifter får lagras. Direktivet utgör dessutom inte hinder för en lagstiftningsåtgärd som gör det möjligt att skyndsamt säkra uppgifter som tjänsteleverantörer har tillgång till, när det uppstår situationer i vilka det finns behov att lagra dessa uppgifter längre än den lagstadgade fristen för lagring i syfte att klarlägga grova brott eller handlingar som utgör ett hot mot nationell säkerhet, när dessa brott eller handlingar redan har konstaterats eller rimligen kan misstänkas (punkterna 161, 163 och 168 samt punkt 1 i domslutet i domen La Quadrature du Net m.fl.).

Domstolen slog dessutom fast att direktiv 2002/58, jämfört med stadgan, inte utgör hinder för nationell lagstiftning som ålägger leverantörer av elektroniska kommunikationstjänster att i

realtid samla in trafik- och lokaliseringsuppgifter, om denna insamling är begränsad till personer beträffande vilka det finns ett giltigt skäl att misstänka att de på ett eller annat sätt är inblandade i terrorverksamhet och den är underkastad en förhandskontroll antingen av en domstol eller av en oberoende myndighet, vars avgörande har bindande verkan, i syfte att säkerställa att en sådan insamling i realtid endast är tillåten inom ramen för vad som är strängt nödvändigt. I vederbörligen motiverade fall som ställer krav på skyndsamhet ska kontrollen ske utan dröjsmål (punkt 192 samt punkt 2 i domslutet i domen La Quadrature du Net m.fl.).

Domstolen tog slutligen ställning till frågan om bibehållande av verkningarna i tiden av en nationell lagstiftning som konstaterats vara oförenlig med unionsrätten. Domstolen fann härvidlag att en nationell domstol inte får tillämpa en bestämmelse i nationell rätt som ger den behörighet att tidsmässigt begränsa verkningarna av en förklaring om rättsstridighet som den domstolen är skyldig att meddela enligt nationell rätt med avseende på nationell lagstiftning enligt vilken leverantörer av elektroniska kommunikationstjänster åläggs en skyldighet att generellt och odifferentierat lagra trafik- och lokaliseringsuppgifter som är oförenlig med direktiv 2002/58, jämfört med stadgan.

För att ge den hänskjutande domstolen ett användbart svar erinrade EU-domstolen om att reglerna om tillåtlighet och värdering – i ett brottmålsförfarande mot personer som är misstänkta för grova brott – av information och bevisning som erhållits genom en lagring av trafik- och lokaliseringsuppgifter i strid med unionsrätten, på unionsrättens nuvarande stadium i princip uteslutande bestäms av nationell rätt. Domstolen preciserade emellertid att direktivet om integritet och elektronisk kommunikation, tolkat mot bakgrund av effektivitetsprincipen, innebär en skyldighet för en nationell brottmålsdomstol att – inom ramen för ett brottmålsförfarande mot personer som är misstänkta för brott – bortse från information och bevisning som erhållits genom en generell och odifferentierad lagring av trafik- och lokaliseringsuppgifter som inte är förenlig med unionsrätten, om dessa personer inte har möjlighet att på ett effektivt sätt yttra sig över informationen och bevisningen (punkterna 222 och 228 samt punkt 4 i domslutet i domen La Quadrature du Net m.fl.).

Dom av den 2 mars 202 (stora avdelningen), Prokuratuur (Villkor för tillgång till uppgifter om elektronisk kommunikation) (C-746/18, EU:C:2021:152)

I Estland inleddes ett straffrättsligt förfarande mot H.K., som åtalades för stölder, användning av tredje mans bankkort samt övergrepp i rättssak. H.K. dömdes för dessa brott av en domstol i första instans till fängelse i två år. Domen fastställdes i andra instans. De protokoll som gjorde det möjligt att styrka att H.K. hade begått ovannämnda brott grundades bland annat på personuppgifter som genererats i samband med tillhandahållandet av elektroniska kommunikationstjänster. H.K. överklagade avgörandet i andra instans till Riigikohus (Högsta domstolen, Estland), som var osäker på huruvida de utredande myndigheterna hade fått tillgång till dessa uppgifter på villkor som var förenliga med unionsrätten.[45]

Osäkerheten avsåg för det första frågan huruvida omfattningen av den period då de utredande myndigheterna fick tillgång till uppgifterna utgjorde ett kriterium som kunde ligga till grund för bedömningen av hur allvarligt ingreppet i de berörda personernas grundläggande rättigheter,

[45] Närmare bestämt artikel 15.1 i direktiv 2002/58/EG, jämförd med artiklarna 7, 8, 11 och 52.1 i stadgan.

bestående i myndigheternas tillgång till dessa uppgifter, skulle anses vara. Den hänskjutande domstolen ansåg att när denna period är mycket kort eller mängden av de insamlade uppgifterna är mycket begränsad, finns det anledning att fråga sig huruvida målet att bekämpa brottslighet i allmänhet, och inte enbart grov brottslighet, kan motivera ett sådant ingrepp. För det andra önskade den hänskjutande domstolen få klarhet i huruvida den estniska åklagarmyndigheten, med hänsyn till de olika uppdrag som den anförtrotts enligt nationell lagstiftning, kunde anses utgöra en ”oberoende” förvaltningsmyndighet i den mening som avses i domen Tele 2 Sverige och Watson m.fl.,[46] och att åklagarmyndigheten således kunde ge de brottsutredande myndigheterna tillgång till de aktuella uppgifterna.

I sin dom slog domstolen (stora avdelningen) fast att direktiv 2002/58, jämfört med stadgan, utgör hinder mot nationell lagstiftning som gör det möjligt för offentliga myndigheter att få tillgång till trafik- eller lokaliseringsuppgifter – vilka kan ge information om kommunikation som en användare har utfört medelst elektronisk kommunikationsutrustning eller om lokaliseringen av terminalutrustning som denna användare har använt, och ligga till grund för slutsatser beträffande användarens privatliv – i syfte att förebygga, undersöka, avslöja och väcka åtal för brott, utan att det uppställs något krav på att det ska röra sig om grov brottslighet eller förebyggande av allvarliga hot mot allmän säkerhet. Domstolen ansåg att den tidsperiod under vilken myndigheterna ges tillgång till dessa uppgifter, samt mängden och arten av de uppgifter som är tillgängliga under denna period, saknar betydelse i detta avseende. Domstolen fann även att nämnda direktiv, jämfört med stadgan, utgör hinder mot nationell lagstiftning som ger åklagarmyndigheten behörighet att ge offentliga myndigheter tillgång till trafik- och lokaliseringsuppgifter inom ramen för en brottsutredning (punkterna 45 och 59 samt punkterna 1 och 2 i domslutet).

Vad gäller målet bestående i att förebygga, undersöka, avslöja och väcka åtal för brott som eftersträvas genom den aktuella nationella lagstiftningen, fann domstolen att det i enlighet med proportionalitetsprincipen endast är målen bestående i att bekämpa grov brottslighet eller förebygga allvarliga hot mot den allmänna säkerheten som kan motivera att offentliga myndigheter ska få tillgång till ett stort antal trafik- eller lokaliseringsuppgifter som gör det möjligt att dra precisa slutsatser om de berörda personernas privatliv, såvida inte andra faktorer för att bedöma huruvida ansökan om tillgång är proportionerlig – såsom under hur lång tid myndigheterna får tillgång till de begärda uppgifterna – kan leda till att målet bestående i att förebygga, undersöka, avslöja och väcka åtal för brott i allmänhet kan motivera att sådan tillgång ska beviljas (punkterna 33 och 35).

I fråga om åklagarmyndighetens behörighet att ge en offentlig myndighet tillgång till trafik- eller lokaliseringsuppgifter när sistnämnda myndighet ska genomföra en brottsutredning, erinrade domstolen om att det i nationell rätt ska fastställas under vilka villkor leverantörer av elektroniska kommunikationstjänster ska ge behöriga nationella myndigheter tillgång till de uppgifter som de förfogar över. För att kravet på proportionalitet ska anses vara uppfyllt måste sådan lagstiftning emellertid innehålla klara och precisa bestämmelser som reglerar räckvidden och tillämpningen av den aktuella åtgärden samt ange minimikrav, så att de personer vars personuppgifter berörs har tillräckliga garantier för att uppgifterna på ett effektivt sätt är skyddade mot riskerna för missbruk. Denna lagstiftning ska vara rättsligt bindande enligt

[46] Dom av den 21 december 2016, Tele2 Sverige och Watson m.fl. (C-203/15 och C-698/15, EU:C:2016:970, punkt 120).

nationell rätt och i synnerhet ange under vilka omständigheter och på vilka villkor en åtgärd avseende behandling av sådana uppgifter får vidtas, vilket säkerställer att ingreppet begränsas till vad som är strängt nödvändigt (punkt 48).

Domstolen ansåg att det för att säkerställa att dessa villkor uppfylls till fullo i praktiken är av väsentlig betydelse att behöriga nationella myndigheters tillgång till de lagrade uppgifterna är underkastad förhandskontroll av en domstol eller en oberoende myndighet, och att domstolen meddelar sitt avgörande eller myndigheten antar sitt beslut till följd av att dessa myndigheter har framställt en motiverad begäran inom ramen för exempelvis ett förfarande för förebyggande, avslöjande eller lagföring av brott. I vederbörligen motiverade fall som ställer krav på skyndsamhet ska denna kontroll ske utan dröjsmål (punkt 51).

I detta avseende framhöll domstolen att en sådan förhandskontroll bland annat innebär att den domstol eller det organ som ska utföra denna kontroll har alla befogenheter och lämnar alla nödvändiga garantier för att kunna göra en vederbörlig avvägning mellan de olika intressen och rättigheter som är i fråga. Vad särskilt gäller en brottsutredning kräver en sådan kontroll att denna domstol eller detta organ kan säkerställa en korrekt balans mellan de intressen som inom ramen för brottsbekämpning gör sig gällande för att svara mot utredningens behov, å ena sidan, och de grundläggande rättigheter avseende respekt för privatlivet och skydd av personuppgifter som tillkommer de personer vars uppgifter kan komma att lämnas ut, å den andra sidan. När denna kontroll inte utförs av en domstol utan av en oberoende förvaltningsmyndighet måste denna myndighet ha en ställning som innebär att den kan fullgöra sitt uppdrag på ett objektivt och opartiskt sätt, och den måste därför vara fri från all yttre påverkan (punkterna 52 och 53).

Domstolen ansåg att det härav följde att det krav på oberoende som myndigheten med ansvar för sådan förhandskontroll ska uppfylla innebär att myndigheten måste vara fristående i förhållande till den som begär tillgång till uppgifterna, så att myndigheten kan utöva sin kontroll på ett objektivt och opartiskt sätt utan yttre påverkan. På det straffrättsliga området innebär kravet på oberoende att den myndighet som ska utföra förhandskontrollen dels inte får vara involverad i den aktuella brottsutredningen, dels ska ha en neutral ställning i förhållande till parterna i det straffrättsliga förfarandet. Så är inte fallet med en åklagarmyndighet som – såsom är fallet med den estniska åklagarmyndigheten – leder utredningsförfarandet och, i förekommande fall, väcker åtal för det allmännas räkning. Härav följer att en åklagarmyndighet inte kan utföra denna förhandskontroll (punkterna 54, 55 och 57).

IV. Överföring av personuppgifter till tredje land

Dom av den 6 november 2003 (stora avdelningen), Lindqvist (C-101/01, EU:C:2003:596)[47]

I detta mål (se även avsnitt II.3, med rubriken ”Begreppet behandling av personuppgifter”), önskade den hänskjutande domstolen särskilt få klarhet i huruvida Bodil Lindqvist hade gjort en överföring av uppgifter till tredje land i den mening som avses i direktivet.

47 En redogörelse för domen finns i årsrapporten för år 2003, s. 67.

EU-domstolen slog fast att det inte föreligger någon ”överföring av … uppgifter till tredje land”, i den mening som avses i artikel 25 i direktiv 95/46 när en person som befinner sig i en medlemsstat lägger ut personuppgifter på en webbsida som är lagrad hos en fysisk eller juridisk person som hyser den webbplats där sidan kan läsas och som är etablerad i samma medlemsstat eller i en annan medlemsstat, varvid uppgifterna blir åtkomliga för alla som kopplar upp sig på internet, inklusive personer i tredjeland (punkt 71 samt punkt 4 i domslutet).

Med hänsyn dels till det stadium på vilket internets utveckling befann sig vid den tidpunkt då direktiv 95/46 utarbetades, dels till att det i kapitel IV i direktivet, i vilket artikel 25 ingår – som syftar till att säkerställa att medlemsstaterna har kontroll över överföringen av personuppgifter till tredje land och till att överföring av personuppgifter till ett tredje land skall förbjudas om inte det landet garanterar en adekvat skyddsnivå –, inte anges några kriterier som är tillämpliga på internetanvändning, kan det inte antas att gemenskapslagstiftaren hade för avsikt att med tanke på framtiden låta ett sådant utläggande av uppgifter på en webbsida omfattas av begreppet överföring av uppgifter till tredje land, även om dessa på detta sätt blir åtkomliga för sådana personer i tredje land som har tekniska möjligheter att få tillgång till hemsidan (punkterna 63, 64 och 68).

Dom av den 6 oktober 2015, (stora avdelningen), Schrems (C-362/14, EU:C:2015:650)[48]

Maximillian Schrems, österrikisk medborgare och användare av det sociala nätverket Facebook, hade inkommit med klagomål till Data Protection Commissioner (datatillsynsmyndigheten, Irland), på grund av att Facebook Ireland till Förenta staterna hade överfört personuppgifter rörande sina användare och lagrat dem på servrar i det landet, där de var föremål för behandling. Maximillian Schrems ansåg att Förenta staternas rätt och praxis inte gav tillräckligt skydd mot övervakning från myndigheterna av de uppgifter som överförs till det landet. Data Protection Commissioner hade avslagit klagomålet, bland annat med motiveringen att kommissionen i sitt beslut 2000/520/EG,[49] hade slagit fast att Förenta staterna enligt det så kallade safe harbor-systemet,[50] säkerställer en adekvat skyddsnivå för de överförda personuppgifterna.

