Rättsfallssamlingen

FÖRSLAG TILL AVGÖRANDE AV GENERALADVOKAT
YVES BOT
föredraget den 23 september 2015 [1]

**Mål C-362/14**

**Maximillian Schrems**
**mot**
**Data Protection Commissioner**

(begäran om förhandsavgörande från High Court (Irland))

”Begäran om förhandsavgörande — Personuppgifter — Skydd för enskilda personer med avseende på behandling av personuppgifter — Europeiska unionens stadga om de grundläggande rättigheterna — Artiklarna 7, 8 och 47 — Direktiv 95/46/EG — Artikel 25 — Beslut 2000/520/EG — Överföring av personuppgifter till Förenta staterna — Bedömning av huruvida skyddsnivån är adekvat eller inte — Klagomål från en enskild person vars uppgifter har överförts till ett tredjeland — Nationell tillsynsmyndighet — Befogenheter”

## I – **Inledning**

1. Som Europeiska kommissionen konstaterade i sitt meddelande av den 27 november 2013 [2] är ”[ö]verföringen av personuppgifter … en viktig och nödvändig del av de transatlantiska förbindelserna. Den utgör en integrerad del av handelsutbytena över Atlanten, också för nya och växande digitala affärsverksamheter, såsom sociala medier eller molntjänster, där stora mängder data överförs från EU till Förenta staterna” [3].

2. Dessa handelsutbyten berörs av kommissionens beslut 2000/520/EG av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (*Safe Harbor Privacy Principles*) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat (nedan kallat *safe harbor*). [4] Detta beslut utgör en rättslig grund för överföring av personuppgifter från unionen till företag i Förenta staterna som har anslutit sig till *safe harbor*-principerna.

3. Nämnda beslut har i dag en besvärlig funktion att fylla; det ska tillåta uppgiftsflöden mellan unionen och Förenta staterna samtidigt som det i enlighet med unionsrättens krav ska garantera en hög skyddsnivå för dessa uppgifter.

1 — Originalspråk: franska.

2 — Meddelande från kommissionen till Europaparlamentet och rådet med rubriken ”Återskapande av förtroendet för dataflöden mellan EU och Förenta staterna” (COM(2013) 846 final).

3 — Sidan 2.

4 — EGT L 215, s. 7, och rättelse i EGT L 115, 2001, s. 14.

4. Ett antal avslöjanden på senare tid har visat att det finns amerikanska program för storskalig underrättelseinsamling. Dessa avslöjanden har gett upphov till tvivel angående huruvida de unionsrättsliga normerna efterlevs vid överföring av personuppgifter till företag i Förenta staterna och väckt oro över *safe harbor*-systemets svagheter.

5. Genom förevarande begäran om förhandsavgörande har domstolen uppmanats att slå fast hur de nationella tillsynsmyndigheterna och kommissionen ska förhålla sig när tillämpningen av beslut 2000/520 inte fungerar som den ska.

6. Bestämmelser om överföring av personuppgifter till tredjeländer finns i kapitel IV i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.[5]

7. I det kapitlet, närmare bestämt i artikel 25.1, slås det fast en princip med innebörden att överföring till ett tredjeland av personuppgifter som är under behandling, eller som är avsedda att behandlas efter överföringen till det landet, endast får ske om nämnda land säkerställer en adekvat skyddsnivå för sådana uppgifter.

8. Om så inte är fallet, det vill säga om ett tredjeland inte garanterar en adekvat skyddsnivå, ska överföring av personuppgifter till det landet förbjudas, något som unionslagstiftaren har angett i skäl 57 i nämnda direktiv.

9. I artikel 25.2 i direktiv 95/46 stadgas att ”[b]edömningen 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”.

10. Med stöd av artikel 25.6 i direktiv 95/46 kan kommissionen konstatera att ett tredjeland genom sin interna lagstiftning eller på grund av sina internationella förpliktelser garanterar en adekvat skyddsnivå för personuppgifter. Om kommissionen antar ett beslut där den gör ett sådant konstaterande, får personuppgifter överföras till det berörda tredjelandet.

