Rättsfallssamlingen

FÖRSLAG TILL AVGÖRANDE AV GENERALADVOKAT
HENRIK SAUGMANDSGAARD ØE
föredraget den 19 december 2019[1]

Mål C-311/18

Data Protection Commissioner
mot
Facebook Ireland Limited,
Maximillian Schrems,
ytterligare deltagare i rättegången:
United States of America,
Electronic Privacy Information Centre,
BSA Business Software Alliance, Inc.,
Digitaleurope

(begäran om förhandsavgörande från High Court (Förvaltningsöverdomstolen, Irland))

”Begäran om förhandsavgörande – Skydd för fysiska personer med avseende på behandling av personuppgifter – Förordning (EU) 2016/679 – Artikel 2.2 – Tillämpningsområde – Överföring av personuppgifter till Amerikas förenta stater för kommersiella syften – Behandling av de överförda uppgifterna som utförs av de offentliga myndigheterna i Amerikas förenta stater för syften som avser den nationella säkerheten – Artikel 45 – Bedömning av huruvida den skyddsnivå som säkerställs i ett tredjeland är adekvat – Artikel 46 – Lämpliga skyddsåtgärder som vidtas av den personuppgiftsansvarige – Standardiserade skyddsbestämmelser – Artikel 58.2 – Tillsynsmyndigheternas befogenheter – Beslut 2010/87/EU – Giltighet – Genomförandebeslut (EU) 2016/1250 – Skölden för skydd av privatlivet i EU och Förenta staterna – Giltighet – Artiklarna 7, 8 och 47 i Europeiska unionens stadga om de grundläggande rättigheterna”

Innehållsförteckning

I. Inledning

1. Eftersom det inte har vidtagits några gemensamma åtgärder för att skydda personuppgifter på global nivå, innebär de gränsöverskridande flödena av personuppgifter en risk för avbrott i den skyddsnivå som säkerställs i Europeiska unionen. För att underlätta dessa flöden och samtidigt begränsa risken för avbrott i skyddsnivån har unionslagstiftaren inrättat tre mekanismer för överföring av personuppgifter från unionen till tredjeland.

1 Originalspråk: franska.

2. Överföring kan för det första ske på grundval av ett beslut genom vilket Europeiska kommissionen har konstaterat att tredjelandet i fråga säkerställer en ”adekvat skyddsnivå” för de överförda personuppgifterna.[2] Om ett sådant beslut inte föreligger tillåts överföring för det andra om överföringen omfattas av ”lämpliga skyddsåtgärder”.[3] Dessa skyddsåtgärder kan ta formen av ett avtal mellan uppgiftsutföraren och uppgiftsinföraren, som innehåller standardskyddsklausuler som har antagits av kommissionen. I dataskyddsförordningen föreskrivs för det tredje vissa undantag som grundar sig bland annat på den registrerades samtycke, varvid överföring till ett tredjeland tillåts även om det inte föreligger något beslut om en adekvat skyddsnivå eller lämpliga skyddsåtgärder.[4]

3. Begäran om förhandsavgörande från High Court (Förvaltningsöverdomstolen, Irland) avser den andra av ovannämnda mekanismer. Begäran avser närmare bestämt giltigheten av beslut 2010/87/EU,[5] i vilket kommissionen har fastställt standardavtalsklausuler för vissa kategorier av överföringar mot bakgrund av artiklarna 7, 8 och 47 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad stadgan).

4. Begäran om förhandsavgörande har ingetts i ett mål mellan Data Protection Commissioner (datatillsynsmyndigheten, Irland, nedan kallad DPC) samt Facebook Ireland Ltd och Maximillian Schrems. Maximillian Schrems ingav en anmälan till DPC avseende att Facebook Ireland överför personuppgifter rörande honom till sitt moderbolag Facebook Inc. i Amerikas förenta stater (nedan kallade Förenta staterna). DPC ansåg att prövningen av anmälan var beroende av huruvida beslut 2010/87 är giltigt. DPC vände sig därför till den hänskjutande domstolen för att denna skulle ställa en fråga till EU-domstolen om detta.

5. Det ska genast påpekas att vid min behandling av tolknings- och giltighetsfrågorna har inga omständigheter framkommit som enligt min mening kan påverka giltigheten av beslut 2010/87.

6. Den hänskjutande domstolen har emellertid också framfört tvivel rörande huruvida den skyddsnivå som Förenta staterna säkerställer är adekvat med hänsyn till de ingrepp som de amerikanska underrättelsetjänsternas verksamhet innebär i utövandet av de grundläggande rättigheterna för de personer vilkas personuppgifter överförs till detta tredjeland. Genom dessa tvivel har den indirekt ifrågasatt kommissionens bedömningar på denna punkt i genomförandebeslut (EU) 2016/1250.[6] Även om det inte är nödvändigt att domstolen avgör denna fråga för att den hänskjutande domstolen ska kunna avgöra det nationella målet och jag därför föreslår att den ska avstå från att göra detta, anger jag nedan subsidiärt skälen till att jag frågar mig huruvida detta beslut är giltigt.

7. I hela min bedömning har jag försökt uppnå en balans mellan nödvändigheten av att visa prov på en ”rimlig grad av pragmatism för att möjliggöra samverkan med resten av världen”[7] och nödvändigheten av att bekräfta de grundläggande värderingar som erkänns i unionens och dess medlemsstaters rättsordningar, särskilt i stadgan.

2 Se artikel 45 i Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning) (EUT L 119, 2016, s. 1) (nedan kallad dataskyddsförordningen).

3 Se artikel 46 i dataskyddsförordningen.

4 Se artikel 49 i dataskyddsförordningen.

5 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 dess lydelse enligt kommissionens genomförandebeslut (EU) 2016/2297 av den 16 december 2016 (EUT L 344, 2016, s. 100) (nedan kallat beslut 2010/87).

6 Kommissionens beslut av den 12 juli 2016 enligt [direktiv 95/46] om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna (EUT L 207, 2016, s. 1) (nedan kallat beslutet om skölden för skydd av privatlivet).

7 Se tal av den tidigare Europeiska datatillsynsmannen (EDPS) P. Hustinx, ”Le droit de l’Union européenne sur la protection des données: la révision de la directive 95/46/CE et la proposition de règlement général sur la protection des données”, s. 49, på adressen https://edps.europa.eu/sites/edp/files/publication/14–09–15_article_eui_fr.pdf.

II. Tillämpliga bestämmelser

A. Direktiv 95/46/EG

8. I artikel 3.2 i direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter [8] föreskrevs följande:

”Detta direktiv gäller inte för sådan behandling av personuppgifter

– som utgör ett led i en verksamhet som inte omfattas av gemenskapsrätten, exempelvis sådan verksamhet som avses i avdelningarna V och VI i Fördraget om Europeiska unionen, och inte under några omständigheter behandlingar som rör allmän säkerhet, försvar, statens säkerhet (inbegripet statens ekonomiska välstånd när behandlingen har samband med frågor om statens säkerhet) och statens verksamhet på straffrättens område,

…”

9. Artikel 13.1 i detta direktiv hade följande lydelse:

”Medlemsstaterna får genom lagstiftning vidta åtgärder för att begränsa omfattningen av de skyldigheter och rättigheter som anges i artiklarna 6.1, 10, 11.1, 12 och 21 i fall då en sådan begränsning är en nödvändig åtgärd med hänsyn till

a) statens säkerhet,

b) försvaret,

c) allmän säkerhet,

d) förebyggande, undersökning, avslöjande av brott eller åtal för brott eller av överträdelser av etiska regler som gäller för lagreglerade yrken,

e) ett viktigt ekonomiskt eller finansiellt intresse hos en medlemsstat eller hos [unionen], inklusive monetära frågor, budgetfrågor och skattefrågor,

f) en tillsyns-, inspektions- eller regleringsfunktion som, även om den är av övergående karaktär, är förbunden med myndighetsutövning i de under punkterna c), d) och e) nämnda fallen,

g) skydd av den registrerades eller andras fri- och rättigheter.”

10. I artikel 25 i nämnda direktiv angavs följande:

”1. Medlemsstaterna skall föreskriva att överföringen av personuppgifter som är under behandling eller som är avsedda att behandlas efter överföring till tredje land endast får ske om ifrågavarande tredje land – utan att detta påverkar tillämpningen av de nationella bestämmelser som antagits till följd av de andra bestämmelserna i detta direktiv – säkerställer en adekvat skyddsnivå.

8 Europaparlamentets och rådets direktiv av den 24 oktober 1995 (EGT L 281, 1995, s. 31), i dess lydelse enligt Europaparlamentets och rådets förordning (EG) nr 1882/2003 av den 29 september 2003 (EUT L 284, 2003, s. 1) (nedan kallat direktiv 95/46).

2. Bedömningen av om skyddsnivån i ett tredje land är adekvat skall ske på grundval av alla de förhållanden som har samband med en överföring eller en grupp av överföringar av uppgifter. Härvid skall särskilt beaktas uppgiftens art, den eller de avsedda behandlingarnas ändamål och varaktighet, ursprungslandet och det slutliga bestämmelselandet, de allmänna respektive särskilda rättsregler som gäller i ifrågavarande tredje land liksom de regler för yrkesverksamhet och säkerhet som gäller där.

…

6. Kommissionen kan, i enlighet med det i artikel 31.2 angivna förfarandet, konstatera att ett tredje land genom sin interna lagstiftning eller på grund av de internationella förpliktelser som – särskilt till följd av sådana förhandlingar som anges i punkt 5 och som gäller skyddet för privatliv och enskilda personers grundläggande fri- och rättigheter – åligger landet har en skyddsnivå som är adekvat i den mening som avses i punkt 2 i denna artikel.

Medlemsstaterna skall vidta de åtgärder som är nödvändiga för att följa kommissionens beslut.”

11. I artikel 26.2 och 26.4 i samma direktiv föreskrevs följande:

”2. Utan att detta påverkar tillämpningen av punkt 1 får en medlemsstat tillåta överföring av personuppgifter till ett tredje land som inte säkerställer en skyddsnivå som är adekvat enligt artikel 25.2, om den registeransvarige ställer tillräckliga garantier för att privatliv och enskilda personers grundläggande fri- och rättigheter skyddas samt för utövningen av motsvarande rättigheter. Sådana garantier kan framgå av lämpliga avtalsklausuler.

…

4. Om kommissionen… beslutar att vissa standardavtalsklausuler erbjuder tillräckliga garantier enligt punkt 2, skall medlemsstaterna vidta nödvändiga åtgärder för att följa kommissionens beslut.”

12. Artikel 28.3 i direktiv 95/46 hade följande lydelse:

”Varje tillsynsmyndighet skall särskilt ha

…

– effektiva befogenheter att ingripa, som till exempel att kunna avge yttranden i enlighet med artikel 20 innan en behandling äger rum, och se till att sådana yttranden i lämplig omfattning offentliggörs, att kunna besluta om blockering, utplåning eller förstöring av uppgifter, att kunna besluta om tillfälligt eller slutligt förbud mot behandling, att kunna ge den registeransvarige varning eller tillrättavisning eller att kunna hänvisa saken till nationella parlament eller till andra politiska institutioner,

…”

B. Dataskyddsförordningen

13. Som det anges i artikel 94.1 i dataskyddsförordningen har direktiv 95/46 upphävts genom denna förordning med verkan från och med den 25 maj 2018, som är det datum då nämnda förordning började tillämpas i enlighet med artikel 99.2 däri.

14. I artikel 2.2 i dataskyddsförordningen föreskrivs följande:

” Denna förordning ska inte tillämpas på behandling av personuppgifter som

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

b) medlemsstaterna utför när de bedriver verksamhet som omfattas av avdelning V kapitel 2 i EU-fördraget,

…

d) behöriga myndigheter utför i syfte att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, i vilket även ingår att skydda mot samt förebygga och förhindra hot mot den allmänna säkerheten.”

15. I artikel 4.2 i samma förordning definieras *behandling* som ”en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring”.

16. I artikel 23 i dataskyddsförordningen föreskrivs följande:

”1. Det ska vara möjligt att i unionsrätten eller i en medlemsstats nationella rätt som den personuppgiftsansvarige eller personuppgiftsbiträdet omfattas av införa en lagstiftningsåtgärd som begränsar tillämpningsområdet för de skyldigheter och rättigheter som föreskrivs i artiklarna 12–22 och 34, samt artikel 5 i den mån dess bestämmelser motsvarar de rättigheter och skyldigheter som fastställs i artiklarna 12–22, om en sådan begränsning sker med respekt för andemeningen i de grundläggande rättigheterna och friheterna och utgör en nödvändig och proportionell åtgärd i ett demokratiskt samhälle i syfte att säkerställa

a) den nationella säkerheten,

b) försvaret,

c) den allmänna säkerheten,

d) förebyggande, förhindrande, utredning, avslöjande eller lagföring av brott eller verkställande av straffrättsliga sanktioner, inbegripet skydd mot samt förebyggande och förhindrande av hot mot den allmänna säkerheten,

e) andra av unionens eller en medlemsstats viktiga mål av generellt allmänt intresse, särskilt ett av unionens eller en medlemsstats viktiga ekonomiska eller finansiella intressen,…,

…

2. Framför allt ska alla lagstiftningsåtgärder som avses i punkt 1 innehålla specifika bestämmelser åtminstone, när så är relevant, avseende

a) ändamålen med behandlingen eller kategorierna av behandling,

b) kategorierna av personuppgifter,

c) omfattningen av de införda begränsningarna,

d) skyddsåtgärder för att förhindra missbruk eller olaglig tillgång eller överföring,

e) specificeringen av den personuppgiftsansvarige eller kategorierna av personuppgiftsansvariga,

f) lagringstiden samt tillämpliga skyddsåtgärder med beaktande av behandlingens art, omfattning och ändamål eller kategorierna av behandling,

g) riskerna för de registrerades rättigheter och friheter, och

h) de registrerades rätt att bli informerade om begränsningen, såvida detta inte kan inverka menligt på begränsningen.”

17. I artikel 44 i denna förordning, med rubriken ”Allmän princip för överföring av uppgifter”, anges följande:

”Överföring av personuppgifter som är under behandling eller är avsedda att behandlas efter det att de överförts till ett tredjeland eller en internationell organisation får bara ske under förutsättning att den personuppgiftsansvarige och personuppgiftsbiträdet, med förbehåll för övriga bestämmelser i denna förordning, uppfyller villkoren i detta kapitel, inklusive för vidare överföring av personuppgifter från tredjelandet eller den internationella organisationen till ett annat tredjeland eller en annan internationell organisation. Alla bestämmelser i detta kapitel ska tillämpas för att säkerställa att den nivå på skyddet av fysiska personer som säkerställs genom denna förordning inte undergrävs.”

18. Artikel 45 i nämnda förordning, med rubriken ”Överföring på grundval av ett beslut om adekvat skyddsnivå”, har följande lydelse:

”1. Personuppgifter får överföras till ett tredjeland eller en internationell organisation om kommissionen har beslutat att tredjelandet, ett territorium eller en eller flera specificerade sektorer i tredjelandet, eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå. En sådan överföring ska inte kräva något särskilt tillstånd.

2. När kommissionen bedömer om en adekvat skyddsnivå föreligger ska den särskilt beakta

a) rättsstatsprincipen, respekten för de mänskliga rättigheterna och de grundläggande friheterna, relevant lagstiftning, både allmän lagstiftning och sektorslagstiftning, inklusive avseende allmän säkerhet, försvar, nationell säkerhet och straffrätt och offentliga myndigheters tillgång till personuppgifter samt tillämpningen av sådan lagstiftning, dataskyddsregler, yrkesregler och säkerhetsbestämmelser, inbegripet regler för vidare överföring av personuppgifter till ett annat tredjeland eller en annan internationell organisation, som ska följas i det landet eller den internationella organisationen, rättspraxis samt faktiska och verkställbara rättigheter för registrerade och effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs,

b) huruvida det finns en eller flera effektivt fungerande oberoende tillsynsmyndigheter i tredjelandet, eller som utövar tillsyn över den internationella organisationen, som har ansvar för att säkerställa och kontrollera att dataskyddsregler följs, inklusive lämpliga verkställighetsbefogenheter, ge de registrerade råd och assistans när det gäller utövandet av deras rättigheter och samarbeta med medlemsstaternas tillsynsmyndigheter, och

c) vilka internationella åtaganden det berörda tredjelandet eller den berörda internationella organisationen har gjort, eller andra skyldigheter som följer av rättsligt bindande konventioner eller instrument samt av dess deltagande i multilaterala eller regionala system, särskilt rörande skydd av personuppgifter.

3. Kommissionen får, efter att ha bedömt om det föreligger en adekvat skyddsnivå, genom en genomförandeakt besluta att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom ett tredjeland, eller en internationell organisation säkerställer en adekvat skyddsnivå i den mening som avses i punkt 2 i den här artikeln. Genomförandeakten ska inrätta en mekanism för regelbunden översyn, minst vart fjärde år, som ska beakta all relevant utveckling i det tredjelandet eller den internationella organisationen….

4. Kommissionen ska fortlöpande övervaka utveckling i tredjeländer och internationella organisationer vilken kan påverka hur beslut som antagits enligt punkt 3 i den här artikeln och beslut som antagits på grundval av artikel 25.6 i [direktiv 95/46] fungerar.

5. Kommissionen ska, när tillgänglig information visar, i synnerhet efter den översyn som avses i punkt 3 i den här artikeln, att ett tredjeland, ett territorium eller en eller flera specificerade sektorer inom tredjelandet i fråga eller en internationell organisation inte längre säkerställer adekvat skydd i den mening som avses i punkt 2 i den här artikeln och, i den mån det behövs, genom genomförandeakter återkalla, ändra eller upphäva det beslut som avses i punkt 3 i den här artikeln utan retroaktiv verkan….

6. Kommissionen ska samråda med tredjelandet eller den internationella organisationen i fråga för att lösa den situation som lett till beslutet enligt punkt 5.

…

9. De beslut som antas av kommissionen på grundval av artikel 25.6 i [direktiv 95/46] ska förbli i kraft tills de ändrats, ersatts eller upphävts av ett kommissionsbeslut som antagits i enlighet med punkt 3 eller 5 i den här artikeln.”

19. Artikel 46 i samma förordning, med rubriken ”Överföring som omfattas av lämpliga skyddsåtgärder”, har följande lydelse:

”1. I avsaknad av ett beslut i enlighet med artikel 45.3, får en personuppgiftsansvarig eller ett personuppgiftsbiträde endast överföra personuppgifter till ett tredjeland eller en internationell organisation efter att ha vidtagit lämpliga skyddsåtgärder, och på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga.

2. Lämpliga skyddsåtgärder enligt punkt 1 får, utan att det krävs särskilt tillstånd från en tillsynsmyndighet, ta formen av

…

c) standardiserade dataskyddsbestämmelser som antas av kommissionen i enlighet med det granskningsförfarande som avses i artikel 93.2,

…

5. Tillstånd från en medlemsstat eller tillsynsmyndighet på grundval av artikel 26.2 i [direktiv 95/46] ska förbli giltigt tills det, vid behov, ändrats, ersatts eller upphävts av den tillsynsmyndigheten. De beslut som fattas av kommissionen på grundval av artikel 26.4 i [direktiv 95/46] ska förbli i kraft tills de, vid behov, ändrats, ersatts eller upphävts av ett kommissionsbeslut som antagits i enlighet med punkt 2 i den här artikeln.”

20. I artikel 58.2, 58.4 och 58.5 i dataskyddsförordningen föreskrivs följande:

”2. Varje tillsynsmyndighet ska ha samtliga följande korrigerande befogenheter:

a) Utfärda varningar till en personuppgiftsansvarig eller personuppgiftsbiträdet om att planerade behandlingar sannolikt kommer att bryta mot bestämmelserna i denna förordning.

b) Utfärda reprimander till en personuppgiftsansvarig eller personuppgiftsbiträdet om behandling bryter mot bestämmelserna i denna förordning.

c) Förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att tillmötesgå den registrerades begäran att få utöva sina rättigheter enligt denna förordning.

d) Förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att se till att behandlingen sker i enlighet med bestämmelserna i denna förordning och om så krävs på ett specifikt sätt och inom en specifik period.

e) Förelägga den personuppgiftsansvarige att meddela den registrerade att en personuppgiftsincident har inträffat.

f) Införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, behandling.

…

i) Påföra administrativa sanktionsavgifter i enlighet med artikel 83 utöver eller i stället för de åtgärder som avses i detta stycke, beroende på omständigheterna i varje enskilt fall.

j) Förelägga om att flödet av uppgifter till en mottagare i tredje land eller en internationell organisation ska avbrytas.

…

4. Utövandet av de befogenheter som tillsynsmyndigheten tilldelas enligt denna artikel ska omfattas av lämpliga skyddsåtgärder, inbegripet effektiva rättsmedel och rättssäkerhet, som fastställs i unionsrätten och i medlemsstaternas nationella rätt i enlighet med stadgan.

5. Varje medlemsstat ska i lagstiftning fastställa att dess tillsynsmyndighet ska ha befogenhet att upplysa de rättsliga myndigheterna om överträdelser av denna förordning och vid behov att inleda eller på övrigt vis delta i rättsliga förfaranden, för att verkställa bestämmelserna i denna förordning.”

C. Beslut 2010/87

21. Kommissionen har antagit tre beslut på grundval av artikel 26.4 i direktiv 95/46, vilka innehåller standardavtalsklausuler som enligt kommissionen ger tillräckliga garantier för skydd av den personliga integriteten och enskildas grundläggande rättigheter och friheter samt för utövandet av motsvarande rättigheter (nedan kallade besluten om standardavtalsklausuler) [9].

9 Kommissionens beslut 2001/497/EG av den 15 juni 2001 om standardavtalsklausuler för överföring av personuppgifter till tredje land enligt direktiv [95/46] (EGT L 181, 2001, s. 19), kommissionens beslut 2004/915/EG av den 27 december 2004 om ändring av beslut [2001/497] om standardavtalsklausuler för överföring av personuppgifter till tredje land (EUT L 385, 2004, s. 74) och beslut 2010/87.

22. Ett av dessa beslut är beslut 2010/87, i vilket det i artikel 1 föreskrivs att ”[d]e standardavtalsklausuler som anges i bilagan till detta beslut ska anses ge tillräckliga garantier för skydd av den personliga integriteten och enskildas grundläggande rättigheter och friheter samt för utövandet av motsvarande rättigheter, i enlighet med vad som föreskrivs i artikel 26.2 i [direktiv 95/46]”.

23. Artikel 3 i detta beslut har följande lydelse:

”I detta beslut avses med

…

c) *uppgiftsutförare*: den registeransvarige som överför personuppgifterna,

d) *uppgiftsinförare*: den registerförare som är etablerad i ett tredjeland och som samtycker till att från uppgiftsutföraren ta emot personuppgifter avsedda för behandling för uppgiftsutförarens räkning efter överföringen, enligt dennes instruktioner och i enlighet med detta beslut, såvida inte uppgiftsinföraren omfattas av ett system i det berörda tredjelandet som garanterar ett tillräckligt skydd i den mening som avses i artikel 25.1 i [direktiv 95/46],

…

f) *tillämplig uppgiftsskyddslagstiftning*: sådan lagstiftning som avser att skydda personers grundläggande fri- och rättigheter, särskilt deras personliga integritet i samband med behandling av personuppgifter, och som är tillämplig på registeransvariga i den medlemsstat där uppgiftsutföraren är etablerad,

…”

24. I artikel 4.1 i beslutet, i dess ursprungliga lydelse, föreskrevs följande:

”Utan att det påverkar rätten för medlemsstaternas behöriga myndigheter att se till att nationella bestämmelser som antagits i enlighet med bestämmelserna i kapitlen II, III, V och VI i [direktiv 95/46] följs, får de använda sina befintliga befogenheter för att förbjuda eller avbryta flöden av uppgifter till tredjeland och därigenom skydda enskilda när det gäller behandling av personuppgifter om dem i fall där

a) det konstateras att uppgiftsinföraren eller en underentreprenör enligt den lagstiftning som gäller för denne ska frångå tillämplig uppgiftsskyddslagstiftning som går utöver de restriktioner som krävs i ett demokratiskt samhälle enligt artikel 13 i [direktiv 95/46], om dessa restriktioner sannolikt har en avsevärt skadlig inverkan på de garantier som ställs i tillämplig uppgiftsskyddslagstiftning eller i standardavtalsklausulerna,

b) en behörig myndighet har fastställt att uppgiftsinföraren eller en underentreprenör inte har följt standardavtalsklausulerna i bilagan, eller

c) det finns skälig grund att anta att standardavtalsklausulerna i bilagan inte följs eller inte kommer att följas och att fortsatt överföring skulle medföra en överhängande risk för allvarlig skada för de registrerade.”

25. I artikel 4 i beslut 2010/87, i dess nuvarande lydelse, som följer av att beslut 2010/87 ändrats genom genomförandebeslut (EU) 2016/2297[10] anges att ”[n]är de behöriga myndigheterna i en medlemsstat utövar sina befogenheter enligt artikel 28.3 i [direktiv 95/46] och detta leder till ett tillfälligt eller slutligt förbud mot dataflöden till tredjeländer i syfte att skydda enskilda personer med avseende på behandlingen av deras personuppgifter, ska den berörda medlemsstaten utan dröjsmål underrätta kommissionen och vidarebefordra underrättelsen till de övriga medlemsstaterna”.

26. Bilagan till beslut 2010/87 innehåller en rad standardavtalsklausuler. I klausul 3, med rubriken ”Tredjepartsberättigande”, föreskrivs följande:

”1. Den registrerade kan i egenskap av berättigad tredjepart åberopa denna klausul och klausulerna 4 b–i, 5 a–e och 5 g–j, 6.1–2, 7, 8.2 samt klausulerna 9–12 gentemot uppgiftsutföraren.

2. Den registrerade kan gentemot uppgiftsinföraren åberopa denna klausul, klausulerna 5 a–e och 5 g, klausulerna 6, 7, 8.2 samt klausulerna 9–12 i sådana fall där uppgiftsutföraren har upphört att existera i faktisk eller rättslig mening, såvida inte en annan enhet enligt avtal eller lag till fullo har övertagit uppgiftsutförarens rättsliga skyldigheter, och som en följd av detta påtar sig uppgiftsutförarens rättigheter och skyldigheter, i vilket fall den registrerade kan åberopa de ovannämnda klausulerna gentemot denna.

…”

27. Klausul 4 i bilagan, med rubriken ”Uppgiftsutförarens skyldigheter”, har följande lydelse:

”Uppgiftsutföraren godtar och garanterar

a) att behandlingen, inbegripet själva överföringen, av personuppgifterna har skett och även i fortsättningen kommer att ske i enlighet med tillämplig uppgiftsskyddslagstiftning (och i förekommande fall anmäls till behöriga myndigheter i den medlemsstat där uppgiftsutföraren är etablerad) och inte strider mot gällande lagar eller andra författningar i den medlemsstaten,

b) att han instruerat och under behandlingen av personuppgifter kommer att instruera uppgiftsinföraren att behandla de överförda personuppgifterna endast för uppgiftsutförarens räkning och i enlighet med tillämplig uppgiftsskyddslagstiftning och klausulerna,

c) att uppgiftsinföraren kommer att ge tillräckliga garantier vad gäller de tekniska och organisatoriska säkerhetsåtgärder som anges i tillägg 2 till detta avtal,

d) att han, mot bakgrund av tillämplig uppgiftsskyddslagstiftning, har funnit säkerhetsåtgärderna lämpliga för att skydda personuppgifter mot oavsiktlig eller olaglig utplåning, oavsiktlig förlust, ändring, otillåtet utlämnande eller otillåten åtkomst, i synnerhet när behandlingen inbegriper överföring av uppgifter över ett nät, och mot varje annan form av olaglig behandling, med hänsyn tagen till teknikens ståndpunkt, kostnaden för vidtagande av åtgärderna och de risker behandlingen innebär och karaktären hos de uppgifter som ska behandlas,

e) att han kommer att se till att säkerhetsåtgärderna följs,

10 Kommissionens beslut av den 16 december 2016 om ändring av beslut [2001/497] och [2010/87] rörande standardavtalsklausuler för överföring av personuppgifter till tredjeländer och till registerförare etablerade i tredjeländer i enlighet med [direktiv 95/46] (EUT L 344, 2016, s. 100).

f) att, om överföringen avser särskilda kategorier av uppgifter, de registrerade har informerats eller informeras senast när överföringen sker eller så snart som möjligt därefter om att deras uppgifter kan komma att överföras till ett tredjeland som inte tillhandahåller adekvat skydd i den mening som avses i [direktiv 95/46],

g) att vidarebefordra anmälningar från uppgiftsinföraren eller eventuella underentreprenörer i enlighet med klausul 5 b och klausul 8.3 till tillsynsmyndigheten om uppgiftsutföraren beslutar att fortsätta överföringen eller häva avbrottet,

h) att på begäran tillhandahålla de registrerade en kopia av klausulerna, med undantag för tillägg 2, och en sammanfattande beskrivning av säkerhetsåtgärderna, samt en kopia av eventuella underentreprenörsavtal som måste ingås enligt klausulerna, såvida inte klausulerna eller avtalet innehåller affärsinformation,

i) att uppgiftsbehandlingen vid en eventuell utläggning på entreprenad utförs i enlighet med klausul 11 av en underentreprenör som tillhandahåller åtminstone samma skyddsnivå för personuppgifter och den registrerades rättigheter som uppgiftsinföraren ska göra enligt klausulerna, och

j) att han kommer att se till att klausul 4 a–i följs.”

28. I klausul 5 i samma bilaga, med rubriken ”Uppgiftsinförarens skyldigheter (1)” anges följande:

”Uppgiftsinföraren godtar och garanterar

a) att behandla personuppgifter för uppgiftsutförarens räkning och enlighet med dennes instruktioner samt dessa klausuler; om han av något skäl inte kan fullgöra detta krav går han med på att omedelbart informera uppgiftsutföraren om detta, varvid uppgiftsutföraren har rätt att avbryta överföringen av uppgifter och/eller häva avtalet,

b) att han inte har anledning att förmoda att den lagstiftning som är tillämplig på honom hindrar honom från att fullfölja uppdragsutförarens instruktioner och sina skyldigheter enligt detta avtal; om lagstiftningen ändras på ett sätt som sannolikt har en avsevärt skadlig inverkan på de garantier som klausulerna innebär, ska han anmäla ändringen till uppgiftsutföraren, varvid uppgiftsutföraren har rätt att avbryta överföringen av uppgifter och/eller häva avtalet,

c) att han har vidtagit de tekniska och organisatoriska säkerhetsåtgärder som anges i tillägg 2 innan de överförda personuppgifterna behandlas,

d) att utan dröjsmål kommer att underrätta uppgiftsutföraren om

   i) varje rättsligt bindande begäran från rättsliga myndigheter om utlämnande av personuppgifterna, om inte detta är förbjudet på grund av exempelvis ett straffrättsligt förbud som syftar till att bevara sekretessen vid brottsutredningar,

   ii) varje oavsiktlig eller otillåten åtkomst, och

   iii) varje förfrågan direkt från de registrerade, utan att svara på dem om han inte givits tillstånd till det,

e) att utan dröjsmål och korrekt handlägga alla frågor från uppgiftsutföraren om behandling av sådana personuppgifter som överförs och att rätta sig efter tillsynsmyndighetens rekommendationer med avseende på behandlingen av de uppgifter som överförs,

f) att på uppgiftsutförarens begäran ställa sin databehandlingsutrustning till förfogande för granskning av den uppgiftsbehandling som dessa klausuler avser; granskningen ska genomföras av uppgiftsutföraren eller av ett inspektionsorgan med oberoende och sakkunniga ledamöter; de av tystnadsplikt bundna ledamöterna utses av uppgiftsutföraren, i förekommande fall enligt överenskommelse med tillsynsmyndigheten,

…”

29. I fotnot 1, som det hänvisas till i rubriken till klausul 5 i bilagan till beslut 2010/87, anges följande:

”Standardavtalsklausulerna är inte oförenliga med obligatoriska krav i den nationella lagstiftning som är tillämplig på uppgiftsinföraren, förutsatt att kraven inte går utöver vad som är nödvändigt i ett demokratiskt samhälle på någon av de grunder som anges i artikel 13.1 i direktiv 95/46/EG, dvs. om det är en nödvändig åtgärd med hänsyn till statens säkerhet, försvaret, den allmänna säkerheten, förebyggande, undersökning, avslöjande av brott eller åtal för brott eller av överträdelser av etiska regler som gäller för lagreglerade yrken, ett för staten viktigt ekonomiskt eller finansiellt intresse eller skydd av den registrerades eller andras fri- och rättigheter. Exempel på sådana obligatoriska krav som inte går utöver vad som krävs i ett demokratiskt samhälle är internationellt erkända sanktioner, krav på skatterapportering eller upplysningsplikt när det gäller bekämpning av penningtvätt.”

30. Klausul 6 i denna bilaga, med rubriken ”Ansvar”, har följande lydelse:

”1. Parterna är överens om att en registrerad som lidit skada till följd av att en part eller en parts underentreprenör brutit mot de skyldigheter som avses i klausul 3 eller klausul 11 har rätt till ersättning från uppgiftsutföraren.

2. Om den registrerade, i situationer där uppgiftsinföraren eller dennes underentreprenör bryter mot någon av sina skyldigheter enligt klausulerna 3 eller 11, inte kan rikta skadeståndsanspråk mot uppgiftsutföraren i enlighet med punkt 1 på grund av att uppgiftsutföraren har upphört att existera i faktisk eller rättslig mening eller har hamnat på obestånd, ska uppgiftsinföraren godta att den registrerade kan rikta ett skadeståndsanspråk mot uppgiftsinföraren som om denne var uppgiftsutföraren, såvida inte en annan enhet enligt avtal eller lag till fullo har övertagit uppgiftsutförarens rättsliga skyldigheter, i vilket fall den registrerade kan göra sina rättigheter gällande gentemot denna enhet.

…”

31. I klausul 7 i nämnda bilaga, med rubriken ”Medling och forum”, anges följande:

”1. Uppgiftsinföraren samtycker till att, om den registrerade åberopar tredje parts rättigheter och/eller kräver ersättning för skador i enlighet med klausulerna, godta den registrerades beslut att

a) inleda medling av tredje part eller, i tillämpliga fall, av tillsynsmyndigheten,

b) hänskjuta tvisten till domstol i den medlemsstat där uppgiftsutföraren är etablerad.

2. Parterna är överens om att den registrerades val inte påverkar dennes materiella eller processuella rätt att söka gottgörelse i enlighet med andra bestämmelser i nationell eller internationell lagstiftning.”

32. I klausul 9 i samma bilaga, med rubriken ”Tillämplig lag”, föreskrivs att standardavtalsklausulerna omfattas av lagen i den medlemsstat där uppgiftsutföraren är etablerad.

D. Beslutet om skölden för skydd av privatlivet

33. Kommissionen har antagit två på varandra följande beslut på grundval av artikel 25.6 i direktiv 95/46, i vilka den har konstaterat att Förenta staterna säkerställer en adekvat skyddsnivå för personuppgifter som överförs till företag som är etablerade i Förenta staterna och som genom ett förfarande för självcertifiering har förklarat att de följer de principer som anges i dessa beslut.

34. Först antog kommissionen beslut 2000/520/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.[11] I domen av den 6 oktober 2015, Schrems,[12] slog domstolen fast att detta beslut var ogiltigt.

35. Till följd av nämnda dom antog kommissionen därefter beslutet om skölden för skydd av privatlivet.

36. I artikel 1 i detta beslut föreskrivs följande:

”1. Vid tillämpningen av artikel 25.2 i [direktiv 95/46] säkerställer Förenta staterna en adekvat skyddsnivå för personuppgifter som överförs från unionen till organisationer i Förenta staterna inom ramen för skölden för skydd av privatlivet i EU och Förenta staterna.

2. Skölden för skydd av privatlivet i EU och Förenta staterna utgörs av de principer som utfärdades av Förenta staterna[s] handelsministerium den 7 juli 2016 enligt vad som anges i bilaga II samt de officiella utfästelser och åtaganden som ingår i de dokument som anges i bilagorna I samt III–VII.