Mot denna bakgrund begärde High Court (Högsta domstolen, Irland) förhandsavgörande från EU-domstolen avseende tolkningen av artikel 25.6 i direktiv 95/46, enligt vilken kommissionen kan konstatera att ett tredjeland garanterar en adekvat skyddsnivå för överförda uppgifter, och avseende giltigheten av beslut 2000/520, som antogs av kommissionen på grundval av artikel 25.6 i direktiv 95/46.

EU-domstolen ogiltigförklarade kommissionens beslut i dess helhet och påpekade därvid inledningsvis att antagandet av beslutet krävde att kommissionen fastställt och vederbörligen motiverat att det aktuella tredjelandet de facto säkerställer en nivå för skyddet av de grundläggande rättigheterna som är väsentligen likvärdig med den nivå som garanteras i

48 En redogörelse för domen finns i årsrapporten för år 2015, s. 53.

49 Kommissionens beslut 2000/520/EG av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat (EGT L 215, 2000, s. 7).

50 Safe harbour-systemet inkluderar en rad principer för skydd av personuppgifter som amerikanska företag kan ansluta sig till frivilligt.

unionens rättsordning. Eftersom kommissionen i beslut 2000/520 inte har angett något sådant, åsidosatte artikel 1 beslutet de krav som slås fast i artikel 25.6 i direktiv 95/46 jämförd med stadgan, och artikeln är därmed ogiltig. Safe harbor-principerna är nämligen uteslutande tillämpliga på självcertifierade amerikanska organisationer som erhåller personuppgifter från unionen, utan att det krävs att amerikanska myndigheter ska iaktta dessa principer. Vidare möjliggör beslut 2000/520 ingrepp i de grundläggande rättigheterna för personer vilkas personuppgifter överförs eller kan komma att överföras från unionen till Förenta staterna, samtidigt som beslutet inte innehåller något konstaterande beträffande förekomsten i Förenta staterna av regler som antagits av staten och som syftar till att begränsa eventuella ingrepp i dessa rättigheter. Inte heller anges att det finns något effektivt rättsligt skydd mot denna typ av ingrepp (punkterna 82, 87–89 och 96–98 samt punkt 2 i domslutet).

Dessutom ogiltigförklarade domstolen artikel 3 i beslut 2000/520, i den mån den berövar de nationella tillsynsmyndigheterna de befogenheter de har i enlighet med artikel 28 i direktiv 95/46, när en person anför omständigheter som innebär att det kan ifrågasättas huruvida ett beslut, i vilket kommissionen konstaterat att ett tredjeland säkerställer en adekvat skyddsnivå, är förenligt med skyddet för privatlivet och enskilda personers grundläggande fri- och rättigheter (punkterna 102–104). Domstolen slog fast att ogiltigförklaringen av artiklarna 1 och 3 i beslut 2000/520 påverkade giltigheten av beslutet i dess helhet (punkterna 105 och 106).

Vad gäller omöjligheten att motivera ett sådant ingrepp påpekade domstolen för det första att en unionslagstiftning som innebär ett ingrepp i de grundläggande rättigheter som garanteras av artiklarna 7 och 8 i stadgan måste föreskriva tydliga och precisa bestämmelser som reglerar räckvidden och tillämpligheten av en åtgärd och slå fast minimikrav, så att de personer vilkas personuppgifter berörs har tillräckliga garantier som möjliggör ett effektivt skydd av deras uppgifter mot risker för missbruk och otillåten åtkomst eller användning. Behovet av sådana garantier är av än större betydelse när personuppgifterna är föremål för automatisk behandling och risken för otillåten åtkomst till uppgifterna är stor (punkt 91).

Vidare, och framför allt, kräver skyddet av den grundläggande rätten till respekt för privatlivet på unionsnivå att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt (punkt 92). En lagstiftning är således inte begränsad till vad som är strängt nödvändigt när den generellt tillåter lagring av samtliga personuppgifter om alla personer vilkas uppgifter har överförts från unionen, utan att det görs några åtskillnader, begränsningar eller undantag med beaktande av det eftersträvade syftet och utan att det föreskrivs något objektivt kriterium som gör det möjligt att avgränsa myndigheternas åtkomst till uppgifterna och att avgränsa deras senare användning till bestämda, strängt begränsade syften som kan motivera det ingrepp som såväl åtkomst som användning av uppgifterna innebär (punkt 93). En lagstiftning som tillåter myndigheterna generell åtkomst till innehållet i elektroniska kommunikationer kränker det väsentliga innehållet i den grundläggande rätten till respekt för privatlivet. En lagstiftning i vilken det inte föreskrivs någon möjlighet för enskilda att använda rättsmedel för att erhålla tillgång till, rätta eller radera uppgifter som rör dem, respekterar inte det väsentliga innehållet i den grundläggande rätten till ett effektivt domstolsskydd, vilken är stadfäst i artikel 47 i stadgan (punkterna 94 och 95).

Yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017 (stora avdelningen) (EU:C:2017:592)

Den 26 juli 2017 uttalade sig domstolen för första gången om huruvida ett utkast till internationellt avtal är förenligt med Europeiska unionens stadga om de grundläggande rättigheterna och, i synnerhet, med bestämmelser om personlig integritet och skydd av personuppgifter.

Europeiska unionen och Kanada hade förhandlat fram ett avtal om överföring och behandling av passageraruppgifter (PNR-avtalet) som undertecknades 2014. Efter att Europeiska unionens råd begärt att Europaparlamentet skulle godkänna avtalet beslutade parlamentet att fråga EU-domstolen om huruvida det föreslagna avtalet var förenligt med unionsrätten.

Det planerade avtalet medger en systematisk och kontinuerlig överföring av PNR-uppgifter för alla flygpassagerare till en kanadensisk myndighet för användning och bevarande och eventuell vidareöverföring till andra myndigheter och andra tredje länder, i syfte att bekämpa terrorism och allvarlig gränsöverskridande brottslighet. I detta hänseende föreskrivs i det tilltänkta avtalet bland annat en lagringsperiod på fem år och särskilda krav för säkerhet och integritet avseende PNR-uppgifterna, såsom en omedelbar maskering av känsliga uppgifter, samt rätt till tillgång till uppgifterna, rättelse och radering och möjligheten att inleda administrativa eller rättsliga förfaranden.

PNR-uppgifter som behandlas i det planerade avtalet omfattar, förutom flygpassagerarnas namn och kontaktuppgifter, bland annat information som behövs för bokningen, såsom resedatum, resrutt, biljettinformation, grupper av personer som är registrerade under samma bokningsnummer, information om betalningssätt eller fakturering, information om bagage samt allmänna noteringar avseende passagerarna.

I sitt yttrande slog domstolen fast att PNR-avtalet inte kunde ingås i sin dåvarande form på grund av att vissa av dess bestämmelser var oförenliga med de grundläggande rättigheter som erkänts av unionen.

Domstolen slog för det första fast att såväl överföring av PNR-uppgifter från unionen till den behöriga kanadensiska myndigheten som den ram som unionen förhandlat fram med Kanada avseende villkoren för lagring av dessa uppgifter, dess användning och eventuella senare överföring till andra kanadensiska myndigheter, till Europol, till Eurojust, till polisiära eller rättsliga myndigheter i medlemsstaterna eller till andra myndigheter i tredjeland, utgör ingrepp i den rättighet som garanteras i artikel 7 i stadgan. Dessa åtgärder utgör även ett ingrepp i den grundläggande rätten till skydd av personuppgifter som är garanterad genom artikel 8 i stadgan, eftersom åtgärderna utgör behandling av personuppgifter (punkterna 125 och 126).

Domstolen påpekade dessutom att även om vissa PNR-uppgifter, betraktade för sig, inte tycks avslöja viktig information om de berörda personernas privatliv, kvarstår det faktum att dessa uppgifter tillsammans kan avslöja bland annat en fullständig resrutt, resmönster, förhållandet mellan två eller flera personer samt information om den finansiella situationen för flygpassagerarna, deras matvanor eller deras hälsotillstånd, och att de även kan tillhandahålla känslig information om dessa passagerare, enligt definitionen i artikel 2 e i det planerade avtalet

(information som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös övertygelse etc.) (punkt 128).

I detta avseende slog domstolen fast att även om ingreppet i fråga skulle kunna motiveras av ett mål av allmänt intresse (allmän säkerhet i kampen mot terroristbrott och grov gränsöverskridande brottslighet), är flera bestämmelser i avtalet inte begränsade till vad som är absolut nödvändigt och föreskriver inte tydliga och precisa regler.

Domstolen påpekade särskilt att, med tanke på risken för en behandling som stred mot principen om icke-diskriminering, skulle överföring av känsliga uppgifter till Kanada kräva en precis och särskilt gedigen motivering och grundas på andra skäl än skyddet för allmän säkerhet mot terrorism och grov gränsöverskridande brottslighet. I detta fall saknades det en sådan motivering. Domstolen fann att bestämmelserna i avtalet om överföring av känsliga uppgifter till Kanada samt behandling och lagring av dessa uppgifter var oförenliga med de grundläggande rättigheterna (punkterna 165 och 232).

Domstolen slog för det andra fast att efter att flygpassagerare lämnat Kanada är fortsatt lagring av PNR-uppgifter för alla flygpassagerare, som det planerade avtalet godtog, inte begränsad till vad som är absolut nödvändigt. Vad gäller passagerare för vilka en risk för terrorism eller allvarlig gränsöverskridande brottslighet inte har identifierats efter ankomsten i Kanada och fram till avresan från det landet, förefaller det nämligen inte, efter att de lämnat landet, finnas ens ett indirekt samband mellan deras PNR-uppgifter och det mål som eftersträvades genom det planerade avtalet, vilket skulle motivera lagring av dessa uppgifter. Däremot kan lagring av PNR-uppgifter rörande flygpassagerare avseende vilka det finns objektiva skäl att anse att de, även efter sin avresa från Kanada, skulle kunna utgöra en risk när det gäller kampen mot terrorism och allvarlig gränsöverskridande brottslighet vara godtagbar också efter deras vistelse i landet, även för en tid av fem år (punkterna 205–207 och 209).

För det tredje slog domstolen fast att den grundläggande rätten till respekt för privatlivet, som nämns i artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna, innebär att den registrerade ska kunna försäkra sig om att dennes personuppgifter behandlas korrekt och lagenligt. För att kunna utföra nödvändiga kontroller, ska den berörda personen ha rätt att få tillgång till uppgifter som rör vederbörande och som är föremål för behandling.

I detta sammanhang påpekade domstolen att det enligt det planerade avtalet är viktigt att passagerare informeras om överföring av PNR-uppgifter till tredjelandet i fråga och om användningen av dessa uppgifter så snart en sådan upplysning inte längre riskerar att skada de utredningar som utförs av de myndigheter som avses i det planerade avtalet. Sådan information är nämligen nödvändig för att göra det möjligt för flygpassagerare att utöva sin rätt att få tillgång till uppgifter som rör dem och, i förekommande fall, att erhålla rättelse av dem samt att, i enlighet med artikel 47 första stycket i stadgan, kunna använda sig av ett effektivt rättsmedel inför en domstol.

I situationer där det finns objektiva grunder som motiverar användningen av PNR-uppgifter för att bekämpa terrorism och allvarlig gränsöverskridande brottslighet och som kräver ett förhandstillstånd från en rättslig myndighet eller ett oberoende administrativt organ, är individuell information om flygpassagerare således nödvändig. Det förhåller sig på samma sätt i de fall där PNR-uppgifterna överförs till andra myndigheter eller till enskilda. Informationen bör

dock inte lämnas före den tidpunkt då den inte längre riskerar att skada de utredningar som utförs av de myndigheter som avses i det planerade avtalet (punkterna 219, 220, 223 och 224).

Dom av den 16 juli 2020 (stora avdelningen), Facebook Ireland och Schrems (C-311/18, EU:C:2015:559)[51]

I dataskyddsförordningen föreskrivs att överföring av personuppgifter till ett tredjeland endast får ske under förutsättning att det aktuella tredjelandet säkerställer en adekvat skyddsnivå för dessa uppgifter. Enligt denna förordning kan kommissionen besluta att tredjelandet i fråga, med hänsyn till dess interna lagstiftning och internationella åtaganden, säkerställer en adekvat skyddsnivå.[52] I avsaknad av ett sådant beslut om adekvat skyddsnivå får en sådan överföring endast äga rum efter att uppgiftsutföraren som är etablerad i unionen har vidtagit lämpliga skyddsåtgärder, vilka bland annat kan utgöras av standardiserade dataskyddsbestämmelser som antas av kommissionen, och under förutsättning att det finns lagstadgade rättigheter och effektiva rättsmedel för de registrerade.[53] Vidare innehåller dataskyddsförordningen noggranna bestämmelser om villkoren för att en sådan överföring ska få äga rum i avsaknad av ett beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder.[54]

Maximillian Schrems är medborgare i Österrike och bosatt i den medlemsstaten. Han har använt Facebook sedan år 2008. Liksom för alla Facebookanvändare i unionen överfördes Maximillian Schrems personuppgifter, helt eller delvis, av Facebook Ireland till servrar tillhörande Facebook Inc., vilka är belägna i Förenta staterna där uppgifterna behandlas. Maximillian Schrems gjorde en anmälan till den irländska dataskyddsmyndigheten och begärde i huvudsak att myndigheten skulle förbjuda dessa överföringar. Han anförde att gällande rätt och praxis i Förenta staterna inte säkerställde ett tillräckligt skydd mot myndigheternas tillgång till personuppgifter som överförs till detta land. Detta klagomål avslogs med motiveringen att kommissionen i beslut 2000/520[55] hade konstaterat att Förenta staterna säkerställer en adekvat skyddsnivå. I dom meddelad den 6 oktober 2015 med anledning av en tolkningsfråga som hänskjutits av High Court (Förvaltningsdomstolen, Irland) slog EU-domstolen fast att detta beslut var ogiltigt (kallad domen i målet Schrems I)[56] (punkterna 52 och 53).