11. Med stöd av denna bestämmelse har kommissionen antagit beslut 2000/520. Av artikel 1.1 i det beslutet följer att *safe harbor*-principerna om integritetsskydd, tillämpade i enlighet med den vägledning som ges i frågor och svar-texten,[6] anses garantera en adekvat skyddsnivå för personuppgifter som överförs från unionen till företag i Förenta staterna.

12. Beslut 2000/520 tillåter således överföring av personuppgifter från medlemsstaterna till företag belägna i Förenta staterna och som har förpliktat sig att följa *safe harbor*-principerna.

13. I bilaga I till beslut 2000/520 redovisas ett antal principer som företag frivilligt kan ansluta sig till. Dessa principer kompletteras av begränsningar och ett specifikt tillsynssystem. Antalet företag som hade anslutit sig till vad som skulle kunna ses som en ”uppförandekod” uppgick år 2013 till mer än 3 200.

14. *Safe harbor*-systemet bygger på en lösning som kombinerar självcertifiering och egenkontroll från privata företags sida med ingripanden från det allmännas sida.

5 — EGT L 281, s. 31. Direktivet i sin lydelse enligt Europaparlamentets och rådets förordning (EG) nr 1882/2003 av den 29 september 2003 (EUT L 284, s. 1) (nedan kallat direktiv 95/46)

6 — Nedan kallad FoS.

15. *Safe harbor*-principerna har utarbetats ”i samråd med näringslivet och allmänheten [för] att underlätta handel och affärsverksamhet mellan USA och EU. De är endast avsedda att tillämpas på de organisationer i USA som tar emot personuppgifter från EU och syftet är att dessa organisationer skall uppfylla villkoren för *safe harbor* samt den presumtion om ’adekvat skyddsnivå’ som därmed skapas” [7].

16. *Safe harbor*-principerna, som redovisas i bilaga I till beslut 2000/520, innebär bland annat följande:

— En meddelandeskyldighet som innebär att ”[e]n organisation måste meddela den enskilde anledningen till att den samlar in och använder uppgifter om honom eller henne, hur den enskilde kontaktar organisationen om han eller hon har frågor eller klagomål, vilken slags tredje man som får ta del av uppgifterna samt vilka valmöjligheter och tillvägagångssätt som organisationen ger den enskilde att begränsa uppgifternas användning och utlämnande. Detta meddelande … skall lämnas vid det tillfälle då den enskilde för första gången ombeds lämna personuppgifter till en viss organisation eller så snart därefter det är praktiskt möjligt, men i alla händelser innan organisationen använder sådana uppgifter för ett annat ändamål än det för vilket de ursprungligen insamlades eller behandlades av den organisation som överför uppgifterna eller lämnar ut dem till tredje part för första gången” [8].

— En skyldighet för organisationerna att ge den enskilde möjlighet att bestämma (*opt out*) huruvida hans eller hennes personuppgifter får lämnas ut till tredje part eller användas för ett ändamål som inte stämmer överens med det eller de syften som de ursprungligen insamlades för eller som den enskilde i efterhand har gett sitt tillstånd till. När det gäller känsliga uppgifter ”skall den enskilde ges möjlighet att genom att bekräfta eller göra ett uttryckligt val (opt in) ange om uppgifterna får lämnas ut till en tredje part eller användas för ett annat ändamål än det för vilket de ursprungligen samlades in eller den enskilde i efterhand har gett sitt tillstånd till genom att välja (opt out)” [9].

— Regler för vidare överföring av uppgifter med innebörden att en organisation för att få lämna ut uppgifter till tredje part måste tillämpa principerna om meddelande och valmöjlighet. [10]

— En skyldighet avseende uppgiftssäkerhet som innebär att ”[o]rganisationer som skapar, lagrar, använder eller sprider personuppgifter skall vidta rimliga försiktighetsåtgärder för att se till att de inte går förlorade, missbrukas eller utan tillstånd tas fram, utlämnas, förvanskas eller förstörs” [11].