3. Vid tillämpningen av punkt 1 överförs personuppgifter enligt skölden för skydd av privatlivet i EU och Förenta staterna när de överförs från unionen till organisationer i Förenta staterna som ingår i den ’förteckning över organisationer som anslutit sig till skölden’ som förvaltas och offentliggörs av Förenta staternas handelsministerium i enlighet med avsnitten I och III i de principer som anges i bilaga II.”

37. Bilaga III A till beslutet, med rubriken ”Ombudsmannen för skölden för skydd av privatlivet i EU och Förenta staterna när det gäller signalspaning”, som bifogades en skrivelse från John Kerry, dåvarande Secretary of State (utrikesminister, Förenta staterna), daterad den 7 juli 2016, innehåller ett memorandum med en beskrivning av ett nytt förfarande med en ”chefssamordnare för internationell it-diplomati” (nedan kallad ombudsmannen) som utses av utrikesministern.

38. Enligt ordalydelsen i detta memorandum inrättades detta förfarande ”för att handlägga förfrågningar om tillgång till uppgifter som överförts från [unionen] till Förenta staterna inom ramen för skölden för skydd av privatlivet rörande nationell säkerhet, standardavtalsklausuler, bindande företagsregler samt ’undantag’ eller ’möjliga framtida undantag’ genom förfaranden som fastställts enligt tillämpliga amerikanska lagar och policyer, samt hur sådana förfrågningar ska besvaras”.

III. Målet vid den nationella domstolen, giltighetsfrågorna och förfarandet vid domstolen

39. Maximillian Schrems, som är österrikisk medborgare och bosatt i Österrike, är användare av det sociala nätverket Facebook. Alla användare av detta sociala nätverk med hemvist inom unionen måste i samband med att de registrerar sig ingå ett avtal med Facebook Ireland, som är ett dotterbolag till moderbolaget Facebook Inc., vilket i sin tur har sitt säte i Förenta staterna. Användarnas personuppgifter överförs helt eller delvis till servrar tillhörande Facebook Inc. belägna i Förenta staterna, där uppgifterna behandlas.

11 Beslut av den 26 juli 2000 i enlighet med direktiv [95/46] (EGT L 215, 2000, s. 7) (nedan kallat Safe Harbor-beslutet).

12 C-362/14 (EU:C:2015:650) (nedan kallad domen Schrems).

40. Den 25 juni 2013 ingav Maximillian Schrems en anmälan till DPC, i vilken han begärde att Facebook Ireland skulle förbjudas att överföra personuppgifter rörande honom till Förenta staterna. I anmälan hävdade han att gällande lagstiftning och praxis i detta tredjeland inte garanterar ett tillräckligt skydd för lagrade personuppgifter mot intrång till följd av de offentliga myndigheternas övervakningsverksamhet. Maximillian Schrems hänvisade till Edward Snowdens avslöjanden om de amerikanska underrättelsetjänsternas verksamhet, särskilt verksamheten vid National Security Agency (NSA) (Nationella säkerhetsmyndigheten, Förenta staterna).

41. Anmälan avslogs bland annat med motiveringen att alla frågor om huruvida skyddet av personuppgifter i Förenta staterna var adekvat måste avgöras i överensstämmelse med Safe Harbor-beslutet. I detta beslut hade kommissionen konstaterat att Förenta staterna erbjöd en adekvat skyddsnivå för personuppgifter som överfördes till företag etablerade i Förenta staterna som hade anslutit sig till de principer som angavs i beslutet.

42. Maximillian Schrems överklagade DPC:s beslut att avslå hans anmälan till High Court (Förvaltningsöverdomstolen). Denna bedömde att även om Maximillian Schrems inte formellt hade ifrågasatt Safe Harbor-beslutets giltighet, hade han genom sitt överklagande i själva verkat hävdat att det system som inrättats genom detta beslut var olagligt. Mot denna bakgrund hänsköt High Court (Förvaltningsöverdomstolen) frågor till EU-domstolen för att få klarhet i huruvida de myndigheter i medlemsstaterna som ansvarar för dataskyddet (nedan kallade tillsynsmyndigheterna), när de ska pröva en anmälan rörande skyddet för en persons fri- och rättigheter med avseende på behandling av personuppgifter rörande vederbörande som har överförts till ett tredjeland, är bundna av kommissionens konstateranden enligt artikel 25.6 i direktiv 95/46 avseende att skyddsnivån i detta tredjeland är adekvat, trots att den som har ingett anmälan bestrider dessa konstateranden.

43. EU-domstolen slog i punkterna 51 och 52 i domen Schrems fast att tillsynsmyndigheterna är bundna av ett beslut om en adekvat skyddsnivå så länge som beslutet inte har ogiltigförklarats, och konstaterade därefter följande i punkterna 63 och 65:

”63. … [Det] ankommer … på en nationell tillsynsmyndighet att med vederbörlig omsorg utreda en begäran om skydd för sina fri- och rättigheter med avseende på behandling av personuppgifter som framställts av en person vars personuppgifter överförts, eller kan komma att överföras, till ett tredjeland som varit föremål för ett kommissionsbeslut med stöd av artikel 25.6 i direktiv 95/46, och i samband med vilken vederbörande … gör gällande att beslutet inte är förenligt med skyddet för privatlivet och enskilda personers grundläggande fri- och rättigheter.

…

65. Om den nationella tillsynsmyndigheten… anser att det finns fog för de invändningar som framförts av [denna person], måste myndigheten, i enlighet med artikel 28.3 första stycket tredje strecksatsen i direktiv 95/46, särskilt jämförd med artikel 8.3 i stadgan, ha befogenhet att inleda rättsliga förfaranden. Det ankommer härvidlag på den nationella lagstiftaren att föreskriva rättsmedel som gör det möjligt för den nationella tillsynsmyndigheten att vid nationella domstolar göra gällande de invändningar som den anser att det finns fog för, så att nationella domstolar, för det fall att de delar myndighetens tvivel angående kommissionsbeslutets giltighet, kan hänskjuta en begäran om förhandsavgörande för att pröva detta besluts giltighet.”

44. I nämnda dom prövade domstolen även huruvida Safe Harbor-beslutet var giltigt mot bakgrund av de krav som följer av direktiv 95/46 jämfört med stadgan. Till följd av denna prövning konstaterade den att beslutet i fråga var ogiltigt.[13]

13 Se domen Schrems (punkt 106).

45. Till följd av domen Schrems ogiltigförklarade den hänskjutande domstolen DPC:s beslut om avslag på Maximillian Schrems anmälan och återförvisade ärendet till DPC för prövning. DPC inledde en utredning och anmodade Maximillian Schrems att omformulera sin anmälan med beaktande av att Safe Harbor-beslutet hade ogiltigförklarats.

46. Maximillian Schrems begärde därför att Facebook Ireland skulle ange vilka rättsliga grunder överföringarna av personuppgifter rörande användarna av det sociala nätverket Facebook från unionen till Förenta staterna baserar sig på. Utan att ange samtliga de rättsliga grunder som överföringarna baserade sig på hänvisade Facebook Ireland till beslut 2010/87 samt till ett avtal om överföring och behandling av uppgifter (*data transfer processing agreement*) som hade ingåtts mellan Facebook Ireland och Facebook Inc. och som gällde från och med den 20 november 2015.

47. I sin omformulerade anmälan gjorde Maximillian Schrems gällande att klausulerna i detta avtal inte överensstämmer med standardavtalsklausulerna i bilagan till beslut 2010/87. Vidare hävdade Maximillian Schrems att dessa standardavtalsklausuler i vart fall inte kan utgöra grund för överföring av personuppgifter rörande honom till Förenta staterna. Detta är fallet eftersom Facebook Inc. enligt amerikansk rätt är skyldigt att ställa användarnas personuppgifter till förfogande för amerikanska myndigheter såsom NSA och Federal Bureau of Investigation (FBI) (Federala utredningsbyrån, Förenta staterna) inom ramen för övervakningsprogram som hindrar utövandet av de rättigheter som garanteras i artiklarna 7, 8 och 47 i stadgan. Maximillian Schrems hävdade att det inte finns något rättsmedel som gör det möjligt för de registrerade att göra gällande sin rätt till respekt för privatlivet och skydd av personuppgifter. Under dessa omständigheter begärde Maximillian Schrems att DPC skulle avbryta överföringen i enlighet med artikel 4 i beslut 2010/87.

48. Inom ramen för DPC:s utredning erkände Facebook Ireland att företaget fortsätter att överföra personuppgifterna för användare av det sociala nätverket Facebook som är bosatta i unionen till Förenta staterna och härvid till stor del grundar sig på standardavtalsklausulerna i bilagan till beslut 2010/87.

49. DPC:s utredning syftade till att avgöra dels huruvida Förenta staterna säkerställer ett adekvat skydd för unionsmedborgarnas personuppgifter, dels, om så inte är fallet, huruvida besluten om standardavtalsklausuler innehåller tillräckliga garantier vad gäller skyddet för unionsmedborgarnas grundläggande rättigheter och friheter.

50. I ett utkast till beslut (*draft decision*) ansåg DPC preliminärt att amerikansk lagstiftning inte erbjuder något effektivt rättsmedel i den mening som avses i artikel 47 i stadgan för unionsmedborgare vilkas personuppgifter överförs till Förenta staterna, där uppgifterna riskerar att behandlas av amerikanska organ på ett sätt som är oförenligt med artiklarna 7 och 8 i stadgan. De garantier som föreskrivs i klausulerna i bilagorna till besluten om standardavtalsklausuler avhjälper inte denna brist, eftersom de inte är bindande för amerikanska myndigheter eller organ och endast ger de registrerade avtalsrättsliga rättigheter gentemot uppgiftsutföraren och/eller uppgiftsinföraren.

51. Under dessa omständigheter bedömde DPC att den inte kan avgöra anmälan från Maximillian Schrems utan att EU-domstolen har prövat huruvida besluten om standardavtalsklausuler är giltiga. DPC inledde därför, i enlighet med vad som slås fast i punkt 65 i domen Schrems, ett förfarande vid den hänskjutande domstolen i syfte att denna, för det fall att den delar DPC:s tvivel, skulle hänskjuta en begäran om förhandsavgörande till EU-domstolen angående giltigheten av dessa beslut.

52. Förenta staternas regering, Electronic Privacy Information Centre (EPIC), Business Software Alliance (BSA) och Digitaleurope tilläts intervenera vid den hänskjutande domstolen.

53. High Court (Förvaltningsöverdomstolen) inhämtade bevisning från parterna i tvisten och lyssnade till de argument som anfördes av parterna och av intervenienterna, för att den skulle kunna avgöra om den delar DPC:s tvivel rörande giltigheten av besluten om standardavtalsklausuler. Den bevisning som presenterades av experter avsåg framför allt bestämmelser i Förenta staternas lagstiftning. Enligt irländsk rätt betraktas utländsk lagstiftning som en faktisk omständighet som ska fastställas genom bevisning på samma sätt som alla andra omständigheter. På grundval av denna bevisning utvärderade den hänskjutande domstolen de bestämmelser i Förenta staternas lagstiftning som tillåter att myndigheter och regeringsorgan utövar övervakning, funktionen hos två officiellt erkända övervakningsprogram (”PRISM” och ”Upstream”), de olika rättsmedel som är tillgängliga för enskilda vilkas rättigheter har kränkts genom övervakningsåtgärder samt de systematiska garantierna och kontrollmekanismerna. Den hänskjutande domstolen redogjorde för resultaten av sin utvärdering i en dom av den 3 oktober 2017, vilken bifogats begäran om förhandsavgörande (nedan kallad domen från High Court (Förvaltningsöverdomstolen) av den 3 oktober 2017).

54. I nämnda dom hänvisade den hänskjutande domstolen, bland de rättsliga grunder som tillåter att amerikanska underrättelsetjänster avlyssnar utländska kommunikationer, till avsnitt 702 i Foreign Intelligence Surveillance Act (FISA) (lag om underrättelseverksamhet och övervakning utomlands) och Executive Order 12333 (presidentorder nr 12333) (nedan kallad EO 12333).

55. Enligt konstaterandena i nämnda dom kan Attorney General (justitieministern, Förenta staterna) tillsammans med Director of National Intelligence (DNI) (chefen för den nationella underrättelsetjänsten, Förenta staterna) enligt avsnitt 702 i FISA, i syfte att inhämta utländska underrättelseuppgifter, utfärda årliga tillstånd för övervakning av personer som inte är amerikanska medborgare och inte är permanent bosatta i Förenta staterna (så kallade icke-amerikanska personer), om de skäligen kan antas befinna sig utanför Förenta staternas territorium.[14] Med begreppet utländsk underrättelseinformation avses enligt FISA information relaterad till regeringens förmåga att skydda sig mot utländska attacker, terrorism och spridning av massförstörelsevapen och till genomförandet av Förenta staternas utrikespolitik.[15]

56. Dessa årliga tillstånd, liksom förfarandena för målinriktning på personer som ska övervakas och för behandling (”minimering”) av den insamlade informationen,[16] måste godkännas av Foreign Intelligence Surveillance Court (FISC) (Domstolen för övervakning av utländsk underrättelseinformation, Förenta staterna). Medan den ”traditionella” övervakning som utförs på grundval av andra bestämmelser i FISA kräver att ”sannolika skäl” har fastställts föreligga som föranleder misstanke om att de övervakade personerna tillhör eller är agenter för en utländsk makt, är övervakningsverksamhet som vidtas enligt avsnitt 702 i FISA inte underordnad några sådana krav på att ”sannolika skäl” har fastställts eller på att FISC har godkänt målinriktningen på bestämda personer. Dessutom är – också detta enligt den hänskjutande domstolens konstateranden – förfarandena för minimering inte tillämpliga på icke-amerikanska personer som befinner sig utanför Förenta staterna.

57. I praktiken går det till så att när FISC har beviljat tillstånd sänder NSA direktiv till leverantörer av elektroniska kommunikationstjänster etablerade i Förenta staterna. Dessa direktiv innehåller sökkriterier, så kallade ”urvalstermer”, avseende de personer som övervakningen inriktas på (såsom telefonnummer eller e-postadresser). Leverantörerna är då skyldiga att till NSA överföra de uppgifter

14 50 U.S.C. 1881 a.

15 50 U.S.C. 1881 e.

16 Den hänskjutande domstolen har konstaterat att förfarandena för målinriktning avser det sätt på vilket den verkställande makten fastställer att en viss person skäligen kan antas vara en icke-amerikansk person som befinner sig utanför Förenta staterna och att målinriktning på denna person kan resultera i inhämtande av utländska underrättelseuppgifter. Förfarandena för minimering omfattar inhämtande, lagring, användning och spridning av all icke offentlig information om amerikanska personer som erhållits enligt avsnitt 702 i FISA.

som motsvarar urvalstermerna och måste upprätthålla sekretessen för de direktiv som de erhållit. De kan inge en ansökan till FISC om ändring av eller avvikelse från ett direktiv utfärdat av NSA. FISC:s beslut kan överklagas till Foreign Intelligence Surveillance Court of Review (FISCR) (Appellationsdomstolen för övervakning av utländsk underrättelseinformation, Förenta staterna).

58. High Court (Förvaltningsöverdomstolen) konstaterade att avsnitt 702 i FISA utgör den rättsliga grunden för programmen PRISM och Upstream.

59. Inom ramen för programmet PRISM är leverantörer av elektroniska kommunikationstjänster skyldiga att till NSA överföra alla kommunikationer ”från” eller ”till” den urvalsterm som NSA har meddelat. En del av kommunikationerna överförs till FBI och Central Intelligence Agency (CIA) (Centrala underrättelsetjänsten, Förenta staterna). År 2015 övervakades 94 386 personer och år 2011 inhämtade Förenta staternas regering mer än 250 miljoner kommunikationer inom ramen för detta program.

60. Programmet Upstream bygger på obligatoriskt bistånd från de företag som handhar driften av den ”ryggrad” – det vill säga det nätverk av kablar, switchar och routrar – via vilken telekommunikationerna och internetkommunikationerna går. Dessa företag är skyldiga att låta NSA kopiera och filtrera trafikflödena på internet i syfte att inhämta kommunikationer ”från”, ”till” eller ”rörande” en urvalsterm som anges i ett direktiv från detta organ. Med kommunikationer rörande en urvalsterm avses kommunikationer som refererar till denna urvalsterm, utan att den icke-amerikanska person som associeras med urvalstermen i fråga nödvändigtvis deltar i kommunikationen. Även om det av ett yttrande från FISC av den 26 april 2017 framgår att den amerikanska regeringen från och med det datumet inte längre samlar in och inhämtar kommunikationer ”rörande” en urvalsterm, framgår det inte av yttrandet att NSA har upphört med att kopiera och filtrera de kommunikationsflöden som går via dess övervakningssystem. Programmet Upstream innebär således att NSA har tillgång till såväl metadata som innehållet i kommunikationerna. Sedan 2011 har NSA inom ramen för programmet Upstream samlat in omkring 26,5 miljoner kommunikationer per år, vilket emellertid endast utgör en liten del av de kommunikationer som omfattas av filtreringsprocessen inom ramen för detta program.

61. Enligt konstaterandena från High Court (Förvaltningsöverdomstolen) tillåter EO 12333 dessutom övervakning av elektroniska kommunikationer utanför Förenta staternas territorium genom att, i syfte att inhämta utländsk underrättelseinformation, möjliggöra åtkomst till uppgifter som antingen är under överföring till Förenta staternas territorium eller överförs via detta territorium utan att vara avsedda att behandlas där samt insamling och lagring av dessa uppgifter. I EO 12333 definieras begreppet ”utländsk underrättelseinformation” så, att det inbegriper information avseende utländska regeringars, organisationers och personers kapacitet, avsikter eller aktiviteter.[17]

62. EO 12333 ger NSA befogenhet för åtkomst till de undervattenskablar på botten av Atlanten genom vilka uppgifter överförs från unionen till Förenta staterna och ger således NSA åtkomst till uppgifterna i fråga innan de når fram till Förenta staterna och därigenom omfattas av bestämmelserna i FISA. Det finns emellertid inga bevis för att något program skulle ha genomförts i enlighet med denna presidentorder.

63. Även om det i EO 12333 föreskrivs begränsningar för insamlingen, lagringen och spridningen av information, är dessa begränsningar inte tillämpliga när det gäller icke-amerikanska personer. Dessa omfattas enbart av de garantier som anges i Presidential Policy Directive 28 (presidentens policydirektiv 28, nedan kallat PPD 28), vilket är tillämpligt på all verksamhet för insamling och

17 EO 12333, punkt 3.5 e.

användning av utländska underrättelseuppgifter som erhålls genom signalspaning. I PPD 28 föreskrivs att respekt för privatlivet är en av de faktorer som ska beaktas vid planeringen av denna verksamhet, att insamlingen endast ska syfta till att inhämta utländska underrättelseuppgifter och kontraspionageuppgifter och att nämnda verksamhet ska vara ”så anpassad som möjligt”.

64. Den verksamhet som NSA grundar på EO 12333, vilken när som helst kan ändras eller återkallas av Förenta staternas president, är enligt den hänskjutande domstolen inte reglerad i lag, är inte föremål för någon rättslig tillsyn och kan inte vara föremål för rättslig prövning.

65. Mot bakgrund av ovannämnda konstateranden anser den hänskjutande domstolen att Förenta staterna genomför en urskillningslös massbehandling av personuppgifter, vilket innebär en risk för kränkning av de rättigheter som de registrerade har enligt artiklarna 7 och 8 i stadgan.

66. Den hänskjutande domstolen har dessutom angett att unionsmedborgarna inte har tillgång till samma rättsmedel som amerikanska medborgare mot olaglig behandling av personuppgifter som utförs av de amerikanska myndigheterna. Det fjärde tillägget till Förenta staternas konstitution, vilket utgör det viktigaste skyddet mot olaglig övervakning, är inte tillämpligt på unionsmedborgare som inte har någon betydande frivillig koppling till Förenta staterna. Även om de sistnämnda har tillgång till vissa andra rättsmedel, är hindren för att använda sig av dem avsevärda.

67. Framför allt krävs det enligt artikel III i Förenta staternas konstitution för att väcka talan vid federal domstol att den berörda personen visar att han eller hon har talerätt (*standing*). Talerätt förutsätter bland annat att vederbörande visar att han eller hon lidit faktisk skada, som dels är konkret och ska beskrivas i detalj, dels är befintlig eller omedelbart förestående. Den hänskjutande domstolen har konstaterat, bland annat med hänvisning till domen från Supreme Court of the United States (Förenta staternas högsta domstol), Clapper mot Amnesty International US,[18] att detta villkor i praktiken är alltför svårt att uppfylla, särskilt eftersom det inte finns någon skyldighet att underrätta de registrerade om övervakningsåtgärder som vidtas mot dem.[19] En del av de rättsmedel som är tillgängliga för unionsmedborgarna omfattas dessutom av andra begränsande villkor, såsom att det måste visas att man lidit ekonomisk skada. Den suveräna immunitet som underrättelsetjänsterna tillerkänns och hemligstämplingen av informationen i fråga hindrar också utövandet av vissa rättsmedel.[20]

68. High Court (Förvaltningsöverdomstolen) har även beskrivit olika mekanismer för kontroll och tillsyn av underrättelsetjänsternas verksamhet.

69. Bland dessa återfinns den mekanism genom vilken FISC årligen certifierar program grundade på avsnitt 702 i FISA, inom ramen för vilken FISC emellertid inte godkänner individuella urvalstermer. När det gäller insamlin av utländska underrättelseuppgifter på grundval av EO 12333 görs ingen föregående domstolskontroll.

70. Den hänskjutande domstolen har vidare hänvisat till flera mekanismer för utomrättslig tillsyn av underrättelseverksamheten. Den har särskilt nämnt Inspectors General (allmänna inspektörer, Förenta staterna), som finns vid varje underrättelsetjänst och har i uppgift att utöva tillsyn över övervakningsverksamheten. Vidare finns Privacy and Civil Liberties Oversight Board (PCLOB) (Styrelsen för tillsyn av personlig integritet och medborgerliga fri- och rättigheter, Förenta staterna),

18 133 S.Ct. 1138 (2013).

19 Den hänskjutande domstolen har konstaterat att det emellertid finns ett undantag från principen att det inte krävs någon upplysning till den person som omfattas av en övervakningsåtgärd, nämligen om den amerikanska regeringen försöker använda uppgifter som samlats in enligt avsnitt 702 i FISA mot denna person inom ramen för ett straffrättsligt eller administrativt förfarande.

20 Den hänskjutande domstolen har särskilt påpekat att även om bestämmelserna i Privacy Act (lag om skydd för privatlivet), enligt vilken fysiska personer ska ges tillgång till information rörande dem som vissa organ innehar i samband med vissa tredjeländer, har utsträckts till unionsmedborgarna genom Judicial Redress Act (JRA) (lag om rätt till domstolsprövning), finns NSA inte med bland de organ som förtecknas i JRA.

ett oberoende organ inom den verkställande makten som mottar rapporter från de ombud för medborgerliga fri- och rättigheter eller personlig integritet (*civil liberties or privacy officers*) som utses vid varje underrättelsetjänst. PCLOB sammanställer regelbundna rapporter till kongressutskotten och presidenten. Underrättelsetjänsterna ska, bland annat till DNI, anmäla incidenter avseende åsidosättande av reglerna och förfarandena för insamling av utländsk underrättelseinformation. Dessa incidenter ska även rapporteras till FISC. Förenta staternas kongress har också, via underrättelseutskotten i representanthuset och i senaten, ansvar för att kontrollera verksamheten avseende utländsk underrättelseinformation.

71. High Court (Förvaltningsöverdomstolen) har emellertid betonat den grundläggande skillnaden mellan, å ena sidan, de regler som syftar till att säkerställa att uppgifterna erhålls lagligt och inte missbrukas när de väl har erhållits och, å andra sidan, de tillgängliga rättsmedlen när dessa regler har åsidosatts. Skyddet för de registrerades grundläggande rättigheter säkerställs endast om effektiva rättsmedel ger dem möjlighet att göra gällande sina rättigheter för det fallet att nämnda regler har åsidosatts.

72. Under dessa omständigheter anser den hänskjutande domstolen att det finns fog för de argument som DPC har anfört avseende att de begränsningar som föreskrivs i amerikansk lagstiftning när det gäller rätten till rättslig prövning för de personer vilkas uppgifter överförs från unionen inte är förenliga med det väsentliga innehållet i den rättighet som garanteras i artikel 47 i stadgan och i vart fall utgör ett oproportionerligt ingrepp i utövandet av denna rättighet.

73. Enligt High Court (Förvaltningsöverdomstolen) påverkas denna bedömning inte av att Förenta staternas regering har infört den ombudsmannamekanism som beskrivs i beslutet om skölden för skydd av privatlivet. Efter att ha betonat att denna mekanism är tillgänglig för unionsmedborgare som på skälig grund bedömer att deras personuppgifter har överförts i enlighet med besluten om standardavtalsklausuler,[21] har High Court (Förvaltningsöverdomstolen) påpekat att ombudsmannen inte utgör en domstol som uppfyller kraven i artikel 47 i stadgan och framför allt inte är oberoende av den verkställande makten.[22] High Court (Förvaltningsöverdomstolen) är även tveksam till huruvida ett ingripande av ombudsmannen, vars beslut inte kan vara föremål för rättslig prövning, motsvarar ett effektivt rättsmedel. Ett ingripande av ombudsmannen möjliggör nämligen inte för de personer vilkas personuppgifter har samlats in, behandlats eller delats olagligt att erhålla skadestånd eller ett föreläggande om att de olagliga handlingarna ska upphöra, eftersom ombudsmannen varken bekräftar eller förnekar att en person har varit föremål för elektronisk övervakning.

74. Efter att sålunda ha redogjort för sina farhågor rörande huruvida de skyddsåtgärder som föreskrivs i amerikansk rätt är väsentligen likvärdiga med de krav som följer av artiklarna 7, 8 och 47 i stadgan har den hänskjutande domstolen ifrågasatt huruvida de standardavtalsklausuler som föreskrivs i besluten om standardavtalsklausuler – vilka på grund av sin natur inte är bindande för de amerikanska myndigheterna – kan säkerställa skyddet för de registrerades grundläggande rättigheter. Den hänskjutande domstolen har mot denna bakgrund konstaterat att den delar DPC:s tvivel om huruvida besluten är giltiga.

75. Den hänskjutande domstolen anser särskilt att artikel 28.3 i direktiv 95/46, vilken det hänvisas till i artikel 4 i beslut 2010/87, inte räcker för att skingra dessa tvivel i den del tillsynsmyndigheterna däri tillerkänns befogenhet att avbryta eller förbjuda flöden av uppgifter som grundas på de standardavtalsklausuler som föreskrivs i detta beslut. Förutom att denna befogenhet enligt den hänskjutande domstolen endast är av diskretionär natur frågar den sig mot bakgrund av skäl 11 i

21 Den hänskjutande domstolen har på denna punkt hänvisat till bilaga III A till beslutet om skölden för skydd av privatlivet (se punkterna 37 och 38 ovan).

22 Den hänskjutande domstolen har hänvisat till domen av den 27 januari 2005, Denuit och Cordenier (C-125/04, EU:C:2005:69, punkt 12).

beslut 2010/87 huruvida det är möjligt att utöva den, när de konstaterade bristerna inte avser ett särskilt undantagsfall utan är av allmän och systematisk karaktär.[23] Den hänskjutande domstolen anser även att risken för att skiljaktiga beslut fattas i olika medlemsstater kan utgöra hinder för att det överlåts på tillsynsmyndigheterna att konstatera sådana brister.

76. Mot denna bakgrund beslutade High Court (Förvaltningsöverdomstolen) genom beslut av den 4 maj 2018,[24] vilket inkom till EU-domstolen den 9 maj 2018, att vilandeförklara målet och ställa följande frågor till EU-domstolen:

”1) I de fall då personuppgifter överförs av ett privat företag från en medlemsstat i [unionen] till ett privat företag i ett tredje land i kommersiellt syfte enligt [beslut 2010/87] och kan behandlas ytterligare i det tredje landet av dess myndigheter för att säkerställa den nationella säkerheten, men även för brottsbekämpande syften och genomförandet av utrikespolitiken i tredje land, ska unionsrätten (inklusive [stadgan]) tillämpas på överföring av uppgifter trots bestämmelserna i artikel 4.2 FEU i fråga om nationell säkerhet och bestämmelserna i artikel 3.2 första strecksatsen i [direktiv 95/46] i fråga om den allmänna säkerheten, försvaret, statens säkerhet?

2) a) Vid fastställandet av huruvida en enskild persons rättigheter har kränkts på grund av överföringen av uppgifter från [unionen] till ett tredje land enligt [beslut 2010/87] där de kan bli föremål för vidare behandling för ändamål som berör nationell säkerhet, är den relevanta jämförelsegrunden vid tillämpningen av [direktiv 95/46]

i) stadgan, FEU, FEUF, [direktiv 95/46], [Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, som undertecknades i Rom den 4 november 1950 (nedan kallad Europakonventionen)] (eller andra unionsrättsliga bestämmelser), eller

ii) den nationella lagstiftningen i en eller fler medlemsstater?

b) Om den relevanta jämförelsegrunden är ii), ska dåäven praxis i samband med den nationella säkerheten i en eller flera medlemsstater också användas som jämförelsegrund?

3) Vid bedömningen av om ett tredje land garanterar den skyddsnivå som föreskrivs i EU-lagstiftningen för personuppgifter som överförs till det landet i den mening som avses i artikel 26 i [direktiv 95/46], bör skyddsnivån i tredje land bedömas mot bakgrund av

a) regler som är tillämpliga i tredje land till följd av dess interna lagstiftning eller dess internationella förpliktelser samt praxis vad gäller att säkerställa iakttagandet av dessa regler, inbegripet de regler för yrkesverksamhet och säkerhet som gäller där,

eller

23 I skäl 11 i beslut 2010/87 anges följande: ”Tillsynsmyndigheterna i medlemsstaterna har en nyckelroll i samband med denna avtalsmekanism när det gäller att se till att personuppgifter omfattas av tillräckligt skydd efter överföring. I de undantagsfall då uppgiftsutföraren vägrar eller inte kan ge uppgiftsinföraren korrekta instruktioner och det finns en överhängande risk för att de registrerade lider allvarlig skada, bör standardavtalsklausulerna medge tillsynsmyndigheterna rätten att genomföra inspektioner hos uppgiftsinförare och underentreprenörer och i förekommande fall fatta beslut som är bindande för uppgiftsinföraren eller underentreprenören. Tillsynsmyndigheterna bör ha rätt att förbjuda eller avbryta en uppgiftsöverföring eller en serie överföringar som sker enligt standardavtalsklausuler i de undantagsfall där det fastställts att en överföring på avtalsbasis sannolikt har en avsevärt skadlig inverkan på de garantier och åtaganden som ska säkerställa adekvat skydd för den registrerade.”

24 Facebook Ireland överklagade beslutet om att begära förhandsavgörande till Supreme Court (Högsta domstolen, Irland). Överklagandet ogillades genom dom av den 31 maj 2019, Data Protection Commissioner mot Facebook Ireland Limited och Maximillian Schrems, överklagande nr 2018/68 (nedan kallad domen från Supreme Court (Högsta domstolen) av den 31 maj 2019).

b) de regler som avses i punkt a tillsammans med den administrativa praxis, regleringspraxis och efterlevnadspraxis samt politiska skyddsåtgärder, förfaranden, protokoll, tillsynsmekanismer och utomrättsliga åtgärder som gäller i tredje land?

4) Mot bakgrund av de omständigheter som har fastställts av High Court ([Förvaltningsöverdomstolen]) med avseende på amerikansk lag, föreligger en kränkning av enskilda personers rättigheter enligt artiklarna 7 och/eller 8 i stadgan om personuppgifter överförs från [unionen] till Förenta staterna enligt [beslut 2010/87]?

5) Mot bakgrund av de omständigheter som har fastställts av High Court med avseende på amerikansk lag

a) är den skyddsnivå som tillhandahålls i Förenta staterna förenlig med det väsentliga innehållet i en enskild persons rätt till domstolsprövning vid kränkning av hans eller hennes rättigheter rörande uppgiftsskydd som garanteras genom artikel 47 i stadgan om personuppgifter överförs från [unionen] till Förenta staterna enligt [beslut 2010/87]?

Om svaret i punkt a är jakande,

b) Är de begränsningar som föreskrivs i amerikansk lag för en enskild persons rätt till domstolsprövning i samband med Förenta staternas nationella säkerhet proportionerliga i den mening som avses i artikel 52 i stadgan och håller de sig inom ramen för vad som är nödvändigt i ett demokratiskt samhälle för att skydda den nationella säkerheten?

6) a) Vilken skyddsnivå ska tilldelas med avseende på personuppgifter som överförts till ett tredje land enligt standardavtalsklausuler som antagits i enlighet med ett kommissionsbeslut enligt artikel 26.4 [i direktiv 95/46] mot bakgrund av bestämmelserna i [detta direktiv], och i synnerhet artiklarna 25 och 26 jämförda med stadgan?

b) Vilka faktorer ska beaktas vid bedömningen av om den skyddsnivå som tilldelas med avseende på personuppgifter som överförs till ett tredje land enligt [beslut 2010/87] uppfyller kraven i [direktiv 95/46] och stadgan?

7) Innebär den omständigheten att standardavtalsklausuler tillämpas mellan uppgiftsutföraren och uppgiftsinföraren och är inte bindande för de nationella myndigheterna i tredje land som kan komma att kräva att uppgiftsinföraren ger säkerhetstjänsten i det landet tillgång till de personuppgifter som överförts enligt bestämmelserna i beslut [2010/87] för ytterligare behandling av personuppgifter att bestämmelserna inte kan säkerställa en adekvat skyddsnivå som föreskrivs i artikel 26.2 i [direktiv 95/46]?

8) Om en uppgiftsinförare i ett tredje land omfattas av lagar om övervakning som enligt [tillsynsmyndigheten] står i strid med [standardavtalsklausulerna] eller artiklarna 25 och 26 i [direktiv 95/46] och/eller stadgan, är en [tillsynsmyndighet] skyldig att utöva sina befogenheter att ingripa enligt artikel 28.3 i [direktiv 95/46] för att avbryta dataflödet eller kan dessa befogenheter enbart utövas i undantagsfall mot bakgrund av skäl 11 i [beslut 2010/87], eller kan en [tillsynsmyndighet] utnyttja sitt utrymme för skönsmässig bedömning för att inte avbryta dataflödet?

9) a) Utgör [beslutet om skölden för skydd av privatlivet] vid tillämpningen av artikel 25.6 i [direktiv 95/46], ett konstaterande med allmän giltighet som är bindande för [tillsynsmyndigheter] och medlemsstaternas domstolar, vilket innebär att Förenta staterna säkerställer en adekvat skyddsnivå i den mening som avses i artikel 25.2 i [direktiv 95/46], till följd av dess interna lagstiftning eller de internationella förpliktelser som landet har ingått?

b) Om så inte är fallet, vilken betydelse, om någon, har beslutet om skölden för skydd av privatlivet vid bedömningen av om de garantier som föreskrivs för uppgifter som överförs till Förenta staterna enligt [beslut 2010/87] är adekvata?

10) Mot bakgrund av vad som fastställts av High Court med avseende på amerikansk rätt, säkerställer en ombudsman för skölden för skydd av privatlivet enligt [bilaga III A till] beslutet om skölden för skydd av privatlivet tillsammans med den befintliga rättsordningen i Förenta staterna att Förenta staterna tillhandahåller ett rättsmedel för registrerade vars personuppgifter överförs till Förenta staterna enligt [beslut 2010/87] som är förenligt med artikel 47 i stadgan?

11) Utgör [beslut 2010/87] ett åsidosättande av artiklarna 7, 8 och/eller 47 i stadgan?”