Med anledning av domen i målet Schrems I upphävde den irländska domstolen beslutet att avslå Maximillian Schrems klagomål och återförvisade ärendet till dataskyddsmyndigheten. Denna myndighet anmodade därefter Maximillian Schrems att omformulera sitt klagomål med hänsyn till EU-domstolens ogiltigförklaring av beslut 2000/520. I det omformulerade klagomålet vidhöll Maximillian Schrems att Förenta staterna inte säkerställer en tillräcklig skyddsnivå för personuppgifter som överförs till detta land. Han begärde att myndigheten för framtiden skulle avbryta eller förbjuda den överföring av hans personuppgifter från unionen till Förenta staterna som Facebook Ireland numera genomför på grundval av de standardiserade

---

51 En redogörelse för domen finns i årsrapporten för år 2020, s. 26–29.

52 Artikel 45 i dataskyddsförordningen.

53 Artikel 46.1 och 46.2 c i dataskyddsförordningen.

54 Artikel 49 i dataskyddsförordningen.

55 Kommissionens beslut 2000/520/EG av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat (EGT L 215, 2000, s.7).

56 Domstolens dom av den 6 oktober 2015, Schrems, C-362/14, EU:C:2015:650 (se även pressmeddelande nr 117/15).

dataskyddsbestämmelser som återfinns i bilagan till beslut 2010/87/EU.[57] Den irländska dataskyddsmyndigheten ansåg att frågan hur klagomålet skulle handläggas var beroende av giltigheten av beslut 2010/87 och inledde därför ett förfarande vid High Court (Förvaltningsdomstolen) i syfte att få denna att vända sig till EU-domstolen med en begäran om förhandsavgörande. Efter att detta förfarande inletts antog kommissionen beslut (EU) 2016/1250 om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna[58] (punkterna 54, 55 och 57).

Med begäran om förhandsavgörande önskade den hänskjutande domstolen att EU-domstolen skulle klargöra tillämpligheten av dataskyddsförordningen på överföringar av personuppgifter som grundar sig på de standardiserade dataskyddsbestämmelser som återfinns i beslut 2010/87, dels vad avser den skyddsnivå som krävs enligt denna förordning i samband med en sådan överföring, dels vad avser de skyldigheter som åvilar tillsynsmyndigheterna i detta sammanhang. High Court (Förvaltningsdomstolen) reste även frågan om giltigheten av såväl beslut 2010/87 som beslut 2016/1250.

EU-domstolen konstaterade att det vid prövningen av beslut 2010/87 mot bakgrund av Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad stadgan) inte har framkommit någon omständighet som påverkar beslutets giltighet. Däremot ogiltigförklarade domstolen beslut 2016/1250 (punkterna 4 och 5 i domslutet).

Domstolen fann till att börja med att unionsrätten, och särskilt dataskyddsförordningen, är tillämplig på en överföring av personuppgifter i kommersiellt syfte från en näringsidkare etablerad i en medlemsstat till en annan näringsidkare etablerad i ett tredjeland, trots att dessa uppgifter, under eller efter denna överföring, kan komma att behandlas av myndigheterna i det tredjelandet för ändamål som avser allmän säkerhet, försvar och nationell säkerhet. Domstolen preciserade att denna typ av behandling av personuppgifter av myndigheterna i ett tredjeland inte innebär att en sådan överföring faller utanför förordningens tillämpningsområde (punkterna 86, 88 och 89 samt punkt 1 i domslutet).

När det gäller den skyddsnivå som krävs i samband med en sådan överföring, konstaterade domstolen att kraven enligt bestämmelserna i dataskyddsförordningen i detta avseende, som hänför sig till lämpliga skyddsåtgärder, lagstadgade rättigheter och effektiva rättsmedel, ska tolkas så, att personer vars personuppgifter överförs till ett tredjeland med stöd av standardiserade dataskyddsbestämmelser ska åtnjuta en skyddsnivå som är väsentligen likvärdig med den som garanteras inom unionen genom denna förordning, jämförd med stadgan. Domstolen angav härvidlag att vid bedömningen av den skyddsnivå som säkerställs i samband med en sådan överföring ska hänsyn tas till såväl de avtalsvillkor som överenskommits mellan uppgiftsutföraren, som är etablerad i unionen, och mottagaren av överföringen i det berörda tredjelandet, som de relevanta delarna av rättssystemet i det tredjelandet såvitt avser den åtkomst som myndigheterna i det tredjelandet eventuellt har till överförda personuppgifter (punkt 105 samt punkt 2 i domslutet).

---

[57] Kommissionens beslut av den 5 februari 2010 om standardavtalsklausuler för överföring av personuppgifter till registerförare etablerade i tredjeland i enlighet med Europaparlamentets och rådets direktiv 95/46/EG (EUT L 39, 2010, s. 5), i ändrad lydelse enligt kommissionens genomförandebeslut (EU) 2016/2297 av den 16 december 2016 (EUT L 344, 2016, s. 100).

[58] Kommissionens genomförandebeslut (EU) 2016/1250 av den 12 juli 2016 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna (EUT L 207, 2016, s. 1).

När det gäller de skyldigheter som åvilar tillsynsmyndigheterna i samband med en sådan överföring slog domstolen fast att såvida det inte finns ett giltigt kommissionsbeslut om adekvat skyddsnivå är dessa myndigheter skyldiga att avbryta eller förbjuda en överföring av personuppgifter till tredjeland, när de, med beaktande av samtliga omständigheter i samband med denna överföring, anser att dessa klausuler inte iakttas eller inte kan iakttas i det tredjelandet och att det skydd för överförda personuppgifter som krävs enligt unionsrätten inte kan säkerställas med andra medel, förutsatt att uppgiftsutföraren som är etablerad i unionen inte själv har avbrutit eller upphört med överföringen (punkt 121 samt punkt 3 i domslutet).

Domstolen prövade därefter giltigheten av beslut 2010/87. Enligt domstolen påverkas inte giltigheten av detta beslut enbart av den omständigheten att de dataskyddsbestämmelser som återfinns i detta beslut, på grund av deras avtalsrättsliga karaktär, inte är bindande för myndigheterna i sådana tredjeländer till vilka personuppgifter kan komma att överföras. Domstolen angav däremot att denna giltighet beror på huruvida ett sådant beslut innehåller effektiva mekanismer som i praktiken gör det möjligt att säkerställa att den skyddsnivå som krävs enligt unionsrätten iakttas och att överföringar av personuppgifter med stöd av sådana dataskyddsbestämmelser avbryts eller förbjuds om dessa bestämmelser åsidosätts eller är omöjliga att iaktta. Domstolen konstaterade att beslut 2010/87 innehåller sådana mekanismer. Domstolen framhöll i detta avseende bland annat att detta beslut innebär en skyldighet för uppgiftsutföraren och mottagaren av överföringen att i förväg kontrollera att den skyddsnivå som krävs enligt unionsrätten iakttas i det berörda tredjelandet. Beslutet innebär även en skyldighet för mottagaren att informera uppgiftsutföraren om att mottagaren eventuellt inte kan iaktta de standardiserade skyddsklausulerna, varvid det åligger uppgiftsutföraren att avbryta överföringen av uppgifter och/eller häva avtalet med den förstnämnde (punkterna 132, 136, 137, 142 och 148 samt punkt 4 i domslutet).

Domstolen prövade slutligen giltigheten av beslut 2016/1250 utifrån de krav som följer av dataskyddsförordningen, mot bakgrund av bestämmelserna i stadgan som garanterar respekten för privatlivet och familjelivet, skyddet av personuppgifter och rätten till ett effektivt rättsmedel. Domstolen påpekade att detta beslut i likhet med beslut 2000/520 ger företräde för krav avseende nationell säkerhet, allmänintresset och efterlevnaden av amerikansk lagstiftning, vilket således gör ingrepp i personers grundläggande rättigheter möjliga när deras personuppgifter överförs till detta tredjeland. Enligt domstolen är de begränsningar av skyddet av personuppgifter som följer av Förenta staternas interna bestämmelser om åtkomst till och användning av sådana uppgifter som överförts från unionen till Förenta staterna, vilka kommissionen har bedömt i beslut 2016/1250, inte reglerade på ett sådant sätt att de uppfyller krav som är väsentligen likvärdiga med dem som i unionsrätten uppställs genom proportionalitetsprincipen, eftersom de övervakningsprogram som grundar sig på dessa bestämmelser inte är begränsade till vad som är strikt nödvändigt. Domstolen grundade sig på de konstateranden som gjorts i detta beslut och påpekade – när det gäller vissa övervakningsprogram – att det av nämnda bestämmelser inte framgår att det föreligger några begränsningar av behörigheten att genomföra dessa övervakningsprogram och att det inte heller finns några garantier för icke-amerikaner som eventuellt omfattas av dessa. Domstolen angav vidare att även om dessa bestämmelser visserligen innehåller krav som är bindande för amerikanska myndigheter i samband med genomförandet av de berörda övervakningsprogrammen, så innehåller de dock inte några rättigheter till förmån för berörda personer som kan göras gällande mot amerikanska myndigheter vid domstol (punkterna 164, 165, 180–182, 184 och 185).

När det gäller kravet på domstolsskydd slog domstolen fast att ombudsmannamekanismen i beslut 2016/1250, tvärtemot kommissionens bedömning i detta beslut, inte tillhandahåller dessa personer något rättsmedel inför ett organ som ger garantier som är väsentligen likvärdiga med dem som krävs enligt unionsrätten, vilka kan säkerställa såväl oavhängigheten hos den ombudsman som avses i denna mekanism som förekomsten av rättsregler som ger ombudsmannen behörighet att anta bindande beslut gentemot amerikanska underrättelsetjänster. Med stöd av dessa skäl ogiltigförklarade domstolen beslut 2016/1250 (punkterna 195–197 och 201 samt punkt 5 i domslutet).

V. Skydd av personuppgifter på internet

1. Rätt att motsätta sig behandling av personuppgifter (”rätten att bli glömd”)

Dom av den 13 maj 2014 (stora avdelningen), Google Spain och Google (C-131/12, EU:C:2014:317)

I denna dom (se även avsnitt II.3, med rubriken ”Begreppet behandling av personuppgifter”), preciserade domstolen räckvidden av rätten till tillgång och rätten att motsätta sig behandling av personuppgifter på internet, vilka föreskrivs i direktiv 95/46.

När domstolen uttalade sig om omfattningen av ansvaret för den som driver en sökmotor på internet slog domstolen i huvudsak fast att för att respektera rätten till tillgång och rätten att motsätta sig behandling enligt artiklarna 12 b och 14 a i direktiv 95/46, under förutsättning att de villkor som anges i nämnda artiklar är uppfyllda, är den som driver en sökmotor på internet, under vissa omständigheter, således skyldig att från förteckningen över sökresultat som visas efter det att en sökning gjorts på grundval av en persons namn avlägsna länkar till webbsidor som publicerats av tredje män och som innehåller information om denna person. Domstolen klargjorde att en sådan skyldighet kan föreligga även i de fall då detta namn eller dessa uppgifter inte raderas på förhand eller samtidigt från dessa webbsidor och, i förekommande fall, även om offentliggörandet i sig på dessa webbsidor är lagligt (punkt 88 samt punkt 3 i domslutet).

Angående frågan huruvida direktivet ger den registrerade möjlighet att begära att länkar till webbsidor tas bort från en sådan förteckning över sökresultat på grund av att den registrerade önskar att de uppgifter som avser denne ska ”glömmas bort” efter en viss tid, påpekade domstolen för det första att även ursprungligen laglig behandling av korrekta uppgifter med tiden kan bli oförenlig med direktivet när uppgifterna inte längre är nödvändiga för de ändamål för vilka de samlats in eller på annat sätt behandlats, bland annat när dessa uppgifter inte är adekvata, inte eller inte längre är relevanta eller är för omfattande i förhållande till de ändamål för vilka de behandlas eller den tid som har förflutit (punkt 93). Om det, till följd av en begäran från den registrerade, konstateras att upptagandet av dessa länkar i förteckningen, vid denna tidpunkt, är oförenligt med direktivet, ska uppgifter och länkar i förteckningen strykas (punkt 94). I detta hänseende påpekade domstolen att det för att en rätt att förhindra att informationen rörande hans eller hennes person inte längre ska kopplas till vederbörandes namn genom en förteckning över sökresultat ska anses föreligga inte krävs att den berörda personen orsakas skada av att informationen i fråga återfinns i förteckningen över sökresultat (punkt 96 samt punkt 4 i domslutet).

Domstolen påpekade slutligen att eftersom den berörda personen, med hänsyn till dennes grundläggande rättigheter enligt artiklarna 7 och 8 i stadgan, får begära att informationen i fråga inte längre ska göras tillgänglig för den breda allmänheten genom att upptas i en sådan förteckning över sökresultat, väger dessa rättigheter i princip inte bara tyngre än sökmotorleverantörens ekonomiska intressen, utan också tyngre än den breda allmänhetens intresse av att hitta denna information vid en sökning på den berörda personens namn. Så är emellertid inte fallet om ingreppet i den berörda personens grundläggande rättigheter av särskilda skäl, såsom den roll den berörda personen spelar i det offentliga livet, är motiverat av den breda allmänhetens övervägande intresse av att få tillgång till informationen i fråga genom att den upptas i förteckningen över sökresultat (punkt 97 samt punkt 4 i domslutet).

2. Behandling av personuppgifter och immateriella rättigheter

Dom av den 29 januari 2008 (stora avdelningen), Promusicae (C-275/06, EU:C:2008:54)[59]

Promusicae, en spansk organisation utan vinstsyfte bestående av producenter och utgivare av musikaliska och audiovisuella verk, hade väckt talan vid spansk domstol med yrkande om att Telefónica de España SAU (bolag vars verksamhet omfattar tillhandahållande av internetanslutningstjänster) skulle förpliktas att förete uppgifter om identitet och hemvist för vissa personer som detta bolag förser med internetuppkoppling och vars IP-adress och datum och klockslag för uppkoppling var kända. Enligt Promusicae använde dessa personer ett fildelningsprogram kallat ”peer-to-peer” eller ”P2P”) (öppen metod för delning av innehåll, som är självständig, decentraliserad och som har avancerade sökfunktioner samt ned- och uppladdningsfunktioner) och gjorde från sin egen persondator ljudupptagningar som Promusicaes medlemmar ägde rättigheterna till tillgängliga för andra användare. Promusicae yrkade därför att Telefónica skulle föreläggas att förete ovannämnda upplysningar för att Promusicae skulle kunna väcka talan mot berörda personer.