— En skyldighet avseende dataintegritet som innebär att organisationerna, i den omfattning som krävs för de ändamål för vilka uppgifterna har samlats in, ska ”vidta nödvändiga åtgärder för att se till att uppgifterna är tillförlitliga för det avsedda ändamålet samt riktiga, fullständiga och aktuella”. [12]

— En rättighet för enskilda vilkas personuppgifter innehas av en organisation att med vissa förbehåll ”ha tillgång till de[ssa] personuppgifter … och … ha möjlighet att rätta, ändra eller utplåna dessa uppgifter då de är felaktiga”. [13]

— En skyldighet att inrätta ”mekanismer för att se till att [*safe harbor*-]principerna följs, att de enskilda som uppgifterna rör och som drabbats av att principerna inte följts kan vidta rättsliga åtgärder samt att det blir påföljder för den organisation som inte följer principerna”. [14]

7 — Andra stycket i bilaga I till beslut 2000/520.

8 — Se bilaga I under rubriken ”Meddelande”.

9 — Se bilaga I under rubriken ”Valmöjlighet”.

10 — Se bilaga I under rubriken ”Vidare överföring”.

11 — Se bilaga I under rubriken ”Säkerhet”.

12 — Se bilaga I under rubriken ”Dataintegritet”.

13 — Se bilaga I under rubriken ”Tillgång”.

14 — Se bilaga I under rubriken ”Genomförande och uppföljning”.

17. En amerikansk organisation som önskar ansluta sig till *safe harbor*-principerna ska dels ange i sin policy för skydd av privatlivet att den ska offentliggöra sin anslutning till dessa principer och i praktiken följa dessa, dels självcertifiera sig genom att underrätta Förenta staternas handelsministerium om att den efterlever nämnda principer. [15]

18. Det finns flera sätt för organisationer att efterleva *safe harbor*-principerna. De kan exempelvis ”anslut[a] sig till ett integritetsskyddsprogram som utarbetats inom den privata sektorn och som följer principerna” eller ansluta sig till *safe harbor* genom att ”utarbeta en egen policy för integritetsskydd under förutsättning att denna överensstämmer med principerna. … Dessutom kan organisationer som är underställda i USA gällande lagar, förordningar, förvaltningslagar eller andra lagsamlingar (eller bestämmelser) som effektivt skyddar den personliga integriteten med avseende på personuppgifter … åtnjuta de förmåner som *safe harbor* för med sig” [16].

19. För kontroll av att *safe harbor*-principerna efterlevs finns det flera olika ordningar, som kombinerar privata klagomålsförfaranden med offentlig tillsyn. Kontrollen kan exempelvis ombesörjas genom ett system för tvistlösning utanför domstol med en oberoende tredje part som skiljeman. Dessutom kan företag förbinda sig att samarbeta med EU:s arbetsgrupp för skydd av enskilda med avseende på behandlingen av personuppgifter. Behörighet att pröva klagomål har den federala konkurrensmyndigheten (Federal Trade Commission) (nedan kallad FTC) med stöd av sina befogenheter enligt section 5 i lagen om den federala konkurrensmyndigheten (Federal Trade Commission Act) och transportministeriet (Department of Transportation) med stöd av sina befogenheter enligt section 41712 (i kapitel 49) i Förenta staternas lagsamling (United States Code).

20. Av fjärde stycket i bilaga I till beslut 2000/520 följer att efterlevnaden av *safe harbor*-principerna kan begränsas bland annat ”till vad som är nödvändigt för att uppfylla krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden” och ”av lagar, myndighetsföreskrifter eller rättspraxis som skapar motstridiga skyldigheter eller ger explicita befogenheter, förutsatt att organisationen då den utövar dessa befogenheter kan visa att avvikelsen från principerna begränsar sig till vad som är nödvändigt för att de övergripande legitima intressen som är beroende av dessa befogenheter skall kunna tillgodoses”. [17]

21. Medlemsstaternas behöriga myndigheter får tillfälligt förbjuda överföring av uppgifter, om ett antal villkor är uppfyllda. Dessa villkor anges i artikel 3.1 i beslut 2000/520.