77. DPC, Facebook Ireland, Maximillian Schrems, Förenta staternas regering, EPIC, BSA, Digitaleurope, Irland, den belgiska, den tjeckiska, den tyska, den nederländska, den österrikiska, den polska och den portugisiska regeringen, Förenade kungarikets regering, Europaparlamentet och kommissionen har inkommit med skriftliga yttranden till domstolen. DPC, Facebook Ireland, Maximillian Schrems, Förenta staternas regering, EPIC, BSA, Digitaleurope, Irland, den tyska, den franska, den nederländska och den österrikiska regeringen, Förenade kungarikets regering, parlamentet, kommissionen och Europeiska dataskyddsstyrelsen (European Data Protection Board, EDPB) var företrädda vid förhandlingen den 9 juli 2019.

IV. Bedömning

A. Inledande anmärkningar

78. Sedan domstolen genom domen Schrems ogiltigförklarade Safe Harbor-beslutet har överföringen av personuppgifter till Förenta staterna fortsatt på grundval av andra rättsliga grunder. Särskilt har uppgiftsutförarna kunnat använda sig av avtal med uppgiftsinförarna som innehåller standardklausuler utarbetade av kommissionen. Dessa klausuler utgör även den rättsliga grunden för överföring till ett stort antal andra tredjeländer, avseende vilka kommissionen inte har antagit något beslut om en adekvat skyddsnivå.[25] Enligt beslutet om skölden för skydd av privatlivet kan företag som har självcertifierat sin anslutning till de principer som anges i detta beslut numera överföra personuppgifter till Förenta staterna utan några ytterligare formaliteter.

79. Som det uttryckligen anges i begäran om förhandsavgörande och som BSA, Digitaleurope, Irland, den österrikiska och den franska regeringen, parlamentet och kommissionen har betonat, handlar det nationella mål som är anhängigt vid High Court (Förvaltningsöverdomstolen) endast om huruvida det beslut genom vilket kommissionen införde de standardavtalsklausuler som har åberopats till stöd för den överföring som avses i anmälan från Maximillian Schrems, det vill säga beslut 2010/87,[26] är giltigt.

80. Det nationella målet har sitt upphov i en ansökan, i vilken DPC begärde att den hänskjutande domstolen skulle hänskjuta en fråga till EU-domstolen avseende giltigheten av beslut 2010/87. Enligt den hänskjutande domstolen rör det nationella målet således utövandet av det rättsmedel som EU-domstolen genom punkt 65 i domen Schrems har ålagt medlemsstaterna att inrätta.

25 BSA har uppgett att 70 % av de företag som är medlemmar i BSA och som har svarat på en undersökning rörande denna fråga har förklarat att de använder standardavtalsklausuler som den huvudsakliga grunden för överföring av personuppgifter till tredjeländer. Även Digitaleurope bedömer att standardavtalsklausulerna utgör det huvudsakliga rättsliga instrumentet till stöd för överföring av personuppgifter.

26 Även om den hänskjutande domstolen har angett att begäran om förhandsavgörande avser giltigheten av de tre besluten om standardavtalsklausuler, eftersom dessa prövades i DPC:s utkast till beslut och domen av den 3 oktober 2017, hänvisas i giltighetsfrågorna uteslutande till beslut 2010/87. Detta beror på att Facebook Ireland vid den hänskjutande domstolen angav att detta beslut utgör den rättsliga grunden för överföringen av uppgifterna rörande de europeiska användarna av det sociala nätverket Facebook till Förenta staterna. Min bedömning avser således endast detta beslut.

81. Det ska erinras om att domstolen i punkt 63 i nämnda dom slog fast att en tillsynsmyndighet är skyldig att med vederbörlig omsorg utreda en anmälan i vilken en person, vars personuppgifter har eller kan komma att överföras till ett tredjeland som varit föremål för ett beslut om en adekvat skyddsnivå, gör gällande att beslutet inte är förenligt med de grundläggande rättigheter som föreskrivs i stadgan. I punkt 65 i samma dom slås fast att om denna myndighet anser att det finns fog för de invändningar som framförts i anmälan, måste den, i enlighet med artikel 28.3 första stycket tredje strecksatsen i direktiv 95/46 (som motsvaras av artikel 58.5 i dataskyddsförordningen) jämförd med artikel 8.3 i stadgan, ha befogenhet att inleda rättsliga förfaranden. Den nationella lagstiftaren måste föreskriva rättsmedel som gör det möjligt för tillsynsmyndigheten att vid nationella domstolar göra gällande dessa invändningar, så att nationella domstolar, för det fall att de delar tillsynsmyndighetens tvivel, kan hänskjuta en begäran om förhandsavgörande avseende beslutets giltighet.

82. I likhet med den hänskjutande domstolen anser jag att dessa konstateranden är analogt tillämpliga när en tillsynsmyndighet vid prövningen av en anmälan som ingetts till den tvivlar på, inte huruvida ett beslut om en adekvat skyddsnivå är giltigt, utan huruvida ett sådant beslut som beslut 2010/87, i vilket standardavtalsklausuler för överföring av personuppgifter till tredjeländer fastställts, är giltigt. I motsats till vad den tyska regeringen har gjort gällande spelar det ingen roll om dessa tvivel har föranletts av de invändningar som framförts av den som ingett anmälan eller om tillsynsmyndigheten på eget initiativ ifrågasätter giltigheten av beslutet i fråga. De krav som följer av artikel 58.5 i dataskyddsförordningen och artikel 8.3 i stadgan, som EU-domstolens resonemang grundar sig på, är nämligen tillämpliga oavsett den rättsliga grunden för den överföring som avses i anmälan till tillsynsmyndigheten och de skäl som föranlett denna att tvivla på giltigheten av det beslut som avses i anmälan.

83. Med detta sagt ska det konstateras att DPC har anmodat den hänskjutande domstolen att ställa frågor till EU-domstolen om giltigheten av beslut 2010/87, eftersom DPC anser att ett klargörande från EU-domstolen är nödvändigt för prövningen av den anmälan genom vilken Maximillian Schrems har begärt att DPC ska utöva sin befogenhet enligt artikel 28.3 andra strecksatsen i direktiv 95/46 – numera enligt artikel 58.2 f i dataskyddsförordningen – att avbryta överföringen av hans personuppgifter från Facebook Ireland till Facebook Inc.

84. Medan det nationella målet således endast avser huruvida beslut 2010/87 hypotetiskt är giltigt, avser det bakomliggande förfarandet vid DPC myndighetens utövande av sina korrigerande befogenheter *i ett specifikt fall*. Jag kommer att föreslå att EU-domstolen ska pröva de ställda frågorna endast i den mån det är nödvändigt för att avgöra huruvida beslut 2010/87 är giltigt, eftersom en sådan prövning räcker för att den hänskjutande domstolen ska kunna avgöra det mål som är anhängigt vid den.[27]

85. Innan jag går in på bedömningen av huruvida detta beslut är giltigt behöver vissa invändningar tillbakavisas som har framförts mot att begäran om förhandsavgörande tas upp till prövning.

B. Huruvida begäran om förhandsavgörande kan tas upp till prövning

86. Det har invänts mot huruvida begäran om förhandsavgörande kan tas upp till prövning och detta av olika skäl som huvudsaklig avser att direktiv 95/46, vilket det hänvisas till i giltighetsfrågorna, inte är tidsmässigt tillämpligt (*ratione temporis*) (avsnitt 1), att förfarandet vid DPC inte är tillräckligt långt framskridet för att prövningen ska vara motiverad (avsnitt 2) och att osäkerhet kvarstår kring de faktiska omständigheter som den hänskjutande domstolen har beskrivit (avsnitt 3).

27 Se punkterna 167 till 186 nedan.

87. Innan jag bemöter dessa invändningar om rättegångshinder ska det erinras om att frågor som hänskjuts till EU-domstolen enligt artikel 267 FEUF presumeras vara relevanta. Enligt fast rättspraxis kan domstolen avvisa en begäran om förhandsavgörande endast då det är uppenbart att den begärda tolkningen av unionsrätten inte har något samband med de verkliga omständigheterna eller saken i det nationella målet eller då frågorna är hypotetiska eller EU-domstolen inte har tillgång till sådana uppgifter om de faktiska eller rättsliga omständigheterna som är nödvändiga för att kunna ge ett användbart svar på de frågor som ställts till den. [28]

1. Den tidsmässiga tillämpligheten (ratione temporis) av direktiv 95/46

88. Facebook Ireland har gjort gällande att giltighetsfrågorna inte kan tas upp till prövning, eftersom det i dem hänvisas till direktiv 95/46, trots att detta direktiv har upphävts och ersatts av dataskyddsförordningen med verkan från och med den 25 maj 2018. [29]

89. Jag delar synsättet att giltigheten av beslut 2010/87 ska prövas mot bakgrund av bestämmelserna i dataskyddsförordningen.

90. I artikel 94.2 i dataskyddsförordningen föreskrivs att ”[h]änvisningar till det upphävda direktivet ska anses som hänvisningar till denna förordning”. Av detta följer enligt min mening att hänvisningen i beslut 2010/87 till artikel 26.4 i direktiv 95/46 som rättslig grund, ska förstås som en hänvisning till artikel 46.2 c i dataskyddsförordningen, vilken i allt väsentligt har samma innehåll. [30] De genomförandebeslut som kommissionen innan dataskyddsförordningen trädde i kraft hade antagit enligt artikel 26.4 i direktiv 95/46 ska följaktligen tolkas mot bakgrund av denna förordning. Det är också mot bakgrund av denna förordning som deras giltighet vid behov ska bedömas.

91. Detta konstaterande påverkas inte av den rättspraxis enligt vilken lagligheten av en unionsrättsakt ska bedömas mot bakgrund av de faktiska och rättsliga omständigheter som förelåg vid tiden för rättsaktens antagande. Denna rättspraxis avser nämligen prövningen av huruvida en unionsrättsakt är giltig mot bakgrund av de relevanta faktiska omständigheterna vid tiden för dess antagande [31] eller mot bakgrund av förfaranderegleрna för dess antagande. [32] Däremot har domstolen upprepade gånger prövat giltigheten av sekundärrättsakter mot bakgrund av överordnade materiella normer som trätt i kraft efter rättsaktens antagande. [33]

28 Se, bland annat, dom av den 10 december 2018, Wightman m.fl. (C-621/18, EU:C:2018:999, punkt 27), och dom av den 19 november 2019, A. K. m.fl. (Oberoendet för avdelningen för disciplinära mål vid högsta domstolen) (C-585/18, C-624/18 och C-625/18, EU:C:2019:982, punkt 98).

29 Se artiklarna 94.1 och 99.1 i dataskyddsförordningen.

30 Det ska betonas att enligt artikel 46.5 i dataskyddsförordningen ska de beslut som fattats av kommissionen på grundval av artikel 26.4 i direktiv 95/46 förbli i kraft tills de ändrats, ersatts eller upphävts.

31 Se, bland annat, dom av den 7 februari 1979, Frankrike/kommissionen (15/76 och 16/76, EU:C:1979:29, punkt 7), dom av den 17 maj 2001, IECC/kommissionen (C-449/98 P, EU:C:2001:275, punkt 87), och dom av den 17 oktober 2013, Schaible (C-101/12, EU:C:2013:661, punkt 50).

32 Se, bland annat, dom av den 16 april 2015, parlamentet/rådet (C-540/13, EU:C:2015:224, punkt 35), dom av den 16 april 2015, parlamentet/rådet (C-317/13 och C-679/13, EU:C:2015:223, punkt 45), och dom av den 22 september 2016, parlamentet/rådet (C-14/15 och C-116/15, EU:C:2016:715, punkt 48).

33 Det ska särskilt påpekas att i domen Schrems bedömde domstolen giltigheten av Safe Harbor-beslutet mot bakgrund av bestämmelserna i stadgan, vilken antogs vid en senare tidpunkt än det beslutet. Se även dom av den 17 mars 2011, AJD Tuna (C-221/09, EU:C:2011:153, punkt 48), och dom av den 11 juni 2015, Pfeifer & Langen (C-51/14, EU:C:2015:380, punkt 42).

92. Även om den omständigheten att det i tolknings- och giltighetsfrågorna hänvisas till en rättsakt som inte längre är tidsmässigt tillämplig (*ratione temporis*) motiverar att frågorna omformuleras, kan det emellertid inte medföra att de inte kan tas upp till prövning.[34] Som DPC och Maximillian Schrems har gjort gällande kan hänvisningarna i tolknings- och giltighetsfrågorna till direktiv 95/46 dessutom förklaras av tidsschemat för förfarandet i förevarande mål, eftersom frågorna hade hänskjutits till EU-domstolen innan dataskyddsförordningen trädde i kraft.

93. De bestämmelser i dataskyddsförordningen som kommer att behandlas vid bedömningen av tolknings- och giltighetsfrågorna – det vill säga framför allt artiklarna 45, 46 och 58 – återger i vart fall i allt väsentligt innehållet i artiklarna 25, 26 och 28 i direktiv 95/46, med viss utveckling så när som på vissa nyanser. Vad gäller de aspekter av bestämmelserna som är relevanta för att avgöra huruvida beslut 2010/87 är giltigt, ser jag inget skäl till att ge dessa bestämmelser i dataskyddsförordningen en annan räckvidd än den som motsvarande bestämmelser i direktiv 95/46 har.[35]

2. Den prelimära karaktären hos de tvivel som uttryckts av DPC

94. Enligt den tyska regeringen kan begäran om förhandsavgörande inte tas upp till prövning, eftersom det för att inleda ett rättsligt förfarande i enlighet med punkt 65 i domen Schrems krävs att tillsynsmyndigheten har bildat sig en slutgiltig uppfattning om huruvida det finns fog för de invändningar som har anförts mot det ifrågavarande beslutets giltighet. Så är inte fallet här, eftersom DPC har uttryckt sina tvivel om giltigheten av beslut 2010/87 – som Maximillian Schrems för övrigt inte har invänt mot – i ett utkast till beslut som meddelats preliminärt och inte påverkar ett eventuellt ingivande av ytterligare synpunkter från Facebook Ireland och Maximillian Schrems.

95. Att DPC:s tvivel är av preliminär karaktär påverkar enligt min mening inte huruvida begäran om förhandsavgörande kan tas upp till prövning. De kriterier som avgör om en tolknings- eller en giltighetsfråga kan tas upp till prövning ska nämligen bedömas mot bakgrund av saken i det nationella målet såsom den har angetts av den hänskjutande domstolen.[36] Det framgår att saken i det nationella målet avser giltigheten av beslut 2010/87. Av ordalydelsen i begäran om förhandsavgörande och den därtill bifogade domen framgår att den hänskjutande domstolen har bedömt att de tvivel som uttryckts av DPC – oavsett om de är preliminära eller slutgiltiga – är välgrundade och att den följaktligen har ställt frågor till EU-domstolen om giltigheten av detta beslut. Under dessa omständigheter är ett klargörande från EU-domstolen i denna fråga utan tvekan relevant för att den hänskjutande domstolen ska kunna avgöra målet.

3. Osäkerheten kring de faktiska omständigheter som har fastställts

96. Förenade kungarikets regering har hävdat att den hänskjutande domstolens beskrivning av de faktiska omständigheterna är bristfällig på flera punkter, vilket gör att giltighetsfrågorna inte kan tas upp till prövning. Den hänskjutande domstolen har inte klarlagt huruvida personuppgifterna rörande Maximillian Schrems faktiskt har överförts till Förenta staterna och inte heller, om så är fallet, huruvida de har samlats in av de amerikanska myndigheterna. Den rättsliga grunden för den eventuella överföringen har inte heller angetts med säkerhet, eftersom det i begäran om förhandsavgörande endast anges att uppgifterna rörande de europeiska användarna av det sociala nätverket Facebook ”till stor del” överförs på grundval av de standardavtalsklausuler som föreskrivs i beslut 2010/87. Det har i vart fall inte fastställts att det avtal mellan Facebook Ireland och Facebook

34 Se, bland annat, dom av den 15 juli 2010, Pannon Gép Centrum (C-368/09, EU:C:2010:441, punkterna 30–35), dom av den 10 februari 2011, Andersson (C-30/10, EU:C:2011:66, punkterna 20 och 21), och dom av den 25 oktober 2018, Roche Lietuva (C-413/17, EU:C:2018:865, punkterna 17–20).

35 Se förslag till avgörande av generaladvokaten Bobek i målet Fashion ID (C-40/17, EU:C:2018:1039, punkt 87).

36 Se punkt 87 ovan.

Inc. som har åberopats till stöd för den omtvistade överföringen troget återger dessa klausuler. Också den tyska regeringen har bestritt att begäran om förhandsavgörande kan tas upp till prövning, av det skälet att den hänskjutande domstolen inte har utrett huruvida Maximillian Schrems otvetydigt har samtyckt till överföringen i fråga, i vilket fall överföringen är förenlig med artikel 26.1 i direktiv 95/46 (vars innehåll i allt väsentligt återges i artikel 49.1 a i dataskyddsförordningen).

97. Dessa argument påverkar inte att begäran om förhandsavgörande är relevant mot bakgrund av saken i det nationella målet. Eftersom det nationella målet har sitt upphov i DPC:s utövande av det rättsmedel som föreskrivs i punkt 65 i domen Schrems, består själva saken i att den nationella domstolen ska begära ett förhandsavgörande om giltigheten av beslut 2010/87. Den tyska regeringen och Förenade kungarikets regering har egentligen bestritt att giltighetsfrågorna är nödvändiga för att DPC konkret ska kunna uttala sig om anmälan från Maximillian Schrems och inte för att avgöra huruvida beslut 2010/87 är giltigt.

98. Inte heller för det bakomliggande förfarande som har föranlett det nationella målet saknar frågorna avseende giltigheten av beslut 2010/87 emellertid relevans. Den hänskjutande domstolen har nämligen fastställt att Facebook Ireland har fortsatt att överföra uppgifter rörande sina användare till Förenta staterna efter det att Safe Harbor-beslutet ogiltigförklarades och att denna överföring åtminstone delvis grundar sig på beslut 2010/87. Det ankommer dessutom uteslutande på den hänskjutande domstolen att bedöma i vilket skede av förfarandet den har behov av ett förhandsavgörande från EU-domstolen, även om det kan vara fördelaktigt att alla de relevanta faktiska omständigheterna har fastställts innan den utövar sin befogenhet enligt artikel 267 FEUF. [37]

99. Mot bakgrund av det ovan anförda anser jag att begäran om förhandsavgörande kan tas upp till prövning.

C. Huruvida unionsrätten är tillämplig på överföring av personuppgifter för kommersiella syften till ett tredjeland som kan komma att behandla uppgifterna för syften som avser den nationella säkerheten (den första frågan)

100. Genom den första frågan vill den hänskjutande domstolen få klarhet i huruvida unionsrätten är tillämplig på överföring av personuppgifter från ett bolag i en medlemsstat till ett bolag i ett tredjeland som utförs av kommersiella skäl, om uppgifterna efter det att överföringen har inletts kan komma att behandlas av offentliga myndigheter i tredjelandet för syften som inbegriper att skydda den nationella säkerheten.

101. Betydelsen av denna fråga för att avgöra det nationella målet ligger i den omständigheten att om en sådan överföring inte omfattas av unionsrättens tillämpningsområde, är samtliga de invändningar som i förevarande mål har framställts mot giltigheten av beslut 2010/87 ogrundade.

102. Enligt artikel 3.2 i direktiv 95/46 omfattades behandling av personuppgifter för syften som avsåg den nationella säkerheten, såsom den hänskjutande domstolen har påpekat, inte av direktivets tillämpningsområde. I artikel 2.2 i dataskyddsförordningen anges att denna förordning inte ska tillämpas bland annat på behandling av personuppgifter som utgör ett led i en verksamhet som inte omfattas av unionsrätten eller behandling som behöriga myndigheter utför i syfte att skydda den allmänna säkerheten. Dessa bestämmelser speglar den befogenhet som medlemsstaterna förbehålls enligt artikel 4.2 FEU när det gäller skyddet av den nationella säkerheten.

37 Se, för ett liknande resonemang, dom av den 1 april 1982, Holdijk m.fl. (141/81 till 143/81, EU:C:1982:122, punkt 5), och dom av den 9 december 2003, Gasser (C-116/02, EU:C:2003:657, punkt 27).

103. DPC, Maximillian Schrems, Irland, den tyska, den österrikiska, den belgiska, den tjeckiska, den nederländska, den polska och den portugisiska regeringen, parlamentet och kommissionen har gjort gällande att den överföring som avses i anmälan från Maximillian Schrems inte omfattas av dessa bestämmelser och att den följaktligen omfattas av unionsrättens tillämpningsområde. Facebook Ireland har hävdat det motsatta. Jag instämmer i förstnämnda åsikt.

104. Det ska härvid betonas att överföring av personuppgifter från en medlemsstat till ett tredjeland i sig utgör ”behandling” i den mening som avses i artikel 4.2 i dataskyddsförordningen, som utförs inom en medlemsstats territorium. [38] Den första giltighetsfrågan syftar just till ett fastställande av huruvida unionsrätten är tillämplig *på den behandling som själva överföringen utgör*. Denna fråga avser inte huruvida unionsrätten är tillämplig på den eventuella ytterligare behandling av de till Förenta staterna överförda personuppgifterna som de amerikanska myndigheterna utför för syften som avser den nationella säkerheten, vilken inte omfattas av dataskyddsförordningens territoriella tillämpningsområde. [39]

105. För att fastställa huruvida unionsrätten är tillämplig på den ifrågavarande överföringen av uppgifter ska således endast den verksamhet beaktas inom ramen för vilken överföringen utförs. Det saknar betydelse vilket syftet är med den eventuella ytterligare behandling av de överförda uppgifterna som utförs av de offentliga myndigheterna i det tredjeland som är bestämmelseland. [40]

106. Av begäran om förhandsavgörande framgår att den överföring som avses i anmälan från Maximillian Schrems ingår i en kommersiell verksamhet. Överföringen äger inte rum i syfte att möjliggöra för de amerikanska myndigheterna att ytterligare behandla uppgifterna i fråga för syften som avser den nationella säkerheten.

107. Det synsätt som Facebook Ireland har anfört skulle frånta dataskyddsförordningens bestämmelser om överföring till tredjeländer deras ändamålsenliga verkan, eftersom det aldrig kan uteslutas att uppgifter som överförs inom ramen för en kommersiell verksamhet efter överföringen kommer att behandlas för syften som avser den nationella säkerheten.

108. Den tolkning som jag föreslår finner stöd i ordalydelsen i artikel 45.2 a i dataskyddsförordningen. I denna bestämmelse anges att när kommissionen antar ett beslut om en adekvat skyddsnivå ska den bland annat beakta det aktuella tredjelandets lagstiftning *avseende nationell säkerhet*. Av detta kan man sluta sig till att möjligheten att uppgifterna kommer att behandlas av myndigheterna i det tredjeland som är bestämmelseland i syfte att skydda den nationella säkerheten inte innebär att unionsrätten inte är tillämplig på den behandling som överföringen av uppgifterna till tredjelandet i fråga utgör.

38 Se, för ett liknande resonemang, dom av den 30 maj 2006, parlamentet/rådet och kommissionen (C-317/04 och C-318/04, EU:C:2006:346, punkt 56) (nedan kallad domen PNR), och domen Schrems (punkt 45). Artikel 4.2 i dataskyddsförordningen återger i allt väsentligt den definition av begreppet ”behandling” som gavs i artikel 2 b i direktiv 95/46.

39 Enligt artikel 3.1 i dataskyddsförordningen ska denna förordning tillämpas på all behandling av personuppgifter inom ramen för den verksamhet som bedrivs av en personuppgiftsansvarig eller ett personuppgiftsbiträde som är etablerad i unionen, oavsett om behandlingen utförs i unionen eller inte. Frågan om huruvida unionsrätten är tillämplig på behandling som ett tredjelands underrättelsetjänster utför utanför unionen ska skiljas från frågan om relevansen av de regler och den praxis som kringgärdar denna behandling i tredjelandet i fråga när det gäller att avgöra huruvida en adekvat skyddsnivå säkerställs där. Det sistnämnda är föremål för den andra giltighetsfrågan och behandlas i punkterna 201–229 nedan.

40 I mitt förslag till avgörande i målet Ministerio Fiscal (C-207/16, EU:C:2018:300, punkt 47) betonade jag skillnaden mellan, å ena sidan, direkt behandling av personuppgifter inom ramen för statens ”regala” verksamhet och, å andra sidan, kommersiell behandling som följs av att offentliga myndigheter använder personuppgifterna.

109. Domstolens resonemang och konstateranden i domen Schrems vilar också på denna premiss. I den domen prövade domstolen särskilt huruvida Safe Harbor-beslutet var giltigt mot bakgrund av artikel 25.6 i direktiv 95/46 jämförd med stadgan, i den del det avsåg överföring av personuppgifter till Förenta staterna, där uppgifterna kunde komma att samlas in och behandlas i syfte att skydda den nationella säkerheten. [41]

110. Mot bakgrund av det ovan anförda anser jag att unionsrätten är tillämplig på överföring av personuppgifter från en medlemsstat till ett tredjeland när överföringen ingår i en kommersiell verksamhet, oavsett om de överförda uppgifterna riskerar att behandlas av de offentliga myndigheterna i detta tredjeland i syfte att skydda den nationella säkerheten.

D. Den skyddsnivå som krävs när överföringen grundar sig på standardavtalsklausuler (den sjätte frågans första del)

111. Genom den sjätte frågans första del vill den hänskjutande domstolen få klarhet i vilken skyddsnivå för de registrerades grundläggande rättigheter som måste säkerställas för att personuppgifter ska kunna överföras till ett tredjeland på grundval av de standardavtalsklausuler som föreskrivs i beslut 2010/87.

112. Den hänskjutande domstolen har betonat att EU-domstolen i domen Schrems tolkade artikel 25.6 i direktiv 95/46 (vars innehåll i allt väsentligt återges i artikel 45.3 i dataskyddsförordningen), i den del det däri föreskrevs att kommissionen får anta ett beslut om en adekvat skyddsnivå först efter att ha försäkrat sig om att tredjelandet i fråga säkerställer en adekvat skyddsnivå, så att det krävs att detta tredjeland säkerställer en nivå för skyddet av de grundläggande rättigheterna och friheterna som är *väsentligen likvärdig* den skyddsnivå som garanteras inom unionen enligt detta direktiv jämfört med stadgan. [42]

113. I detta sammanhang har EU-domstolen genom den sjätte giltighetsfrågans första del anmodats att fastställa huruvida tillämpningen av ”standardavtalsklausuler” som har antagits av kommissionen i enlighet med artikel 26.4 i direktiv 95/46 – vilka motsvarar de ”standardiserade dataskyddsbestämmelser” som anges i artikel 46.2 c i dataskyddsförordningen – måste möjliggöra uppnåendet av en skyddsnivå som motsvarar samma standard, det vill säga ”väsentlig likvärdighet”.

114. I artikel 46.1 i dataskyddsförordningen föreskrivs att en personuppgiftsansvarig i avsaknad av ett beslut om en adekvat skyddsnivå får överföra personuppgifter till ett tredjeland ”endast … efter att ha vidtagit *lämpliga skyddsåtgärder*, och på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga” (min kursivering). [43] Enligt artikel 46.2 c i dataskyddsförordningen kan dessa skyddsåtgärder ta formen av standardiserade dataskyddsbestämmelser som utarbetats av kommissionen.

115. I likhet med DPC, Maximillian Schrems och Irland anser jag att de ”lämpliga skyddsåtgärder” som den personuppgiftsansvarige ska vidta enligt artikel 46.1 i dataskyddsförordningen måste säkerställa att de personer vilkas uppgifter överförs, precis som vid överföring baserad på ett beslut om en adekvat skyddsnivå, åtnjuter en skyddsnivå för sina rättigheter som är väsentligen likvärdig den som följer av dataskyddsförordningen jämförd med stadgan.

41 På samma sätt prövade domstolen i yttrande 1/15 (PNR-avtalet mellan EU och Kanada) av den 26 juli 2017 (EU:C:2017:592) (nedan kallat yttrande 1/15) huruvida ett förslag till internationellt avtal mellan Kanada och unionen avseende personuppgifter, som när de väl överförts till Kanada var avsedda att behandlas av de offentliga myndigheterna i syfte att skydda den nationella säkerheten, var förenligt med artiklarna 7, 8 och 47 i stadgan.

42 Domen Schrems (punkt 73). Domstolen har bekräftat detta konstaterande i yttrande 1/15 (punkt 134).

43 I artikel 26.2 i direktiv 95/46 föreskrevs att en medlemsstat får tillåta en sådan överföring ”om den registeransvarige ställer *tillräckliga garantier* för att privatliv och enskilda personers grundläggande fri- och rättigheter skyddas samt för utövningen av motsvarande rättigheter” (min kursivering). Begreppen ”tillräckliga garantier” och ”lämpliga skyddsåtgärder”, vilka används i nämnda bestämmelse respektive artikel 46.1 i dataskyddsförordningen, har enligt min mening samma innebörd.

116. Denna slutsats följer av syftet med denna bestämmelse och det instrument som den ingår i.

117. Artiklarna 45 och 46 i dataskyddsförordningen syftar till att säkerställa att den höga skyddsnivå för personuppgifter som föreskrivs i denna förordning vidmakthålls när uppgifterna överförs till länder utanför unionen. Kapitel V i dataskyddsförordningen, som handlar om överföring till tredjeländer, inleds med artikel 44, som har rubriken ”Allmän princip för överföring av uppgifter” och i vilken det anges att alla bestämmelser i detta kapitel ska tillämpas för att säkerställa att den skyddsnivå som säkerställs genom dataskyddsförordningen inte undergrävs vid överföring till ett tredjeland. [44] Denna bestämmelse syftar till att förhindra att de skyddsstandarder som följer av unionsrätten kringgås genom att personuppgifter överförs till ett tredjeland för att behandlas där. [45] Mot bakgrund av detta syfte är det ingen skillnad om överföringen grundas på ett beslut om en adekvat skyddsnivå eller på skyddsåtgärder som den personuppgiftsansvarige har vidtagit, bland annat genom avtalsklausuler. Kraven på skydd av de grundläggande rättigheter som garanteras i stadgan är de samma oavsett på vilken rättslig grund en viss överföring baseras. [46]

118. Det sätt på vilket en hög skyddsnivå vidmakthålls skiljer sig däremot beroende på den rättsliga grunden för överföringen.

119. Ett beslut om en adekvat skyddsnivå, å ena sidan, syftar till ett fastställande av att tredjelandet i fråga självt säkerställer en skyddsnivå som är väsentligen likvärdig den som måste uppnås i unionen. För att anta ett beslut om en adekvat skyddsnivå avseende ett tredjeland krävs att kommissionen först har utvärderat den skyddsnivå som säkerställs i tredjelandets lagstiftning och praxis mot bakgrund av de faktorer som anges i artikel 45.3 i dataskyddsförordningen. Personuppgifter kan då överföras till tredjelandet i fråga utan att den personuppgiftsansvarige måste erhålla ett särskilt tillstånd.

120. De lämpliga skyddsåtgärder som ska vidtas av den personuppgiftsansvarige, å andra sidan, syftar – som det beskrivs närmare i nästa avsnitt – till att säkerställa en hög skyddsnivå när de tillgängliga skyddsåtgärderna i det tredjeland som är bestämmelseland inte är tillräckliga. Även om artikel 46.1 i dataskyddsförordningen tillåter att personuppgifter överförs till tredjeländer som inte säkerställer en adekvat skyddsnivå, får således personuppgifter överföras i enlighet med denna bestämmelse endast om lämpliga skyddsåtgärder har vidtagits genom andra medel. De standardavtalsklausuler som kommissionen har antagit utgör härvid en allmän mekanism som kan tillämpas på överföringen oavsett vilket tredjeland som är bestämmelseland och vilken skyddsnivå som säkerställs där.

E. Huruvida beslut 2010/87 är giltigt mot bakgrund av artiklarna 7, 8 och 47 i stadgan (den sjunde, den åttonde och den elfte frågan)

121. Genom den sjunde frågan vill den hänskjutande domstolen få klarhet i huruvida beslut 2010/87 är ogiltigt, eftersom det inte är bindande för myndigheterna i de tredjeländer till vilka uppgifter överförs i enlighet med de standardavtalsklausuler som föreskrivs i bilagan till detta beslut och särskilt eftersom det inte hindrar att nämnda myndigheter kräver att uppgiftsinföraren ställer uppgifterna till deras förfogande. Genom denna fråga ifrågasätts således själva möjligheten att säkerställa en adekvat skyddsnivå för sådana uppgifter genom mekanismer som uteslutande är av avtalskaraktär. Den elfte frågan avser mer allmänt giltigheten av beslut 2010/87 mot bakgrund av artiklarna 7, 8 och 47 i stadgan.

44 I skäl 6 i dataskyddsförordningen anges att en ”hög skyddsnivå” för personuppgifter bör säkerställas inom unionen såväl som vid överföring till tredjeländer. Se även skäl 101 i dataskyddsförordningen.

45 Se domen Schrems (punkt 73) och yttrande 1/15 (punkt 214).

46 Detta påverkar inte möjligheten att även i avsaknad av lämpliga skyddsåtgärder överföra personuppgifter i enlighet med de undantag som föreskrivs i artikel 49.1 i dataskyddsförordningen.

122. Genom den åttonde frågan har EU-domstolen anmodats att avgöra huruvida en tillsynsmyndighet är skyldig att använda sig av sina befogenheter enligt artikel 58.2 f och j i dataskyddsförordningen för att avbryta en överföring till tredjeland som grundar sig på de standardavtalsklausuler som föreskrivs i beslut 2010/87, om den anser att uppgiftsinföraren har skyldigheter i tredjelandet i fråga som hindrar denne från att följa klausulerna och som får till verkan att ett lämpligt skydd för de överförda uppgifterna inte säkerställs. Eftersom svaret på denna fråga enligt min mening påverkar giltigheten av beslut 2010/87,[47] behandlar jag den tillsammans med den sjunde och den elfte frågan.

123. Ordalydelsen i artikel 46.1 i dataskyddsförordningen, där det föreskrivs att *”[i] avsaknad av ett beslut i enlighet med artikel 45.3*, får en personuppgiftsansvarig eller ett personuppgiftsbiträde endast överföra personuppgifter till ett tredjeland… *efter att ha vidtagit* lämpliga skyddsåtgärder…” (min kursivering), framhäver den logik som ligger till grund för sådana avtalsmekanismer som den som föreskrivs i beslut 2010/87. Som det betonas i skälen 108 och 114 i dataskyddsförordningen syftar dessa mekanismer till att möjliggöra överföring till tredjeländer avseende vilka kommissionen inte har antagit något beslut om en adekvat skyddsnivå, varvid de eventuella bristerna i det skydd som säkerställs i tredjelandets rättsordning *kompenseras* genom de skyddsåtgärder som uppgiftsutföraren och uppgiftsinföraren genom avtal åtar sig att iaktta.

124. Eftersom skälet till de avtalsmässiga skyddsåtgärdernas existens just är att de ska kompensera för möjliga brister i det skydd som det tredjeland som är bestämmelseland säkerställer, oavsett vilka dessa brister är, kan giltigheten av ett beslut genom vilket kommissionen konstaterar att vissa standardklausuler på ett adekvat sätt kompenserar för dessa brister inte vara beroende av den skyddsnivå som säkerställs i respektive tredjeland till vilka uppgifter kan överföras. Giltigheten av ett sådant beslut är endast beroende av hur pålitliga de skyddsåtgärder som föreskrivs i klausulerna är, när det gäller att kompensera för de eventuella brister i skyddet i det tredjeland som är bestämmelseland. Vid utvärderingen av skyddsåtgärdernas effektivitet ska hänsyn även tas till det skydd som tillsynsmyndigheternas befogenheter enligt artikel 58.2 i dataskyddsförordningen innebär.