Mot denna bakgrund beslutade Juzgado de lo Mercantil nr 5 de Madrid (Handelsdomstol nr 5 i Madrid, Spanien) att ställa frågor till EU-domstolen om huruvida den europeiska lagstiftningen ålägger medlemsstaterna att, i syfte att säkerställa ett effektivt skydd för upphovsrätten, föreskriva en skyldighet att lämna ut personuppgifter i ett tvistemål.

Begäran om förhandsavgörande handlar således om hur skyddet för olika grundläggande rättigheter kan förenas med varandra, vilket är nödvändigt. I detta fall ska rätten till skydd för privatlivet, å ena sidan, förenas med rätten till skydd för egendom och rätten till ett effektivt rättsmedel, å andra sidan.

I detta hänseende slog domstolen fast att direktiv 2000/31/EG om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (direktiv om elektronisk handel),[60] direktiv 2001/29/EG om harmonisering av vissa aspekter av upphovsrätt

59 En redogörelse för domen finns i årsrapporten för år 2008, s. 46.

60 Europaparlamentets och rådets direktiv 2000/31/EG om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt den elektroniska handeln, på den inre marknaden (”Direktiv om elektronisk handel”) (EGT L 178, 2000, s. 1).

och närstående rättigheter i informationssamhället,[61] direktiv 2004/48/EG om säkerställande av skyddet för immateriella rättigheter,[62] och direktiv 2002/58 inte ålägger medlemsstaterna att, i ett fall som det som var i fråga i det nationella målet, föreskriva en skyldighet att lämna ut personuppgifter i syfte att säkerställa ett effektivt skydd för upphovsrätten inom ramen för ett tvistemål. Unionsrätten innebär emellertid ett krav på att medlemsstaterna, när de införlivar dessa direktiv med nationell rätt, ska utgå från en tolkning av direktiven som gör det möjligt att uppnå en korrekt balans mellan de olika grundläggande rättigheter som åtnjuter skydd enligt gemenskapens rättsordning. Vid tillämpningen av införlivandebestämmelserna för dessa direktiv ska myndigheterna och domstolarna i medlemsstaterna inte bara tolka sin nationella lagstiftning på ett sätt som står i överensstämmelse med direktiven, utan även se till att de inte tolkar den på ett sätt som strider mot grundläggande rättigheter eller allmänna gemenskapsrättsliga principer, såsom proportionalitetsprincipen (se punkt 70 samt domslutet).

Dom av den 24 november 2011, Scarlet Extended (C-70/10, EU:C:2011:771)[63]

Upphovsrättsorganisationen Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) hade konstaterat att internetanvändare som använde tjänster från internetleverantören Scarlet Extended SA (nedan kallat Scarlet) utan tillstånd och utan att betala ersättning, laddade ned sådana verk som fanns i organisationens katalog från internet med hjälp av ”peer to peer”-nät. SABAM hade väckt talan vid nationell domstol och i första instans förpliktades Scarlet att få sådana överträdelser av upphovsrätten att upphöra genom att göra det omöjligt för kunderna att med hjälp av ”peer to peer”-program skicka och ta emot elektroniska filer innehållande musikaliska verk ur SABAM:s repertoar.

Scarlet överklagade beslutet till Cour d’appel de Bruxelles (Appellationsdomstolen i Bryssel, Belgien), som vilandeförklarade målet för att begära ett förhandsavgörande från EU-domstolen om huruvida ett sådant föreläggande var förenligt med EU-rätten.

Domstolen slog fast att direktiven 95/46, 2000/31, 2001/29, 2002/58 och 2004/48, jämförda med varandra och tolkade mot bakgrund av de krav som följer av skyddet av de tillämpliga grundläggande rättigheterna ska tolkas så, att de utgör hinder för att Scarlet föreläggs att i förebyggande syfte och på egen bekostnad införa ett system för filtrering av all elektronisk kommunikation som passerar via internetleverantörens tjänster, framför allt med hjälp av ”peer-to-peer”-program, vilket är tillämpligt utan åtskillnad i förhållande till samtliga av internetleverantörens kunder, och utan begränsningar i tiden, och vilket kan upptäcka överföring inom internetleverantörens nät av elektroniska filer innehållande musikaliska eller audiovisuella verk samt filmverk, till vilka den som har yrkat föreläggande gör anspråk på att inneha de immateriella rättigheterna, i syfte att blockera överföringen av sådana filer vars utväxling innebär upphovsrättsintrång (punkt 54 samt domslutet).

61 Europaparlamentets och rådets direktiv 2001/29/EG av den 22 maj 2001 om harmonisering av vissa aspekter av upphovsrätt och närstående rättigheter i informationssamhället (EGT L 167, 2001, s. 10).

62 Europaparlamentets och rådets direktiv 2004/48/EG av den 29 april 2004 om säkerställande av skyddet för immateriella rättigheter (EUT L 157, 2004, s. 45, och rättelse i EUT L 195, 2004, s. 16).

63 En redogörelse för domen finns i årsrapporten för år 2011, s. 37.

Enligt domstolen är ett sådant föreläggande nämligen inte förenligt med förbudet i artikel 15.1 i direktiv 2000/31 att ålägga en leverantör en allmän skyldighet att övervaka eller med kravet på att se till att avvägningen är rimlig mellan immaterialrätten å ena sidan och näringsfriheten, rätten till skydd av personuppgifter och friheten att ta emot och sprida uppgifter å andra sidan (punkterna 40 och 49).

I detta sammanhang påpekade domstolen att föreläggandet om att införa det omtvistade filtreringssystemet innebär att det måste göras en systematisk undersökning av allt innehåll och att det måste ske en insamling och identifiering av IP-adresserna tillhörande de användare som har initierat utskicken av olagligt innehåll på nätet. Dessa adresser utgör skyddade personuppgifter eftersom de gör det möjligt att exakt identifiera användarna (punkt 51). Det är vidare utrett att föreläggandet riskerar att kränka informationsfriheten, eftersom det finns en risk för att systemet inte gör en tillräckligt tydlig åtskillnad mellan lagligt och olagligt innehåll, med följden att införandet av systemet kan leda till blockering av meddelanden med lagligt innehåll. Det är nämligen ostridigt att frågan huruvida en överföring är laglig också beror på tillämpningen av lagstadgade undantag från upphovsrätten, vilka varierar från en medlemsstat till en annan. Det är dessutom möjligt att vissa verk inte är skyddade av upphovsrätt i vissa medlemsstater, eller att de berörda upphovsrättsmännen har lagt ut dem på internet för gratis användning (punkt 52).

Följaktligen slog domstolen fast att den nationella domstolen, genom att utfärda ett föreläggande enligt vilket internetleverantören Scarlet blir skyldig att införa det omtvistade filtreringssystemet, inte uppfyller kravet på att se till att avvägningen är rimlig mellan immaterialrätten å ena sidan och näringsfriheten, rätten till skydd av personuppgifter och friheten att ta emot och sprida uppgifter å andra sidan (punkt 53).

Dom av den 19 april 2012, Bonnier Audio m.fl. (C-461/10, EU:C:2012:219)

Högsta domstolen (Sverige) begärde förhandsavgörande från domstolen rörande tolkningen av direktiv 2002/58 och direktiv 2004/48 i ett mål mellan, å ena sidan, Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB och Storyside AB (nedan kallade Bonnier Audio m.fl.) och, å andra sidan, Perfect Communication Sweden AB (nedan kallat ePhone) angående ePhones bestridande av ett yrkande om informationsföreläggande, framställt av Bonnier Audio m.fl.

Bonnier Audio m.fl. var förlag och innehade bland annat ensamrätt att ge ut 27 verk i ljudboksformat, att framställa exemplar av verken samt att göra verken tillgängliga för allmänheten. Bonnier Audio m.fl. gjorde gällande att någon hade gjort intrång i deras ensamrätt genom att dessa 27 verk utan deras samtycke hade överförts till allmänheten genom en FTP-server (”file transfer protocol”), vilken möjliggjorde överföring av filer mellan datorer via internet. Bonnier Audio m.fl. ansökte vid svensk domstol om informationsföreläggande och yrkade att namn på och adress till den som registrerats som användare av den IP-adress varifrån de aktuella filerna antogs ha överförts skulle lämnas ut.

Beslutet överklagades till Högsta domstolen, som frågade EU-domstolen huruvida unionsrätten utgör hinder för tillämpningen av en nationell bestämmelse som är införd med stöd av artikel 8 i direktiv 2004/48 och som innebär att en internetleverantör i en civilprocess, i syfte att en viss

abonnent ska kunna identifieras, föreläggs att ge en upphovsrättsinnehavare eller dennes rättsinnehavare information om vilken abonnent som av internetleverantören tilldelats en viss IP-adress, från vilken adress intrång påstås ha skett. En förutsättning för frågan var att sökanden visat sannolika skäl för intrång i viss upphovsrätt och att åtgärden var proportionell.

Domstolen erinrade inledningsvis om att artikel 8.3 i direktiv 2004/48 jämförd med artikel 15.1 i direktiv 2002/58 inte hindrar att medlemsstaterna föreskriver en skyldighet att lämna ut personuppgifter till enskilda för att dessa ska kunna väcka talan i tvistemål angående upphovsrättsintrång, men att dessa bestämmelser inte heller ålägger medlemsstaterna att föreskriva en sådan skyldighet. Myndigheterna och domstolarna i medlemsstaterna ska emellertid inte bara tolka sin nationella lagstiftning på ett sätt som står i överensstämmelse med direktiven, utan även se till att de inte tolkar den på ett sätt som strider mot grundläggande rättigheter eller allmänna gemenskapsrättsliga principer, såsom proportionalitetsprincipen (punkterna 55 och 56).

I detta avseende konstaterade domstolen att enligt den nationella lagstiftningen krävdes för ett föreläggande att lämna ut uppgifterna i fråga bland annat att det förelåg sannolika skäl för immaterialrättsintrång, att den begärda informationen kunde antas underlätta utredningen av ett upphovsrättsintrång eller en överträdelse avseende en sådan rättighet och att skälen för åtgärden uppvägde den olägenhet eller det men i övrigt som åtgärden innebar för den som drabbades av den eller för något annat motstående intresse (punkt 58).

Följaktligen slog domstolen fast att direktiven 2002/58 och 2004/48 inte utgör hinder för en nationell lagstiftning såsom den som är i fråga i det nationella målet, då lagstiftningen gör det möjligt för en nationell domstol, som mottagit en begäran om föreläggande att lämna ut personuppgifter från en enskild som har talerätt, att göra en avvägning mellan de motstående intressen som föreligger, med beaktande av omständigheterna i det enskilda fallet och med tillbörlig hänsyn till de krav som följer av proportionalitetsprincipen (punkt 61 samt domslutet).

Dom av den 17 juni 2021, M.I.C.M. (C-597/19, EU:C:2021:492)

Företaget Mircom International Content Management & Consulting (M.I.C.M.) Limited (nedan kallat Mircom) framställde en begäran om information från internetleverantören Telenet BVBA vid Ondernemingsrechtbank Antwerpen (Näringsdomstolen i Antwerpen, Belgien). Syftet med ansökan var att Telenet skulle förpliktas att lämna ut identifieringsuppgifter för sina kunder på grundval av ip-adresser som samlats in av ett specialiserat företag för Mircoms räkning. Internetanslutningarna för Telenets kunder användes för att dela filmer som ingick i Mircoms katalog via ett peer-to-peer-nätverk med hjälp av Bittorrent-protokollet. Telenet bestred Mircoms begäran.

Det var mot denna bakgrund som den hänskjutande domstolen frågade EU-domstolen om delning av fragment av en mediefil som innehåller ett skyddat verk via nämnda nätverk utgör en överföring till allmänheten enligt unionsrätten. Den hänskjutande domstolen önskade vidare få klarlagt om en innehavare av immateriella rättigheter såsom Mircom, som inte själv använder dessa rättigheter men kräver skadestånd från påstådda intrångsgörare, kan dra nytta av de

åtgärder, förfaranden och sanktioner som föreskrivs i unionsrätten för att säkerställa att rättigheterna iakttas, exempelvis genom att begära information. Slutligen bad den hänskjutande domstolen EU-domstolen att klargöra huruvida det sätt som Mircom samlat in kundernas ip-adresser på var lagligt liksom om det var tillåtet att lämna ut de uppgifter som Mircom begärt av Telenet.

EU-domstolen slog fast att unionsrätten[64] i princip inte utgör hinder vare sig för en systematisk registrering, av innehavaren av immateriella rättigheter eller av en tredje part för dennes räkning, av ip-adresser till användare av peer-to-peer-nätverk vilkas internetuppkopplingar påstås ha använts i intrångsgörande verksamhet (behandling av uppgifter i tidigare led), eller för överföring av användarnas namn och postadresser till denna rättsinnehavare eller till en tredje part för en senare ersättningstalan (behandling av uppgifter i kommande led). Initiativ och begäran i detta avseende ska emellertid vara berättigade och proportionella och får inte utgöra missbruk, och de ska regleras i nationell lagstiftning som begränsar räckvidden av de rättigheter och skyldigheter som omfattas av unionsrätten. Domstolen preciserade att unionsrätten inte föreskriver någon skyldighet för ett sådant bolag som Telenet att lämna ut personuppgifter till enskilda för att de ska kunna väcka talan i tvistemål om upphovsrättsintrång. Unionsrätten medger emellertid att medlemsstaterna inför en sådan skyldighet (punkterna 97 och 125–127 samt punkt 3 i domslutet).