22. Förevarande begäran om förhandsavgörande ger upphov till frågor angående tillämpningen av beslut 2000/520 mot bakgrund av artiklarna 7, 8 och 47 i Europeiska unionens stadga om de grundläggande rättigheterna (nedan kallad stadgan) och artiklarna 25.6 och 28 i direktiv 95/46. Begäran har framställts inom ramen för en tvist mellan Maximillian Schrems och Data Protection Commissioner (dataskyddsombudsmannen) (nedan kallad ombudsmannen) rörande ombudsmannens beslut att inte utreda ett klagomål från Maximillian Schrems sida avseende den omständigheten att Facebook Ireland Ltd (nedan kallat Facebook Ireland) lagrar personuppgifter om sina användare på servrar i Förenta staterna.

23. Maximillian Schrems är österrikisk medborgare med hemvist i Österrike. Han har sedan 2008 varit användare av det sociala nätverket Facebook.

15 — Artikel 1.2 och 1.3 i beslut 2000/520. Se även FoS 6 i bilaga II.

16 — Tredje stycket i bilaga I.

17 — Se även avsnitt B i bilaga IV.

24. Alla Facebook-användare med hemvist inom unionen måste ingå ett avtal med Facebook Ireland, ett dotterbolag till moderbolaget Facebook Inc. med säte i Förenta staterna (nedan kallat Facebook USA). Uppgifterna om användare knutna till Facebook Ireland med hemvist inom unionen överförs helt eller delvis till servrar tillhörande Facebook USA som är belägna i Förenta staterna och lagras på dessa.

25. Maximillian Schrems lämnade den 25 juni 2013 in ett klagomål till ombudsmannen där han gjorde gällande att Förenta staternas rätt och praxis inte garanterar något reellt skydd mot statlig övervakning för uppgifter som lagras i Förenta staterna. Att så är fallet framgick enligt Maximillian Schrems av Edward Snowdens avslöjanden i maj 2013 om den verksamhet som bedrivs av amerikanska underrättelseorgan, särskilt National Security Agency (nedan kallat NSA).

26. Enligt dessa avslöjanden ska NSA bland annat ha inrättat ett program kallat Prism och inom ramen för detta ha fått fri åtkomst till stora datamängder på servrar i Förenta staterna som tillhör eller kontrolleras av ett antal internet- och teknikbolag, inbegripet Facebook USA.

27. Ombudsmannen bedömde att han saknade skyldighet att utreda klagomålet, eftersom detta saknade rättslig grund. Därvid fann han att det inte fanns några bevis för att NSA hade tagit del av Maximillian Schrems uppgifter. Dessutom skulle klagomålet enligt hans uppfattning avslås med hänvisning till beslut 2000/520, i vilket kommissionen konstaterade att Förenta staterna, inom ramen för *safe harbor*-systemet, garanterar en adekvat skyddsnivå för överförda personuppgifter. Alla ärenden som rör huruvida skyddet av sådana uppgifter i Förenta staterna är adekvat ska enligt ombudsmannen behandlas i överensstämmelse med det beslutet, vilket gjorde att han ansåg sig förhindrad att utreda det problem som togs upp i klagomålet.

28. Den nationella lagstiftning som föranledde ombudsmannen att avslå klagomålet är följande.

29. Enligt section 10.1 i 1988 års dataskyddslag (Data Protection Act 1988) i dess lydelse enligt 2003 års dataskyddslag (Data Protection (Amendment) Act 2003) (nedan kallad dataskyddslagen) har ombudsmannen behörighet att pröva klagomål. I denna bestämmelse föreskrivs följande:

”a) Ombudsmannen får pröva eller låta pröva huruvida bestämmelser i denna lag har åsidosatts, åsidosätts eller riskerar att åsidosättas i förhållande till en enskild, om den enskilde har lämnat in ett klagomål till ombudsmannen avseende åsidosättande av någon av dessa bestämmelser eller om ombudsmannen bedömer att ett sådant åsidosättande kan föreligga.

b) Om en enskild lämnar in ett klagomål till ombudsmannen med stöd av led a i denna punkt, ska ombudsmannen

i) utreda eller låta utreda klagomålet, utom om han eller hon finner att detta är grundlöst eller har ingetts mot bättre vetande, och

ii) om han eller hon inte inom rimlig tid lyckas få de berörda parterna att göra upp i godo såvitt avser ämnet för klagomålet, skriftligen delge klaganden sitt beslut avseende klagomålet och, för den händelse att beslutet går klaganden emot, underrätta klaganden om möjligheten att med stöd av section 26 i denna lag överklaga beslutet till domstol inom 21 dagar från delgivningen.”