125. Som DPC, Maximillian Schrems, BSA, Irland, den österrikiska, den franska, den polska och den portugisiska regeringen och kommissionen har hävdat kan det skydd som följer av standardavtalsklausulerna försvagas eller till och med omintetgöras, om uppgiftsinföraren enligt lagstiftningen i det tredjeland som är bestämmelseland åläggs skyldigheter som strider mot kraven i dessa klausuler. Det rättsliga sammanhang som råder i det tredjeland som är bestämmelseland kan, beroende på de konkreta omständigheterna kring överföringen,[48] göra det omöjligt att uppfylla de skyldigheter som föreskrivs i standardavtalsklausulerna.

126. Den avtalsmekanism som föreskrivs i artikel 46.2 c i dataskyddsförordningen vilar under dessa omständigheter, som Maximillian Schrems och kommissionen har betonat, på att uppgiftsutföraren och i andra hand tillsynsmyndigheterna görs ansvariga. Den personuppgiftsansvarige eller vid behov tillsynsmyndigheten måste för varje specifik överföring *från fall till fall* granska huruvida lagstiftningen i det tredjeland som är bestämmelseland hindrar genomförandet av standardklausulerna och följaktligen hindrar ett lämpligt skydd för de överförda uppgifterna, vilket innebär att överföringen måste förbjudas eller avbrytas.

47 Se punkt 128 nedan.

48 Föreställ dig till exempel att ett tredjeland föreskriver en skyldighet för telekomtjänsteleverantörer att ge de offentliga myndigheterna åtkomst till de överförda uppgifterna utan några begränsningar eller garantier. Även om dessa leverantörer då inte förmår uppfylla standardavtalsklausulerna, är de företag som inte ålagts denna skyldighet dock inte förhindrade från att uppfylla dem.

127. Mot bakgrund av det ovan anförda anser jag att den omständigheten att beslut 2010/87 och de standardavtalsklausuler som det innehåller inte är bindande för myndigheterna i det tredjeland som är bestämmelseland inte i sig gör detta beslut ogiltigt. Huruvida beslut 2010/87 är förenligt med artiklarna 7, 8 och 47 i stadgan beror enligt min uppfattning på huruvida det finns tillräckligt pålitliga mekanismer som gör det möjligt att säkerställa att de överföringar som grundar sig på standardavtalsklausulerna kan avbrytas eller förbjudas, om klausulerna åsidosätts eller om det är omöjligt att följa dem.

128. I artikel 46.1 i dataskyddsförordningen föreskrivs att en överföring som grundar sig på lämpliga skyddsåtgärder endast får ske ”på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga”. Det måste kontrolleras om de garantier som föreskrivs i klausulerna i bilagan till beslut 2010/87, kompletterade med tillsynsmyndigheternas befogenheter, gör det möjligt att säkerställa att detta villkor är uppfyllt. Detta är enligt min mening fallet endast om det föreligger en *skyldighet* – för de personuppgiftsansvariga (avsnitt 1) och, för det fallet att dessa underlåter att vidta åtgärder, tillsynsmyndigheterna (avsnitt 2) – att avbryta eller förbjuda en överföring, om standardklausulerna inte kan uppfyllas på grund av en konflikt mellan de skyldigheter som följer av dessa klausuler och de skyldigheter som åläggs enligt lagstiftningen i det tredjeland som är bestämmelseland.

1. De skyldigheter som åligger de personuppgiftsansvariga

129. I standardavtalsklausulerna i bilagan till beslut 2010/87 föreskrivs att klausulerna inte ska åberopas till stöd för en överföring till det tredjeland som är bestämmelseland, i det fallet att en konflikt föreligger mellan de skyldigheter som föreskrivs i klausulerna och de krav som följer av lagstiftningen i tredjelandet i fråga, och att om överföringen redan har inletts på grundval av nämnda klausuler ska uppgiftsutföraren underrättas om konflikten och kunna avbryta överföringen.

130. Enligt klausul 5 a förbinder sig uppgiftsinföraren sig att behandla de överförda personuppgifterna för uppgiftsutförarens räkning samt i enlighet med dennes instruktioner och standardavtalsklausulerna. Om uppgiftsinföraren inte kan uppfylla detta krav, går han med på att omedelbart informera uppgiftsutföraren om detta, varvid uppgiftsutföraren har rätt att avbryta överföringen av uppgifter och/eller häva avtalet.[49]

131. I fotnot 1 till klausul 5 anges att standardklausulerna inte åsidosätts när uppgiftsinföraren iakttar obligatoriska krav i den nationella lagstiftning som är tillämplig i tredjelandet, förutsatt att dessa krav inte går utöver vad som är nödvändigt i ett demokratiskt samhälle för att skydda något av de intressen som anges i artikel 13.1 i direktiv 95/46 (vars innehåll i allt väsentligt återges i artikel 23.1 i dataskyddsförordningen), bland annat den allmänna säkerheten och statens säkerhet. Ett åsidosättande av standardklausulerna i syfte att uppfylla en motstridig skyldighet som föreskrivs i lagstiftningen i det tredjeland som är bestämmelseland och som går utöver vad som är proportionerligt för att skydda ett legitimt intresse som erkänns av unionen betraktas däremot som ett åsidosättande av nämnda klausuler.

132. Enligt min mening, och som Maximillian Schrems och kommissionen har gjort gällande, kan klausul 5 a inte tolkas så, att den innebär att det är valfritt att avbryta överföringen eller häva avtalet, om uppgiftsinföraren inte klarar av att uppfylla standardklausulerna. Även om det i denna klausul endast anges att uppgiftsutföraren har en sådan rättighet, ska ordalydelsen förstås mot bakgrund av

49 Det ska dock påpekas att enligt klausul 5 d i är uppgiftsinföraren befriad från skyldigheten att underrätta uppgiftsutföraren om en rättsligt bindande begäran från rättsliga myndigheter i tredjelandet om utlämnande av personuppgifter, om tredjelandets lagstiftning utgör hinder för en sådan underrättelse. I ett sådant fall har uppgiftsutföraren inte möjlighet att avbryta överföringen om detta utlämnande – som han inte har kännedom om – strider mot standardklausulerna. Emellertid är uppgiftsinföraren enligt klausul 5 a fortsatt skyldig att i förekommande fall informera uppgiftsutföraren om den omständigheten att han anser att lagstiftningen i tredjelandet i fråga hindrar honom från att uppfylla sina skyldigheter enligt de överenskomna avtalsklausulerna.

den avtalsram som klausulen ingår i. Den omständigheten att uppgiftsutföraren har en rätt att *i sina bilaterala relationer med uppgiftsinföraren* avbryta överföringen eller häva avtalet, om uppgiftsinföraren inte förmår följa standardklausulerna, påverkar inte den skyldighet som åligger uppgiftsutföraren att göra detta *med hänsyn till de krav på att skydda de registrerades rättigheter som följer av dataskyddsförordningen*. Varje annan tolkning skulle göra beslut 2010/87 ogiltigt, eftersom de standardavtalsklausuler som föreskrivs i beslutet då inte skulle göra det möjligt att kringgärda överföringen med ”lämpliga skyddsåtgärder”, såsom det krävs enligt artikel 46.1 i dataskyddsförordningen jämförd med bestämmelserna i stadgan. [50]

133. Enligt ordalydelsen i klausul 5 b ska uppgiftsinföraren intyga att han inte har anledning att förmoda att den lagstiftning som är tillämplig på honom hindrar honom från att fullfölja uppdragsutförarens instruktioner och sina skyldigheter enligt avtalet. Om lagstiftningen ändras på ett sätt som sannolikt har en avsevärt skadlig inverkan på de garantier som standardklausulerna innebär, ska han anmäla ändringen till uppgiftsutföraren, varvid uppgiftsutföraren har rätt att avbryta överföringen av uppgifter och/eller häva avtalet. Enligt klausul 4 g ska uppgiftsutföraren vidarebefordra anmälan från uppgiftsinföraren till den behöriga tillsynsmyndigheten, om uppgiftsutföraren beslutar att fortsätta överföringen.

134. Här är det nödvändigt att göra några preciseringar rörande vad som ska ingå i den undersökning som avtalsparterna ska vidta för att mot bakgrund av fotnoten till klausul 5 avgöra om de skyldigheter som lagstiftningen i tredjelandet ålägger uppgiftsinföraren medför ett åsidosättande av standardklausulerna och följaktligen hindrar att överföringen kringgärdas av lämpliga skyddsåtgärder. Denna problematik har huvudsakligen framhävts i den sjätte giltighetsfrågans andra del.

135. En sådan undersökning innebär enligt min mening att samtliga de omständigheter som kännetecknar varje överföring ska beaktas, vilket kan inbegripa uppgifternas art och huruvida det eventuellt rör sig om känsliga uppgifter, de mekanismer som inrättats av uppgiftsutföraren och/eller uppgiftsinföraren för att säkerställa säkerheten för uppgifterna, [51] typ av behandling som de offentliga myndigheterna i tredjelandet kommer att utföra och syftet med den, villkoren för denna behandling och de begränsningar och garantier som tredjelandet säkerställer. De faktorer som karakteriserar de offentliga myndigheternas behandlingsverksamhet och de tillämpliga garantierna enligt tredjelandets rättsordning kan enligt min mening sammanfalla med de som anges i artikel 45.2 i dataskyddsförordningen.

136. I standardavtalsklausulerna i bilagan till beslut 2010/87 föreskrivs vidare rättsligt verkställbara rättigheter och rättsmedel mot uppgiftsutföraren och i andra hand mot uppgiftsinföraren till förmån för de registrerade.

137. I klausul 3.1, under rubriken ”Tredjepartsberättigande”, föreskrivs således att den registrerade har rätt att väcka talan mot uppgiftsutföraren i fall av åsidosättande av bland annat klausul 5 a eller b. Enligt klausul 3.2 kan den registrerade åberopa denna klausul mot uppgiftsinföraren, om uppgiftsutföraren har upphört att existera i faktisk eller rättslig mening.

50 Av rättspraxis framgår att bestämmelserna i en genomföranderättsakt ska tolkas i överensstämmelse med bestämmelserna i den grundrättsakt genom vilken lagstiftaren har godkänt antagandet av genomföranderättsakten (se, för ett liknande resonemang, bland annat, dom av den 26 juli 2017, Republiken Tjeckien/kommissionen, C-696/15 P, EU:C:2017:595, punkt 51, dom av den 17 maj 2018, Evonik Degussa C-229/17, EU:C:2018:323, punkt 29, och dom av den 20 juni 2019, ExxonMobil Production Deutschland, C-682/17, EU:C:2019:518, punkt 112). Dessutom ska en unionsrättsakt så långt det är möjligt tolkas på ett sätt som inte påverkar dess giltighet och som överensstämmer med primärrätten i dess helhet, bland annat med bestämmelserna i stadgan (se, bland annat, dom av den 14 maj 2019, M m.fl. (Återkallande av flyktingstatus), C-391/16, C-77/17 och C-78/17, EU:C:2019:403, punkt 77 och där angiven rättspraxis).

51 I skäl 109 i dataskyddsförordningen uppmuntras uppgiftsutföraren och uppgiftsinföraren att utöver de standardiserade dataskyddsbestämmelserna vidta ytterligare skyddsåtgärder, bland annat genom avtal.

138. Klausul 6.1 ger alla registrerade som har lidit skada till följd av ett åsidosättande av de skyldigheter som avses i klausul 3 rätt till ersättning från uppgiftsutföraren. Enligt klausul 7.1 samtycker uppgiftsinföraren till att, om den registrerade åberopar tredje parts rättigheter och/eller kräver ersättning för skador, godta den registrerades beslut att antingen inleda medling av tredje part eller, i tillämpliga fall, av tillsynsmyndigheten eller vända sig till domstol i den medlemsstat där uppgiftsutföraren är etablerad.

139. Utöver de rättsmedel som de registrerade har tillgång till enligt standardavtalsklausulerna i bilagan till beslut 2010/87 kan de, om de anser att klausulerna har åsidosatts, begära att tillsynsmyndigheterna ska utöva sina korrigerande befogenheter i enlighet med artikel 58.2 i dataskyddsförordningen, vilken det hänvisas till i artikel 4 i beslut 2010/87. [52]

2. De skyldigheter som åligger tillsynsmyndigheterna

140. Av de skäl som anges nedan anser jag, i likhet med Maximillian Schrems, Irland, den tyska, den österrikiska, den belgiska, den nederländska och den portugisiska regeringen och EDPB, att tillsynsmyndigheterna enligt artikel 58.2 i dataskyddsförordningen är skyldiga att, om de efter en noggrann undersökning anser att uppgifter som överförs till ett tredjeland inte omfattas av ett lämpligt skydd på grund av att de överenskomna avtalsklausulerna inte iakttas, vidta lämpliga åtgärder för att åtgärda denna rättsstridighet, om nödvändigt genom att förelägga om att överföringen ska avbrytas.

141. För det första ska det påpekas att i motsats till vad DPC har anfört innehåller beslut 2010/87 ingen bestämmelse enligt vilken tillsynsmyndigheternas utövande av sina befogenheter enligt artikel 58.2 f och j i dataskyddsförordningen, att ”[i]nföra en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, behandling” och ”[f]örelägga om att flödet av uppgifter till en mottagare i tredje land … ska avbrytas”, är begränsat till undantagsfall.

142. Enligt artikel 4.1 i beslut 2010/87 i dess ursprungliga lydelse var tillsynsmyndigheternas befogenhet att avbryta eller förbjuda gränsöverskridande flöden visserligen begränsad till vissa situationer där det fastställts att en överföring på avtalsbasis riskerade att ha en avsevärt skadlig inverkan på de garantier som var avsedda att skydda den registrerade. Numera innehåller artikel 4, i dess lydelse till följd av de ändringar som kommissionen infogade 2016 för att följa domen Schrems, [53] emellertid endast en hänvisning till dessa befogenheter, utan att på något sätt begränsa dem. Ett genomförandebeslut som har antagits av kommissionen, såsom beslut 2010/87, kan i vart fall inte begränsa de befogenheter som tillsynsmyndigheterna tilldelas i själva dataskyddsförordningen. [54]

143. Detta konstaterande påverkas inte av skäl 11 i beslut 2010/87, där det anges att tillsynsmyndigheterna endast i ”undantagsfall” kan utöva sin befogenhet att avbryta och förbjuda en överföring. Detta skäl, som fanns med redan i beslutets ursprungliga lydelse, hänförde sig till den tidigare artikel 4.1 i beslutet, vilken begränsade tillsynsmyndigheternas befogenheter. När beslut 2010/87 reviderades genom beslut 2016/2297 underlät kommissionen att stryka detta skäl eller att ändra det för att anpassa dess innehåll till bestämmelserna i den nya artikel 4. I skäl 5 i beslut 2016/2297 bekräftas dock tillsynsmyndigheternas befogenhet att avbryta eller förbjuda varje

52 Även om det i artikel 4.1 i beslut 2010/87 hänvisas till artikel 28.3 i direktiv 95/46 ska det erinras om att enligt artikel 94.2 i dataskyddsförordningen ska hänvisningar till detta direktiv anses som hänvisningar till motsvarande bestämmelser i dataskyddsförordningen.

53 Se skälen 6 och 7 i beslut 2016/2297. I punkterna 101–104 i domen Schrems fastslog domstolen att en bestämmelse i Safe Harbor-beslutet genom vilken de befogenheter som tillsynsmyndigheterna tilldelats genom artikel 28 i direktiv 95/46 begränsades till ”undantagsfall” var ogiltig, eftersom kommissionen inte var behörig att inskränka dessa befogenheter.

54 Se domen Schrems (punkt 103).

överföring som de anser strider mot unionsrätten, bland annat på grund av att uppgiftsinföraren inte iakttar standardavtalsklausulerna. Skäl 11 i beslut 2010/87 måste betraktas som obsolet, eftersom detta skäl numera motsäger såväl ordalydelsen som syftet med en rättsligt bindande bestämmelse i beslutet. [55]

144. För det andra ska det påpekas att i motsats till vad DPC också har hävdat utgör utövandet av den befogenhet att avbryta och förbjuda en överföring som föreskrivs i artikel 58.2 f och j i dataskyddsförordningen inte heller enbart en möjlighet som tillsynsmyndigheterna skönsmässigt kan besluta om. Detta konstaterande följer enligt min mening av en tolkning av artikel 58.2 i dataskyddsförordningen jämförd med andra bestämmelser i denna förordning och i stadgan, liksom av den allmänna systematiken i beslut 2010/87 och dess syften.

145. Artikel 58.2 i dataskyddsförordningen ska läsas mot bakgrund av artikel 8.3 i stadgan och artikel 16.2 FEUF. Enligt dessa bestämmelser ska oberoende tillsynsmyndigheter kontrollera iakttagandet av de krav som den grundläggande rätten till skydd för personuppgifter innebär. Uppdraget att tillse att kraven avseende skydd av personuppgifter iakttas, vilket också nämns i artikel 57.1 a i dataskyddsförordningen, innebär en skyldighet för tillsynsmyndigheterna att agera på ett sådant sätt att en korrekt tillämpning av denna förordning säkerställs.

146. En tillsynsmyndighet ska således med vederbörlig omsorg utreda en anmälan från en person som anser att hans eller hennes personuppgifter har överförts till ett tredjeland i strid med de standardavtalsklausuler som är tillämpliga på överföringen. [56] Enligt artikel 58.1 i dataskyddsförordningen tilldelas tillsynsmyndigheterna omfattande utredningsbefogenheter för detta ändamål. [57]

147. Den behöriga tillsynsmyndigheten är även skyldig att vidta lämpliga åtgärder mot de eventuella kränkningar av den registrerades rättigheter som tillsynsmyndigheten har konstaterat vid sin utredning. Härvid förfogar tillsynsmyndigheterna enligt artikel 58.2 i dataskyddsförordningen över en vid uppsättning medel (de olika korrigerande befogenheter som anges i denna bestämmelse) när det gäller att fullgöra den uppgift som den är ålagd. [58]

148. Även om det ankommer på den behöriga tillsynsmyndigheten att själv välja vilket medel som är effektivast mot bakgrund av samtliga omständigheter kring överföringen i fråga, är den skyldig att fullständigt fullgöra det tillsynsuppdrag som den har anförtrotts. Vid behov måste tillsynsmyndigheten avbryta överföringen, om uppgiftsutföraren inte själv har avbrutit den och tillsynsmyndigheten konstaterar att standardavtalsklausulerna inte iakttas och att ett lämpligt skydd för de överförda uppgifterna inte kan säkerställas med andra medel.

149. Denna tolkning stöds av artikel 58.4 i dataskyddsförordningen, där det föreskrivs att utövandet av de befogenheter som tillsynsmyndigheterna tilldelas enligt denna artikel ska omfattas av lämpliga skyddsåtgärder, inbegripet effektiva rättsmedel i enlighet med artikel 47 i stadgan. I artikel 78.1 och 78.2 i dataskyddsförordningen erkänns dessutom att varje person har rätt till ett effektivt rättsmedel mot ett rättsligt bindande beslut rörande vederbörande som meddelats av en tillsynsmyndighet eller när en tillsynsmyndighet underlåter att behandla ett klagomål från vederbörande. [59]

55 Ingressen till en unionsrättsakt har i vart fall inget rättsligt bindande värde och kan inte åberopas till stöd för undantag från bestämmelserna i rättsakten. Se dom av den 19 november 1998, Nilsson m.fl. (C-162/97, EU:C:1998:554, punkt 54), dom av den 12 maj 2005, Meta Fackler (C-444/03, EU:C:2005:288, punkt 25), och dom av den 10 januari 2006, IATA och ELFAA (C-344/04, EU:C:2006:10, punkt 76).

56 Se, analogt, domen Schrems (punkt 63).

57 Det ska tilläggas att enligt klausul 8.2 i bilagan till beslut 2010/87 är avtalsparterna överens om att låta tillsynsmyndigheten genomföra inspektioner hos uppgiftsinföraren på samma villkor som skulle gälla för en revision hos uppgiftsutföraren enligt tillämplig lagstiftning.

58 Se, för ett liknande resonemang, domen Schrems (punkt 43).

59 Enligt skäl 141 i dataskyddsförordningen bör varje person ha rätt till ett effektivt rättsmedel i enlighet med artikel 47 i stadgan, om tillsynsmyndigheten ”inte agerar när så är nödvändigt för att skydda [vederbörandes] rättigheter”. Se även skälen 129 och 143 i dataskyddsförordningen.

150. Dessa bestämmelser innebär, som Maximillian Schrems, BSA, Irland, den polska regeringen, Förenade kungarikets regering och kommissionen har gjort gällande, att ett beslut, genom vilket en tillsynsmyndighet avstår från att förbjuda eller avbryta en överföring till ett tredjeland efter anmälan från en person som har åberopat att det finns en risk för att hans uppgifter behandlas på ett sätt som kränker hans grundläggande rättigheter, kan vara föremål för rättslig prövning. Erkännandet av en rätt till rättslig prövning förutsätter att det föreligger en normbunden behörighet för tillsynsmyndigheterna och inte endast en befogenhet att företa skönsmässiga bedömningar. Som Maximillian Schrems och kommissionen dessutom har betonat förutsätter utövandet av en effektiv domstolskontroll att den myndighet som har vidtagit den omtvistade åtgärden har motiverat den tillräckligt.[60] Denna motiveringsskyldighet gäller enligt min mening även tillsynsmyndigheternas val att använda sig av någon av de befogenheter som de innehar enligt artikel 58.2 i dataskyddsförordningen.

151. De argument genom vilka DPC har gjort gällande att det ändå inte är säkerställt att beslut 2010/87 är giltigt, även om tillsynsmyndigheterna är skyldiga att avbryta eller förbjuda en överföring när skyddet för den registrerades rättigheter så kräver, behöver också bemötas.

152. DPC anser för det första att en sådan skyldighet inte avhjälper de systemiska problem som beror på avsaknaden av tillräckliga garantier i ett tredjeland som Förenta staterna. Tillsynsmyndigheternas befogenheter kan nämligen utövas endast från fall till fall, medan de brister som karakteriserar amerikansk lagstiftning är av en allmän och strukturell karaktär. Av detta följer en risk för att olika tillsynsmyndigheter fattar skiljaktiga beslut om jämförbara överföringar.

153. Härvid går det inte att förbise de praktiska svårigheter som beror på att lagstiftaren har valt att ålägga tillsynsmyndigheterna ansvaret för att se till att de registrerades grundläggande rättigheter respekteras i samband med specifika överföringar eller flöden till en given mottagare. Jag anser emellertid inte att dessa svårigheter innebär att beslut 2010/87 är ogiltigt.

154. Enligt unionsrätten krävs det nämligen inte att det finns en övergripande förebyggande lösning för alla överföringar till ett visst tredjeland som kan medföra samma risker för kränkning av de grundläggande rättigheterna.

155. Risken för en fragmentering av olika tillsynsmyndigheters tillvägagångssätt är dessutom en integrerad del av arkitekturen i den decentraliserade tillsyn som lagstiftaren eftersträvat.[61] Vidare har det, som den tyska regeringen har betonat, genom kapitel VII i dataskyddsförordningen, med rubriken ”Samarbete och enhetlighet”, inrättats mekanismer som är avsedda att förhindra denna risk. I artikel 60 i dataskyddsförordningen föreskrivs i fall av gränsöverskridande behandling av uppgifter ett förfarande för samarbete mellan de berörda tillsynsmyndigheterna och tillsynsmyndigheten för den personuppgiftsansvariges verksamhetsställe (kallad den ansvariga tillsynsmyndigheten).[62] I fall av skiljaktiga åsikter ska tvisten avgöras av EDPB.[63] Denna är även behörig att på begäran av en tillsynsmyndighets avge yttranden om alla frågor som är av intresse för flera medlemsstater.[64]

60 Se, bland annat, dom av den 28 juli 2011, Samba Diouf (C-69/10, EU:C:2011:524, punkt 57), och dom av den 17 november 2011, Gaydarov (C-430/10, EU:C:2011:749, punkt 41).

61 Se dom av den 5 juni 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388, punkterna 69–73).

62 Se artikel 56.1 i dataskyddsförordningen. Enligt artikel 61 i denna förordning är tillsynsmyndigheterna skyldiga att bistå varandra. Enligt artikel 62 i samma förordning får de genomföra gemensamma insatser.

63 Se artikel 65 i dataskyddsförordningen.

64 Se artikel 64.2 i dataskyddsförordningen.

156. DPC har för det andra gjort gällande att beslut 2010/87 är ogiltigt mot bakgrund av artikel 47 i stadgan, eftersom tillsynsmyndigheterna kan skydda de registrerades rättigheter endast för framtiden, men inte kan erbjuda någon lösning för dem vilkas uppgifter redan har överförts. DPC har särskilt påpekat att i artikel 58.2 i dataskyddsförordningen föreskrivs inte någon rätt till åtkomst, rättelse och radering av de uppgifter som har samlats in av de offentliga myndigheterna i tredjelandet i fråga eller någon möjlighet till ersättning för skada som de registrerade har lidit.

157. När det gäller den påstådda avsaknaden av en rätt till åtkomst, rättelse och radering av de insamlade uppgifterna, måste det konstateras att om det inte finns något effektivt rättsmedel i det tredjeland som är bestämmelseland, är det inte möjligt att genom de rättsmedel som inom unionen föreskrivs mot den personuppgiftsansvarige erhålla åtkomst till dessa uppgifter från de offentliga myndigheterna i tredjelandet i fråga, eller rättelse eller radering av dem.

158. Enligt min mening motiverar denna invändning dock inte att beslut 2010/87 skulle vara oförenligt med artikel 47 i stadgan. Giltigheten av detta beslut är nämligen inte beroende av den skyddsnivå som föreligger i de tredjeländer till vilka uppgifter kan överföras på grundval av de standardavtalsklausuler som anges i beslutet. Om lagstiftningen i det tredjeland som är bestämmelseland hindrar uppgiftsinföraren från att iaktta dessa klausuler, genom att det krävs att offentliga myndigheter ska ges åtkomst till uppgifterna utan att det föreskrivs någon möjlighet till ett lämpligt rättsmedel, ankommer det på tillsynsmyndigheterna att utöva sina korrigerande befogenheter, om uppgiftsutföraren inte har avbrutit överföringen i enlighet med klausul 5 a eller b i bilagan till beslut 2010/87.

159. Som Maximillian Schrems har betonat har de personer vilkas rättigheter har kränkts dessutom numera, enligt artikel 82 i dataskyddsförordningen, rätt till ersättning från den personuppgiftsansvarige eller personuppgiftsbiträdet för den materiella eller immateriella skada de har lidit till följd av en överträdelse av denna förordning. [65]

160. Såsom framgår av ovanstående överväganden har det vid min bedömning inte framkommit några omständigheter som kan påverka giltigheten av beslut 2010/87 mot bakgrund av artiklarna 7, 8 och 47 i stadgan.

F. Inte nödvändigt att svara på de övriga giltighetsfrågorna eller pröva giltigheten av beslutet om skölden för skydd av privatlivet

161. I detta avsnitt anger jag skälen till att jag bedömer att domstolen inte behöver svara på den andra till den femte samt den nionde och den tionde giltighetsfrågan eller uttala sig om giltigheten av beslutet om skölden för skydd av privatlivet, huvudsakligen eftersom saken i det nationella målet är begränsad till giltigheten av beslut 2010/87.

162. Den andra giltighetsfråga avser identifieringen av de skyddsstandarder som ett tredjeland ska iaktta för att uppgifter lagenligt ska kunna överföras dit på grundval av standardavtalsklausuler, om uppgifterna efter överföringen kan komma att behandlas av myndigheterna i detta tredjeland för syften som avser den nationella säkerheten. Den tredje frågan som har ställts till EU-domstolen avser fastställandet av de faktorer som karakteriserar den skyddsordning som är tillämplig i det tredjeland som är bestämmelseland, vilka ska beaktas i syfte att kontrollera om skyddsordningen uppfyller dessa standarder.

65 I artikel 83.5 c i dataskyddsförordningen föreskrivs även att den personuppgiftsansvarige ska påföras sanktionsavgifter vid överträdelse av artiklarna 44–49 i denna förordning.

163. Genom den fjärde, den femte och den tionde frågan vill den hänskjutande domstolen få klarhet i huruvida lagstiftningen i Förenta staterna, med beaktande av de omständigheter som den har konstaterat avseende denna lagstiftning, föreskriver lämpliga skyddsåtgärder mot ingrepp från de amerikanska underrättelsetjänsterna i utövandet av de grundläggande rättigheterna till respekt för privatlivet, skydd av personuppgifter och ett effektivt domstolsskydd.

164. Den nionde giltighetsfrågan avser vilken betydelse det har, inom ramen för den granskning genom vilken en tillsynsmyndighet kontrollerar om en överföring till Förenta staterna som baserar sig på standardavtalsklausulerna i beslut 2010/87 åtföljs av lämpliga garantier, att kommissionen i beslutet om skölden för skydd av privatlivet har konstaterat att Förenta staterna säkerställer en adekvat skyddsnivå för de registrerades grundläggande rättigheter mot sådana ingrepp.

165. Den hänskjutande domstolen har inte uttryckligen ställt någon fråga om huruvida beslutet om skölden för skydd av privatlivet är giltigt, även om den genom den fjärde, den femte och den tionde giltighetsfrågan, såsom det förklaras nedan,[66] indirekt har ifrågasatt huruvida det finns fog för kommissionens konstaterande i det beslutet att skyddsnivån är adekvat.

166. Med beaktande av de omständigheter som framgår av min bedömning ovan kan ett klarläggande från EU-domstolen rörande dessa frågor inte enligt min mening påverka dess slutsats om huruvida beslut 2010/87 hypotetiskt är giltigt och således inte heller påverka avgörandet av tvisten i det nationella målet (avsnitt 1). Även om EU-domstolens svar på nämnda frågor skulle kunna visa sig vara användbara för DPC i ett senare skede, när det gäller att inom ramen för det bakomliggande förfarandet till denna tvist avgöra huruvida överföringarna i fråga konkret ska avbrytas på grund av den påstådda avsaknaden av lämpliga garantier, anser jag att det är alltför tidigt att avgöra dessa frågor inom ramen för förevarande mål (avsnitt 2).

1. Svar från EU-domstolen är inte nödvändigt med avseende på saken i det nationella målet

167. Det ska erinras om att det nationella målet föranleddes av att DPC utövade det rättsmedel som beskrivs i punkt 65 i domen Schrems, där det anges att varje medlemsstat ska göra det möjligt för en tillsynsmyndighet att begära att en nationell domstol ska hänskjuta en fråga till EU-domstolen avseende giltigheten av ett beslut om en adekvat skyddsnivå – eller, analogt, ett beslut om inrättande av standardavtalsklausuler – om tillsynsmyndigheten anser detta vara nödvändigt för att utreda en anmälan som ingetts till den.

168. High Court (Förvaltningsöverdomstolen) har betonat att dess enda alternativ när den erhöll begäran från DPC var att antingen inge den begäran om förhandsavgörande rörande giltigheten av beslut 2010/87 som DPC hade begärt, för det fall att den instämde i DPC:s tvivel rörande giltigheten av detta beslut, eller avslå DPC:s begäran i motsatt fall. Den hänskjutande domstolen anser att om den hade valt sistnämnda alternativ, borde den ha ogillat talan, eftersom DPC:s begäran inte hade något annat föremål.[67]

66 Se punkt 175 nedan.

67 Dom av High Court (Förvaltningsöverdomstolen) av den 3 oktober 2017 (punkt 337).

169. Enligt samma linje har Supreme Court (Högsta domstolen), till följd av ett överklagande som Facebook Ireland ingav avseende begäran om förhandsavgörande, beskrivit det nationella målet som ett fastställelseförfarande varigenom DPC har begärt att den hänskjutande domstolen ska ställa en fråga till EU-domstolen om huruvida beslut 2010/87 är giltigt. Den enda materiella fråga som har anförts vid den hänskjutande domstolen och EU-domstolen avser följaktligen, enligt Irlands högsta domstol, giltigheten av beslut 2010/87. [68]

170. Mot bakgrund av den således avgränsade saken i det nationella målet har den hänskjutande domstolen ställt de tio första frågorna till EU-domstolen, eftersom den anser att en prövning av dem bidrar till den helhetsbedömning som är nödvändig för att EU-domstolen, som svar på den elfte frågan, ska kunna uttala sig om huruvida beslut 2010/87 är giltigt mot bakgrund av artiklarna 7, 8 och 47 i stadgan. Den elfte frågan följer, enligt begäran om förhandsavgörande, logiskt av de föregående frågorna.

171. Den andra till den femte samt den nionde och den tionde frågan vilar enligt min uppfattning på premissen att giltigheten av beslut 2010/87 är beroende av den skyddsnivå för de grundläggande rättigheterna som föreskrivs i de tredjeländer till vilka uppgifter kan överföras på grundval av de standardavtalsklausuler som föreskrivs i beslutet. Som det framgår av min bedömning avseende den sjunde frågan [69] anser jag att denna premiss är felaktig. En prövning av lagstiftningen i det tredjeland som är bestämmelseland spelar roll endast när kommissionen antar ett beslut om en adekvat skyddsnivå eller när den personuppgiftsansvarige – eller vid behov den behöriga tillsynsmyndigheten – inom ramen för en överföring som baserar sig på lämpliga skyddsåtgärder i den mening som avses i artikel 46.1 i dataskyddsförordningen kontrollerar att de skyldigheter som lagstiftningen i detta tredjeland ålägger uppgiftsinföraren inte hindrar effektiviteten i det skydd som säkerställs genom dessa åtgärder.

172. EU-domstolens svar på ovannämnda frågor kan följaktligen inte påverka dess svar på den elfte frågan. [70] Därför finns det inte heller någon anledning att svara på dem med avseende på saken i det nationella målet.

173. Jag föreslår att domstolen prövar förevarande mål endast med avseende på saken i det nationella målet. Domstolen bör enligt min mening inte gå utöver vad som krävs för att avgöra det nationella målet, genom att pröva giltighetsfrågorna med avseende på det bakomliggande förfarandet vid DPC. Som det anges nedan beror min uppmaning till återhållsamhet på en önskan att inte påverka den normala gången i det förfarande som måste återupptas vid DPC efter det att EU-domstolen har uttalat sig om giltigheten av beslut 2010/87. Vidare förefaller det, med hänsyn till omständigheterna i förevarande mål och även med hänsyn till vad förfarandet vid DPC handlar om, något förhastat om domstolen skulle behandla den problematik som anförts i den andra till femte samt den nionde och den tionde frågan.

68 I domen från Supreme Court (Högsta domstolen) av den 31 maj 2019 (punkt 2.7) konstateras att ”[t]he sole relief claimed by the DPC is, in substance, a reference to the CJEU under Article 267 [TFEU]”. I punkt 2.9 i samma dom konstateras vidare följande: ”Here, the only issue of substance which arises before either the Irish courts or the CJEU is the question of the validity or otherwise of Union measures. Whatever the view taken by the CJEU on that issue, *the Irish courts will have no further role, for the measures under question will either be found to be valid or invalid and in either event, that will be the end of the matter*” (min kursivering).

69 Se punkt 124 ovan.

70 Av detta samma skäl uttryckte Supreme Court (Högsta domstolen) i sin dom av den 31 maj 2019 (punkterna 8.1–8.5), även om den medgav att den inte är behörig att ifrågasätta den hänskjutande domstolens beslut att ställa giltighetsfrågor till domstolen eller ändra deras ordalydelse, tvivel om huruvida vissa av frågorna är nödvändiga. I punkt 8.5 i den domen anges särskilt följande: ”The sole purpose of the proceedings before the courts in Ireland was to enable the High Court to refer that question of validity to the CJEU and obtain a definitive answer from the only court which has competence to make the decision in question. It is difficult, therefore, to see how the High Court needs answers to many of the questions which have been referred, for the answers to those questions are only relevant to the question of the validity of the challenged measures….”

2. Skälen till att EU-domstolen inte bör utföra en prövning med avseende på saken i förfarandet vid DPC

174. Maximillian Schrems begärde i sin anmälan till DPC att denna tillsynsmyndighet skulle utöva sin befogenhet enligt artikel 58.2 f i dataskyddsförordningen och förelägga Facebook Ireland att avbryta överföringen av personuppgifter rörande honom till Förenta staterna, vilken utförs på grundval av avtalsklausuler. Till stöd för denna begäran åberopade Maximillian Schrems huvudsakligen att dessa avtalsmässiga skyddsåtgärder inte är lämpliga med beaktande av det ingrepp i utövandet av hans grundläggande rättigheter som följer av de amerikanska underrättelsetjänsternas verksamhet.