3. Borttagande av länkar till personuppgifter

Dom av den 24 september 2019 (stora avdelningen), GC m.fl. (Borttagande av länkar till känsliga uppgifter) (C-136/17, EU:C:2019:773)[65]

I denna dom preciserade domstolen (stora avdelningen) vilka skyldigheter en sökmotorleverantör har vid en begäran om borttagande av länkar till känsliga uppgifter.

Google hade vägrat att bifalla fyra personers begäran om att, från den lista över sökresultat som visas av sökmotorn efter en sökning på personernas respektive namn, ta bort olika länkar som ledde till webbsidor publicerade av tredje man, med bland annat tidningsartiklar. De fyra personerna gav in klagomål till Commission nationale de l'informatique et des libertés (CNIL) (Frankrike), som dock inte ålade Google att ta bort länkarna i fråga. Efter överklagande till Conseil d'État (Högsta förvaltningsdomstolen, Frankrike) begärde den domstolen att EU-domstolen skulle precisera vilka skyldigheter som åligger en sökmotorleverantör vid en begäran om borttagande enligt direktiv 95/46.

EU-domstolen erinrade för det första om att behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt uppgifter som rör hälsa och sexualliv är förbjuden,[66] med vissa undantag. När det gäller behandling av uppgifter om lagöverträdelser, brottmålsdomar eller säkerhetsåtgärder

64 Artikel 6.1 f i dataskyddsförordningen och artikel 15.1 i direktiv 2002/58.
65 En redogörelse för domen finns i årsrapporten för år 2019, s. 117 och 118.
66 Artikel 8.1 i direktiv 95/46 och artikel 9.1 i förordning 2016/679.

kan den i princip endast utföras under kontroll av en myndighet eller om lämpliga och specifika garantier föreskrivs i nationell rätt[67] (punkterna 39 och 40).

Domstolen har slagit fast att förbudet mot och begränsningarna av behandlingen av dessa särskilda kategorier av uppgifter är tillämpliga på en sökmotorleverantör i likhet med alla andra ansvariga för behandling av personuppgifter. Syftet med dessa förbud och begränsningar är nämligen att säkerställa ett utökat skydd mot sådan behandling som, på grund av att uppgifterna är särskilt känsliga, kan utgöra ett särskilt allvarligt ingrepp i den grundläggande rätten till respekt för privatlivet och skydd av personuppgifter (punkterna 42–44).

Sökmotorleverantören är emellertid inte ansvarig för den omständigheten att personuppgifter återfinns på en webbsida som publicerats av tredje man, utan för hänvisningen till den sidan. Förbudet mot och begränsningarna av behandlingen av känsliga uppgifter gäller således endast sökmotorleverantören vad beträffar hänvisningen, och därmed i samband med den prövning som sökmotorleverantören, under tillsyn av behöriga nationella myndigheter, gör när den har mottagit en begäran från den berörda personen (punkterna 46 och 47).

För det andra har domstolen slagit fast att när en sökmotorleverantör har mottagit en begäran om borttagande som avser känsliga uppgifter är denne, med vissa undantag, i princip skyldig att efterkomma denna begäran. När det gäller dessa undantag kan sökmotorleverantören bland annat vägra att efterkomma en sådan begäran när denne konstaterar att länkarna leder till uppgifter som offentliggjorts av den berörda personen själv,[68] förutsatt att hänvisningen till länkarna uppfyller övriga villkor för att behandling av personuppgifter ska vara tillåten och såvida inte personen i fråga av skäl som hänför sig till hans eller hennes specifika situation har rätt att göra invändningar mot hänvisningen[69] (punkterna 65 och 69).

I alla händelser ska en sökmotorleverantör som mottar en begäran om borttagande pröva om det är strikt nödvändigt att inkludera en länk till en webbsida med känsliga uppgifter som redovisas efter en sökning på den registrerades namn för att skydda informationsfriheten för de internetanvändare som eventuellt är intresserade av att få tillgång till den webbsidan genom en sådan sökning. Domstolen har betonat att även om rätten till respekt för privatlivet och skydd av personuppgifter i allmänhet har företräde framför internetanvändarnas informationsfrihet, kan denna avvägning i det enskilda fallet vara beroende av uppgifternas art och hur känsliga de är beträffande den berörda personens privatliv samt allmänhetens intresse av att få tillgång till denna information, vilket kan variera bland annat med hänsyn till personens roll i det offentliga livet (punkterna 66 och 68).

För det tredje har domstolen slagit fast att det vid en begäran om borttagande av länkar till uppgifter om ett straffrättsligt förfarande mot den berörda personen, som hänför sig till ett tidigare skede i förfarandet och inte längre motsvarar den aktuella situationen, ankommer på sökmotorleverantören att bedöma om nämnda person, med beaktande av samtliga omständigheter i det enskilda fallet, har rätt att kräva att uppgifterna i det aktuella skedet inte längre kopplas till dennes namn genom en lista över sökresultat som visas efter en sökning på

67 Artikel 8.5 i direktiv 95/46 och artikel 10 i förordning 2016/679.
68 Artikel 8.2 e i direktiv 95/46 och artikel 9.2 e i förordning 2016/679.
69 Artikel 14 första stycket a i direktiv 95/46 och artikel 21.1 i förordning 2016/679.

dennes namn. Även om så inte skulle vara fallet, av den anledningen att det är strikt nödvändigt att inkludera länken för att förena rätten till respekt för privatlivet och till skydd för den registrerades personuppgifter med eventuellt intresserade internetanvändares informationsfrihet, måste sökmotorleverantören i alla händelser, senast i samband med begäran om borttagande av länkar, ordna listan över sökresultat på ett sådant sätt att det helhetsintryck som listan ger internetanvändarna återspeglar den aktuella rättsliga situationen, vilket bland annat fordrar att länkar till webbsidor med information om detta redovisas överst på listan (punkterna 77 och 78).

Dom av den 24 september 2019 (stora avdelningen), Google (Territoriell räckvidd för rätten till borttagande av länkar) (C-507/17, EU:C:2019:772)[70]

Commission nationale de l'Informatique et des Libertés (CNIL) (Frankrike) utfärdade ett föreläggande mot Google. Föreläggandet innebar att när en person har begärt att länkar till vissa webbsidor som innehåller personuppgifter om honom eller henne ska tas bort från den träfflista som visas vid en sökning på personens namn, och Google efterkommer denna begäran, så är bolaget skyldigt att se till att länkarna tas bort oavsett vilken toppdomän som har använts vid sökningen i Googles sökmotor. Efter Googles vägran att rätta sig efter föreläggandet beslutade CNIL att påföra bolaget en sanktionsavgift om 100 000 euro. Google överklagade beslutet till Conseil d'État, som ansökte om att EU-domstolen närmare skulle precisera den territoriella räckvidden för sökmotorleverantörens skyldighet att genomföra rätten till borttagande av länkar med tillämpningen av direktiv 95/46.

Först och främst erinrade EU-domstolen om att fysiska personer har möjlighet att med stöd av unionsrätten göra gällande sin rätt till borttagande av länkar mot en sökmotorleverantör som förfogar över ett eller flera verksamhetsställen inom unionen oavsett om behandlingen av personuppgifter (i det aktuella fallet länkningen till webbsidor som innehåller personuppgifter om den person som gör denna rätt gällande) utförs inom unionen eller inte.[71]

När det gäller räckvidden för rätten till borttagande av länkar fann domstolen att sökmotorleverantörens skyldighet att ta bort länkarna inte omfattar samtliga versioner av dess sökmotor, men däremot samtliga de versioner av sökmotorn som motsvarar medlemsstaternas landsdomäner. Domstolen framhöll i detta avseende att ett universellt borttagande visserligen, med hänsyn till internets och sökmotorernas egenskaper, kan leda till att unionslagstiftarens syfte att säkerställa en hög skyddsnivå för personuppgifter i hela unionen uppfylls. Det framgår dock inte på något sätt av unionsrätten[72] att lagstiftaren, i syfte att säkerställa att detta syfte uppfylls, skulle ha valt att tillerkänna rätten till borttagande av länkar räckvidd utöver medlemsstaternas territorier. Domstolen angav särskilt att medan unionsrätten har inrättat mekanismer för samarbete mellan medlemsstaternas tillsynsmyndigheter för att dessa ska kunna nå fram till ett gemensamt beslut, grundat på en avvägning mellan å ena sidan rätten till respekt för privatlivet och till skydd av personuppgifter och å andra sidan det intresse som allmänheten i olika medlemsstater har av att få tillgång till viss information, så är några sådana

70 En redogörelse för domen finns i årsrapporten för år 2019, s. 118 och 119.
71 Artikel 4.1 a i direktiv 95/46 och artikel 3.1 i förordning 2016/679.
72 Artiklarna 12 b och 14 första stycket a i direktiv 95/46 och artikel 17.1 i förordning 2016/679.

mekanismer i nuläget inte planerade vad gäller borttagande av länkar utanför unionen (punkterna 62 och 73).

Den skyldighet att ta bort länkar som sökmotorleverantören har enligt unionsrätten omfattar i nuläget inte endast den version av sökmotorn som motsvarar landsdomänen för den medlemsstat där den person som har rätt till borttagandet av länkar är bosatt, utan samtliga versioner som motsvarar medlemsstaternas landsdomäner. Syftet med detta är bland annat att säkra en enhetlig och hög skyddsnivå i hela unionen. Dessutom åligger det sökmotorleverantören att vid behov vidta åtgärder som är tillräckligt effektiva för att hindra, eller åtminstone i betydande utsträckning avhålla, unionens internetanvändare från att, i förekommande fall med användning av en version av sökmotorn som motsvarar landsdomänen för en stat utanför unionen, skaffa sig tillgång till de länkar som borttagandet avser, och det ankommer på den nationella domstolen att pröva huruvida de åtgärder som vidtagits av sökmotorleverantören uppfyller detta krav (punkt 70).

Slutligen underströk EU-domstolen att även om unionsrätten inte kräver att ett borttagande av länkar ska omfatta samtliga versioner av sökmotorn, så innehåller den inte heller något förbud mot detta. Medlemsstaternas myndigheter och domstolar förblir således behöriga att tillämpa de nationella normerna för skydd av grundläggande rättigheter för att göra en avvägning mellan å ena sidan den registrerades rätt till respekt för sitt privatliv och till skydd av personuppgifter som rör honom eller henne, och å andra sidan rätten till informationsfrihet, och de behåller sin behörighet att efter denna avvägning, i förekommande fall, förelägga sökmotorleverantören att ta bort länkarna från samtliga versioner av sökmotorn (punkterna 65 och 72).

4. Samtycke från användaren av en webbplats till lagring av information

Dom av den 1 oktober 2019 (stora avdelningen), Planet49 (C-673/17, EU:C:2019:801)[73]

Domstolen slog i denna dom fast att samtycket till lagring av information eller tillgång till information genom kakor som redan är lagrade i webbplatsanvändarens terminalutrustning inte är giltigt när samtycket är resultatet av en på förhand ikryssad ruta, och detta oberoende av om informationen i fråga utgör personuppgifter eller inte. Domstolen har dessutom slagit fast att tjänsteleverantören ska upplysa webbplatsanvändaren om kakornas funktionstid samt om möjligheten för tredje part att få tillgång till dessa kakor.

Det nationella målet avsåg en reklamtävling som anordnats av Planet49 på webbplatsen www.dein-macbook.de. De internetanvändare som önskade delta behövde uppge namn och adress på en webbsida med kryssrutor. Den ruta som tillåter installationen av kakor hade kryssats i på förhand. Bundesgerichtshof (Federala högsta domstolen, Tyskland), vid vilken talan hade väckts av den tyska sammanslutningen av konsumentskyddsorganisationer, hyste tvivel om huruvida ett samtycke som en användare lämnar genom den på förhand ikryssade rutan var giltigt, samt omfattningen av den informationsskyldighet som åligger tjänsteleverantören.

Begäran om förhandsavgörande avsåg i huvudsak tolkningen av begreppet samtycke i direktiv 2002/58,[74] jämförd med direktiv 95/46,[75] och med dataskyddsförordningen.[76]

För det första påpekade domstolen att artikel 2 h i direktiv 95/46, till vilket artikel 2 f i direktiv 2002/58 hänvisar, definierar samtycke som ”varje slag av frivillig, särskild och informerad viljeyttring genom vilken den registrerade godtar behandling av personuppgifter som rör honom”. Domstolen påpekade att kravet på att den berörda personen ska avge en ”viljeyttring” tydligt pekar på ett aktivt och inte ett passivt beteende. Ett samtycke som lämnas genom en på förhand ikryssad ruta innebär emellertid inte något aktivt beteende från webbplatsanvändarens sida. Vidare tyder förberedelsearbetet inför antagandet av artikel 5.3 i direktiv 2002/58 – som sedan ändringen genom direktiv 2009/136 föreskriver att användaren ska ha ”gett sitt samtycke” till lagringen av kakor – på att användarens samtycke inte längre kan presumeras utan måste följa av användarens aktiva beteende. Slutligen föreskrivs ett aktivt samtycke i dataskyddsförordningen,[77] där det i artikel 4 led 11 krävs en viljeyttring i form av bland annat ”en entydig bekräftande handling” och där skäl 32 i denna förordning uttryckligen anger att ”[t]ystnad, på förhand ikryssade rutor eller inaktivitet” inte bör utgöra samtycke (punkterna 49, 52, 56 och 62).

Domstolen har således slagit fast att ett samtycke inte är giltigt om lagring av information eller tillgång till information som redan är lagrad i en webbplatsanvändares terminalutrustning tillåts genom en på förhand ikryssad ruta som användaren måste avmarkera för att vägra samtycke.

73 En redogörelse för domen finns i årsrapporten för år 2019, s. 120 och 121.

74 Artiklarna 2 f och 5.3 i direktiv 2002/58, i dess lydelse enligt Europaparlamentets och rådets direktiv 2009/136/EG av den 25 november 2009 (EUT L 337, 2009, s. 11).