175. I sitt resonemang ifrågasatte Maximillian Schrems kommissionens konstaterande i beslutet om skölden för skydd av privatlivet att Förenta staterna säkerställer en adekvat skyddsnivå för uppgifter som överförs i enlighet med detta beslut, med beaktande av de begränsningar som har införts för de amerikanska underrättelsetjänsternas åtkomst till och användning av dessa uppgifter och det rättsliga skydd som de registrerade erbjuds.[71] Av de farhågor som preliminärt har uttryckts av DPC,[72] liksom av den hänskjutande domstolen i den fjärde, den femte och den tionde frågan, framgår indirekt att även de tvivlar på huruvida det finns fog för kommissionens konstaterande.

176. I beslutet om skölden för skydd av privatlivet konstateras förvisso endast att skyddsnivån är adekvat för personuppgifter som i enlighet med de principer som anges i beslutet överförs till företag etablerade i Förenta staterna som har självcertifierat sin anslutning till dessa principer.[73] Konstaterandena i beslutet går emellertid utöver kontexten för de överföringar som omfattas av det, eftersom de avser gällande lagstiftning och praxis i detta tredjeland rörande behandlingen av de överförda uppgifterna för syften som avser skyddet av den nationella säkerheten. Som Facebook Ireland, Maximillian Schrems, Förenta staternas regering och kommissionen har påpekat är den övervakning som utövas av de amerikanska underrättelsetjänsterna, liksom de garantier mot riskerna för missbruk som den omfattar och de mekanismer som syftar till att kontrollera att garantierna iakttas, tillämpliga oavsett vilken rättslig grund i unionsrätten som åberopas till stöd för överföringen.

177. Mot denna bakgrund kan frågan huruvida ovannämnda konstateranden i beslutet om skölden för skydd av privatlivet är bindande för tillsynsmyndigheterna, när dessa prövar huruvida en överföring som utförs på grundval av standardavtalsklausuler är lagenlig, vara relevant för DPC:s behandling av anmälan från Maximillian Schrems. Vid ett jakande svar på denna fråga, uppkommer frågan huruvida detta beslut faktiskt är giltigt.

178. Jag avråder emellertid EU-domstolen från att avgöra dessa frågor enbart i syfte att hjälpa DPC att pröva nämnda anmälan, eftersom de inte behöver besvaras för att den hänskjutande domstolen ska kunna avgöra det nationella målet. Eftersom det förfarande som föreskrivs i artikel 267 FEUF endast avser en dialog mellan domstolar, behöver EU-domstolen inte komma med klargöranden enbart i syfte att bistå en administrativ myndighet inom ramen för det förfarande som har föranlett det nationella målet.

71 Se skälen 64–141 i beslutet om skölden för skydd av privatlivet. Det ska erinras om att som det framgår av artikel 1.2 i detta beslut utgörs skölden för skydd av privatlivet inte endast av de principer som de företag som vill överföra uppgifter på grundval av nämnda beslut måste följa, utan också av de officiella utfästelser och åtaganden som erhållits från Förenta staternas regering och som framgår av de dokument som är bifogade beslutet.

72 DPC:s utkast till beslut antogs före beslutet om skölden för skydd av privatlivet. Som DPC angav i utkastet hade den, även om den preliminärt konstaterade att de garantier som föreskrivs i Förenta staternas lagstiftning åtminstone inte gör det möjligt att säkerställa att överföringar till detta tredje land är förenliga med artikel 47 i stadgan, *i detta skede inte granskat eller beaktat de nya arrangemang som förutsågs i utkastet till avtal avseende "skölden för skydd", eftersom detta inte ännu hade antagits*. High Court (Förvaltningsöverdomstolen) konstaterade följande i punkt 307 i domen av den 3 oktober 2017: "It is fair to conclude… that the decision of the Commission in regard to the adequacy of the protections afforded to EU citizens against interference by the intelligence authorities in the [U.S.] with the fundamental rights of EU citizens whose data are transferred from the [EU] to the [U.S.], conflicts with the case made by the DPC to this court".

73 Se artikel 1.1 och 1.3 samt skälen 14–16 i beslutet om skölden för skydd av privatlivet.

179. Denna återhållsamhet är enligt min mening desto mer nödvändig, eftersom frågan huruvida beslutet om skölden för skydd av privatlivet är giltigt inte uttryckligen har ställts till EU-domstolen och eftersom detta beslut dessutom redan är föremål för en talan om ogiltigförklaring vid Europeiska unionens tribunal.[74]

180. Genom att uttala sig om ovannämnda problematik skulle EU-domstolen dessutom, enligt min mening, påverka den normala gången i det förfarande som måste återupptas efter det att den har meddelat sin dom i förevarande mål. Inom ramen för nämnda förfarande åligger det DPC att pröva anmälan från Maximillian Schrems med beaktande av domstolens svar på den elfte giltighetsfrågan. Om domstolen, såsom jag har föreslagit och tvärtemot vad DPC har gjort gällande vid den, slår fast att beslut 2010/87 inte är ogiltigt mot bakgrund av artiklarna 7, 8 och 47 i stadgan, bör DPC enligt min mening ges möjlighet att på nytt pröva handlingarna i det ärende som den har att avgöra. För det fall att DPC skulle anse att den inte kan avgöra anmälan från Maximillian Schrems utan att EU-domstolen först har avgjort huruvida beslutet om skölden för skydd av privatlivet hindrar utövandet av dess befogenhet att avbryta överföringen i fråga och skulle bekräfta att den tvivlar på giltigheten av nämnda beslut, kan denna myndighet på nytt vända sig till de nationella domstolarna, så att dessa kan ställa en fråga till EU-domstolen rörande detta.[75]

181. Ett förfarande skulle då inledas som skulle ge parterna och alla de berörda som avses i artikel 23 andra stycket i domstolens stadga möjlighet att inkomma med synpunkter till domstolen specifikt rörande giltigheten av beslutet om skölden för skydd av privatlivet, genom att i förekommande fall ange vilka särskilda bedömningar man invänder mot och skälen till att man anser att kommissionen har överskridit sitt begränsade utrymme för skönsmässig bedömning.[76] Inom ramen för ett sådant förfarande skulle kommissionen ha möjlighet att exakt och i detalj bemöta alla eventuella invändningar mot nämnda beslut. Även om förevarande mål har gett parterna och de berörda som inkommit med synpunkter till domstolen tillfälle att diskutera vissa relevanta aspekter i syfte att utvärdera huruvida beslutet om skölden för skydd av privatlivet är förenligt med artiklarna 7, 8 och 47 i stadgan, förtjänar denna fråga med hänsyn till sin betydelse en uttömmande och djupgående diskussion.

182. Försiktigheten kräver enligt min mening att dessa förfarandesteg har tagits innan EU-domstolen prövar hur beslutet om skölden för skydd av privatlivet inverkar på en tillsynsmyndighets prövning av en ansökan om att avbryta en överföring till Förenta staterna som utförs med stöd av artikel 46.1 i dataskyddsförordningen och uttalar sig om huruvida detta beslut är giltigt.

183. Detta är fallet särskilt eftersom det på grundval av de handlingar som har ingetts till domstolen inte är möjligt att konstatera att DPC:s prövning av Maximillian Schrems anmälan nödvändigtvis är beroende av huruvida beslutet om skölden för skydd av privatlivet hindrar tillsynsmyndigheternas utövande av sin befogenhet att avbryta en överföring som grundar sig på standardavtalsklausuler.

184. Det är inte uteslutet att DPC kan föranledas att avbryta överföringen i fråga av andra skäl än den påstått inadekvata skyddsnivån i Förenta staterna mot kränkningar av de registrerades grundläggande rättigheter till följd av de amerikanska underrättelsetjänsternas verksamhet. Den hänskjutande domstolen har särskilt preciserat att Maximillian Schrems i anmälan till DPC hävdade att de

74 Det anhängiga målet T-738/16, La Quadrature du Net m.fl./kommissionen (EUT C 6, 2017, s. 39).

75 Det ska dessutom påpekas att DPC i sina skriftliga yttranden inte har tagit ställning till inverkan av beslutet om skölden för skydd av privatlivet på prövningen av den anmälan som ingetts till den.

76 Se domen Schrems (punkt 78).

avtalsklausuler som Facebook Ireland åberopat till stöd för överföringen i fråga inte troget återger klausulerna i bilagan till beslut 2010/87. Maximillian Schrems har dessutom hävdat att nämnda överföring inte omfattas av tillämpningsområdet för nämnda beslut, utan av tillämpningsområdet för de andra besluten om standardavtalsklausuler. [77]

185. Vidare har DPC och den hänskjutande domstolen betonat att Facebook Ireland inte har åberopat beslutet om skölden för skydd av privatlivet till stöd för den överföring som avses i anmälan från Maximillian Schrems, [78] vilket bekräftades av detta företag vid förhandlingen. Även om Facebook Inc. självcertifierade sin anslutning till principerna om skölden för skydd av privatlivet den 30 september 2016 [79] har Facebook Ireland försäkrat att denna anslutning endast gäller överföringen av vissa kategorier av uppgifter, det vill säga uppgifter som rör kommersiella parter till Facebook Inc. Det är enligt min mening olämpligt att EU-domstolen föregriper de frågor som kan komma att ställas rörande detta genom att pröva huruvida, för det falle att Facebook Ireland inte kan åberopa beslut 2010/87 till stöd för överföringen i fråga, denna överföring icke desto mindre omfattas av beslutet om skölden för skydd av privatlivet, trots att Facebook Ireland inte har anfört detta argument vare sig vid den hänskjutande domstolen eller vid DPC.

186. Av detta drar jag slutsatsen att det inte finns någon anledning för domstolen att besvara den andra till den femte samt den nionde och den tionde giltighetsfrågan eller pröva giltigheten av beslutet om skölden för skydd av privatlivet.

G. Subsidiära synpunkter avseende verkningarna och giltigheten av beslutet om skölden för skydd av privatlivet

187. Även om jag mot bakgrund av ovanstående bedömning föreslår att domstolen ska avstå från att uttala sig om hur beslutet om skölden för skydd av privatlivet inverkar på prövningen av en anmälan av det slag som Maximillian Schrems har ingett till DPC och huruvida detta beslut är giltigt, anser jag det vara ändamålsenligt att subsidiärt och med vissa förbehåll lämna några icke-uttömmande synpunkter rörande detta.

1. Hur beslutet om skölden för skydd av privatlivet inverkar på en tillsynsmyndighets prövning av en anmälan som avser lagligheten hos en överföring som grundas på avtalsmässiga skyddsåtgärder

188. Den nionde giltighetsfrågan avser huruvida konstaterandet i beslutet om skölden för skydd av privatlivet avseende att Förenta staterna säkerställer en adekvat skyddsnivå med beaktande av de begränsningar som har införts i de amerikanska myndigheternas åtkomst till och användning av de överförda uppgifterna för syften som avser den nationella säkerheten och med beaktande av det rättsliga skyddet för de registrerade hindrar att en tillsynsmyndighet avbryter en överföring till detta tredjeland som utförs i enlighet med standardavtalsklausuler.

77 Till stöd för detta påstående har Maximillian Schrems gjort gällande att när det gäller behandlingen av personuppgifter rörande användarna av det sociala nätverket Facebook bör Facebook Inc. inte endast betraktas som ett personuppgiftsbiträde, utan också som en ”personuppgiftsansvarig” i den mening som avses i artikel 4.7 i dataskyddsförordningen. Se dom av den 5 juni 2018, Wirtschaftsakademie Schleswig-Holstein (C-210/16, EU:C:2018:388, punkt 30).

78 Se domen från High Court (Förvaltningsöverdomstolen) av den 3 oktober 2017 (punkt 66).

79 Se webbplatsen för ”skölden för skydd av uppgifter” (https://www.privacyshield.gov/participant_search).

189. Jag anser att denna problematik ska ses mot bakgrund av punkterna 51 och 52 i domen Schrems, där det framgår att ett beslut om en adekvat skyddsnivå är bindande för tillsynsmyndigheterna så länge det inte har ogiltigförklarats. En tillsynsmyndighet som har mottagit en anmälan från en person vars uppgifter överförs till det tredjeland som avses i ett beslut om en adekvat skyddsnivå kan således inte avbryta överföringen av det skälet att skyddsnivån inte är adekvat där, utan att domstolen först har ogiltigförklarat beslutet i fråga. [80]

190. Den hänskjutande domstolen vill få klarhet i huruvida detta konstaterande, när det rör sig om ett beslut om en adekvat skyddsnivå – såsom beslutet om skölden för skydd av privatlivet eller, dessförinnan, Safe Harbor-beslutet – som vilar på företagens frivilliga anslutning till de principer som anges i beslutet, endast gäller i den mån överföringen till tredjelandet i fråga omfattas av detta beslut, eller om det också gäller när överföringen utförs på en annan rättslig grund.

191. Enligt Maximillian Schrems, den tyska, en nederländska, den polska och den portugisiska regeringen samt kommissionen fråntar konstaterandet om en adekvat skyddsnivå i beslutet om skölden för skydd av privatlivet inte tillsynsmyndigheterna deras befogenhet att avbryta eller förbjuda en överföring till Förenta staterna som utförs i enlighet med standardavtalsklausuler. Om överföringen till Förenta staterna inte grundar sig på beslutet om skölden för skydd av privatlivet, är tillsynsmyndigheterna inte formellt bundna av detta beslut vid utövandet av de befogenheter som de har enligt artikel 58.2 i dataskyddsförordningen. Dessa myndigheter kan med andra ord distansera sig från kommissionens konstateranden avseende att det föreligger en adekvat skyddsnivå mot ingrepp från de amerikanska offentliga myndigheterna i de registrerades utövande av sina grundläggande rättigheter. Den nederländska regeringen och kommissionen har preciserat att tillsynsmyndigheterna icke desto mindre måste beakta dessa konstateranden när de utövar dessa befogenheter. Enligt den tyska regeringen kan tillsynsmyndigheterna endast göra motsatta bedömningar efter att ha vidtagit en prövning i sak av kommissionens konstateranden, omfattande relevanta utredningar.

192. Facebook Ireland och Förenta staternas regering har däremot gjort gällande att den bindande verkan av ett beslut om en adekvat skyddsnivå med hänsyn till kraven på rättssäkerhet och en enhetlig tillämpning av unionsrätten innebär att tillsynsmyndigheterna inte är behöriga att ifrågasätta konstaterandena i nämnda beslut, och detta inte ens inom ramen för prövningen av en anmälan som syftar till att utverka att överföringar som utförs till tredjelandet i fråga på en annan grund än detta beslut ska avbrytas.

193. Jag instämmer i det förstnämnda av dessa båda synsätt. Eftersom tillämpningsområdet för beslutet om skölden för skydd av privatlivet är begränsat till överföringar som utförs till företag som har självcertifierat sig i enlighet med detta beslut, kan nämnda beslut inte vara formellt bindande för tillsynsmyndigheterna när det rör sig om överföringar som inte omfattas av detta tillämpningsområde. Beslutet om skölden för skydd av privatlivet är avsett att säkerställa rättssäkerheten endast till förmån för de uppgiftsutförare som överför uppgifter inom den ram som inrättats genom detta beslut. Det oberoende som tillsynsmyndigheterna tillerkänns enligt artikel 52 i dataskyddsförordningen hindrar enligt min mening också att de är bundna av konstateranden som kommissionen gjort i ett beslut om en adekvat skyddsnivå som inte ens omfattas av dess tillämpningsområde.

194. Konstaterandena i beslutet om skölden för skydd av privatlivet avseende att Förenta staterna säkerställer en adekvat skyddsnivå mot ingrepp i samband med de amerikanska underrättelsetjänsternas verksamhet ska naturligtvis utgöra utgångspunkten för tillsynsmyndighetens bedömning när den från fall till fall utvärderar om en överföring grundad på standardavtalsklausuler

80 Se, för ett liknande resonemang, domen Schrems (punkt 59).

ska avbrytas på grund av sådana ingrepp. Om den behöriga tillsynsmyndigheten emellertid efter en fördjupad utredning bedömer att den inte kan instämma i dessa konstateranden vad gäller den överföring som den uppmärksammats på, har den enligt min mening möjlighet att utöva de befogenheter som den tillerkänns i artikel 58.2 f och j i dataskyddsförordningen.

195. För det fall att domstolen ger förevarande fråga ett annat svar än det som jag har föreslagit, måste det prövas huruvida dessa befogenheter icke desto mindre bör återställas på grund av att beslutet om skölden för skydd av privatlivet är ogiltigt.

2. Huruvida beslutet om skölden för skydd av privatlivet är giltigt

196. Nedanstående påpekanden ger upphov till vissa frågetecken kring huruvida det finns fog för bedömningarna i beslutet om skölden för skydd av privatlivet avseende att Förenta staterna säkerställer en adekvat skyddsnivå i den mening som avses i artikel 45.1 i dataskyddsförordningen när det gäller de amerikanska underrättelsetjänsternas verksamhet för övervakning av elektroniska kommunikationer. Dessa påpekanden är inte avsedda att utgöra ett slutgiltigt eller uttömmande ställningstagande om giltigheten av detta beslut. De innehåller endast vissa betraktelser som kan visa sig vara användbara för domstolen för det fall att den, tvärtemot vad jag har föreslagit, skulle vilja avgöra denna fråga.

197. Av skäl 64 och punkt I.5 i bilaga II till beslutet om skölden för skydd av privatlivet framgår att företagens anslutning till de principer som anges i detta beslut kan begränsas bland annat av kraven i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden samt av motstridiga skyldigheter som följer av amerikansk rätt.

198. Kommissionen har därför bedömt de garantier som föreskrivs i Förenta staternas lagstiftning vad gäller tillgången till överförda uppgifter och de amerikanska offentliga myndigheternas användning av dem för ändamål som framför allt rör nationell säkerhet.[81] Den har erhållit vissa åtaganden från den amerikanska regeringen avseende dels begränsningar av de amerikanska myndigheternas åtkomst till och användning av överförda uppgifter, dels rättsligt skydd för de registrerade.[82]

199. Maximillian Schrems har vid EU-domstolen gjort gällande att beslutet om skölden för skydd av privatlivet är ogiltigt av det skälet att de beskrivna garantierna inte räcker för att säkerställa en adekvat skyddsnivå för de grundläggande rättigheterna för de personer vilkas uppgifter överförs till Förenta staterna. DPC, EPIC samt den österrikiska, den polska och den portugisiska regeringen har, utan att direkt ifrågasätta beslutets giltighet, invänt mot de bedömningar som kommissionen gjort i beslutet avseende att skyddsnivån mot de ingrepp som följer av de amerikanska underrättelsetjänsternas verksamhet är adekvat. Dessa tvivel speglar farhågor som har uttryckts av parlamentet,[83] EDPB[84] och EDPS.[85]

81 Se skäl 65 i beslutet om skölden för skydd av privatlivet.

82 Se bilagorna III–VII till beslutet om skölden för skydd av privatlivet.

83 Parlamentets resolution av den 6 april 2017 om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och USA, P8_TA(2017)0131, och av den 5 juli 2018 om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och USA, P8_TA(2018)0315.

84 Se Artikel 29-arbetsgruppen för skydd av personuppgifter (nedan kallad Artikel 29-arbetsgruppen), *Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, 13 april 2016, WP 238; Artikel 29-arbetsgruppen, *EU-US Privacy Shield – First Annual Joint Review*, 28 november 2017, WP 255, och EDPB, *EU-US Privacy Shield – Second Annual Joint Review*, 22 januari 2019. Artikel 29-arbetsgruppen inrättades enligt artikel 29.1 i direktiv 95/46, där det angavs att den skulle vara rådgivande och oberoende. I enlighet med artikel 29.2 bestod gruppen av en företrädare för varje nationell tillsynsmyndighet, en företrädare för varje myndighet som inrättats för gemenskapens institutioner och organ samt en företrädare för kommissionen. I och med att dataskyddsförordningen trädde i kraft ersattes Artikel 29-arbetsgruppen av EDPB (se artikel 94.2 i denna förordning).

85 Se EDPS, yttrande 4/2016 av den 30 maj 2016 om utkastet till beslut om huruvida ett adekvat skydd säkerställs genom bestämmelserna om integritetsskydd mellan EU och Förenta staterna. EDPS inrättades genom artikel 1.2 i 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). EDPS utövar tillsyn över tillämpningen av bestämmelserna i denna förordning.

200. Innan jag granskar huruvida det finns fog för konstaterandet om en adekvat skyddsnivå i beslutet om skölden för skydd av privatlivet är det nödvändigt att precisera den metod som ska tillämpas vid denna granskning.

a) Preciseringar rörande innehållet i granskningen av huruvida ett beslut om en adekvat skyddsnivå är giltigt

1) Ramarna för den jämförelse som gör det möjligt att utvärdera om skyddsnivån är ”väsentligen likvärdig”

201. Enligt artikel 45.3 i dataskyddsförordningen och domstolens praxis [86] får kommissionen besluta att ett tredjeland säkerställer en adekvat skyddsnivå först efter att på ett vederbörligen motiverat sätt ha konstaterat att skyddsnivån för de registrerades grundläggande rättigheter där är ”väsentligen likvärdig” med den som krävs i unionen enligt denna förordning jämförd med stadgan.

202. För att kontrollera om den skyddsnivå som säkerställs i ett tredjeland är adekvat är det således nödvändigt att jämföra de regler och den praxis som gäller i detta tredjeland med de skyddsnormer som gäller i unionen. Genom den andra frågan har den hänskjutande domstolen begärt att EU-domstolen ska precisera ramarna för denna jämförelse. [87]

203. Den hänskjutande domstolen vill mer specifikt få klarhet i huruvida den exklusiva befogenhet som medlemsstaterna tillerkänns enligt artikel 4.2 FEU och artikel 2.2 i dataskyddsförordningen när det gäller skyddet av den nationella säkerheten innebär att unionens rättsordning inte omfattar några skyddsstandarder mot vilka de skyddsåtgärder som i ett tredjeland reglerar de offentliga myndigheternas behandling av överförda uppgifter för syften som avser den nationella säkerheten ska jämföras i syfte att avgöra om de är adekvata. Om så är fallet, vill den hänskjutande domstolen veta hur den relevanta referensramen ska fastställas.

204. Det ska erinras om att själva syftet med de begränsningar för internationella överföringar av personuppgifter som föreskrivs i unionsrätten, genom att det krävs att det ska säkerställas att skyddsnivån för de registrerades rättigheter vidmakthålls, är att förhindra risken för att de standarder som är tillämpliga i unionen kringgås. [88] Mot bakgrund av denna målsättning är det, som Facebook Ireland har gjort gällande, inte motiverat att ett tredjeland förväntas uppfylla krav som inte motsvarar de skyldigheter som åligger medlemsstaterna.

205. Enligt artikel 51.1 i stadgan är denna tillämplig på medlemsstaterna endast när de tillämpar unionsrätten. Huruvida ett beslut om en adekvat skyddsnivå är giltigt mot bakgrund av de begränsningar i de registrerades utövande av sina grundläggande rättigheter som följer av lagstiftningen i det tredjeland som är bestämmelseland är följaktligen beroende av en jämförelse mellan dessa begränsningar och de begränsningar som medlemsstaterna får tillämpa enligt bestämmelserna i stadgan, *endast i den mån liknande lagstiftning i en medlemsstat omfattas av unionsrättens tillämpningsområde*.

86 Se punkt 112 ovan.

87 Det ska erinras om att en utvärdering av huruvida den skyddsnivå som garanteras av ett tredjeland är väsentligen likvärdig den som krävs inom unionen också ska göras när den personuppgiftsansvarige eller, vid behov, den behöriga tillsynsmyndigheten, inom ramen för en specifik överföring som grundar sig på de standardavtalsklausuler som föreskrivs i beslut 2010/87, kontrollerar huruvida de offentliga myndigheterna i det tredjeland som är bestämmelseland ålägger uppgiftsinföraren krav som går utöver vad som är nödvändigt i ett demokratiskt samhälle (se klausul 5 i bilagan till beslut 2010/87 och tillhörande fotnot). Se punkterna 115, 134 och 135 ovan.

88 Se punkt 117 ovan.

206. Vid bedömningen av huruvida en adekvat skyddsnivå säkerställs i det tredjeland som är bestämmelseland kan man emellertid inte bortse från de eventuella ingrepp i utövandet av de registrerades grundläggande rättigheter som följer av statliga åtgärder inom bland annat området nationell säkerhet vilka inte skulle omfattas av unionsrättens tillämpningsområde, om de vidtogs av en medlemsstat. Vid denna bedömning krävs enligt artikel 45.2 a i dataskyddsförordningen att detta tredjelands gällande lagstiftning i fråga om nationell säkerhet beaktas utan några som helst begränsningar.

207. Bedömningen av huruvida skyddsnivån är adekvat mot bakgrund av sådana statliga åtgärder innebär enligt min mening en jämförelse mellan de garantier som åtföljer de statliga åtgärderna och den skyddsnivå som krävs i unionen enligt medlemsstaternas lagstiftning, inbegripet deras åtaganden enligt Europakonventionen. Eftersom medlemsstaterna genom sin anslutning till Europakonventionen är skyldiga att göra sin interna lagstiftning förenlig med bestämmelserna i denna konvention, och detta, såsom Facebook Ireland, den tyska och den tjeckiska regeringen och kommissionen har betonat, utgör en gemensam nämnare för medlemsstaterna, betraktar jag dessa bestämmelser som den relevanta jämförelsegrunden vid denna bedömning.

208. Som det har angetts ovan [89] har kraven avseende Förenta staternas nationella säkerhet företräde framför de självcertifierade företagens skyldigheter enligt beslutet om skölden för skydd av privatlivet. Huruvida detta beslut är giltigt beror således på huruvida dessa krav kringgärdas av garantier som säkerställer en skyddsnivå som är väsentligen likvärdig den som ska säkerställas i unionen.

209. För att svara på denna fråga är det nödvändigt att först identifiera de standarder – det vill säga de som följer av stadgan eller också av Europakonventionen – som lagstiftning om övervakning av elektroniska kommunikationer liknande den som kommissionen granskade i beslutet om skölden för skydd av privatlivet måste uppfylla inom unionen. Fastställandet av de tillämpliga standarderna är beroende av huruvida lagstiftning som avsnitt 702 i FISA och EO 12333 om den härrörde från en medlemsstat skulle omfattas av den begränsning av dataskyddsförordningens tillämpningsområde som föreskrivs i artikel 2.2 i denna förordning jämförd med artikel 4.2 FEU.

210. Av ordalydelsen i artikel 4.2 FEU och fast rättspraxis framgår att unionsrätten och särskilt sekundärrättsakterna om skydd av personuppgifter inte är tillämpliga på verksamhet som avser skyddet av den nationella säkerheten, eftersom denna verksamhet utövas av staten eller statliga myndigheter och inte har någon beröring med områden där enskilda är verksamma. [90]

211. Denna princip innebär *för det första* att lagstiftning inom området skydd av den nationella säkerheten inte omfattas av unionsrättens tillämpningsområde, om den uteslutande reglerar statlig verksamhet och inte reglerar verksamhet som utövas av enskilda. Unionsrätten är följaktligen, enligt min mening, inte tillämplig på nationella åtgärder avseende insamling och användning av personuppgifter som genomförs direkt av staten för syften som avser skyddet av den nationella

89 Se punkt 197 ovan.

90 Se, bland annat, dom av den 6 november 2003, Lindqvist (C-101/01, EU:C:2003:596, punkterna 43 och 44), domen PNR (punkt 58), dom av den 16 december 2008, Satakunnan Markkinapörssi och Satamedia (C-73/07, EU:C:2008:727, punkt 41), dom av den 21 december 2016, Tele2 Sverige och Watson m.fl. (C-203/15 och C-698/15, EU:C:2016:970, punkt 69) (nedan kallad domen Tele2 Sverige), och dom av den 2 oktober 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788, punkt 32) (nedan kallad domen Ministerio Fiscal).

säkerheten, utan att några särskilda skyldigheter åläggs privata aktörer. Särskilt ska påpekas, vilket kommissionen gjorde gällande vid förhandlingen, att en sådan åtgärd som EO 12333, som ger statens säkerhetstjänster direkt åtkomst till uppgifter under själva överföringen, inte skulle omfattas av unionsrättens tillämpningsområde, om den antogs av en medlemsstat. [91]

212. En långt mer komplicerad fråga är *för det andra* huruvida nationella bestämmelser som, liksom avsnitt 702 i FISA, ålägger leverantörer av elektroniska kommunikationstjänster att bistå behöriga myndigheter inom området nationell säkerhet, så att dessa kan få tillgång till vissa personuppgifter också faller utanför unionsrättens tillämpningsområde.

213. Medan domen PNR talar för att denna fråga ska besvaras jakande kan resonemanget i domen Tele2 Sverige och domen Ministerio Fiscal motivera ett nekande svar på denna fråga.

214. I domen PNR ogiltigförklarade domstolen det beslut genom vilket kommissionen hade konstaterat att en adekvat skyddsnivå för flygpassagerares personuppgifter förelåg när PNR-uppgifter (Passenger Name Records) överfördes till den behöriga amerikanska tull- och gränsskyddsmyndigheten. [92] Domstolen slog fast att den behandling som detta beslut avsåg – det vill säga överföring av PNR-uppgifter från lufttrafikföretag till myndigheten i fråga – *med hänsyn till sitt syfte* omfattades av det undantag från tillämpningsområdet för direktiv 95/46 som föreskrivs i artikel 3.2 i direktivet. Enligt domstolen var denna behandling inte nödvändig för tillhandahållandet av en tjänst, utan för att säkerställa allmän säkerhet och tillgodose repressiva syften. Eftersom överföringen i fråga skedde inom en ram som hade inrättats av de offentliga myndigheterna och för syften som avsåg den allmänna säkerheten, var den undantagen från tillämpningsområdet för detta direktiv trots den omständigheten att PNR-uppgifterna initialt insamlades av privata operatörer inom ramen för en kommersiell verksamhet som omfattades av detta tillämpningsområde och överföringen sköttes av dessa operatörer. [93]

215. I den efterföljande domen Tele2 Sverige [94] slog domstolen fast att nationella bestämmelser som grundar sig på artikel 15.1 i direktiv 2002/58/EG [95] och som reglerar såväl lagring av trafik- och lokaliseringsuppgifter hos leverantörer av telekommunikationstjänster som de offentliga myndigheternas tillgång till de lagrade uppgifterna för de syften som anges i denna bestämmelse – vilka inbegriper brottsbekämpning och skyddet av den nationella säkerheten – omfattas av tillämpningsområdet för detta direktiv och följaktligen av stadgan. Enligt domstolen omfattas varken

91 För att undvika förvirring på denna punkt ska det betonas att kommissionen i beslutet om skölden för skydd av privatlivet inte kunde avgöra om Förenta staterna faktiskt avlyssnar kommunikationer under överföringen via de transatlantiska kablarna, eftersom de amerikanska myndigheterna inte hade vare sig bekräftat eller tillbakavisat detta påstående (se skäl 75 i detta beslut och skrivelsen från Robert Litt av den 22 februari 2016, som är bifogad i bilaga VI.I a till beslutet). Eftersom Förenta staternas regering inte hade förnekat att uppgifter som är under överföring samlas in med stöd av EO 12333, borde kommissionen emellertid enligt min mening, innan den konstaterade att skyddet var tillräckligt, ha erhållit försäkringar från den amerikanska regeringen om att en sådan insamling, för det fallet att den äger rum, kringgärdas av tillräckliga garantier mot riskerna för missbruk. Det var mot denna bakgrund som kommissionen i skälen 68–77 i nämnda beslut granskade de begränsningar och garantier som i enlighet med PPD 28 ska tillämpas i en sådan situation.

92 Det rörde sig om 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).

93 Domen PNR (punkterna 56–58). I domen av den 10 februari 2009, Irland/parlamentet och rådet (C-301/06, EU:C:2009:68, punkterna 90 och 91) fastslog domstolen vidare att resonemanget i domen PNR inte kunde överföras på den behandling som avsågs i Europaparlamentets och rådets direktiv 2006/24/EG av den 15 mars 2006 om lagring av uppgifter som genererats eller behandlats i samband med tillhandahållande av allmänt tillgängliga elektroniska kommunikationstjänster eller allmänna kommunikationsnät och om ändring av direktiv 2002/58/EG (EUT L 105, 2006, s. 54). Domstolen motiverade detta konstaterande med den omständigheten att till skillnad från det beslut som avsågs i domen PNR reglerade direktiv 2006/24 uteslutande tjänsteleverantörers verksamhet på den inre marknaden och innebar inte någon reglering av offentliga brottsbekämpande myndigheters verksamhet. Genom detta resonemang verkar det som om domstolen *e contrario* ansåg att resonemanget i domen PNR kunde ha överförts på bestämmelser om dessa myndigheters tillgång till eller användning av de lagrade uppgifterna.

94 Domen Tele2 Sverige (punkterna 67–81).

95 Europaparlamentets och rådets direktiv av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) (EGT L 201, 2002, s. 37).

bestämmelserna om lagring av uppgifter eller bestämmelserna om åtkomst till lagrade uppgifter av det undantag från direktivets tillämpningsområde som föreskrivs i artikel 1.3 i direktivet, där det bland annat hänvisas till statens verksamhet på straffrättens område och för skydd av den nationella säkerheten.[96] Domstolen bekräftade denna praxis i domen Ministerio Fiscal.[97]

216. Avsnitt 702 i FISA skiljer sig emellertid från en sådan lagstiftning, eftersom det inte ålägger leverantörer av elektroniska kommunikationstjänster en skyldighet att lagra uppgifter eller vidta någon annan behandling i avsaknad av en begäran från underrättelsetjänsterna om åtkomst till uppgifterna.

217. Frågan uppkommer då huruvida nationella åtgärder, som ålägger leverantörerna en skyldighet att *oberoende av en eventuell skyldighet att lagra uppgifter* göra uppgifter tillgängliga för offentliga myndigheter för syften som avser den nationella säkerheten, omfattas av dataskyddsförordningens tillämpningsområde och följaktligen av stadgan.[98]

218. Enligt ett *första synsätt* skulle de båda ovannämnda linjerna i rättspraxis, så långt det är möjligt, kunna förenas genom att domstolens konstaterande i domen Tele2 Sverige och domen Ministerio Fiscal avseende unionsrättens tillämplighet på åtgärder som reglerar de offentliga myndigheternas åtkomst till uppgifter för syften som avser bland annat skydd av den nationella säkerheten[99] tolkades så, att det endast avser situationer där uppgifterna har lagrats *i enlighet med en lagstadgad skyldighet* som införts i enlighet med artikel 15.1 i direktiv 2002/58. Detta konstaterande skulle däremot inte vara tillämpligt på det faktiska sammanhanget i domen PNR, vilket var ett annat, det vill säga att uppgifter som lufttrafikföretagen på eget initiativ lagrade i kommersiellt syfte överfördes till en behörig amerikansk myndighet för inre säkerhet.

219. Enligt ett *andra synsätt*, som kommissionen har förespråkat och som jag anser vara mer övertygande, innebär resonemanget i domen Tele2 Sverige och domen Ministerio Fiscal att unionsrätten är tillämplig på nationella regler som ålägger leverantörer av elektroniska kommunikationstjänster att bistå de myndigheter som ansvarar för den nationella säkerheten, så att dessa kan få tillgång till vissa uppgifter, *oavsett om dessa regler åtföljs av en föregående skyldighet att lagra uppgifterna*.

220. Kärnan i detta resonemang vilar inte på syftet med bestämmelserna i fråga, såsom i domen PNR, utan på den omständigheten att dessa bestämmelser reglerar leverantörernas verksamhet genom att de åläggs att behandla uppgifter. Denna verksamhet utgör inte statens verksamhet inom de områden som avses i artikel 1.3 i direktiv 2002/58 och artikel 3.2 i direktiv 95/46, vilkas innehåll i allt väsentligt återges i artikel 2.2 i dataskyddsförordningen.

96 Eftersom direktiv 2002/58 konkretiserar kraven i direktiv 95/46, vilket har upphävts genom dataskyddsförordningen som till stor del har samma innehåll, är rättspraxisen avseende tolkningen av artikel 1.3 i direktiv 2002/58 enligt min mening analogt tillämplig på tolkningen av artikel 2.2 i dataskyddsförordningen. Se, för ett liknande resonemang, domen Tele2 Sverige (punkt 69) och domen Ministerio Fiscal (punkt 32).

97 Domen Ministerio Fiscal (punkterna 34, 35 och 37).

98 Samma fråga har ställts i ytterligare tre begäranden om förhandsavgörande som är anhängiga vid domstolen. Se mål C-623/17, Privacy International (EUT C 22, 2018, s. 29) och de förenade målen C-511/18 och C-512/18, La Quadrature du Net m.fl. och French Data Network m.fl. (EUT C 392, 2018, s. 7).

99 Även om domstolen i domen Tele2 Sverige koncentrerade sig på att pröva huruvida de ingrepp som följde av de ifrågavarande åtgärderna för lagring och åtkomst var motiverade mot bakgrund av syftet att bekämpa brottsligheten, gäller den slutsats som den kom fram till även, med nödvändig anpassning, när sådana åtgärder syftar till att skydda den nationella säkerheten. I artikel 15.1 i direktiv 2002/58 anges nämligen, bland de syften som kan motivera sådana åtgärder, såväl brottsbekämpning som skyddet av den nationella säkerheten. Enligt artikel 1.3 i direktiv 2002/58 och artikel 2.2 i dataskyddsförordningen är dessutom statens verksamhet inom såväl området nationell säkerhet som det straffrättsliga området uteslutna från tillämpningsområdet för dessa rättsakter. De åtgärder som avsågs i det mål som föranledde domen Tele2 Sverige hade dessutom även ett syfte som var kopplat till den nationella säkerheten. I punkt 119 i den domen uttalade sig domstolen uttryckligen om huruvida åtgärder som avsåg lagring och åtkomst till trafik- och lokaliseringsuppgifter var motiverade mot bakgrund av syftet att skydda den nationella säkerheten, i den del det omfattade kampen mot terrorism.

221. I domen Tele2 Sverige påpekade domstolen således att ”tillgång till uppgifter som leverantörerna lagrat … rör … behandling av personuppgifter *från leverantörernas sida*, och denna behandling omfattas av direktivets tillämpningsområde”. [100] På samma sätt slog den i domen Ministerio Fiscal fast att lagstiftning som ålägger leverantörerna att ge de behöriga myndigheterna tillgång till lagrade uppgifter ”med nödvändighet medför behandling av personuppgifter *från leverantörernas sida*”. [101]

222. Den personuppgiftsansvariges tillhandahållande av uppgifter till en offentlig myndighet motsvarar definitionen av ”behandling” i artikel 4.2 i dataskyddsförordningen. [102] Det samma gäller den föregående filtreringen av uppgifter med användning av sökkriterier i syfte att isolera de uppgifter som de offentliga myndigheterna har begärt åtkomst till. [103]

223. Av det ovan anförda drar jag slutsatsen att enligt domstolens resonemang i domen Tele2 Sverige och domen Ministerio Fiscal är dataskyddsförordningen och följaktligen stadgan tillämpliga på nationell lagstiftning som ålägger en leverantör av elektroniska kommunikationstjänster att, oberoende av eventuella lagstadgade skyldigheter att lagra uppgifter, bistå de myndigheter som ansvarar för den nationella säkerheten genom att tillhandahålla dem uppgifter, i förekommande fall efter att ha filtrerat dem.

224. Denna tolkning förefaller dessutom, åtminstone implicit, följa av domen Schrems. Såsom DPC, den österrikiska och den polska regeringen och kommissionen har betonat slog domstolen i den domen, inom ramen för prövningen av giltigheten av Safe Harbor-beslutet, fast att det i lagstiftningen i det tredjeland som avses i ett beslut om en adekvat skyddsnivå måste föreskrivas skyddsåtgärder som är väsentligen likvärdiga med de som följer av bland annat artiklarna 7, 8 och 47 i stadgan mot ingrepp i de registrerades grundläggande rättigheter som vidtas av de offentliga myndigheterna i syfte att säkerställa den nationella säkerheten. [104]

225. Av detta följer mer specifikt att en nationell åtgärd, enligt vilken leverantörer av elektroniska kommunikationstjänster åläggs att tillgodose en begäran från de behöriga nationella säkerhetstjänsterna om åtkomst till vissa uppgifter, som dessa leverantörer oberoende av eventuella lagstadgade skyldigheter lagrar inom ramen för sin kommersiella verksamhet, varvid de begärda uppgifterna identifierats i förväg genom tillämpning av urvalstermer (såsom inom programmet PRISM), inte omfattas av artikel 2.2 i dataskyddsförordningen. Det samma gäller en nationell åtgärd enligt vilken det krävs att de företag som handhar driften av ”ryggraden” för telekommunikationer ska ge de myndigheter som ansvarar för den nationella säkerheten åtkomst till de uppgifter som överförs via den infrastruktur som de driver (såsom inom programmet Upstream).

226. När uppgifterna i fråga väl befinner sig i händerna på de statliga myndigheterna omfattas den ytterligare lagring och användning av uppgifterna som dessa myndigheter vidtar i syften som avser den nationella säkerheten däremot enligt min mening av det undantag som föreskrivs i artikel 2.2 i dataskyddsförordningen, och detta av samma skäl som de som anges i punkt 211 ovan, vilket innebär att de inte omfattas av tillämpningsområdet för denna förordning och följaktligen inte av stadgan.

100 Domen Tele2 Sverige (punkt 78, min kursivering). Som användningen av ordet ”dessutom” visar var det endast till stöd för sitt konstaterande avseende tillämpligheten av direktiv 2002/58 som domstolen, i punkt 79 i den domen, betonade det nära sambandet mellan skyldigheten att lagra uppgifterna i fråga i det mål som föranlett den domen och bestämmelserna om de nationella myndigheternas åtkomst till de lagrade uppgifterna.

101 Domen Ministerio Fiscal (punkt 37, min kursivering).

102 Se, för ett liknande resonemang, domen Ministerio Fiscal (punkt 38).

103 Se, för ett liknande resonemang, dom av den 13 maj 2014, Google Spain och Google (C-131/12, EU:C:2014:317, punkt 28).

104 Domen Schrems (punkterna 91–96). I skälen 90, 124 och 141 i beslutet om skölden för skydd av privatlivet hänvisar kommissionen dessutom till bestämmelserna i stadgan och godtar således principen att begränsningar av de grundläggande rättigheterna i syfte att skydda den nationella säkerheten måste vara förenliga med stadgan.

227. Mot bakgrund av det ovan anförda anser jag att prövningen av huruvida beslutet om skölden för skydd av privatlivet är giltigt mot bakgrund av de begränsningar av de däri angivna principerna som kan följa av de amerikanska underrättelsetjänsternas verksamhet innebär en dubbel kontroll.

228. *För det första* ska det prövas huruvida Förenta staterna säkerställer en skyddsnivå som är väsentligen likvärdig den som följer av bestämmelserna i dataskyddsförordningen och stadgan, när det gäller de begränsningar som följer av tillämpningen av avsnitt 702 i FISA, i den del denna bestämmelse ger NSA möjlighet att ålägga leverantörerna att tillhandahålla denna myndighet personuppgifter.

229. Bestämmelserna i Europakonventionen utgör *för det andra* den relevanta referensramen när det gäller att utvärdera om de begränsningar som genomförandet av EO 12333 kan medföra, i den del den tillåter att underrättelsetjänsterna själva samlar in personuppgifter utan att använda sig av privata operatörer, påverkar huruvida den skyddsnivå som Förenta staterna säkerställer är adekvat. Dessa bestämmelser tillhandahåller också de jämförelsenormer som gör det möjligt att bedöma huruvida skyddsnivån är adekvat med hänsyn till dessa myndigheters lagring och användning av de inhämtade uppgifterna för syften som avser den nationella säkerheten.

230. Emellertid måste det också fastställas huruvida ett konstaterande av en adekvat skyddsnivå förutsätter att insamlingen av uppgifter enligt EO 12333 åtföljs av en skyddsnivå som är väsentligen likvärdig den som ska säkerställas i unionen, *även i den mån denna insamling sker utanför Förenta staternas territorium* under själva överföringen av uppgifterna från unionen till detta tredjeland.

2) Nödvändigheten att säkerställa en adekvat skyddsnivå under överföringen av uppgifterna

231. Tre olika ståndpunkter har anförts vid domstolen avseende huruvida det är nödvändigt att kommissionen, vid utvärderingen av huruvida ett tredjeland säkerställer en adekvat skyddsnivå, beaktar nationella åtgärder som tredjelandet i fråga har vidtagit med avseende på myndigheternas åtkomst till uppgifter utanför tredjelandets territorium under överföringen av uppgifter från unionen till detta territorium.

232. För det första har Facebook Ireland, Förenta staternas regering och Förenade kungarikets regering hävdat att förekomsten av sådana åtgärder inte har någon inverkan på ett konstaterande om en adekvat skyddsnivå. Till stöd för detta synsätt har de gjort gällande att det är omöjligt för ett tredjeland att kontrollera alla kommunikationsvägar utanför dess territorium som används för överföring av uppgifter från unionen, vilket innebär att det antagligen aldrig kan garanteras att ett annat tredjeland inte i hemlighet samlar in uppgifter under själva överföringen.

233. För det andra har DPC, Maximillian Schrems, EPIC, den österrikiska och den nederländska regeringen, parlamentet och EDPB gjort gällande att det krav på vidmakthållande av skyddsnivån som anges i artikel 44 i dataskyddsförordningen innebär att denna nivå måste vara adekvat under hela överföringen, inbegripet när uppgifterna överförs via undervattenskablar innan de når det tredjeland som är bestämmelseland.

234. För det tredje har kommissionen, samtidigt som den erkänner denna princip, hävdat att syftet med ett konstaterande om en adekvat skyddsnivå begränsar sig till det skydd som tredjelandet i fråga säkerställer *inom sina gränser*, vilket innebär att den omständigheten att en adekvat skyddsnivå inte garanteras *under själva överföringen* till detta tredjeland inte påverkar giltigheten av ett beslut om en adekvat skyddsnivå. Dock ankommer det på den personuppgiftsansvarige att i enlighet med artikel 32 i dataskyddsförordningen säkerställa säkerheten vid överföringen genom att så långt det är möjligt skydda personuppgifterna under överföringen till tredjelandet i fråga.

235. Det ska härvid påpekas att enligt artikel 44 i dataskyddsförordningen ska en överföring till tredjeland uppfylla de villkor som anges i bestämmelserna i kapitel V i denna förordning i den mån uppgifterna kan komma att behandlas ”efter det att de överförts”. Denna formulering kan förstås så att den antingen betyder att dessa villkor ska iakttas *när uppgifterna väl har kommit fram till bestämmelselandet*, vilket Förenta staternas regering har hävdat i sitt skriftliga svar på domstolens frågor, eller att de är tillämpliga *efter det att överföringen har inletts* (inbegripet under själva överföringen).

236. Eftersom ordalydelsen i artikel 44 i dataskyddsförordningen inte är övertygande, föranleder mig en teleologisk tolkning att instämma i den andra av dessa tolkningar och således att ansluta mig till det andra av de ovan angivna synsätten. Om det skulle anses att kravet på vidmakthållande av den skyddsnivå som föreskrivs i denna bestämmelse endast gällde de övervakningsåtgärder som genomförs inom det tredjeland som är bestämmelseland, skulle det nämligen kunna kringgås genom att tredjelandet i fråga tillämpade övervakningsåtgärder utanför sitt territorium under själva överföringen av uppgifterna. För att undvika denna risk måste utvärderingen av huruvida den skyddsnivå som säkerställs av ett tredjeland är adekvat avse samtliga bestämmelser i detta tredjelands rättsordning, bland annat inom området nationell säkerhet,[105] vilket omfattar såväl bestämmelserna om den övervakning som genomförs på dess territorium som de bestämmelser som möjliggör övervakning av uppgifter under själva överföringen till detta territorium.[106]

237. Med detta sagt har det, såsom EDPB har betonat, inte bestritts att utvärderingen av huruvida skyddsnivån är adekvat endast ska avse, som det framgår av artikel 45.1 i dataskyddsförordningen, bestämmelserna i rättsordningen för *det tredjeland som är bestämmelseland för uppgifterna*. Den omständigheten att det, såsom Facebook Ireland, Förenta staternas regering och Förenade kungarikets regering har gjort gällande, är omöjligt att garantera att ett annat tredjeland inte i hemlighet samlar in dessa uppgifter under själva överföringen påverkar inte denna utvärdering. En sådan risk kan dessutom inte uteslutas ens efter det att uppgifterna har nått det tredjeland som är bestämmelseland.

238. Det är dessutom också riktigt att kommissionen, när den bedömer huruvida ett tredjeland säkerställer en adekvat skyddsnivå, eventuellt kan råka ut för att tredjelandet i fråga döljer förekomsten av vissa hemliga övervakningsprogram för den. Av detta följer emellertid inte att kommissionen, *om den får kännedom om sådana program*, kan underlåta att beakta dem vid sin granskning av huruvida skyddsnivån är adekvat. Likaså är kommissionen, om den efter antagandet av ett beslut om en adekvat skyddsnivå får kännedom om förekomsten av vissa hemliga övervakningsprogram som tredjelandet i fråga genomför på sitt territorium under överföringen till detta land, skyldig att ompröva sitt konstaterande att detta tredjeland säkerställer en adekvat skyddsnivå, om avslöjandet ger upphov till tvivel i detta hänseende.[107]

105 Se, för ett liknande resonemang, domen Schrems (punkterna 74 och 75).

106 Se, för ett liknande resonemang, EDPB, *EU-US Privacy Shield – Second Annual Joint Review*, 22 januari 2019 (s. 17, punkt 86).

107 Se artikel 45.5 i dataskyddsförordningen. Se även domen Schrems (punkt 76).

3) Beaktandet av kommissionens och den hänskjutande domstolens fastställande av de faktiska omständigheterna rörande Förenta staternas lagstiftning

239. Även om domstolen inte är behörig att vidta en tolkning av lagstiftningen i ett tredjeland som skulle vara bindande i tredjelandets rättsordning, är giltigheten av beslutet om skölden för skydd av privatlivet beroende av huruvida det fanns fog för kommissionens bedömningar avseende den skyddsnivå som säkerställs i Förenta staternas lagstiftning och praxis avseende de grundläggande rättigheterna för personer vilkas uppgifter överförs till detta tredjeland. Kommissionen var nämligen skyldig att motivera sitt konstaterande om en adekvat skyddsnivå med beaktande av de faktorer som anges i artikel 45.2 i dataskyddsförordningen, bland annat innehållet i tredjelandets lagstiftning.[108]

240. I domen av den 3 oktober 2017 tillhandahöll High Court (Förvaltningsöverdomstolen), efter att ha bedömt den bevisning som hade lagts fram av parterna i tvisten, en ingående beskrivning av relevanta aspekter av amerikansk lagstiftning.[109] Denna beskrivning sammanfaller i stort med kommissionens konstateranden i beslutet om skölden för skydd av privatlivet avseende innehållet i reglerna för de amerikanska underrättelsetjänsternas insamling av och åtkomst till de överförda uppgifterna samt avseende rättsmedlen och tillsynsmekanismerna i samband med denna verksamhet.

241. Den hänskjutande domstolen har, i likhet med flera av de parter och berörda som har inkommit med synpunkter till domstolen, snarare ifrågasatt de rättsliga konsekvenser som kommissionen har grundat på dessa konstateranden – det vill säga slutsatsen att Förenta staterna säkerställer en adekvat skyddsnivå för de grundläggande rättigheterna för de personer vilkas uppgifter överförs på grundval av detta beslut – än den beskrivning av innehållet i amerikansk rätt som den har tillhandahållit.

242. Under dessa omständigheter kommer jag att bedöma giltigheten av beslutet om skölden för skydd av privatlivet mot bakgrund av de konstateranden som kommissionen själv gjorde avseende innehållet i amerikansk rätt, genom att undersöka om kommissionens konstateranden motiverade antagandet av detta beslut om en adekvat skyddsnivå.

243. Jag instämmer härvid inte i det synsätt som har anförts av DPC och Maximillian Schrems, enligt vilket de konstateranden som High Court (Förvaltningsöverdomstolen) har gjort rörande lagstiftningen i Förenta staterna är bindande för EU-domstolen vid prövningen av huruvida beslutet om skölden för skydd av privatlivet är giltigt. Dessa har gjort gällande att eftersom utländsk rätt utgör en faktisk omständighet enligt irländsk processrätt, är den hänskjutande domstolen ensam behörig att fastställa dess innehåll.

244. Enligt fast rättspraxis är den nationella domstolen förvisso ensam behörig att fastställa de relevanta faktiska omständigheterna samt att tolka nationell rätt och tillämpa denna i det mål den har att avgöra.[110] Denna rättspraxis speglar funktionsfördelningen mellan EU-domstolen och den hänskjutande domstolen inom ramen för det förfarande som inrättats genom artikel 267 FEUF. Medan EU-domstolen är ensam behörig att tolka unionsrätten och avgöra sekundärrättens giltighet, ankommer det på den nationella domstolen, när den har att avgöra ett konkret mål som är anhängigt vid den, att fastställa den faktiska och rättsliga bakgrunden i målet så att EU-domstolen kan ge den ett användbart svar.

108 Således förklarades Safe Harbor-beslutet ogiltigt av det skälet att kommissionen i sitt beslut inte hade angett att Förenta staterna faktiskt säkerställde en adekvat skyddsnivå i sin interna lagstiftning eller på grund av sina internationella förpliktelser (domen Schrems, punkt 97). Framför allt hade kommissionen inte konstaterat att det fanns vare sig regler som staten antagit i syfte att begränsa eventuella ingrepp i de registrerades grundläggande rättigheter (domen Schrems, punkt 88) eller ett effektivt rättsligt skydd mot sådana ingrepp (domen Schrems, punkt 89).

109 Dess konstateranden sammanfattas i punkterna 54–73 ovan.

110 Se, bland annat, dom av den 4 maj 1999, Sürül (C-262/96, EU:C:1999:228, punkt 95), dom av den 11 september 2008, Eckelkamp m.fl. (C-11/07, EU:C:2008:489, punkt 32), och dom av den 26 oktober 2016, Senior Home (C-195/15, EU:C:2016:804, punkt 20).

245. Med beaktande av syftet med den hänskjutande domstolens exklusiva behörighet kan ovannämnda rättspraxis enligt min mening inte tillämpas när det gäller fastställandet av ett tredjelands lagstiftning, som en faktor som kan påverka EU-domstolens konstaterande av huruvida en sekundärrättsakt är giltig.[111] Eftersom ett konstaterande av att en sådan rättsakt är ogiltig har allmängiltig (*erga omnes*) verkan i unionens rättsordning,[112] kan EU-domstolens konstaterande inte vara beroende av ursprunget till begäran om förhandsavgörande. Som Facebook Ireland och Förenta staternas regering har betonat skulle EU-domstolens konstaterande vara beroende av ursprunget till begäran om förhandsavgörande, om den var bunden av den hänskjutande domstolens konstateranden avseende ett tredjelands lagstiftning, eftersom sådana konstateranden kan variera beroende på vilken nationell domstol de härrör från.

246. Mot bakgrund av ovanstående överväganden anser jag att när svaret på en fråga som avser giltigheten av en unionsrättsakt innebär att innehållet i ett tredjelands lagstiftning behöver utvärderas, är EU-domstolen inte bunden av den hänskjutande domstolens konstateranden avseende detta tredjelands lagstiftning, även om den kan beakta dem. EU-domstolen kan vid behov avvika från dem eller komplettera dem genom att med iakttagande av principen om ett kontradiktoriskt förfarande beakta andra källor för att fastställa de omständigheter som är nödvändiga för att bedöma giltigheten av rättsakten i fråga.[113]

4) Innebörden av standarden ”väsentlig likvärdighet”

247. Det ska erinras om att giltigheten av beslutet om skölden för skydd av privatlivet beror på huruvida de personer vilkas uppgifter överförs från unionen till Förenta staterna garanteras en skyddsnivå enligt detta tredjelands rättsordning som är ”väsentligen likvärdig” med den som garanteras i medlemsstaterna enligt dataskyddsförordningen och stadgan och, inom de områden som inte omfattas av unionsrättens tillämpningsområde, genom medlemsstaternas åtaganden enligt Europakonventionen.

248. Som domstolen betonade i domen Schrems[114] innebär denna standard inte att skyddsnivån måste vara ”identisk” med den som krävs i unionen. Även om de medel som ett tredjeland använder för att skydda de registrerades rättigheter kan skilja sig från de som föreskrivs i dataskyddsförordningen jämförd med stadgan, ”måste dessa medel … visa sig i praktiken kunna säkerställa ett skydd som är väsentligen likvärdigt med det skydd som garanteras inom unionen”.

249. Av detta följer även enligt min mening att lagstiftningen i det tredjeland som är bestämmelseland kan spegla dess egen värdeskala, enligt vilken de olika förevarande intressenas respektive tyngd kan skilja sig från den som de tilldelas i unionens rättsordning. Det skydd för personuppgifter som gäller inom unionen uppfyller dessutom en särskilt hög standard jämfört med den skyddsnivå som gäller i resten av världen. Kriteriet ”väsentlig likvärdighet” ska därför, anser jag, tillämpas så, att en viss flexibilitet bibehålls i syfte att beakta olika rättsliga och kulturella traditioner. Detta kriterium innebär emellertid, utan att tömma det på sitt innehåll, att vissa minimigarantier och allmänna krav på skydd för de grundläggande rättigheterna som följer av stadgan och Europakonventionen har en motsvarighet i rättsordningen i det tredjeland som är bestämmelseland.[115]

111 Se dom från Supreme Court (Högsta domstolen) av den 31 maj 2019 (punkt 6.18).

112 Se dom av den 13 maj 1981, International Chemical Corporation (66/80, EU:C:1981:102, punkterna 12 och 13).

113 Se dom av den 22 mars 2012, GLS (C-338/10, EU:C:2012:158, punkterna 15, 33 och 34), i vilken domstolen, vid bedömningen av giltigheten av en förordning om införande av en antidumpningstull, beaktade statistik från Eurostat som kommissionen hade lagt fram på begäran av domstolen. Se även dom av den 22 oktober 1991, Nölle (C-16/90, EU:C:1991:402, punkterna 17, 23 och 24). Likaså beaktade domstolen i domen Schrems (punkt 90) vissa meddelanden från kommissionen inom ramen för sin prövning av huruvida Safe Harbor-beslutet var giltigt.

114 Domen Schrems (punkterna 73 och 74).

115 Se, för ett liknande resonemang, Artikel 29-arbetsgruppen, *Adequacy Referential (updated)*, 28 november 2017, WP 254 (s. 3, 4 och 9).

250. Enligt artikel 52.1 i stadgan ska varje begränsning i utövandet av de rättigheter och friheter som erkänns i stadgan vara föreskriven i lag, vara förenlig med det väsentliga innehållet i dessa rättigheter och friheter och, med beaktande av proportionalitetsprincipen, vara nödvändig och faktiskt svara mot ett mål av allmänt samhällsintresse som erkänns av unionen eller behovet av skydd för andra människors rättigheter och friheter. Dessa krav motsvarar väsentligen de som anges i artikel 8.2 i Europakonventionen. [116]

251. Enligt artikel 52.3 i stadgan ska de rättigheter som erkänns i artiklarna 7, 8 och 47 i stadgan, i den mån de motsvarar de rättigheter som föreskrivs i artiklarna 8 och 13 i Europakonventionen, ha samma innebörd och räckvidd som i konventionen, vilket dock inte hindrar att unionsrätten tillförsäkrar dem ett mer långtgående skydd. Mot denna bakgrund, och som det framgår av mitt resonemang nedan, är de standarder som följer av artiklarna 7, 8 och 47 i stadgan, såsom de har tolkats av EU-domstolen, i vissa hänseenden mer strikta än de som följer av artikel 8 i Europakonventionen, såsom den tolkats av Europeiska domstolen för de mänskliga rättigheterna (nedan kallad Europadomstolen).

252. Det ska även påpekas att mål är anhängiga vid båda dessa domstolar, i vilka de har anmodats att ompröva vissa aspekter i respektive rättspraxis. Vid Europadomstolen har således två av dess senare domar avseende övervakning av elektroniska kommunikationer – nämligen domen Centrum för Rättvisa mot Sverige [117] och domen Big Brother Watch mot Förenade kungariket [118] – hänskjutits till stora avdelningen för omprövning. Vid EU-domstolen har tre nationella domstolar gjort framställningar om begäran om förhandsavgörande, vilka har föranlett en diskussion om huruvida en viss förändring av den rättspraxis som följer av domen Tele2 Sverige är nödvändig. [119]

253. Efter dessa preciseringar kommer jag nu att undersöka huruvida beslutet om skölden för skydd av privatlivet är giltigt mot bakgrund av artikel 45.1 i dataskyddsförordningen jämförd med stadgan och Europakonventionen, i den del dessa garanterar rätten till dels respekt för privatlivet och skydd för personuppgifter (avsnitt b), dels ett effektivt domstolsskydd (avsnitt c).

b) Huruvida beslutet om skölden för skydd av privatlivet är giltigt mot bakgrund av rätten till respekt för privatlivet och skydd för personuppgifter

254. Genom den fjärde frågan har den hänskjutande domstolen ifrågasatt huruvida den skyddsnivå som Förenta staterna säkerställer för de registrerades grundläggande rätt till respekt för privatlivet och skydd för personuppgifter är väsentligen likvärdig den skyddsnivå som garanteras inom unionen.

1) Huruvida ingrepp föreligger

255. I skälen 67–124 i beslutet om skölden för skydd av privatlivet framhöll kommissionen möjligheten att de amerikanska offentliga myndigheterna inom ramen för program grundade framför allt på avsnitt 702 i FISA eller EO 12333 får tillgång till uppgifter som överförs från unionen och använder dem för syften som avser den nationella säkerheten.

116 I artikel 8.2 i Europakonventionen används emellertid inte begreppet ”det väsentliga innehållet” i rätten till respekt för privatlivet. Se fotnot 161 nedan.

117 Europadomstolen, 19 juni 2018 (CE:ECHR:2018:0619JUD003525208) (nedan kallad domen Centrum för Rättvisa).

118 Europadomstolen, 13 september 2018 (CE:ECHR:2018:0913JUD005817013) (nedan kallad domen Big Brother Watch).

119 Se de mål som det hänvisas till i fotnot 98 ovan och målet C-520/18, Ordre des barreaux francophones et germanophone m.fl. (EUT C 408, 2018, s. 39).

256. Genomförandet av dessa program medför intrång från de amerikanska underrättelsetjänsternas sida som, om de härrörde från myndigheterna i en medlemsstat, skulle betraktas som ingrepp i utövandet av den rätt till respekt för privatlivet som garanteras i artikel 7 i stadgan och artikel 8 i Europakonventionen. De registrerade exponeras även för en risk för att deras personuppgifter behandlas på ett sätt som inte uppfyller kraven i artikel 8 i stadgan. [120]

257. Det ska från första början preciseras att rätten till respekt för privatlivet och skydd för personuppgifter inte endast omfattar skydd av innehållet i kommunikationerna utan även skydd av trafikuppgifterna [121] och lokaliseringsuppgifterna (tillsammans kallade metadata). Såväl EU-domstolen som Europadomstolen har de facto erkänt att metadata precis som datainnehållet kan avslöja väldigt exakta uppgifter om en persons privatliv. [122]

258. Vid fastställandet av om det föreligger ett ingrepp i utövandet av den rättighet som garanteras i artikel 7 i stadgan är det enligt EU-domstolens praxis av föga betydelse huruvida uppgifterna i fråga är av känslig art och huruvida de berörda har fått utstå olägenheter på grund av övervakningsåtgärden i fråga. [123]

259. Med detta sagt medför de övervakningsprogram som grundar sig på avsnitt 702 i FISA i första hand ingrepp i utövandet av de grundläggande rättigheterna för de personer vilkas kommunikationer motsvarar de urvalstermer som har valts av NSA och som leverantörerna av elektroniska kommunikationstjänster följaktligen överför till NSA. [124] Den skyldighet som åligger leverantörerna att *tillhandahålla* NSA uppgifter innebär, i den del som den avviker från principen om att kommunikationer ska vara konfidentiella, [125] i sig ett ingrepp även om underrättelsetjänsterna inte senare söker i eller använder uppgifterna. [126] Dessa myndigheters *lagring* och faktiska *åtkomst* till metadata och innehållet i de kommunikationer som de tillhandahålls samt *användningen* av dessa uppgifter utgör ytterligare ingrepp. [127]

260. Enligt vad som har konstaterats av den hänskjutande domstolen [128] och andra källor, såsom rapporten från PCLOB om de program som genomförs enligt avsnitt 702 i FISA, vilken den amerikanska regeringen har uppmärksammat EU-domstolen på, [129] har NSA vidare, inom ramen för programmet Upstream, *för filtreringssyften tillgång* till omfattande korpusar (”paket”) med uppgifter som härrör från kommunikationsflödet via ”ryggraden” för telekommunikationer och som omfattar kommunikationer som inte innehåller de av NSA identifierade urvalstermerna. NSA kan endast snabbt, på automatiserad väg undersöka dessa uppgiftskorpusar för att avgöra om de innehåller

120 Även om en behandling samtidigt kan strida mot både artikel 7 och artikel 8 i stadgan är den relevanta bedömningsramen vad gäller tillämpningen av artikel 8 strukturellt olik den som gäller för artikel 7. Rätten till skydd för personuppgifter innebär enligt artikel 8.2 i stadgan att ”[d]essa uppgifter ska behandlas lagenligt för bestämda ändamål och på grundval av den berörda personens samtycke eller någon annan legitim och lagenlig grund” och att ”[v]ar och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem”. En kränkning av denna rättighet förutsätter att personuppgifterna har behandlats i strid med dessa krav. Detta är fallet bland annat om behandlingen inte vilar vare sig på den registrerades samtycke *eller på någon annan legitim och lagenlig grund*. Medan frågan om huruvida ett ingrepp föreligger och frågan om huruvida ingreppet är motiverat är konceptuellt olika frågor inom ramen för artikel 7 överlappar de varandra när det gäller artikel 8 i stadgan.

121 I artikel 2 andra stycket led b i direktiv 2002/58 definieras begreppet ”trafikuppgifter” som ”alla uppgifter som behandlas i syfte att överföra en kommunikation via ett elektroniskt kommunikationsnät eller för att fakturera den”.

122 Se dom av den 8 april 2014, Digital Rights Ireland m.fl. (C-293/12 och C-594/12, EU:C:2014:238, punkt 27) (nedan kallad domen Digital Rights Ireland), och domen Tele2 Sverige (punkt 99). Se även Europadomstolen, 2 augusti 1984, Malone mot Förenade kungariket (CE:ECHR:1984:0802JUD000869179, § 84), och 8 februari 2018, Ben Faiza mot Frankrike (CE:ECHR:2018:0208JUD003144612, § 66).

123 Se domen Digital Rights Ireland (punkt 33), yttrande 1/15 (punkt 124) och domen Ministerio Fiscal (punkt 51).

124 Se skälen 78–81 och bilaga VI.II till beslutet om skölden för skydd av privatlivet.

125 Se domen Digital Rights Ireland (punkt 32).

126 Se, för ett liknande resonemang, yttrande 1/15 (punkterna 124 och 125), varav det framgår att utlämnande av personuppgifter till tredje man utgör ett ingrepp i utövandet av de grundläggande rättigheterna för de berörda personerna oavsett hur de används senare.

127 Se, för ett liknande resonemang, domen Digital Rights Ireland (punkt 35), domen Schrems (punkt 87) och yttrande 1/15 (punkterna 123–126).

128 Se punkt 60 ovan.

129 PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of the [FISA]*, 2 juli 2014 (nedan kallad rapporten från PCLOB), s. 84 och 111. Se även Artikel 29-arbetsgruppen, *EU-U.S. Privacy Shield – First Annual Joint Review*, 28 november 2017, WP 255 (B.1.1, s. 15).

urvalstermerna. Endast de sålunda filtrerade kommunikationerna lagras sedan i NSA:s databaser. Denna åtkomst till uppgifter i syfte att filtrera dem utgör också enligt min mening ett ingrepp i utövandet av de registrerades rätt till respekt för privatlivet, oavsett hur de uppgifter som filtrerats fram senare används. [130]

261. Tillhandahållandet och filtreringen av uppgifterna i fråga, [131] underrättelsetjänsternas tillgång till uppgifterna, liksom den eventuella lagringen, analysen och användningen av dem omfattas av begreppet ”behandling” i den mening som avses i artikel 4.2 i dataskyddsförordningen och artikel 8.2 i stadgan. Dessa behandlingar måste följaktligen uppfylla de krav som föreskrivs i sistnämnda bestämmelse. [132]

262. Övervakningen i enlighet med EO 12333 kan, å sin sida, innebära direkt åtkomst för underrättelsetjänsterna till uppgifter under själva överföringen, vilket utgör ett ingrepp i utövandet av den rättighet som garanteras i artikel 8 i Europakonventionen. Till detta ingrepp kommer det ingrepp som utgörs av den eventuella senare användningen av dessa uppgifter.

2) Huruvida ingreppen kan anses vara ”föreskrivna i lag”

263. Kravet att varje ingrepp i utövandet av de grundläggande rättigheterna ska vara ”föreskrivet i lag” i den mening som avses i artikel 52.1 i stadgan och artikel 8.2 i Europakonventionen innebär enligt praxis från EU-domstolen [133] och Europadomstolen [134] inte endast att den åtgärd som utgör ingreppet måste ha en rättslig grund i nationell lagstiftning, utan även att denna rättsliga grund måste uppfylla vissa krav på tillgänglighet och förutsebarhet, så att risken för godtycklighet förhindras.

264. De parter och berörda som har inkommit med yttranden till domstolen i detta hänseende är oeniga om huruvida avsnitt 702 i FISA och EO 12333 uppfyller villkoret avseende förutsebarhet.

265. Detta villkor kräver, såsom det har tolkats av EU-domstolen [135] och Europadomstolen, [136] att lagstiftning som innebär ett ingrepp i utövandet av rätten till respekt för privatlivet måste innehålla tydliga och precisa bestämmelser som reglerar omfattningen och tillämpningen av åtgärden i fråga och som ålägger minimikrav, så att de registrerade ges garantier som är tillräckliga för att skydda deras personuppgifter mot riskerna för missbruk och mot all olaglig åtkomst eller användning av dessa uppgifter. I sådana bestämmelser måste särskilt anges under vilka omständigheter och på vilka villkor de offentliga myndigheterna kan lagra personuppgifter, ha tillgång till dem och använda dem. [137] I själva den rättsliga grund som möjliggör ingreppet ska dessutom räckvidden av begränsningen i utövandet av rätten till respekt för privatlivet definieras. [138]

130 Se fotnot 126 ovan.

131 Se punkt 222 ovan.

132 Se yttrande 1/15 (punkt 123 och där angiven rättspraxis).

133 Se, bland annat, yttrande 1/15 (punkt 146).

134 Se, bland annat, Europadomstolen, 2 augusti 1984, Malone mot Förenade kungariket (CE:ECHR:1984:0802JUD000869179, § 66), beslut av den 29 juni 2006, Weber och Saravia mot Tyskland (CE:ECHR:2006:0629DEC005493400, § 84 och där angiven rättspraxis) (nedan kallat beslutet Weber och Saravia) och dom av den 4 december 2015, Zakharov mot Ryssland (CE:ECHR:2015:1204JUD004714306, § 228) (nedan kallad domen Zakharov).