75 Artikel 2h i direktiv 95/46.

76 Artikel 6.1 a i förordning 2016/679.

77 Se ovan.

Domstolen tillägger att det inte är tillräckligt att en sådan användare trycker på knappen för att delta i den aktuella pristävlingen för att det ska anses att användaren har lämnat ett giltigt samtycke till lagring av kakor (punkt 63).

För det andra har domstolen slagit fast att artikel 5.3 i direktiv 2002/58 har till syfte att skydda användaren från intrång i dennes privatliv, oavsett om intrånget rör personuppgifter eller inte. Av detta följer att begreppet samtycke inte ska tolkas olika beroende på om den lagrade eller hämtade informationen i webbplatsanvändarens terminalutrustning utgör personuppgifter eller inte (punkterna 69 och 71).

För det tredje påpekade domstolen att artikel 5.3 i direktiv 2002/58 kräver att användaren har lämnat sitt samtycke efter att ha fått tillgång till tydlig och fullständig information, bland annat om ändamålet med behandlingen av uppgifterna. Tydlig och fullständig information innebär att en användare enkelt måste kunna avgöra följderna av ett eventuellt samtycke och säkerställa att ett välgrundat samtycke lämnas. Domstolen har i detta avseende slagit fast att information om kakornas funktionstid och om huruvida tredje parter ges tillgång till kakorna eller inte utgör en del av den tydliga och fullständiga information som tjänsteleverantören ska lämna till webbplatsanvändaren (punkterna 73–75 och 81).

VI. Nationella tillsynsmyndigheter

1. Innebörden av kravet på oberoende

Dom av den 9 mars 2010 (stora avdelningen), kommissionen/Tyskland (C-518/07, EU:C:2010:125)[78]

Europeiska kommissionen hade yrkat att domstolen skulle fastställa att Förbundsrepubliken Tyskland hade underlåtit att uppfylla sina skyldigheter enligt artikel 28.1 andra stycket i direktiv 95/46 genom att ställa de tillsynsmyndigheter som är behöriga i fråga om övervakning av behandling av personuppgifter inom den icke-offentliga sektorn i de olika delstaterna under statlig kontroll och genom att således inte korrekt genomföra kravet på att de myndigheter som har till uppgift att säkerställa skyddet av sådana uppgifter ska vara ”fullständigt oberoende”.

Förbundsrepubliken Tyskland ansåg att det enligt artikel 28.1 andra stycket i direktiv 95/46 krävs att tillsynsmyndigheterna är verksamhetsmässigt oberoende, i den meningen att myndigheterna ska vara oberoende i förhållande till den icke-offentliga sektor som är föremål för deras tillsyn, och att de inte får vara utsatta för påverkan utifrån. Enligt Förbundsrepubliken Tyskland utgör inte den statliga kontroll som utövas i de tyska delstaterna en sådan påverkan utifrån, utan en form av intern kontroll inom förvaltningen, som utförs av myndigheter som hör till samma förvaltning som tillsynsmyndigheterna och som, precis som tillsynsmyndigheterna, är skyldiga att genomföra de mål som eftersträvas med direktiv 95/46.

78 En redogörelse för domen finns i årsrapporten för år 2010, s. 34.

Domstolen slog fast att den garanti för de nationella tillsynsmyndigheternas oberoende som föreskrivs i direktiv 95/46 är avsedd att säkerställa en effektiv och tillförlitlig övervakning av att bestämmelserna om skydd för enskilda personer med avseende på behandling av personuppgifter följs, och den ska tolkas mot bakgrund av det syftet. Garantin har inte införts för att dessa myndigheter själva och deras ombud ska ges en särskild ställning, utan för att förstärka skyddet av de personer och organ som berörs av deras beslut. Av detta följer att tillsynsmyndigheterna, i utövandet av sina uppgifter, måste handla objektivt och opartiskt (punkt 25).

Domstolen slog fast att de tillsynsmyndigheter som är behöriga i fråga om övervakning av behandling av personuppgifter inom den icke-offentliga sektorn måste åtnjuta ett sådant oberoende att de kan utöva sina uppgifter utan påverkan utifrån. Detta oberoende utesluter inte bara all påverkan från de organ som är föremål för övervakning utan också varje åläggande eller all annan påverkan utifrån, direkt eller indirekt, som kan hindra nämnda myndigheter från att fullgöra sin uppgift att säkerställa en riktig avvägning mellan skyddet för rätten till privatliv och ett fritt flöde av personuppgifter. Risken för att kontrollmyndigheter kan påverka tillsynsmyndigheternas beslut i politiskt hänseende är i sig tillräcklig för att hindra tillsynsmyndigheterna från att utöva sina uppgifter på ett oberoende sätt. För det första kan dessa myndigheter visa en ”föregripande hörsamhet” med hänsyn till kontrollmyndighetens beslutspraxis. För det andra förutsätter den roll som väktare av rätten till privatliv som nämnda tillsynsmyndigheter har, att deras beslut, och följaktligen de själva, är höjda över varje misstanke om partiskhet. Domstolen fann att statlig kontroll över de nationella tillsynsorganen därför inte är förenlig med kravet på oberoende (punkterna 30, 36 och 37 samt domslutet).

Dom av den 16 oktober 2012 (stora avdelningen), kommissionen/Österrike (C-614/10, EU:C:2012:631)

Europeiska kommissionen yrkade att domstolen skulle fastställa att Republiken Österrike hade underlåtit att uppfylla sina skyldigheter enligt artikel 28.1 andra stycket i direktiv 95/46 genom att inte vidta alla nödvändiga åtgärder för att den i Österrike gällande lagstiftningen skulle uppfylla kravet på oberoende när det gäller Datenschutzkommission (kommissionen för skydd av uppgifter), vilken inrättats som tillsynsmyndighet för skyddet av personuppgifter.

Domstolen slog fast att Österrike hade gjort sig skyldigt till ett fördragsbrott med anledning av att den österrikiska lagstiftningen inte uppfyller det krav på oberoende som uppställs i direktiv 95/46 avseende tillsynsmyndigheten, eftersom tillsynsmyndighetens administrativa ledamot är en federal tjänsteman som står under sin arbetsgivares överinseende, tillsynsmyndighetens kansli är integrerat i förbundskanslerns kansli och förbundskanslern har en ovillkorlig rätt till upplysningar rörande samtliga aspekter av tillsynsmyndighetens administration.

Domstolen erinrade inledningsvis om att begreppet ”fullständigt oberoende” i artikel 28.1 andra stycket i direktiv 95/46 innebär att tillsynsmyndigheterna ska åtnjuta ett sådant oberoende att de kan utöva sina uppgifter utan påverkan utifrån. Den omständigheten att en sådan myndighet är funktionellt oberoende på så sätt att dess ledamöter är oberoende och inte bundna av några instruktioner vid utövandet av sitt uppdrag är inte i sig tillräckligt för att skydda myndigheten från externt inflytande. Det oberoende som krävs i detta sammanhang syftar nämligen till att utesluta inte bara direkt påverkan i form av instruktioner utan även varje form av indirekt påverkan som kan styra tillsynsmyndighetens beslutsfattande. Dessutom förutsätter den roll

som väktare av rätten till privatliv som tillsynsmyndigheterna har att deras beslut, och följaktligen de själva, är höjda över varje misstanke om partiskhet (punkterna 41–43 och 52).

Domstolen har klargjort att för att kunna uppfylla det krav på oberoende som anges i nämnda bestämmelse i direktiv 95/46 behöver en nationell tillsynsmyndighet inte ha en särskild budgetpost, motsvarande vad som föreskrivs i artikel 43.3 i förordning (EG) nr 45/2001. Medlemsstaterna är inte skyldiga att införa bestämmelser motsvarande dem i kapitel V i förordning nr 45/2001 i sin nationella lagstiftning för att säkerställa fullständigt oberoende för sin(a) tillsynsmyndighet(er) och kan således föreskriva, budgeträttsligt sett, att tillsynsmyndigheten sorterar under ett visst ministerium. Det förhållandet att en sådan myndighet förses med nödvändig personal och utrustning får dock inte hindra den från att utöva sina uppgifter ”fullständigt oberoende” i den mening som avses i artikel 28.1 andra stycket i direktiv 95/46 (punkt 58).

Dom av den 8 april 2014 (stora avdelningen), kommissionen/Ungern (C-288/12, EU:C:2014:237)[79]

I detta mål yrkade kommissionen att domstolen skulle fastställa att Ungern hade underlåtit att uppfylla sina skyldigheter enligt direktiv 95/46 genom att avsluta mandatet för datatillsynsmyndigheten i förtid.

Domstolen slog fast att en medlemsstat som avslutar mandatet för datatillsynsmyndigheten i förtid underlåter att uppfylla sina skyldigheter enligt direktiv 95/46 (punkt 62 samt punkt 1 i domslutet).

Det oberoende som de tillsynsmyndigheter som är behöriga i fråga om övervakning av behandling av personuppgifter ska åtnjuta utesluter nämligen bland annat varje åläggande eller all annan påverkan utifrån, direkt eller indirekt, som kan inverka på deras beslutsfattande och som kan hindra nämnda myndigheter från att fullgöra sin uppgift att säkerställa en riktig avvägning mellan skyddet för rätten till privatliv och ett fritt flöde av personuppgifter (punkt 51).

Domstolen erinrade dessutom om att ett funktionellt oberoende inte i sig är tillräckligt för att tillsynsmyndigheterna ska vara skyddade från varje påverkan utifrån. Risken för att medlemsstatens kontrollmyndigheter kan påverka tillsynsmyndigheternas beslut i politiskt hänseende räcker för att hindra tillsynsmyndigheterna från att utöva sina uppgifter på ett oberoende sätt. Om medlemsstaterna kunde avsluta en tillsynsmyndighets mandat före utgången av den ursprungligen föreskrivna mandattiden utan att iaktta de bestämmelser och skyddsregler som i detta syfte föreskrivits i tillämplig lagstiftning, skulle den risk för att mandatet ska avslutas i förtid som skulle hänga över tillsynsmyndigheten under hela mandattiden kunna leda till ett slags hörsamhet från myndighetens sida gentemot den politiska makten som vore oförenlig med kravet på oberoende. I en sådan situation kan tillsynsmyndigheten inte heller anses kunna stå över varje misstanke om partiskhet (punkterna 52–55).

79 En redogörelse för domen finns i årsrapporten för år 2014, s. 62.

2. Fastställande av tillämplig lag och av behörig tillsynsmyndighet

Dom av den 1 oktober 2015, Weltimmo (C-230/14, EU:C:2015:639)[80]

Nemzeti Adatvédelmi és Információszabadság Hatóság (den nationella myndigheten för uppgiftsskydd och informationsfrihet, Ungern) påförde Weltimmo, som är ett bolag som är registrerat i Slovakien och som driver webbplatser för fastighetsannonser som avser egendom belägen i Ungern, böter med motiveringen att Weltimmo inte hade raderat annonsörernas personuppgifter från dessa webbplatser, trots att annonsörerna begärt detta, och hade lämnat sådana uppgifter till inkassoföretag i syfte att erhålla betalning för obetalda fakturor. Enligt den ungerska tillsynsmyndigheten hade bolaget Weltimmo därigenom brutit mot den ungerska lagstiftning som införlivar direktiv 95/46.

Kúria (Högsta domstolen, Ungern), vid vilken ett överklagande anhängiggjorts, ansåg det vara oklart hur tillämplig lag skulle fastställas och hur det ska fastställas vilken behörighet den ungerska tillsynsmyndigheten har mot bakgrund av artiklarna 4.1 och 28 i direktiv 95/46. Med anledning av detta ställde Kúria (Högsta domstolen) flera tolkningsfrågor till domstolen.

När det gäller tillämplig nationell rätt slog domstolen fast att artikel 4.1 a i direktiv 95/46 ska tolkas så, att lagstiftning om skydd av personuppgifter i en annan medlemsstat än den där den personuppgiftsansvarige är registrerad får tillämpas under förutsättning att den personuppgiftsansvarige utövar verklig och faktisk verksamhet – även om verksamheten är ytterst liten – i den medlemsstaten med hjälp av en stabil struktur och att den aktuella behandlingen utförs som ett led i verksamheten. För att avgöra om detta är fallet får den nationella domstolen beakta att den personuppgiftsansvariges verksamhet, i vilken behandlingen av uppgifter utförs som ett led, består i drift av webbplatser med fastighetsannonser vilka avser fast egendom belägen i den medlemsstaten och vilka är avfattade på den medlemsstatens språk och att verksamheten således huvudsakligen eller fullständigt riktar sig mot den medlemsstaten. Den nationella domstolen får även beakta att den personuppgiftsansvarige har en företrädare i den medlemsstaten som har ansvar för att driva in fordringar med anledning av verksamheten och för att företräda den personuppgiftsansvarige i administrativa förfaranden och domstolsförfaranden beträffande behandlingen av de aktuella uppgifterna. Frågan om vilket land de personer som berörs av behandlingen av uppgifter är medborgare i saknar däremot betydelse (punkt 41 samt punkt 1 i domslutet).

När det gäller behörighet och befogenheter för den tillsynsmyndighet som tar emot klagomål i enlighet med artikel 28.4 i direktiv 95/46, ansåg domstolen att denna myndighet kan pröva dessa klagomål oavsett vilken nationell lagstiftning som är tillämplig och innan den ens vet vilken nationell lagstiftning som är tillämplig på den aktuella behandlingen (punkt 54). Om den emellertid finner att en annan medlemsstats rättsordning är tillämplig kan den inte vidta sanktionsåtgärder utanför sin egen medlemsstat. Under sådana förhållanden ska den i enlighet med skyldigheten att samarbeta enligt artikel 28.6 i samma direktiv, anmoda tillsynsmyndigheten i den andra medlemsstaten att fastställa en eventuell överträdelse av rättsordningen i den staten och vidta sanktionsåtgärder om den rättsordningen tillåter det, i förekommande fall med

80 En redogörelse för domen finns i årsrapporten för år 2015, s. 55.

stöd av de upplysningar som den andra myndigheten har vidarebefordrat (punkterna 57 och 60 samt punkt 2 i domslutet).

3. Nationella tillsynsmyndigheters befogenheter

Dom av den 6 oktober 2015 (stora avdelningen), Schrems (C-362/14, EU:C:2015:650)

I detta mål (se även avsnitt iv, med rubriken ”Överföring av personuppgifter till tredjeland”) slog domstolen bland annat fast att nationella tillsynsmyndigheter har behörighet att kontrollera överföringar av personuppgifter till tredje land.

I detta avseende konstaterade domstolen för det första att de nationella tillsynsmyndigheterna har en rad befogenheter och att dessa, vilka anges på ett icke-uttömmande sätt i artikel 28.3 i direktiv 95/46, utgör nödvändiga resurser för att utöva myndigheternas uppgifter. Således har dessa myndigheter bland annat undersökningsbefogenheter, såsom befogenheten att inhämta alla uppgifter som är nödvändiga för att sköta tillsynen, effektiva befogenheter att ingripa, såsom befogenheten att besluta om tillfälligt eller slutligt förbud mot behandling av uppgifter, och även befogenhet att inleda rättsliga förfaranden (punkt 43).

Vad gäller möjligheten att kontrollera överföringar av personuppgifter till tredjeländer framgår det förvisso av artikel 28.1 och 28.6 i direktiv 95/46 att de nationella tillsynsmyndigheternas befogenheter avser behandling av personuppgifter inom den medlemsstats territorium till vilken dessa myndigheter hör, varför dessa myndigheter inte har några befogenheter, med stöd av denna artikel 28, vad gäller behandling av sådana uppgifter inom ett tredjelands territorium (punkt 44).

Emellertid utgör åtgärden att låta överföra personuppgifter från en medlemsstat till ett tredjeland i sig en behandling av personuppgifter som utförs inom en medlemsstats territorium. Enligt artikel 8.3 i stadgan och artikel 28 i direktiv 95/46 är de nationella tillsynsmyndigheterna ansvariga för kontrollen av efterlevnaden av unionsbestämmelserna om skyddet av enskilda personer med avseende på behandlingen av personuppgifter. Respektive tillsynsmyndighet har således befogenhet att kontrollera huruvida en överföring till ett tredjeland av personuppgifter från den medlemsstat till vilken myndigheten hör uppfyller de krav som följer av detta direktiv (punkterna 45 och 47).

Dom av den 5 juni 2018 (stora avdelningen), Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388)

Domstolen prövade i denna dom (se även avsnitt II.5, med rubriken ”Begreppet ‘personuppgiftsansvarig”), som bland annat rörde tolkningen av artiklarna 4 och 28 i direktiv 95/46, omfattningen av tillsynsmyndigheternas befogenheter att ingripa med avseende på en behandling av personuppgifter som innebär ett deltagande av flera aktörer.

Domstolen fann att när ett företag som är etablerat utanför unionen (såsom det amerikanska bolaget Facebook) har flera etableringsställen i olika medlemsstater, ska tillsynsmyndigheten i en medlemsstat ha rätt att utöva de befogenheter som den tilldelas genom artikel 28.3 i direktivet, i

förhållande till ett av företagets etableringsställen som är beläget i den medlemsstaten (i det aktuella fallet Facebook Germany), trots att detta etableringsställe, enligt fördelningen av uppgifterna inom koncernen, endast ansvarar för försäljning av reklamplats och annan marknadsföring på den medlemsstatens territorium och ansvaret för insamling och behandling av personuppgifter inom hela unionen uteslutande ankommer på ett etableringsställe som är beläget i en annan medlemsstat (i detta fall Facebook Ireland) (punkt 64 samt punkt 2 i domslutet).

Vidare förtydligade domstolen att när tillsynsmyndigheten i en medlemsstat har för avsikt att med avseende på ett organ etablerat i denna medlemsstat utöva de befogenheter att ingripa som avses i artikel 28.3 i direktiv 95/46 på grund av överträdelser av reglerna om skydd av personuppgifter som begåtts av en tredje part som är ansvarig för behandlingen av uppgifterna och som har sitt säte i en annan medlemsstat (i detta fall Facebook Ireland), är denna myndighet behörig att fristående från tillsynsmyndigheten i den sistnämnda medlemsstaten (Irland) bedöma lagenligheten av en sådan behandling av uppgifter, och denna myndighet får utöva sina befogenheter att ingripa mot det organ som är etablerat på dess territorium utan att dessförinnan anmoda tillsynsmyndigheten i den andra medlemsstaten att ingripa (punkt 74 samt punkt 3 i domslutet).

Dom av den 15 juni 2021 (stora avdelningen), Facebook Ireland m.fl. (C-645/19, EU:C:2021:483)

Den 11 september 2015 väckte ordföranden för det belgiska rådet för skydd av privatlivet (nedan kallat skyddsrådet) talan vid Nederlandstalige rechtbank van eerste aanleg Brussel (Nederländskspråkiga förstainstansdomstolen i Bryssel, Belgien) om förbudsföreläggande mot Facebook Ireland, Facebook Inc. och Facebook Belgium, och yrkade att de åsidosättanden av dataskyddslagstiftningen som Facebook påstods ha gjort sig skyldigt till skulle upphöra. Dessa åsidosättanden bestod bland annat i insamling och användning av information om surfvanorna hos de belgiska internetanvändarna, oavsett om dessa var innehavare av ett Facebook-konto eller ej, med hjälp av olika tekniker, såsom kakor, sociala insticksprogram (social plug-ins)[81] och pixlar.

Den 16 februari 2018 förklarade sig nämnda domstol behörig att pröva talan och fann i sak att det sociala nätverket Facebook inte hade informerat de belgiska internetanvändarna tillräckligt om insamlingen och användningen av de berörda uppgifterna. Internetanvändarnas samtycke till insamlingen och behandlingen av uppgifterna ansågs för övrigt vara ogiltigt.

Den 2 mars 2018 överklagade Facebook Ireland, Facebook Inc. och Facebook Belgium domen till Hof van beroep te Brussel (Appellationsdomstolen i Bryssel, Belgien), som är hänskjutande domstol i förevarande mål. Vid den domstolen förde den belgiska dataskyddsmyndigheten (nedan kallad dataskyddsmyndigheten) talan i egenskap av skyddsrådets rättsliga efterträdare. Den hänskjutande domstolen förklarade sig endast vara behörig att pröva överklagandet från Facebook Belgium.

[81] Exempel på detta är knapparna ”Gilla” och ”Dela”.

Den hänskjutande domstolen var osäker på vilken inverkan tillämpningen av systemet med ”en enda kontaktpunkt” enligt dataskyddsförordningen[82] har på dataskyddsmyndighetens behörighet, och undrade särskilt huruvida dataskyddsmyndigheten, vad gäller de faktiska omständigheterna efter den dag då dataskyddsförordningen trädde i kraft, det vill säga den 25 maj 2018, kunde väcka talan mot Facebook Belgium, när det hade konstaterats att det är Facebook Ireland som är ansvarig för behandlingen av de aktuella uppgifterna. Sedan det datumet var det, bland annat i enlighet med principen ”en enda kontaktpunkt” enligt dataskyddsförordningen, endast den irländska dataskyddskommissionären som är behörig att väcka talan om förbudsföreläggande, och endast i irländsk domstol (punkterna 36 och 37).

I sin dom, som meddelades av stora avdelningen, förtydligade EU-domstolen vilka befogenheter de nationella tillsynsmyndigheterna har enligt dataskyddsförordningen. Den slog bland annat fast att förordningen, under vissa villkor, tillåter en nationell tillsynsmyndighet att utöva sin befogenhet att upplysa en domstol i den medlemsstat där myndigheten är belägen om påstådda överträdelser av dataskyddsförordningen och att inleda eller delta i rättsliga förfaranden med avseende på gränsöverskridande uppgiftsbehandling,[83] även om myndigheten inte är ”ansvarig myndighet” för den behandlingen (punkt 1 i domslutet).

Domstolen preciserade för det första på vilka villkor en nationell tillsynsmyndighet, som inte är ansvarig myndighet vad gäller en viss gränsöverskridande behandling, ska utöva sin befogenhet att upplysa en domstol i en medlemsstat om påstådda överträdelser av dataskyddsförordningen och att vid behov inleda eller delta i rättsliga förfaranden, för att verkställa bestämmelserna i nämnda förordning. Det krävs sålunda dels att dataskyddsförordningen ger denna tillsynsmyndighet behörighet att anta ett beslut i vilket det konstateras att behandlingen strider mot förordningens bestämmelser, dels att denna befogenhet utövas med iakttagande av förordningens förfaranden för samarbete och enhetlighet[84] (punkt 75 samt punkt 1 i domslutet).

Det föreskrivs nämligen i dataskyddsförordningen att man för gränsöverskridande behandlingar ska tillämpa ett system med ”en enda kontaktpunkt”[85] som bygger på en behörighetsfördelning mellan en ”ansvarig tillsynsmyndighet” och övriga berörda tillsynsmyndigheter. Detta system kräver ett nära, lojalt och effektivt samarbete mellan dessa myndigheter för att säkerställa en konsekvent och enhetlig tillämpning av bestämmelserna om skydd av personuppgifter och därigenom se till att bestämmelserna ges en ändamålsenlig verkan. I detta hänseende stadgas det i dataskyddsförordningen att det i princip är den ansvariga tillsynsmyndigheten som är behörig att anta ett beslut i vilket det konstateras att en gränsöverskridande behandling strider mot bestämmelserna i denna förordning,[86] medan andra nationella tillsynsmyndigheters behörighet att anta ett sådant beslut, om än ett preliminärt sådant, utgör ett undantag.[87] Den ansvariga tillsynsmyndigheten får vid utövandet av sin behörighet dock inte göra avkall på den oumbärliga dialogen eller det lojala och effektiva samarbetet med de andra berörda

---

82 I artikel 56.1 i dataskyddsförordningen föreskrivs följande: ”Utan att det påverkar tillämpningen av artikel 55 ska tillsynsmyndigheten för den personuppgiftsansvariges eller personuppgiftsbiträdets huvudsakliga verksamhetsställe eller enda verksamhetsställe vara behörig att agera som ansvarig tillsynsmyndighet för den personuppgiftsansvariges eller personuppgiftsbiträdets gränsöverskridande behandling.”

83 I den mening som avses i artikel 4.23 i dataskyddsförordningen.

84 Dessa föreskrivs i artiklarna 56 och 60 i dataskyddsförordningen.

85 Artikel 56.1 i dataskyddsförordningen.

86 Artikel 60.7 i dataskyddsförordningen.

87 I artiklarna 56.2 och 66 i dataskyddsförordningen anges undantagen från principen om den ansvariga tillsynsmyndighetens behörighet att fatta beslut.

tillsynsmyndigheterna. Den ansvariga tillsynsmyndigheten får, inom ramen för detta samarbete, därför inte bortse från de övriga berörda tillsynsmyndigheternas synpunkter, och varje relevant och motiverad invändning från en av dessa myndigheter får till följd att den ansvariga tillsynsmyndighetens antagande av utkastet till beslut hindras, åtminstone tillfälligt (punkterna 50–53, 56–59 och 63–65).

Domstolen preciserade dessutom att det faktum att en tillsynsmyndighet i en medlemsstat som inte är ansvarig tillsynsmyndighet vad gäller en gränsöverskridande uppgiftsbehandling får utöva befogenheten att upplysa en domstol i den medlemsstaten om påstådda överträdelser av dataskyddsförordningen och att inleda eller delta i rättsliga förfaranden endast under förutsättning att den följer reglerna om fördelning av beslutsbefogenheter mellan den ansvariga tillsynsmyndigheten och övriga tillsynsmyndigheter,[88] är förenligt med artiklarna 7, 8 och 47 i stadgan, vilka garanterar den berörda personen rätt till skydd för sina personuppgifter respektive rätt till ett effektivt rättsmedel (punkt 67).

För det andra slog domstolen fast att det för att en tillsynsmyndighet i en medlemsstat som inte är ansvarig tillsynsmyndighet ska ha befogenhet att väcka talan,[89] i ett fall som rör gränsöverskridande behandling av personuppgifter, inte krävs att den personuppgiftsansvarige eller personuppgiftsbiträdet som talan har väckts mot innehar ett huvudsakligt verksamhetsställe eller ett annat verksamhetsställe i den medlemsstat där tillsynsmyndigheten finns. Utövandet av denna befogenhet måste dock omfattas av dataskyddsförordningens territoriella tillämpningsområde,[90] vilket förutsätter att den personuppgiftsansvarige eller personuppgiftsbiträdet, för den gränsöverskridande behandlingen, har ett verksamhetsställe inom unionen (punkterna 80, 83 och 84 samt punkt 2 i domslutet).

För det tredje slog domstolen fast att en tillsynsmyndighet i en medlemsstat som inte är ansvarig tillsynsmyndighet, i ett fall med gränsöverskridande uppgiftsbehandling, vid utövandet av sin befogenhet att upplysa en domstol i den medlemsstaten om påstådda överträdelser av dataskyddsförordningen och att vid behov inleda eller delta i rättsliga förfaranden, får rikta sig mot såväl den personuppgiftsansvariges huvudsakliga verksamhetsställe som är beläget i samma medlemsstat som myndigheten, som mot ett annat av den personuppgiftsansvariges verksamhetsställen, förutsatt att det rättsliga förfarandet avser en uppgiftsbehandling som utförs inom ramen för verksamheten vid det verksamhetsstället, och att myndigheten har rätt att utöva denna befogenhet.