135 Se, bland annat, domen Digital Rights Ireland (punkterna 54 och 65), domen Schrems (punkt 91), domen Tele2 Sverige (punkt 109) och yttrande 1/15 (punkt 141).

136 Se, bland annat, beslut Weber och Saravia (§ 94 och 95), domen Zakharov (§ 236) och Europadomstolen, 12 januari 2016, Szabó och Vissy mot Ungern (CE:ECHR:2016:0112JUD003713814, § 59) (nedan kallad domen Szabó och Vissy).

137 Se domen Tele2 Sverige (punkt 117) och yttrande 1/15 (punkt 190). Se även, bland annat, Europadomstolen, 2 augusti 1984, Malone mot Förenade kungariket (CE:ECHR:1984:0802JUD000869179, § 67), domen Zakharov (§ 229) och domen Szabó och Vissy (§ 62). Europadomstolen har i dessa domar preciserat att kravet på förutsebarhet inte har samma innebörd i fråga om avlyssning av kommunikationer som inom andra områden. I samband med hemliga övervakningsåtgärder kan kravet på förutsebarhet inte innebära att enskilda måste ges möjlighet att förutse om och när hans eller hennes kommunikationer riskerar att avlyssnas av myndigheterna, så att vederbörande kan anpassa sitt beteende därefter.

138 Yttrande 1/15 (punkt 139). Se även, för ett liknande resonemang, Europadomstolen, 25 mars 1983, Silver m.fl. mot Förenade kungariket (CE:ECHR:1983:0325JUD000594772, § 88 och 89).

266. I likhet med Maximillian Schrems och EPIC är jag tveksam till huruvida EO 12333 eller PPD 28, vilket innehåller garantier som åtföljer all signalspaningsverksamhet,[139] är tillräckligt förutsebara för att ha ”egenskapen av lag”.

267. I dessa instrument anges uttryckligen att de inte ger berörda personer några rättsligt verkställbara rättigheter.[140] Berörda personer kan således inte vid domstol åberopa de garantier som föreskrivs i PPD 28.[141] Kommissionen har för övrigt i beslutet om skölden för skydd av privatlivet ansett att de garantier som anges i detta presidentdirektiv, även om de är bindande för underrättelsetjänsterna,[142] ”inte är formulerade i juridiska termer”.[143] EO 12333 och PPD 28 är mer att likna vid interna administrativa instruktioner som kan återkallas eller ändras av Förenta staternas president. Europadomstolen har tidigare slagit fast att interna administrativa direktiv inte har ”egenskapen av lag”.[144]

268. Vad gäller avsnitt 702 i FISA har Maximillian Schrems ifrågasatt huruvida denna bestämmelse är förutsebar, eftersom den inte föreskriver tillräckliga garantier mot riskerna för missbruk när det gäller valet av de urvalskriterier som används för att filtrera uppgifterna. Eftersom denna problematik även berör huruvida de ingrepp som föreskrivs i avsnitt 702 i FISA är strikt nödvändiga, behandlar jag den längre fram i min bedömning.[145]

269. Den tredje giltighetsfrågan sammanfaller med tematiken avseende huruvida villkoret ”egenskapen av lag” är uppfyllt. Genom denna fråga vill den hänskjutande domstolen få klarhet i huruvida bedömningen av om skyddsnivån i ett tredjeland är adekvat ska göras endast med beaktande av de rättsligt bindande regler som är i kraft i tredjelandet i fråga och den praxis som syftar till att säkerställa att de respekteras, eller också med beaktande av de olika icke-bindande instrument och utomrättsliga kontrollmekanismer som tillämpas där.

270. Artikel 45.2 a i dataskyddsförordningen innehåller en icke uttömmande förteckning över omständigheter som kommissionen ska beakta när den bedömer om det föreligger en adekvat skyddsnivå i ett tredjeland. En av de omständigheter som anges är den tillämpliga lagstiftningen och det sätt på vilket den tillämpas. I denna bestämmelse nämns även påverkan av andra typer av normer, såsom yrkesregler och säkerhetsbestämmelser. Dessutom krävs enligt denna bestämmelse att hänsyn ska tas till ”faktiska och verkställbara rättigheter” och ”effektiv administrativ och rättslig prövning för de registrerade vars personuppgifter överförs”.[146]

139 Skälen 69–77 och bilaga VI.I till beslutet om skölden för skydd av privatlivet innehåller en redogörelse för PPD 28. Där anges att detta presidentdirektiv är tillämpligt på såväl underrättelseverksamhet som grundar sig på avsnitt 702 i FISA som på underrättelseverksamhet som genomförs utanför Förenta staterna.

140 I punkt 3.7 c i EO 12333 anges följande: ”[t]his order is intended only to improve the internal management of the executive branch and is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies or entities, its officers, employees, or agents, or any other person.” I artikel 6 d i PPD 28 föreskrivs följande: ”This directive is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.”

141 Se, för ett liknande resonemang, EDPB, *EU-U.S. Privacy Shield – Second Annual Joint Review*, 22 januari 2019 (punkt 99).

142 Se skälen 69 och 77 i beslutet om skölden för skydd av privatlivet.

143 Skäl 76 i beslutet om skölden för skydd av privatlivet.

144 Se Europadomstolen, 25 mars 1983, Silver m.fl. mot Förenade kungariket (CE:ECHR:1983:0325JUD000594772, § 26 och 86).

145 Se punkterna 295–301 nedan. I domen Tele2 Sverige (punkterna 116 och 117) och yttrande 1/15 (punkterna 140 och 141) beskrevs villkoret att lagen ska vara förutsebar så, att det har ett nära samband med villkoret att ingreppet ska vara nödvändigt och proportionerligt. På samma sätt är förekomsten av effektiva garantier mot riskerna för missbruk enligt Europadomstolens rättspraxis en del av såväl villkoret att ingreppet ska vara ”förutsebart” som villkoret att ingreppet ska vara ”nödvändigt i ett demokratiskt samhälle”, och iakttagandet av dessa båda villkor prövas tillsammans. Se, bland annat, Europadomstolen, 18 maj 2010, Kennedy mot Förenade kungariket (CE:ECHR:2010:0518JUD002683905, § 155), domen Zakharov (§ 236), domen Centrum för Rättvisa (§ 107) och domen Big Brother Watch (§ 322).

146 Se även skäl 104 i dataskyddsförordningen.

271. Nämnda bestämmelse innebär enligt min mening, läst som en helhet och mot bakgrund av den icke-uttömmande karaktären av den förteckning som den innehåller, att praxis eller instrument som inte grundar sig på en tillgänglig och förutsebar rättslig grund kan beaktas vid helhetsbedömningen av den skyddsnivå som tredjelandet i fråga säkerställer, som ett stöd för sådana garantier som har en rättslig grund med dessa egenskaper. Som främst DPC, Maximillian Schrems, den österrikiska regeringen och EDPB har gjort gällande kan sådana instrument eller praxis däremot inte ersätta sådana garantier och följaktligen inte heller själva säkerställa den erforderliga skyddsnivån.

3) Avsaknaden av kränkning av det väsentliga innehållet i de grundläggande rättigheterna

272. Kravet i artikel 52.1 i stadgan att varje begränsning av de rättigheter och friheter som erkänns i stadgan ska vara förenlig med det väsentliga innehållet i dessa rättigheter och friheter innebär att om ett ingrepp kränker dessa rättigheter eller friheter, kan inget legitimt mål motivera detta. Ingreppet ska då anses strida mot stadgan, utan att det behöver prövas om ingreppet är ägnat att uppnå detta mål och är nödvändigt för att uppnå det.

273. Domstolen har i detta sammanhang slagit fast att nationell lagstiftning som tillåter myndigheterna generell åtkomst till *innehållet* i elektroniska kommunikationer kränker det väsentliga innehållet i den rätt till respekt för privatlivet som garanteras i artikel 7 i stadgan.[147] Däremot har domstolen, samtidigt som den betonat de risker som är förenade med åtkomst och analys av *trafik- och lokaliseringsuppgifter*,[148] ansett att det väsentliga innehållet i denna rättighet inte påverkas om nationell lagstiftning ger statliga myndigheter generell åtkomst till dessa uppgifter.[149]

274. Avsnitt 702 i FISA kan enligt min mening inte anses ge de amerikanska underrättelsetjänsterna befogenhet för generell åtkomst till innehållet i elektroniska kommunikationer.

275. Underrättelsetjänsternas tillgång till uppgifter i syfte att *eventuellt analysera dem och använda dem* är enligt avsnitt 702 i FISA nämligen begränsad till uppgifter som motsvarar de urvalskriterier som är associerade med enskilda måltavlor.

276. Vidare kan programmet Upstream visserligen innebära generell åtkomst till innehållet i elektroniska kommunikationer *i syfte att filtrera dem på automatisk väg* i den situationen att urvalstermerna inte endast tillämpas på fälten ”från” och ”till”, utan även på allt innehåll i kommunikationsflödena (sökning ”rörande” urvalstermen).[150] Som kommissionen har hävdat och i motsats till vad Maximillian Schrems och EPIC har påstått kan underrättelsetjänsternas tillfälliga åtkomst till allt innehåll i elektroniska kommunikationer enbart i syfte att filtrera det med tillämpning

147 Se domen Schrems (punkt 94). Se även domen Digital Rights Ireland (punkt 39) och domen Tele2 Sverige (punkt 101). Med beaktande av det nära sambandet mellan rätten till respekt för privatlivet och rätten till skydd för personuppgifter anser jag att en nationell åtgärd som ger offentliga myndigheter generell åtkomst till innehållet i kommunikationer också kränker det väsentliga innehållet i den rättighet som stadfästs i artikel 8 i stadgan.

148 Se punkt 257 ovan. I domen Tele2 (punkt 99) betonade domstolen att metadata särskilt gör det möjligt att kartlägga de berörda personerna. Artikel 29-arbetsgruppen påpekade i sitt yttrande 4/2014 om övervakning av elektronisk kommunikation för ändamål som rör underrättelse och nationell säkerhet av den 10 april 2014, WP 215 (s. 5) att metadata tack vare sin strukturerade karaktär är enklare att aggregera och analysera än datainnehållet.

149 Se domen Tele2 Sverige (punkt 99). Vissa kommentatorer har frågat sig huruvida åtskillnaden mellan generell åtkomst till innehållet i kommunikationerna och generell åtkomst till metadata är välgrundad, mot bakgrund av den tekniska utvecklingen och utvecklingen av kommunikationssätten. Se Falot, N. och Hijmans, H., ”Tele2: de afweging tussen privacy en veiligheid nader omlijnd”, *Nederlands Tijdschrift voor Europees Recht*, nr 3, 2017 (s. 48) och Ojanen, T., ”Making essence of the rights real: the Court of Justice of the European Union clarifies the structure of fundamental rights under the Charter” (kommentar till domen Schrems), *European Constitutional Law Review*, 2016 (s. 5).

150 Se fotnot 87 i beslutet om skölden för skydd av privatlivet. Enligt vad EPIC har angett i sina synpunkter och enligt det skriftliga svaret från Förenta staternas regering på de frågor som domstolen ställt krävde FISC emellertid år 2017 att sökningarna ”rörande” en urvalsterm skulle upphöra på grund av oegentligheter som förekommit vid sökningar av denna typ. Kongressen har dock, i den akt om nytt godkännande av FISA som antogs 2018, föreskrivit möjligheten att återinföra denna typ av sökningar efter medgivande av FISC och kongressen. Se även EDPB, *EU-U.S. Privacy Shield – Second Annual Joint Review*, 22 januari 2019 (s. 27, punkt 55).

av urvalskriterier emellertid inte likställas med en generell åtkomst till detta innehåll.[151] Enligt min mening är det ingrepp som följer av denna tidsbegränsade åtkomst, som syftar till automatiserad filtrering, inte lika allvarligt som det som följer av en generell åtkomst för offentliga myndigheter till detta innehåll i syfte att analysera det och eventuellt använda det.[152] Tillfällig åtkomst i syfte att filtrera innehållet ger inte dessa myndigheter möjlighet att lagra metadata eller kommunikationsinnehåll som inte motsvarar urvalskriterierna och framför allt inte, såsom den amerikanska regeringen har påpekat, att kartlägga enskilda som kriterierna inte är inriktade på.

277. Frågan huruvida målinriktningen med användning av urvalstermer inom ramen för de program som grundas på avsnitt 702 i FISA på ett effektivt sätt begränsar underrättelsetjänsternas befogenheter är beroende av regleringen av valet av urvalstermer.[153] Maximillian Schrems har gjort gällande att i avsaknad av en tillräcklig kontroll i detta hänseende föreskrivs i amerikansk rätt inga garantier mot en generell åtkomst till kommunikationsinnehållet redan i filtreringsskedet, vilket innebär att denna åtkomst kränker det väsentliga innehållet i de berörda personernas rätt till respekt för privatlivet.

278. Som jag kommer att redogöra för närmare nedan[154] är jag böjd att instämma i dessa tvivel vad gäller huruvida regleringen av valet av urvalstermer är tillräcklig för att uppfylla kriterierna att ingrepp ska vara förutsebara och proportionerliga. Förekomsten av denna reglering hindrar emellertid, även om den är ofullständig, slutsatsen att avsnitt 702 i FISA tillåter de offentliga myndigheterna en generell åtkomst till innehållet i elektroniska kommunikationer som följaktligen är att likställa med ett ingrepp i det väsentliga innehållet i den rättighet som stadfästs i artikel 7 i stadgan.

279. Det ska även betonas att domstolen i yttrande 1/15 ansåg att det väsentliga innehållet i rätten till skydd för personuppgifter, vilken garanteras i artikel 8 i stadgan, bibehålls, om ändamålen med behandlingen avgränsas och behandlingen åtföljs av regler som är avsedda att bland annat säkerställa säkerheten och sekretessen för uppgifterna samt deras integritet och att skydda dem från olaglig åtkomst och olaglig behandling.[155]

280. I beslutet om skölden för skydd av privatlivet konstaterade kommissionen att i såväl avsnitt 702 i FISA som PPD 28 avgränsas de syften för vilka uppgifter kan samlas in inom ramen för de program som genomförs i enlighet med avsnitt 702 i FISA.[156] Kommissionen påpekade vidare att i PPD 28 föreskrivs regler för åtkomst till uppgifterna och för deras lagring och spridning i syfte att säkerställa

151 Den hänskjutande domstolen gjorde i punkterna 188 och 189 i sin dom av den 3 oktober 2017 åtskillnad mellan å ena sidan sökning ”i bulk” och å andra sidan inhämtning, insamling eller lagring ”i bulk”. Den hänskjutande domstolen anser att även om programmet Upstream innebär sökning ”i bulk” i alla de flöden av uppgifter som överförs via ”ryggraden” för telekommunikationer, är inhämtningen, insamlingen och lagringen riktade i den meningen att de endast avser de uppgifter som innehåller urvalstermerna i fråga.

152 Se, för ett liknande resonemang, domen från Supreme Court (Högsta domstolen) av den 31 maj 2019 (punkterna 11.2 och 11.3). I denna dom konstaterades följande: ”[I]t is inevitable that any screening process designed to identify data of interest will necessarily involve all of the data available, for the whole point of the screening process is to identify within that entire universe of available data the relevant material which may be of interest and thus require closer scrutiny. Perhaps part of the problem lies in the fact that the term ”processing” covers a wide range of activity, apparently, in the view of the DPC, including screening. On the assumption that that is a correct view of the law, then it is technically correct to describe bulk screening as involving indiscriminate processing. But the use of that terminology might be taken to imply that other forms of processing, which are significantly more invasive, are carried out on an indiscriminate basis.”

153 Se yttrande 1/15 (punkt 122). Se även rapporten från Europeiska kommissionen för demokrati genom lag (Venedigkommissionen) ”Rapport sur le contrôle démocratique des agences de collecte de renseignements d’origine électromagnétique”, 15 december 2015, studie nr 719/2013 (CDL-AD(2015)011, s. 11): ”Frågan om huruvida denna process på ett lämpligt sätt begränsar onödiga intrång i oskyldiga personliga kommunikationer betyder i praktiken att det måste avgöras huruvida urvalstermen är tillräckligt relevant och specifik och huruvida algoritmen i det program som används för att identifiera relevanta uppgifter inom ramen för de valda parametrarna är av tillfredsställande kvalitet…”.

154 Se punkterna 297–301 nedan.

155 Yttrande 1/15 (punkt 150).

156 Se skälen 70, 103 och 109 i beslutet om skölden för skydd av privatlivet.

deras säkerhet och skydda dem mot otillåten åtkomst.[157] Som jag anger nedan[158] är jag tveksam särskilt till huruvida syftena med behandlingarna i fråga har angetts tillräckligt tydligt och precist för att säkerställa en skyddsnivå som är väsentligen likvärdig den som gäller i unionens rättsordning. Dessa eventuella brister räcker emellertid inte för att konstatera att liknande program skulle kränka det väsentliga innehållet i rätten till skydd för personuppgifter, om de användes inom unionen.

281. Det ska erinras om att frågan huruvida en adekvat skyddsnivå säkerställs inom ramen för övervakningsverksamhet som genomförs i enlighet med EO 12333 ska bedömas mot bakgrund av bestämmelserna i Europakonventionen. Av beslutet om skölden för skydd av privatlivet framgår att de enda begränsningar av de åtgärder som genomförs på grundval av EO 12333 i syfte att samla in uppgifter om icke-amerikanska personer är de som föreskrivs i PPD 28.[159] I detta presidentdirektiv anges att användningen av utländsk underrättelseinformation ska vara ”så anpassad som möjligt”. Emellertid nämns uttryckligen möjligheten att samla in uppgifter ”i bulk” utanför amerikanskt territorium för vissa specifika ändamål som avser den nationella säkerheten.[160] Enligt Maximillian Schrems skyddar bestämmelserna i PPD 28 – som dessutom inte föreskriver några rättigheter för enskilda – inte de registrerade mot risken för en generell åtkomst till innehållet i deras elektroniska kommunikationer.

282. Det ska härvid endast påpekas att Europadomstolen i sin praxis avseende artikel 8 i Europakonventionen inte har använt begreppet kränkning av det väsentliga innehållet, eller själva kärnan, i rätten till respekt för privatlivet.[161] Europadomstolen har hittills inte ansett att ordningar som tillåter avlyssning av elektroniska kommunikationer, inte ens om de tillåter massavlyssning, *som sådana faller utanför medlemsstaternas utrymme för skönsmässig bedömning*. Europadomstolen anser att sådana ordningar är förenliga med artikel 8.2 i Europakonventionen förutsatt att de åtföljs av ett antal minimigarantier.[162] Under dessa omständigheter är det inte lämpligt att konstatera att en ordning för övervakning av det slag som föreskrivs i EO 12333 inte omfattas av medlemsstaternas utrymme för skönsmässig bedömning, utan att först pröva de eventuella garantier som åtföljer den.

157 Se skälen 83–87 och bilaga VI.I c till beslutet om skölden för skydd av privatlivet. Det ska påpekas att enligt rapporten från PCLOB (s. 51–66) avser de flesta aspekterna av NSA:s förfaranden för ”minimering” i enlighet med avsnitt 702 i FISA endast amerikanska personer. PPD 28 syftar till att utsträcka de tillämpliga garantierna till icke-amerikanska personer. Se PCLOB, *Report to the President on the Implementation of [PPD 28]: Signals Intelligence Activities*, som finns på adressen https://www.pclob.gov/reports/report-PPD28/(s. 2). Med detta sagt omfattas enligt min mening lagringen och användningen av uppgifterna i syften som avser den nationella säkerheten efter det att de offentliga myndigheterna har inhämtat dem inte av unionsrättens tillämpningsområde (se punkt 226 ovan). Huruvida den skyddsnivå som säkerställs inom ramen för denna verksamhet är adekvat ska således bedömas endast mot bakgrund av artikel 8 i Europakonventionen.

158 Se punkterna 283–289 nedan.

159 I skäl 127 i beslutet om skölden för skydd av privatlivet konstaterade kommission särskilt att det fjärde tillägget till Förenta staternas konstitution inte är tillämpligt på icke-amerikanska personer.

160 Se skälen 73 och 74 samt bilaga VI.I b till beslutet om skölden för skydd av privatlivet. Dessa ändamål inbegriper kampen mot spionage och andra hot och verksamheter som utländska makter riktar mot Förenta staterna och dess intressen, hot från terrorister, hot som följer av utveckling, innehav, spridning eller användning av massförstörelsevapen, hot mot cybersäkerheten, hot mot den amerikanska försvarsmakten eller Förenta staternas allierade och hot från gränsöverskridande brottslighet. Enligt fotnot 5 i PPD 28 är begränsningen av de ändamål som motiverar användning av uppgifter som samlats in ”i bulk” inte tillämplig när insamlingen endast är tillfällig och avsedd att underlätta en riktad insamling.

161 Även om bestämmelserna i Europakonventionen inte innehåller begreppet ”det väsentliga innehållet” i de grundläggande rättigheterna, används det motsvarande begreppet ”själva kärnan” i en grundläggande rättighet i Europadomstolens praxis avseende vissa av dessa bestämmelser. Se bland annat, vad gäller själva kärnan i rätten till en rättvis rättegång, vilken garanteras i artikel 6 i Europakonventionen, Europadomstolen, 25 maj 1985, Ashingdane mot Förenade kungariket (CE:ECHR:1985:0528JUD000822578, § 57 och 59), 21 december 2000, Heaney and McGuinness mot Irland (CE:ECHR:2000:1221JUD003472097, § 55 och 58), och 23 juni 2016, Baka mot Ungern (CE:ECHR:2016:0623JUD002026112, § 121). När det gäller själva kärnan i rätten att ingå äktenskap, vilken stadfästs i artikel 12 i Europakonventionen, se Europadomstolen, 11 juli 2002, Christine Goodwin mot Förenade kungariket (CE:ECHR:2002:0711JUD002895795, § 99 och 101). Beträffande själva kärnan i rätten till undervisning, vilken garanteras i artikel 2 i protokoll nr 1 till Europakonventionen, se Europadomstolen, 23 juli 1968, belgiska språkmålet (CE:ECHR:1968:0723JUD000147462, § 5).

162 Se, särskilt, domen Centrum för Rättvisa (§ 112–114 och där angiven rättspraxis) och domen Big Brother Watch (§ 337).

4) Huruvida ett legitimt mål eftersträvas

283. Enligt artikel 52.1 i stadgan ska varje begränsning i utövandet av de rättigheter som erkänns i stadgan faktiskt svara mot ett mål av allmänt samhällsintresse som erkänns av unionen. I artikel 8.2 i stadgan föreskrivs vidare att all behandling av personuppgifter som inte stöder sig på den berörda personens samtycke ska vila på en ”legitim och lagenlig grund”. I artikel 8.2 i Europakonventionen anges de ändamål som kan motivera ett ingrepp i utövandet av rätten till respekt för privatlivet.

284. Enligt beslutet om skölden för skydd av privatlivet kan anslutningen till de principer som anges i beslutet begränsas för att uppfylla skyldigheter avseende nationell säkerhet, allmänintresset och rättsefterlevnaden.[163] I skälen 67–124 i detta beslut granskas mer specifikt de begränsningar som följer av de offentliga amerikanska myndigheternas åtkomst till och användning av uppgifter för syften som avser den nationella säkerheten.

285. Skyddet av den nationella säkerheten utgör ett legitimt mål som kan motivera undantag från de krav som följer av dataskyddsförordningen[164] och från de grundläggande rättigheter som stadfästs i artiklarna 7 och 8 i stadgan[165] samt från artikel 8.2 i Europakonventionen. Maximillian Schrems, den österrikiska regeringen och EPIC har emellertid påpekat att de mål som eftersträvas inom ramen för de övervakningsprogram som grundar sig på avsnitt 702 i FISA och på EO 12333 omfattar mer än enbart den nationella säkerheten. Målet med dessa instrument är nämligen att erhålla ”utländsk underrättelseinformation”, vilket är ett begrepp som omfattar olika typer av information, bland annat information som avser den nationella säkerheten utan att nödvändigtvis vara begränsad till detta.[166] Således omfattar begreppet ”utländsk underrättelseinformation”, i den mening som avses i avsnitt 702 i FISA, uppgifter som rör genomförandet av utrikespolitiken.[167] I EO 12333 definieras detta begrepp så att det omfattar information avseende utländska regeringars, organisationers och personers kapacitet, avsikter eller aktiviteter.[168] Maximillian Schrems har ifrågasatt huruvida det sålunda avsedda målet är legitimt, eftersom det går utöver den nationella säkerheten.

286. Enligt min mening kan perimetern för den nationella säkerheten i viss mån omfatta skyddet av intressen som avser genomförandet av utrikespolitiken.[169] Det är dessutom inte otänkbart att vissa andra av de syften, utöver skyddet av den nationella säkerheten, som omfattas av begreppet ”utländsk underrättelseinformation”, såsom det definieras i avsnitt 702 i FISA och i EO 12333, motsvarar viktiga mål av allmänt intresse som kan motivera ett ingrepp i den grundläggande rätten till respekt för privatlivet och skydd för personuppgifter. Dessa mål väger dock mindre tungt än skyddet av den nationella säkerheten vid en avvägning mellan de berörda personernas grundläggande rättigheter och det syfte som eftersträvas med ingreppet.[170]

163 Se punkt 197 ovan.

164 Se artikel 23.1 a i dataskyddsförordningen.

165 Se domen Schrems (punkt 88). Domstolen har betraktat det närliggande begreppet ”allmän säkerhet”, i den mening som avses i de bestämmelser i FEUF som tillåter undantag från de grundläggande friheter som garanteras i fördraget, som ett självständigt unionsrättsligt begrepp som omfattar såväl en medlemsstats inre som yttre säkerhet (se, bland annat, dom av den 26 oktober 1999, Sirdar, C-273/97, EU:C:1999:523, punkt 17, och dom av den 13 september 2016, CS, C-304/14, EU:C:2016:674, punkt 39 och där angiven rättspraxis). Medan den inre säkerheten kan påverkas bland annat genom ett direkt hot mot befolkningens trygghet och fysiska säkerhet i den berörda medlemsstaten, kan den yttre säkerheten påverkas bland annat av risken för en allvarlig störning i de yttre förbindelserna eller i den fredliga samexistensen mellan folken. Utan att unilateralt kunna fastställa innehållet i dessa begrepp har varje medlemsstat ett visst utrymme för skönsmässig bedömning när det gäller att fastställa sina väsentliga säkerhetsintressen. Se särskilt dom av den 2 maj 2018, K. och H. F. (Uppehållsrätt och anklagelser om krigsförbrytelser) (C-331/16 och C-366/16, EU:C:2018:296, punkterna 40–42 och där angiven rättspraxis). Dessa konstateranden kan enligt min mening överföras på tolkningen av begreppet ”nationell säkerhet”, som ett intresse vars skydd kan motivera begränsningar av bestämmelserna i dataskyddsförordningen och av de rättigheter som garanteras i artiklarna 7 och 8 i stadgan.

166 Se skäl 89 och fotnot 97 i beslutet om skölden för skydd av privatlivet.

167 Se punkt 55 ovan.

168 Se punkt 61 ovan.

169 I domen Centrum för Rättvisa (§ 111) slog Europadomstolen fast att övervakningsverksamhet som var avsedd att stödja Sveriges utrikespolitik, försvarspolitik och säkerhetspolitik samt identifiera externa hot som organiserades i Sverige syftade till legitima mål som avsåg den nationella säkerheten.

170 Se domen Tele2 Sverige (punkt 115) och domen Ministerio Fiscal (punkt 55). I dessa domar betonade domstolen att det intresse som har åberopats för att motivera ett ingrepp måste stå i proportion till hur allvarligt ingreppet är.

287. Enligt artikel 52.1 i stadgan krävs det emellertid också att den nationella säkerheten eller ett annat legitimt mål faktiskt eftersträvas genom de åtgärder i vilka ingreppen i fråga föreskrivs.[171] Syftena med ingreppen ska dessutom anges på ett sätt som uppfyller kraven på tydlighet och precision.[172]

288. Enligt Maximillian Schrems är syftet med de övervakningsåtgärder som föreskrivs i avsnitt 702 i FISA och EO 12333 inte angivet med tillräcklig precision för att uppfylla kraven på förutsebarhet och proportionalitet. Detta är fallet särskilt som begreppet ”utländsk underrättelseinformation” ges en väldigt vid definition i dessa instrument. Framför allt konstaterade kommissionen i skäl 109 i beslutet om skölden för skydd av privatlivet att enligt avsnitt 702 i FISA krävs att insamlingen av utländska underrättelseuppgifter ska utgöra ”ett viktigt syfte” med insamlingen, vilket, såsom även EPIC har påpekat, vid första anblicken inte utesluter att andra ej fastställda mål eftersträvas.

289. Även om det inte kan uteslutas att övervakningsåtgärder i enlighet med avsnitt 702 i FISA eller EO 12333 motsvarar legitima mål, är det mot bakgrund av ovan angivna skäl motiverat att fråga sig om dessa mål är tillräckligt tydligt och precist fastställda för att förhindra riskerna för missbruk och för att möjliggöra en kontroll av huruvida de ingrepp som följer av dem är proportionerliga.[173]

5) Huruvida ingreppen är nödvändiga och proportionerliga

290. Domstolen har upprepade gånger betonat att de rättigheter som stadfästs i artiklarna 7 och 8 i stadgan inte utgör absoluta rättigheter, utan ska ses mot bakgrund av deras funktion i samhället och vägas mot andra grundläggande rättigheter, i enlighet med proportionalitetsprincipen.[174] Bland dessa andra rättigheter ingår, som Facebook Ireland har betonat, rätten till säkerhet, som garanteras i artikel 6 i stadgan.

291. Enligt en lika fast rättspraxis ska varje ingrepp i utövandet av de rättigheter som garanteras i artiklarna 7 och 8 i stadgan vara föremål för en strikt kontroll av proportionaliteten.[175]

292. Av domen Schrems framgår särskilt att ”[e]n lagstiftning är … inte begränsad till vad som är strängt nödvändigt när den generellt tillåter lagring av samtliga [uppgifter]… 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”.[176]

171 Artikel 29-arbetsgruppen har i sitt arbetsdokument *Working Document on surveillance of electronic communications for intelligence and national security purposes* av den 5 december 2014, WP 228 (s. 27), insisterat på vikten av att kritiskt utvärdera om övervakningen faktiskt genomförs i syften som avser den nationella säkerheten.

172 Se yttrande 1/15 (punkt 181), i vilket domstolen slog fast att ordalydelsen i de lagbestämmelser i vilka ingreppen föreskrevs inte uppfyllde kraven på tydlighet och precision, vilket innebar att dessa ingrepp inte var begränsade till vad som var strängt nödvändigt. Enligt samma synsätt ansåg generaladvokaten Bot i sitt förslag till avgörande i målet Schrems (C-362/14, EU:C:2015:627, punkterna 181–184) att syftena med övervakningsåtgärderna var alltför allmänt formulerade för att betraktas som mål av allmänintresse, utom vad gällde den nationella säkerheten.

173 EDPS uttryckte liknande tvivel i sitt yttrande 4/2016 av den 30 maj 2016 om utkastet till beslut om huruvida ett adekvat skydd säkerställs genom bestämmelserna om integritetsskydd mellan EU och Förenta staterna (s. 8).

174 Se dom av den 9 november 2010, Volker und Markus Schecke och Eifert (C-92/09 och C-93/09, EU:C:2010:662, punkt 48), yttrande 1/15 (punkt 136) och dom av den 24 september 2019, Google (Territoriell räckvidd för borttagandet av länkar) (C-507/17, EU:C:2019:772, punkt 60).

175 Se, bland annat, dom av den 16 december 2008, Satakunnan Markkinapörssi och Satamedia (C-73/07, EU:C:2008:727, punkt 56), domen Digital Rights Ireland (punkterna 48 och 52), domen Schrems (punkterna 78 och 92) och yttrande 1/15 (punkterna 139 och 140). Se även skäl 140 i beslutet om skölden för skydd av privatlivet.

176 Domen Schrems (punkt 93). Se även, för ett liknande resonemang, domen Digital Rights Ireland (punkt 60).

293. Domstolen har även slagit fast att utom i vederbörligen motiverade brådskande fall ska åtkomsten underkastas förhandskontroll av en domstol eller en oberoende myndighet, vars beslut ska syfta till att begränsa åtkomsten till uppgifterna och deras användning till vad som är strängt nödvändigt för att uppnå det eftersträvade målet. [177]

294. I artikel 23.2 i dataskyddsförordningen fastställs en rad skyddsåtgärder som en medlemsstat ska föreskriva vid undantag från bestämmelserna i denna förordning. Den lagstiftning som tillåter ett sådant undantag ska innehålla bestämmelser om bland annat ändamålen med behandlingen, omfattningen av undantaget, skyddsåtgärder för att förhindra missbruk, lagringstiden och de registrerades rätt att bli informerade om undantaget, såvida detta inte kan inverka menligt på dess ändamål.

295. I förevarande fall har Maximillian Schrems hävdat att avsnitt 702 i FISA inte åtföljs av tillräckliga garantier mot riskerna för missbruk och olaglig åtkomst till uppgifterna. Framför allt är valet av urvalskriterier inte tillräckligt reglerat, vilket innebär att denna bestämmelse inte innehåller några garantier mot en generell åtkomst till innehållet i kommunikationerna.

296. Förenta staternas regering och kommissionen har tvärtom gjort gällande att i avsnitt 702 i FISA begränsas valet av urvalstermer genom objektiva kriterier, eftersom denna bestämmelse endast tillåter insamling av uppgifter från elektroniska kommunikationer rörande icke-amerikanska personer som befinner sig utanför Förenta staterna, i syfte att erhålla utländska underrättelseuppgifter.

297. Enligt min mening kan det betvivlas huruvida dessa kriterier är tillräckligt tydliga och precisa och huruvida det finns tillräckliga garantier för att förhindra riskerna för missbruk.

298. I skäl 109 i beslutet om skölden för skydd av privatlivet anges nämligen att urvalstermerna inte godkänns individuellt av FISC eller något annat oberoende rättsligt eller administrativt organ innan de tillämpas. Enligt kommissionens konstaterande i nämnda skäl ”godkänner FISC … inte individuella övervakningsåtgärder, utan snarare övervakningsprogram… på grundval av årliga certifieringar”, vilket Förenta staternas regering har bekräftat vid domstolen. Enligt vad som preciseras i samma skäl ”innehåller de certifieringar som ska godkännas av FISC inte någon information om de enskilda personer som målinriktningen gäller, utan anger snarare kategorier av utländska underrättelseuppgifter” som kan samlas in. I samma skäl konstaterar kommissionen även att ”FISC bedömer inte – enligt trolig orsak eller någon annan norm – huruvida målinriktningen för de utvalda personerna är lämplig för att inhämta utländska underrättelseuppgifter”, utan kontrollerar villkoret att ”ett viktigt syfte med insamlingen är att erhålla utländska underrättelseuppgifter”.

299. Vidare anges i ovannämnda skäl att enligt avsnitt 702 i FISA får NSA endast samla in kommunikationer ”om det skäligen kan antas att ett visst kommunikationsmedel används för att kommunicera utländsk underrättelseinformation”. I skäl 70 i beslutet om skölden för skydd av privatlivet tilläggs att fastställandet av urvalstermer sker inom den övergripande prioriteringsramen för nationell underrättelseverksamhet (National Intelligence Priorities Framework, NIPF). I beslutet nämns inte några närmare krav som åligger NSA på att ange skälen eller lämna en motivering till valet av urvalstermer mot bakgrund av dessa administrativa prioriteringar. [178]

177 Se domen Tele2 Sverige (punkt 120) och yttrande 1/15 (punkt 202).

178 I rapporten från PCLOB (s. 45) anges följande: ”With respect to the foreign intelligence purpose, the NSA targeting procedures require the analyst only to ”identify” the foreign power or foreign territory regarding which the foreign intelligence information is to be acquired. By policy, but not as a requirement of the targeting procedures, the NSA also requires that all taskings be accompanied by a very brief statement (typically no more than one sentence long) that further explains the analyst's rationale for assessing that tasking the selector in question will result in the acquisition of the types of foreign intelligence information authorized by the Section 702 certification.”