Domstolen preciserade dock att utövandet av denna befogenhet förutsätter att dataskyddsförordningen är tillämplig. I det förevarande fallet, eftersom verksamheten vid Facebook-koncernens verksamhetsställe i Belgien är oupplösligt förbunden med den behandling av personuppgifter som är i fråga i det nationella målet och för vilken Facebook Ireland är ansvarigt när det gäller unionens territorium, ska denna behandling anses utföras ”inom ramen för den verksamhet som bedrivs på personuppgiftsansvarigas … verksamhetsställen”, och

88 Enligt artiklarna 55 och 56, jämförda med artikel 60, i dataskyddsförordningen.

89 Enligt artikel 58.5 i dataskyddsförordningen.

90 Enligt artikel 3.1 i dataskyddsförordningen ska denna förordning tillämpas på behandlingen av personuppgifter ”inom ramen för den verksamhet som bedrivs på personuppgiftsansvarigas eller personuppgiftsbiträdens verksamhetsställen inom unionen, oavsett om behandlingen utförs i unionen eller inte”.

därmed omfattas av dataskyddsförordningens tillämpningsområde (punkterna 94–96 samt punkt 3 i domslutet).

För det fjärde slog domstolen fast att när en tillsynsmyndighet i en medlemsstat, som inte är ansvarig tillsynsmyndighet, före dataskyddsförordningens ikraftträdande har väckt talan vid domstol avseende en gränsöverskridande behandling av personuppgifter, så kan denna talan vidhållas, med stöd av unionsrätten, på grundval av bestämmelserna i direktiv 95/46, som fortsätter att vara tillämpligt på sådana överträdelser av direktivets bestämmelser som begåtts före den dag då det direktivet upphävdes. Dessutom kan denna talan väckas av nämnda myndighet avseende överträdelser som begåtts efter dataskyddsförordningens ikraftträdande, under förutsättning att det sker i en av de situationer där denna förordning, undantagsvis, ger nämnda tillsynsmyndighet befogenhet att anta ett beslut i vilket det konstateras att den aktuella behandlingen av uppgifter strider mot förordningens bestämmelser, och förutsatt att förordningens förfaranden för samarbete och enhetlighet iakttas (punkt 105 samt punkt 4 i domslutet).

För det femte erkände domstolen den direkta effekten av den bestämmelse i dataskyddsförordningen enligt vilken varje medlemsstat i lagstiftning ska fastställa att dess tillsynsmyndighet ska ha befogenhet att upplysa de rättsliga myndigheterna om överträdelser av denna förordning och att vid behov inleda eller delta i rättsliga förfaranden. Följaktligen kan en sådan nationell tillsynsmyndighet åberopa nämnda bestämmelse för att väcka eller återuppta en talan mot enskilda, även om bestämmelsen inte i särskild ordning har genomförts i den berörda medlemsstatens lagstiftning (punkt 113 samt punkt 5 i domslutet).

VII. Territoriell tillämpning av EU:s lagstiftning

Dom av den 13 maj 2014 (stora avdelningen), Google Spain och Google (C-131/12, EU:C:2014:317)

I denna dom (se även avsnitt II.3, med rubriken ”Begreppet behandling av personuppgifter”, och avsnitt V.1, med rubriken ”Rätt att motsätta sig behandling av personuppgifter (”rätten att bli glömd”), uttalade sig domstolen också om det territoriella tillämpningsområdet för direktiv 95/46.

Domstolen slog fast att det utförs en behandling av personuppgifter som ett led i verksamheterna vid ett etableringsställe tillhörande den personuppgiftsansvarige på en medlemsstats territorium, i den mening som avses i direktiv 95/46, när sökmotorleverantören, även när den har sitt säte i en annan medlemsstat, etablerar en filial eller ett dotterbolag i en medlemsstat för att marknadsföra och sälja reklamutrymme hos sökmotorn och filialen eller dotterbolagets verksamhet är riktad mot invånarna i den medlemsstaten (punkterna 55 och 60 samt punkt 2 i domslutet).

Under sådana förhållanden har nämligen sökmotorleverantörens verksamhet och den verksamhet som bedrivs av etableringsstället i den berörda medlemsstaten, även om de är skilda från varandra, ett oupplösligt samband, eftersom verksamheten avseende

reklamutrymme är det som gör sökmotorn ekonomiskt lönsam och sökmotorn är det som gör att verksamheten avseende reklamutrymme kan genomföras (punkt 56).

VIII. Allmänhetens rätt till tillgång till Europeiska unionens institutioners handlingar och skydd av personuppgifter

Dom av den 29 juni 2010 (stora avdelningen), kommissionen/Bavarian Lager (C-28/08 P, EU:C:2010:378)

Bavarian Lager, ett bolag som hade bildats för att importera tyskt öl avsett för utskänkningsställen i Förenade kungariket, kunde inte sälja sina varor, eftersom ett stort antal innehavare av utskänkningsställen i Förenade kungariket var bundna av exklusiva inköpsavtal enligt vilka de var skyldiga att köpa öl från vissa bryggerier.

Enligt Förenade kungarikets bestämmelser om tillhandahållande av öl (nedan kallade GBP) var brittiska bryggerier skyldiga att ge innehavare av pubar möjligheten att köpa öl från ett annat bryggeri förutsatt att det efterjäst på fat. De flesta ölsorter som tillverkas utanför Förenade kungariket kunde emellertid inte anses som ”öl som har efterjäst på fat”, i den mening som avses i GBP. De föll därför inte inom GBP:s tillämpningsområde. Bavarian Lager ansåg att GBP utgjorde en åtgärd med motsvarande verkan som en kvantitativ importrestriktion och framställde därför ett klagomål till kommissionen.

Under det fördragsbrottsförfarande som inletts av kommissionen mot Förenade kungariket hölls ett sammanträde den 11 oktober 1996 vid vilket företrädare för gemenskapsadministrationen, den brittiska administrationen och den europeiska bryggeriorganisationen (BoE) närvarade. Efter att de brittiska myndigheterna hade underrättat kommissionen om en ändring av bestämmelserna i fråga, enligt vilken flasköl skulle kunna säljas som öl från en annan leverantör på samma sätt som fatöl, informerade kommissionen Bavarian Lager att fördragsbrottsförfarandet var vilande.

Bavarian Lager begärde tillgång till hela protokollet från sammanträdet i oktober 1996, med namnen på samtliga deltagare. Kommissionen avslog denna ansökan genom beslut av den 18 mars 2004 med åberopande av bland annat skyddet för privatlivet för dessa personer, såsom dessa garanteras i förordning 45/2001.

Bavarian Lager väckte därefter talan vid tribunalen om ogiltigförklaring av kommissionens beslut. Genom dom av den 8 november 2007 ogiltigförklarade tribunalen kommissionens beslut med motiveringen att enbart den omständigheten att den berörda personens namn förekom i en förteckning över de närvarande vid ett sammanträde, med angivande av den organisation i vars namn och för vars räkning de närvarade vid sammanträdet, varken innebar skada för eller äventyrade skyddet för de berörda personernas privatliv. Kommissionen, med stöd av Förenade kungariket och rådet, överklagade tribunalens dom till domstolen.

Domstolen påpekade inledningsvis att i de fall då en ansökan som grundar sig på förordning nr 1049/2001[91] om allmänhetens tillgång till handlingar syftar till att få tillgång till handlingar som innehåller personuppgifter, blir bestämmelserna i förordning nr 45/2001 tillämpliga i sin helhet, inklusive den bestämmelse enligt vilken mottagaren av en överföring av personuppgifter måste visa att utlämnandet av dem är nödvändigt och den bestämmelse enligt vilken den registrerade ska ha rätt att när som helst, av avgörande och berättigade skäl som rör hans personliga situation, invända mot behandling av uppgifter som rör honom (punkt 63).

Vidare slog domstolen fast att den förteckning över personer som närvarat vid sammanträdet i överträdelseförfarandet, vilken återfinns i protokollet från detta sammanträde, således innehöll personuppgifter i den mening som avses i artikel 2 a i förordning nr 45/2001, eftersom de personer som var närvarande vid sammanträdet därigenom kunde identifieras (punkt 70).

Domstolen slog slutligen fast att kommissionen följde bestämmelserna i artikel 8 b i förordningen när den krävde att sökanden, vad avser de personer som inte hade lämnat sitt uttryckliga samtycke till att personuppgifter som rör dem lämnades ut, visade att det var nödvändigt att dessa personuppgifter lämnades ut (punkt 77).

Om det i samband med en ansökan om tillgång till nämnda protokoll i enlighet med förordning nr 1049/2001, inte lämnats någon uttrycklig och legitim motivering och inte heller anförts något övertygande argument som visar att en överföring av dessa personuppgifter är nödvändig, kan kommissionen nämligen inte göra en avvägning mellan de berörda parternas respektive intressen. Kommissionen kan inte heller kontrollera huruvida det finns skäl att anta att överföringen skulle kunna skada de registrerades legitima intressen enligt artikel 8 b i förordning nr 45/2001 (punkt 78).[92]

Dom av den 16 juli 2015, ClientEarth och PAN Europe/EFSA (C-615/13 P, EU:C:2015:489)

Europeiska myndigheten för livsmedelssäkerhet (Efsa) hade inrättat en arbetsgrupp med uppdrag att utarbeta en vägledning för genomförandet av artikel 8.5 i förordning (EG) nr 1107/2009,[93] i vilken det föreskrivs att sökanden av ett godkännande för utsläppande av växtskyddsmedel på marknaden till dokumentationen ska bifoga expertgranskad (”peer-reviewed”) vetenskaplig litteratur, såsom anvisats av Efsa, om det verksamma ämnet och dess relevanta metaboliter med uppgifter om sidoeffekter på hälsa, miljö och arter som inte är mål för bekämpningen.

Förslaget till vägledning hade varit föremål för offentligt samråd och ClientEarth och Pesticide Action Network Europe (PAN Europe) hade lämnat in kommentarer till förslaget. I detta sammanhang hade de tillsammans gett in en ansökan till Efsa om att få tillgång till ett antal handlingar med anknytning till utarbetandet av utkastet till vägledning, däribland yttrandena från de externa experterna.

---

91 Europaparlamentets och rådets förordning (EG) nr 1049/2001 av den 30 maj 2001 om allmänhetens tillgång till Europaparlamentets, rådets och kommissionens handlingar (EGT L 145, 2001, s. 43).

92 En redogörelse för domen finns i årsrapporten för år 2010, s. 14.

93 Europaparlamentets och rådets förordning (EG) nr 1107/2009 av den 21 oktober 2009 om utsläppande av växtskyddsmedel på marknaden och om upphävande av rådets direktiv 79/117/EEG och 91/414/EEG (EUT L 309, 2009, s. 1).

Efsa beviljade ClientEarth och PAN Europe tillgång till bland annat de enskilda synpunkterna från externa experter angående utkastet till vägledning. Efsa angav emellertid att den hade dolt experternas namn, i enlighet med artikel 4.1 i b i förordning nr 1049/2001 och unionens lagstiftning om skydd av personuppgifter, särskilt förordning nr 45/2001. Efsa gjorde i detta hänseende gällande att ett utlämnande av experternas namn skulle vara att betrakta som en överföring av personuppgifter i den mening som avses i artikel 8 i förordning nr 45/2001 och att villkoren i denna bestämmelse för en sådan överföring inte var uppfyllda.

ClientEarth och PAN Europe väckte talan vid tribunalen om ogiltigförklaring av Efsas beslut. Tribunalen ogillade talan, varefter ClientEarth och PAN Europe överklagade tribunalens dom[94] till domstolen.

Domstolen påpekade för det första att den omständigheten att denna information gjorde det möjligt att knyta ett visst yttrande till en bestämd expert avsåg den en identifierad fysisk person och utgjorde följaktligen en mängd personuppgifter i den mening som avses i artikel 2 a i förordning nr 45/2001. Eftersom begreppen ”personuppgifter” i den mening som avses i artikel 2 a i förordning nr 45/2001 och ”uppgifter avseende privatlivet” inte har samma betydelse, konstaterade domstolen dessutom att ClientEarth och PAN Europes påstående att den omtvistade informationen inte avsåg de berörda experternas privatliv därför var verkningslöst (punkterna 29 och 32).

För det andra prövade domstolen ClientEarth och PAN Europes påstående som grundades dels på att det förelåg ett bristande förtroende gentemot Efsa som ofta anklagats för att vara partisk på grund av att myndigheten anlitat experter med ett personligt intresse som förklaras av deras anknytning till industrin, dels på nödvändigheten att säkerställa öppenhet i myndighetens beslutsprocess. Detta påstående styrktes genom en studie som visade på relationer mellan de flesta sakkunniga medlemmarna i en av Efsas arbetsgrupper och industrins lobbyorganisationer. Mot denna bakgrund ansåg domstolen det nödvändigt att erhålla den omtvistade informationen för att göra det möjligt att konkret kontrollera att var och en av dessa experter utförde sitt vetenskapliga uppdrag för Efsa på ett opartiskt sätt. Domstolen upphävde följaktligen tribunalens dom och fann att tribunalen gjorde fel när den slog fast att de ovannämnda argument som ClientEarth och PAN Europe anfört inte räckte för att styrka att överföring av den omtvistade informationen var nödvändig (punkterna 57–59).

Vid bedömningen av om Efsas omtvistade beslut var lagenligt prövade domstolen om det fanns anledning att anta att de berörda personernas legitima intressen skulle kunna skadas av överföringen. I detta hänseende slog domstolen fast att Efsas påstående att utlämnande av den omtvistade informationen skulle ha riskerat att skada experternas integritet eller privatliv utgör ett allmänt antagande som inte styrks av några andra omständigheter i förevarande fall. Domstolen ansåg tvärtom att ett sådant utlämnande i sig hade gjort det möjligt att skingra de aktuella misstankarna om partiskhet och gett eventuellt berörda experter tillfälle att, i förekommande fall med hjälp av tillgängliga rättsmedel, bestrida att dessa anklagelser om partiskhet var välgrundade. Mot bakgrund av dessa överväganden ogiltigförklarade domstolen Efsas beslut (punkterna 69 och 73).

---

[94] Tribunalens dom av den 13 september 2013, ClientEarth och PAN Europe/Efsa (T-214/11, EU:T:2013:483).

* * *

Domarna i detta faktablad är indexerade i den systematiska översikten över avgöranden under rubrikerna 1.04.03.07, 1.04.03.08, 1.04.03.10, 1.04.03.11, 2.04, 2.05.00, 4.11.01, 4.11.07 och 4.11.11.01.