300. Slutligen hänvisas i skäl 71 i beslutet om skölden för skydd av privatlivet till det krav som fastställs i PPD 28, att insamlingen av utländsk underrättelseinformation ska vara ”så anpassad som möjligt”. Förutom den omständigheten att detta presidentdirektiv inte föreskriver några rättigheter för enskilda är det långt ifrån uppenbart att en väsentlig likvärdighet föreligger mellan kriteriet att en verksamhet ska vara ”så anpassad som möjligt” och kriteriet att verksamheten ska begränsas till det ”strikt nödvändiga”, såsom det krävs enligt artikel 52.1 i stadgan för att motivera ett ingrepp i utövandet av de rättigheter som garanteras i artiklarna 7 och 8 i denna. [179]

301. Mot bakgrund av det ovan anförda är det på grundval av de omständigheter som beskrivs i beslutet om skölden för skydd av privatlivet inte säkert att de övervakningsåtgärder som grundar sig på avsnitt 702 i FISA åtföljs av garantier, avseende begränsning av de personer som kan omfattas av en övervakningsåtgärd och av de mål för vilka uppgifterna kan samlas in, som är väsentligen likvärdiga de som krävs enligt dataskyddsförordningen jämförd med artiklarna 7 och 8 i stadgan. [180]

302. Vad gäller bedömningen av huruvida den övervakning som sker i enlighet med EO 12333 kringgärdas av en adekvat skyddsnivå har Europadomstolen tillerkänt medlemsstaterna ett stort utrymme för skönsmässig bedömning när det gäller att välja metoder för att skydda sin nationella säkerhet, vilket dock begränsas av kravet på att föreskriva lämpliga och tillräckliga garantier mot missbruk. [181] Enligt Europadomstolens praxis avseende hemliga övervakningsåtgärder ska det prövas om den nationella lagstiftning som övervakningsåtgärderna grundar sig på innehåller tillräckliga och effektiva garantier och skydd som är ägnade att uppfylla kraven på ”förutsebarhet” och ”nödvändighet i ett demokratiskt samhälle”. [182]

303. Europadomstolen har i detta sammanhang uppställt ett antal minimigarantier. Dessa garantier utgörs av följande: en tydlig angivelse av det slag av överträdelser som kan föranleda ett avlyssningsbeslut, fastställande av de kategorier av personer vilkas kommunikationer kan komma att avlyssnas, fastställande av en gräns för åtgärdens varaktighet, fastställande av det förfarande som ska följas vid granskning, användning och lagring av insamlade uppgifter, fastställande av försiktighetsåtgärder som ska vidtas vid överföring av uppgifterna till andra parter och fastställande av under vilka omständigheter de registrerade uppgifterna ska raderas eller förstöras. [183]

304. Huruvida de garantier som kringgärdar ingreppet är adekvata och effektiva beror på samtliga omständigheter i det aktuella fallet, bland annat åtgärdernas art, omfattning och varaktighet, vilka skäl som krävs för att besluta om dem, vilka myndigheter som är behöriga att ge tillstånd för, genomföra och kontrollera åtgärderna samt vilket rättsmedel som är tillgängligt enligt nationell rätt. [184]

179 Se, för ett liknande resonemang, Artikel 29-arbetsgruppen, *Opinion 1/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, 13 april 2016, WP 238 (punkt 3.3.1, s. 38), parlamentets resolution av den 6 april 2017 om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och USA, P8_TA(2017)0131 (punkt 17), och parlamentets betänkande av den 20 februari 2017 om stordatas effekter på de grundläggande rättigheterna: integritet, uppgiftsskydd, icke-diskriminering, säkerhet och brottsbekämpning, A8–0044/2017 (punkt 17).

180 Se, för ett liknande resonemang, Artikel 29-arbetsgruppen, *EU-U.S. Privacy Shield – First Annual Joint Review*, 28 november 2017, WP 255 (s. 3), parlamentets resolution av den 5 juli 2018 om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och USA, P8_TA(2018)0315 (punkt 22), och EDPB, *EU-U.S. Privacy Shield – Second Annual Joint Review*, 22 januari 2019 (punkterna 81–83 och 87).

181 Se, bland annat, domen Zakharov (§ 232) och domen Szabó och Vissy (§ 57).

182 Se, bland annat, domen Zakharov (§ 237), domen Centrum för Rättvisa (§ 111) och domen Big Brother Watch (§ 322).

183 Se, bland annat, beslut Weber och Saravia (§ 95), Europadomstolen, 28 juni 2007, Association pour l’intégration européenne et les droits de l’homme och Ekimdjiev (CE:ECHR:2007:0628JUD006254000, § 76) och domen Zakharov (§ 231).

184 Se, bland annat, beslut Weber och Saravia (§ 106), domen Zakharov (§ 232) och domen Centrum för Rättvisa (§ 104).

305. För att bedöma huruvida en hemlig övervakningsåtgärd är motiverad beaktar Europadomstolen särskilt alla de kontroller som vidtas ”när övervakningen beslutas”, ”medan den pågår” och ”efter att den har avslutats”.[185] Vad gäller det första av dessa tre skeden kräver Europadomstolen att övervakningsåtgärden har godkänts av ett oberoende organ. Även om Europadomstolen anser att en domstol innebär de bästa garantierna för ett oberoende, opartiskt och lagenligt förfarande måste organet i fråga inte nödvändigtvis tillhöra rättsväsendet.[186] En fördjupad domstolskontroll i ett senare skede kan kompensera för eventuella brister i tillståndsförfarandet.[187]

306. I förevarande fall framgår det av beslutet om skölden för skydd av privatlivet att de enda garantier som begränsar insamlingen och användningen av uppgifter utanför Förenta staternas territorium återfinns i PPD 28, eftersom avsnitt 702 i FISA inte är tillämpligt utanför Förenta staterna. Jag är inte övertygad om att dessa garantier är tillräckliga för att uppfylla villkoren avseende ”förutsebarhet” och ”nödvändighet i ett demokratiskt samhälle”.

307. För det första föreskrivs i detta presidentdirektiv, som jag redan har påpekat, inga rättigheter för enskilda. Vidare tvivlar jag på att kravet att övervakningen ska vara ”så anpassad som möjligt” är tillräckligt tydligt och precist formulerat för att tillräckligt skydda de berörda personerna mot riskerna för missbruk.[188]. Slutligen fastställs inte i beslutet om skölden för skydd av privatlivet att den övervakning som grundas på EO 12333 är föremål för en förhandskontroll som utförs av ett oberoende organ eller kan vara föremål för efterhandskontroll vid domstol.[189]

308. Under dessa omständigheter frågar jag mig om det finns fog för konstaterandet att Förenta staterna inom ramen för underrättelsetjänsternas verksamhet enligt avsnitt 702 i FISA och EO 12333 säkerställer en adekvat skyddsnivå i den mening som avses i artikel 45.1 i dataskyddsförordningen jämförd med artiklarna 7 och 8 i stadgan och artikel 8 Europakonventionen.

c) Huruvida beslutet om skölden för skydd av privatlivet är giltigt mot bakgrund av rätten till ett effektivt rättsmedel

309. Genom den femte giltighetsfrågan har EU-domstolen anmodats att klargöra huruvida de personer vilkas uppgifter överförs till Förenta staterna där har tillgång till ett domstolsskydd som är väsentligen likvärdigt det som ska säkerställas i unionen enligt artikel 47 i stadgan. Genom den tionde frågan vill den hänskjutande domstolen få klarhet i huruvida den femte frågan ska besvaras jakande med beaktande av den ombudsmannamekanism som har införts genom beslutet om skölden för skydd av privatlivet.

310. Det ska genast konstateras att kommissionen i skäl 115 i detta beslut erkände att det amerikanska rättssystemet innehåller brister vad gäller domstolsskyddet för enskilda.

311. Av ordalydelsen i detta skäl framgår det att ”åtminstone några av de rättsliga grunder som Förenta staternas underrättelsemyndigheter kan tillämpa (t.ex. EO 12333) inte omfattas” av möjligheterna till rättslig prövning. EO 12333 och PPD 28 föreskriver nämligen inga rättigheter för de berörda personerna och kan inte åberopas av dessa vid domstol. Ett effektivt domstolsskydd förutsätter emellertid att enskilda åtminstone har rättigheter som kan åberopas vid domstol.

185 Se, bland annat, Europadomstolen, 6 september 1978, Klass m.fl. mot Tyskland (CE:ECHR:1978:0906JUD000502971, § 55), domen Zakharov (§ 233) och domen Centrum för Rättvisa (§ 105).

186 Se, bland annat, domen Klass (§ 56), Europadomstolen, 18 maj 2010, Kennedy mot Förenade kungariket (CE:ECHR:2010:0518JUD002683905, § 167) och domen Zakharov (§ 233 och 258).

187 Se domen Szabó och Vissy (§ 77) och domen Centrum för Rättvisa (§ 133).

188 Detta gäller desto mer med beaktande av konstaterandena i punkt 281 ovan.

189 Se punkterna 330 och 331 nedan.

312. Vidare framgår det att ”[ä]ven om det i princip finns möjligheter för utländska medborgare att söka rättslig prövning, t.ex. rörande övervakning enligt FISA, är tillgängliga grunder för talan dock begränsade, och talan som väcks … kommer att förklaras oacceptabel när den saknar grund, vilket begränsar möjligheterna att väcka talan vid allmänna domstolar”.

313. Av skälen 116–124 i beslutet om skölden för skydd av privatlivet framgår att inrättandet av ombudsmannamekanismen syftar till att kompensera för dessa begränsningar. I skäl 139 i detta beslut konstaterade kommissionen att ”de *tillsynsmekanismer* och de *mekanismer för handläggning* av klagomål som tillhandahålls genom skölden för skydd av privatlivet … erbjuder de registrerade rättsmedel för att få tillgång till personuppgifter som rör dem och få uppgifterna rättade eller raderade” (min kursivering).

314. Mot bakgrund av de allmänna principer som följer av EU-domstolens och Europadomstolens praxis avseende rätten till rättslig prövning av åtgärder för övervakning av kommunikationer kommer jag nu att undersöka huruvida den rättsliga prövning som föreskrivs i amerikansk rätt, såsom den beskrivs i beslutet om skölden för skydd av privatlivet, gör det möjligt att säkerställa ett adekvat domstolsskydd för de registrerade (avsnitt 1). Därefter kommer jag att undersöka huruvida inrättandet av den utomrättsliga ombudsmannamekanismen vid behov kan fylla eventuella brister i domstolsskyddet för dessa personer (avsnitt 2).

1) Huruvida den rättsliga prövning som föreskrivs i Förenta staternas lagstiftning är effektiv

315. I artikel 47 första stycket i stadgan stadfästs rätten till ett effektivt rättsmedel inför en domstol för var och en vars unionsrättsligt garanterade fri- och rättigheter har kränkts.[190] Enligt andra stycket i denna artikel har var och en rätt att få sin sak prövad inför en oavhängig och opartisk domstol.[191] Tillgången till en oavhängig domstol är en del av det väsentliga innehållet i den rättighet som garanteras i artikel 47 i stadgan.[192]

316. Till denna rätt till domstolsskydd för den enskilde kommer den skyldighet som åligger medlemsstaterna enligt artiklarna 7 och 8 i stadgan att, utom i vederbörligen motiverade brådskande fall, underkasta varje övervakningsåtgärd en förhandskontroll av en domstol eller oberoende myndighet.[193]

190 I förklaringarna avseende stadgan anges i detta hänseende att ”[e]nligt unionsrätten är skyddet [som föreskrivs i artikel 47 i stadgan] ännu mer omfattande [än det som erhålls genom artikel 13 i Europakonventionen], eftersom var och en har rätt att inför en behörig domstol använda sig av ett effektivt rättsmedel”. Se även förslag till avgörande av generaladvokaten Wathelet i målet Berlioz Investment Fund (C-682/15, EU:C:2017:2, punkt 37).

191 Vid bedömningen av huruvida ett organ utgör en domstol i den mening som avses i artikel 47 i stadgan ska ett antal omständigheter beaktas, såsom huruvida organet är upprättat enligt lag, organet är av stadigvarande karaktär, dess jurisdiktion är av tvingande art, förfarandet är kontradiktoriskt, organet tillämpar rättsregler och huruvida det har en oberoende ställning. Se dom av den 27 februari 2018, Associação Sindical dos Juízes Portugueses (C-64/16, EU:C:2018:117, punkt 38 och där angiven rättspraxis).

192 Se, bland annat, dom av den 25 juli 2018, Minister for Justice and Equality (Brister i domstolssystemet) (C-216/18 PPU, EU:C:2018:586, punkterna 59 och 63), dom av den 5 november 2019, kommissionen/Polen (Allmänna domstolars oavhängighet) (C-192/18, EU:C:2019:924, punkt 106), och dom av den 19 november 2019, A. K. m.fl. (Oberoendet för avdelningen för disciplinära mål vid högsta domstolen) (C-585/18, C-624/18 och C-625/18, EU:C:2019:982, punkt 120).

193 Se punkt 293 ovan. I artikel 45.3 a i dataskyddsförordningen föreskrivs att kommissionen vid bedömningen av om skyddsnivån i ett tredjeland är adekvat ska beakta de faktiska möjligheterna till effektiv ”administrativ och *rättslig* prövning” för de registrerade vars personuppgifter överförs (min kursivering). På samma sätt anges i skäl 104 i dataskyddsförordningen att som ett villkor för antagandet av ett beslut om adekvat skyddsnivå bör det krävas att de registrerade tillförsäkras ”effektiv administrativ och *rättslig* prövning” i tredjelandet i fråga (min kursivering). Se även Artikel 29-arbetsgruppen, *EU-U.S. Privacy Shield – First Annual Joint Review*, 28 november 2017, WP 255 (punkt B.3), parlamentets resolution av den 5 juli 2018 om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och USA, P8_TA(2018)0315 (punkterna 25 och 30), och EDPB, *EU-U.S. Privacy Shield – Second Annual Joint Review*, 22 januari 2019 (punkterna 94–97).

317. Som den tyska och den franska regeringen har gjort gällande är rätten att få sin sak prövad inför domstol visserligen inte absolut,[194] eftersom denna rättighet kan begränsas av skäl som avser den nationella säkerheten. Undantag tillåts emellertid endast i den mån de inte kränker det väsentliga innehållet i denna rättighet och är strängt nödvändiga för att uppnå ett legitimt mål.

318. I domen Schrems slog domstolen i detta hänseende fast att 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 rättighet som är stadfäst i artikel 47 i stadgan.[195]

319. Det ska betonas att rätten till tillgång innebär att en person har möjlighet att, med förbehåll för undantag som är strängt nödvändiga för att uppnå ett legitimt intresse, erhålla *bekräftelse* från de offentliga myndigheterna *på huruvida de behandlar personuppgifter rörande honom eller henne*.[196] Detta är enligt min mening den praktiska innebörden av rätten till tillgång när den registrerade inte vet om de offentliga myndigheterna har lagrat personuppgifter rörande honom eller henne, bland annat efter en process för automatiserad filtrering av elektroniska kommunikationsflöden.

320. Av rättspraxis framgår dessutom att myndigheterna i en medlemsstat i princip är skyldiga att informera om att de beviljats tillgång till uppgifterna *så snart en sådan upplysning inte längre riskerar att skada myndigheternas utredningar*.[197] En sådan upplysning är nämligen en förutsättning för utövandet av rätten till rättslig prövning i enlighet med artikel 47 i stadgan.[198] Denna skyldighet fastställs numera i artikel 23.2 h i dataskyddsförordningen.

321. I skälen 111–135 i beslutet om skölden för skydd av privatlivet beskrivs kortfattat alla de rättsmedel som finns att tillgå för personer vilkas uppgifter har överförts, om de befarar att uppgifterna har behandlats av de amerikanska underrättelsetjänsterna efter överföringen. Dessa rättsmedel har också beskrivits i domen från High Court (Förvaltningsöverdomstolen) av den 3 oktober 2017 och i synpunkterna från bland annat Förenta staternas regering.

322. Det är inte nödvändigt att i detalj återge innehållet i dessa beskrivningar. Den hänskjutande domstolen har nämligen ifrågasatt om det föreligger tillräckliga garantier avseende de registrerades rättsliga skydd främst av det skälet att de synnerligen stränga kraven i fråga om talerätt (*standing*),[199] i kombination med en avsaknad av varje skyldighet att upplysa personer om att de har varit föremål för en övervakningsåtgärd *till och med om upplysningen inte längre riskerar syftena*, i praktiken gör det alltför svårt att utöva de rättsmedel som föreskrivs i Förenta staternas lagstiftning. Dessa tvivel delas av DPC, Maximillian Schrems, den österrikiska, den polska och den portugisiska regeringen och EDPB.[200]

194 Se, för ett liknande resonemang, dom av den 28 februari 2013, Omprövning av domen Arango Jaramillo m.fl./EIB (C-334/12 RX-II, EU:C:2013:134, punkt 43).

195 Domen Schrems (punkt 95).

196 I artikel 15.1 i dataskyddsförordningen, under rubriken ”Den registrerades rätt till tillgång”, föreskrivs att den registrerade ”ska ha rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna”. Den ”princip om tillgång” som föreskrivs i punkt II.8 a i bilaga II till beslutet om skölden för skydd av privatlivet har samma innebörd.

197 Domen Tele2 Sverige (punkt 121) och yttrande 1/15 (punkt 220). Som Facebook Ireland har påpekat kan upplysning om att de offentliga myndigheterna fått tillgång till uppgifterna således inte krävas systematiskt. Europadomstolen har i detta sammanhang ansett att ”[d]et är kanske inte praktiskt möjligt att kräva en upplysning i efterhand”, eftersom det hot som är föremål för övervakningsåtgärder ”kan bestå i åratal och till och med decennier” efter det att åtgärderna har upphört, vilket innebär att upplysningen kan ”skada det långsiktiga syfte som ursprungligen motiverade övervakningen” och ”avslöja underrättelsetjänsternas arbetsmetoder, deras verksamhetsområden och… deras agenters identitet” (domen Zakharov, § 287 och där angiven rättspraxis). I avsaknad av en upplysning kan – även om de rättsmedel som är tillgängliga för enskilda då inte kan användas för det fallet att de rättsliga kraven har åsidosatts – andra garantier räcka för att skydda rätten till respekt för privatlivet (se även domen Centrum för Rättvisa, § 164–167 och 171–178). Se punkt 330 nedan.

198 Se fotnot 210 nedan.

199 Se punkt 67 ovan.

200 Se EDPB, *EU-U.S. Privacy Shield – Second Annual Joint Review*, 22 januari 2019 (s. 18, punkt 97).

323. Det ska härvid endast erinras om att reglerna om talerätt inte får kränka rätten till ett effektivt domstolsskydd [201] och konstateras att det i beslutet om skölden för skydd av privatlivet inte nämns något krav på att informera de registrerade om den omständigheten att de har varit föremål för en övervakningsåtgärd. [202] Avsaknaden av en skyldighet att upplysa om en sådan åtgärd, till och med när en upplysning till den berörda personen inte längre skulle skada åtgärdens effektivitet, är problematisk mot bakgrund av den rättspraxis som anges i punkt 320 ovan, eftersom en sådan avsaknad kan hindra utövandet av rättsmedel.

324. I fotnot 169 i beslutet om skölden för skydd av privatlivet erkänns dessutom att de tillgängliga förfarandena ”kräver … antingen att det föreligger skada … eller att det måste bevisas att regeringen har för avsikt att använda eller lämna ut information som erhållits eller härrör från elektronisk övervakning av den berörda personen mot den personen”. Som den hänskjutande domstolen, DPC och Maximillian Schrems har betonat kontrasterar detta krav mot domstolens praxis, enligt vilken det för att fastställa att det föreligger ett ingrepp i rätten till respekt för privatlivet inte är nödvändigt att den berörde har fått utstå eventuella olägenheter på grund av det påstådda ingreppet. [203]

325. Jag finner vidare inte den åsikt övertygande som Facebook Ireland och Förenta staternas regering har anfört, att de brister som kännetecknar domstolsskyddet för personer vilkas uppgifter överförs till Förenta staterna kompenseras genom de förhands- och efterhandskontroller som utförs av FISC samt genom de många tillsynsmekanismer som har inrättats inom den verkställande och lagstiftande makten. [204]

326. FISC kontrollerar inte de enskilda övervakningsåtgärderna innan de genomförs, såsom jag redan har påpekat och som det anges i beslutet om skölden för skydd av privatlivet. [205] Vidare är, som det anges i skäl 109 i detta beslut och som Förenta staternas regering har bekräftat i sitt skriftliga svar på de frågor som ställts av domstolen, syftet med efterhandskontrollen av tillämpningen av urvalstermerna att, om en incident som innebär ett möjligt åsidosättande av förfarandena för målinriktning och minimering anmäls till FISC av en underrättelsetjänst, [206] kontrollera att de villkor för valet av urvalstermer som föreskrivs i den årliga certifieringen har iakttagits. Förfarandet vid FISC tycks således inte omfatta något effektivt rättsmedel för enskilda vilkas uppgifter överförs till Förenta staterna.

327. Även om de utomrättsliga tillsynsmekanismer som nämns i skälen 95–110 i beslutet om skölden för skydd av privatlivet vid behov kan förstärka eventuella rättsmedel vid domstol, är de enligt min mening inte tillräckliga för att säkerställa en adekvat skyddsnivå vad gäller de berörda personernas rätt till rättslig prövning. Särskilt kan de allmänna inspektörer som ingår i respektive underrättelsetjänsts interna organisation inte anses utgöra oberoende tillsynsmekanismer. Den tillsyn som utövas av PCLOB och kongressens underrättelseutskott motsvarar inte heller en mekanism som ger enskilda möjlighet till rättslig prövning av övervakningsåtgärder.

201 Se, bland annat, dom av den 11 juli 1991, Verholen m.fl. (C-87/90–C-89/90, EU:C:1991:314, punkt 24 och där angiven rättspraxis), och dom av den 28 februari 2013, Réexamen Arango Jaramillo m.fl./EIB (C-334/12 RX-II, EU:C:2013:134, punkt 43).

202 Förenta staternas regering har emellertid, liksom den hänskjutande domstolen, preciserat att den person som en övervakningsåtgärd i enlighet med avsnitt 702 i FISA inriktas på ska informeras om åtgärden, om de insamlade uppgifterna används mot vederbörande inom ramen för ett domstolsförfarande.

203 Dom av den 20 maj 2003, Österreichischer Rundfunk m.fl. (C-465/00, C-138/01 och C-139/01, EU:C:2003:294, punkt 75), domen Digital Rights Ireland (punkt 33), domen Schrems (punkt 87) och yttrande 1/15 (punkt 124).

204 Dessa mekanismer beskrivs i skälen 95–110 i beslutet om skölden för skydd av privatlivet, där kommissionen, i kategorin regler som rör ett ”effektivt rättsligt skydd”, skiljer mellan tillsynsmekanismer (se skälen 92–110) och rättslig prövning för enskilda (se skälen 111–124).

205 Se punkt 298 ovan.

206 I skäl 109 i beslutet om skölden för skydd av privatlivet anges att ”[j]ustitieministern och chefen för [NSA] kontrollerar efterlevnaden, och underrättelsetjänsterna är skyldiga att rapportera eventuella fall av bristande efterlevnad till FISC…”.

328. Det ska därför undersökas om inrättandet av ombudsmannamekanismen kan kompensera för bristerna genom att de berörda personerna tillhandahålls ett effektivt rättsmedel vid ett oberoende och opartiskt organ. [207]

329. När det vidare gäller att bedöma huruvida det finns fog för konstaterandet i beslutet om skölden för skydd av privatlivet, att skyddsnivån är adekvat mot bakgrund av de rättsmedel som är tillgängliga för personer som tror att de har varit föremål för övervakning grundad på EO 12333, ska det erinras om att den relevanta referensramen utgörs av bestämmelserna i Europakonventionen.

330. Som jag har angett ovan [208] vidtar Europadomstolen vid bedömningen av huruvida en övervakningsåtgärd uppfyller kraven på ”förutsebarhet” och ”nödvändighet i ett demokratiskt samhälle” i den mening som avses i artikel 8.2 i Europakonventionen [209] en prövning av alla de kontroll- och tillsynsmekanismer som genomförs ”före, under och efter” åtgärdens genomförande. När den enskildes tillgång till rättslig prövning hindras av den omständigheten att det inte är möjligt att upplysa vederbörande om övervakningsåtgärden utan att åtgärdens effektivitet riskeras, [210] kan denna brist uppvägas genom att en oberoende kontroll genomförs innan åtgärden i fråga tillämpas. [211] Europadomstolen har således, även om den anser att en sådan upplysning är ”önskvärd” när den kan lämnas utan att övervakningsåtgärdens effektivitet påverkas, inte uppställt detta som ett krav. [212]

331. Av beslutet om skölden för skydd av privatlivet framgår inte att de registrerade informeras om de övervakningsåtgärder som grundas på EO 12333 eller att dessa åtgärder regleras genom oberoende rättsliga eller administrativa kontrollmekanismer i något skede av antagandet eller genomförandet.

332. Under dessa omständigheter ska det undersökas om ombudsmannamekanismen emellertid kan säkerställa en oberoende kontroll av övervakningsåtgärderna, inbegripet när de grundar sig på EO 12333.

2) Ombudsmannamekanismens inverkan på skyddsnivån för rätten till ett effektivt rättsmedel

333. Enligt skäl 116 i beslutet om skölden för skydd av privatlivet syftar den ombudsmannamekanism som beskrivs i bilaga III A till detta beslut till att ge alla personer vilkas uppgifter överförs från unionen till Förenta staterna ytterligare möjlighet att söka rättslig prövning.

334. För upptagande till prövning av ett klagomål som inges till ombudsmannen gäller inte, som Förenta staternas regering har betonat, några regler av det slag som gäller för talerätt och som reglerar tillgången till amerikansk domstol. I skäl 119 i beslutet preciseras att för att vända sig till ombudsmannen behöver den enskilde inte visa att Förenta staternas regering har haft åtkomst till dennes personuppgifter.

207 Se punkterna 333–340 nedan.

208 Se punkt 305 ovan.

209 I sin praxis avseende åtgärder för övervakning av telekommunikationer har Europadomstolen behandlat frågan om rättsmedel i samband med prövningen av huruvida ett ingrepp i utövandet av den rätt som garanteras i artikel 8 i Europakonventionen hade ”egenskapen av lag” och var nödvändigt (se, bland annat, domen Zakharov, § 236, och domen Centrum för Rättvisa, § 107). I domen av den 1 juli 2008, Liberty m.fl. mot Förenade kungariket (CE:ECHR:2008:0701JUD005824300, § 73), och domen Zakharov, § 307, bedömde Europadomstolen, efter att ha konstaterat att artikel 8 i Europakonventionen hade åsidosatts, att det inte var nödvändigt att separat pröva en invändning som grundade sig på artikel 13 i denna konvention.

210 Europadomstolen har slagit fast att även om avsaknaden av upplysning i ett visst skede inte nödvändigtvis hindrar att en övervakningsåtgärd uppfyller villkoret ”nödvändighet i ett demokratiskt samhälle”, hindrar det tillgången till domstol och följaktligen till ett effektivt rättsmedel (se, bland annat, dom av den 6 september 1978, Klass m.fl. mot Tyskland, CE:ECHR:1978:0906JUD000502971, § 57 och 58, beslut Weber och Saravia, § 135, och domen Zakharov, § 302).

211 Se, för ett liknande resonemang, domen Centrum för Rättvisa (§ 105).

212 I domen Big Brother Watch (§ 317) har Europadomstolen vägrat att bland de minimigarantier som är tillämpliga på en övervakningsordning som kännetecknas av massavlyssning av elektroniska kommunikationer infoga ett krav på att de berörda personerna ska upplysas om övervakningen. Se även domen Centrum för Rättvisa (§ 164). Dessa domar har hänskjutits till Europadomstolens stora avdelning i syfte att bland annat erhålla en omprövning av detta konstaterande.

335. I likhet med DPC, Maximillian Schrems den polska och den portugisiska regeringen och EPIC betvivlar jag att denna mekanism kan kompensera för det otillräckliga rättsliga skydd som erbjuds de personer vilkas uppgifter överförs från unionen till Förenta staterna.

336. För det första ska det påpekas att även om en mekanism för utomrättslig prövning kan utgöra ett effektivt rättsmedel i den mening som avses i artikel 47 FEUF, är detta framför allt endast fallet om organet i fråga har inrättats genom lag och uppfyller kravet på oberoende. [213]

337. Av beslutet om skölden för skydd av privatlivet framgår emellertid att ombudsmannamekanismen, som har sitt upphov i PPD 28, [214] inte har inrättats genom lag. Ombudsmannen utses av utrikesministern och är en del av Förenta staternas utrikesdepartement. [215] Detta beslut innehåller inga uppgifter om att ett återkallande av ombudsmannen eller ett upphävande av dennes utnämning är förenat med särskilda garantier. [216] Även om ombudsmannen presenteras som oberoende gentemot ”underrättelsegemenskapen”, rapporterar han till utrikesministern och är därför inte oberoende av den verkställande makten. [217]

338. Effektiviteten hos ett medel för utomrättslig prövning är vidare också beroende av det ifrågavarande organets kapacitet att anta bindande och motiverade beslut. I beslutet om skölden för skydd av privatlivet finns inga uppgifter om att ombudsmannen fattar sådana beslut. I beslutet fastställs inte att ombudsmannamekanismen ger dem som ansöker därom möjlighet att få tillgång till de uppgifter som rör dem och att erhålla rättelse eller radering av uppgifterna och inte heller att ombudsmannen beviljar ersättning till personer som lidit skada till följd av en övervakningsåtgärd. Särskilt ska påpekas att det av bilaga III A.4 e till detta beslut framgår att ”[o]mbudsmannen kommer varken att bekräfta eller förneka om den enskilda personen har varit föremål för övervakning eller ange vilka specifika avhjälpande åtgärder som har vidtagits”. [218] Även om den amerikanska regeringen har åtagit sig att se till att den berörda enheten vid underrättelsetjänsterna ska vara skyldig att korrigera varje åsidosättande av de tillämpliga normerna som ombudsmannen upptäcker, [219] beskrivs i nämnda beslut inte några rättsliga garantier som åtföljer detta åtagande och som de registrerade kan göra gällande.

213 Begreppet oberoende har för det första en extern aspekt, som förutsätter att den berörda instansen är skyddad mot yttre inblandning eller påtryckningar som kan äventyra dess ledamöters oberoende prövning av de tvister de har att avgöra. För det andra har detta begrepp en intern aspekt som sammanfaller med begreppet ”opartiskhet” och som handlar om att avståndet gentemot parterna och deras respektive intressen vad gäller saken i målet ska vara detsamma. Se, bland annat, dom av den 19 september 2006, Wilson (C-506/04, EU:C:2006:587, punkterna 50–52), dom av den 25 juli 2018, Minister for Justice and Equality (Brister i domstolssystemet) (C-216/18 PPU, EU:C:2018:586, punkterna 63 och 65), och dom av den 19 november 2019, A. K. m.fl. (Oberoendet för avdelningen för disciplinära mål vid högsta domstolen) (C-585/18, C-624/18 och C-625/18, EU:C:2019:982, punkterna 121 och 122). I enlighet med principen om maktdelning ska domstolarnas oberoende garanteras bland annat gentemot den verkställande makten. Se dom av den 19 november 2019, A. K. m.fl. (Oberoendet för avdelningen för disciplinära mål vid högsta domstolen) (C-585/18, C-624/18 och C-625/18, EU:C:2019:982, punkt 127 och där angiven rättspraxis).

214 I bilaga III A till beslutet om skölden för skydd av privatlivet hänvisas i detta sammanhang till avsnitt 4 d i PPD 28.

215 Se skäl 116 i beslutet om skölden för skydd av privatlivet.

216 I domen av den 31 maj 2005, Syfait m.fl. (C-53/03, EU:C:2005:333, punkt 31), betonade domstolen betydelsen av sådana garantier för att uppfylla villkoret avseende oavhängighet. Se även dom av den 24 juni 2019, kommissionen/Polen (Högsta domstolens oavhängighet) (C-619/18, EU:C:2019:531, punkt 76), och dom av den 5 november 2019, kommissionen/Polen (Allmänna domstolars oavhängighet) (C-192/18, EU:C:2019:924, punkt 113).

217 Se skälen 65 och 121 samt bilaga III A.1 till beslutet om skölden för skydd av privatlivet.

218 I skäl 121 i beslutet om skölden för skydd av privatlivet anges dessutom att ”ombudsmannen kommer att behöva ’bekräfta’ att i) klagomålet har blivit ordentligt utrett och att ii) Förenta staternas relevanta lagstiftning – inklusive i synnerhet de begränsningar och garantier som anges i bilaga VI – har följts eller, vid bristande efterlevnad, sådana brister har åtgärdats”.

219 Vid den tredje årliga översynen av skölden för skydd av uppgifter konstaterade kommissionen att enligt förklaringarna från Förenta staternas regering ska FISC, för det fallet att ombudsmannens utredning visar att de förfaranden för målinriktning och minimering som har godkänts av FISC har åsidosatts, uppmärksammas på detta åsidosättande. FISC ska då utföra en oberoende utredning och ska om nödvändigt förelägga den berörda underrättelsetjänsten att avhjälpa åsidosättandet. Se *Commission staff working document accompanying the report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU-U.S. Privacy Shield*, 23 oktober 2019, SWD(2019) 390 final, s. 28. Kommissionen hänvisar där till dokumentet *Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure*, som finns på adressen https://www.state.gov/wp-content/uploads/2018/12/Ombudsperson-Mechanism-Implementation-Procedures-UNCLASSIFIED.pdf (s. 4 och 5).

339. Enligt min mening erbjuder ombudsmannamekanismen således inte ett rättsmedel vid ett oberoende organ som ger de personer vilkas uppgifter överförs en möjlighet att göra gällande sin rätt till tillgång till uppgifterna eller invända mot eventuella åsidosättanden av tillämpliga regler från underrättelsetjänsternas sida.

340. För att den rättighet som garanteras i artikel 47 i stadgan ska anses iakttagen krävs enligt rättspraxis slutligen att ett beslut av en förvaltningsmyndighet som inte själv uppfyller kravet på oberoende ställning ska undergå en senare kontroll av en domstol som ska ha behörighet att pröva alla relevanta frågor.[220] Enligt uppgifterna i beslutet om skölden för skydd av privatlivet är ombudsmannens beslut dock inte föremål för en oberoende domstolskontroll.

341. Under dessa omständigheter kan det, som DPC, Maximillian Schrems, EPIC och den polska och den portugisiska regeringen har gjort gällande, ifrågasättas huruvida det domstolsskydd som enligt Förenta staternas rättsordning erbjuds personer vilkas uppgifter överförs dit från unionen är väsentligen likvärdigt det som följer av dataskyddsförordningen jämförd med artikel 47 i stadgan och artikel 8 Europakonventionen.

342. Mot bakgrund av det ovan anförda hyser jag vissa tvivel om huruvida beslutet om skölden för skydd av privatlivet är förenligt med artikel 45.1 i dataskyddsförordningen jämförd med artiklarna 7, 8 och 47 i stadgan och artikel 8 i Europakonventionen.

V. Förslag till avgörande

343. Jag föreslår att domstolen svarar på de giltighetsfrågor som har ställts av High Court (Förvaltningsöverdomstolen, Irland) på följande sätt:

Vid bedömningen av giltighetsfrågorna har det inte framkommit några uppgifter som kan påverka giltigheten av kommissionens beslut 2010/87/EU 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, i dess lydelse enligt kommissionens genomförandebeslut (EU) 2016/2297 av den 16 december 2016.

220 Se dom av den 16 maj 2017, Berlioz Investment Fund (C-682/15, EU:C:2017:373, punkt 55), och dom av den 13 december 2017, El Hassani (C-403/16, EU:C:2017:960, punkt 39).