30. I det aktuella fallet fann ombudsmannen att Maximillian Schrems klagomål var ”grundlöst” eller hade ”ingetts mot bättre vetande” i den bemärkelsen att det inte skulle kunna bifallas eftersom det saknade rättslig grund. Det var därför som han beslutade att inte utreda klagomålet.

31. Section 11 i dataskyddslagen reglerar överföring av personuppgifter till mottagare utanför Irland. I section 11.2 a föreskrivs följande:

”När, i ärende som regleras av denna lag, fråga uppkommer

i) om huruvida en sådan adekvat skyddsnivå som avses i punkt 1 i denna section garanteras av ett land eller territorium utanför Europeiska ekonomiska samarbetsområdet [(EES)] till vilket personuppgifter kommer att överföras, och

ii) det har gjorts ett konstaterande från unionens sida med avseende på den ifrågavarande typen av överföring,

ska frågan avgöras i överensstämmelse med det konstaterandet.”

32. I section 11.2 b i dataskyddslagen definieras ”konstaterande från unionens sida” enligt följande:

”I underpunkt a i denna punkt betyder ’konstaterande från unionens sida’ ett konstaterande som … kommissionen har gjort med stöd av artikel 25.4 eller 25.6 i [direktiv 95/46], inom ramen för förfarandet enligt artikel 31.2 i [detta direktiv], i syfte att slå fast huruvida en sådan adekvat skyddsnivå som avses i punkt 1 i denna section garanteras av ett land eller territorium utanför [EES].”

33. Ombudsmannen framhöll att beslut 2000/520 utgör ett ”konstaterande från unionens sida” i den mening som avses i section 11.2 a i dataskyddslagen, varför alla frågor rörande det adekvata i uppgiftsskyddet i det tredjeland till vilka uppgifterna överförs ska avgöras i överensstämmelse med det konstaterandet. Eftersom påståendet att personuppgifter överfördes till ett tredjeland som i praktiken inte garanterade en adekvat skyddsnivå var kärnpunkten i Maximillian Schrems klagomål, gjorde ombudsmannen bedömningen att arten av beslut 2000/520 och dess själva existens hindrade honom från att pröva frågan.

34. Maximillian Schrems överklagade ombudsmannens beslut att avslå hans klagomål till High Court, som efter att ha granskat den bevisning som hade framlagts i målet fann att elektronisk övervakning och uppfångande av personuppgifter fyller nödvändiga och oundgängliga syften av allmänt intresse, nämligen att upprätthålla den nationella säkerheten och förhindra grov brottslighet. Härvid har High Court påpekat att övervakning och uppfångande av personuppgifter som överförs från unionen till Förenta staterna tjänar legitima ändamål med koppling till kampen mot terrorism.

35. High Court anser emellertid också att Edward Snowdens avslöjanden har visat att NSA och andra liknande organ har gått alldeles för långt. Foreign Intelligence Surveillance Court (nedan kallad FISC), en domstol som inrättades genom 1978 års lag om övervakning av utländska underrättelsetjänster (Foreign Intelligence Surveillance Act of 1978)[18], utövar förvisso tillsyn, men förfarandet inför den domstolen är enligt High Court hemligt och inte kontradiktoriskt. Utöver att beslut rörande åtkomst till personuppgifter fattas med stöd av amerikansk rätt, har unionsmedborgarna dessutom enligt High Court i praktiken inte någon rätt att yttra sig i frågan om övervakning och uppfångande av deras personuppgifter.

18 — Se section 702 i den lagen, i dess lydelse enligt 2008 års lag (Foreign Intelligence Surveillance Act of 2008). Det är med stöd av denna section som NSA upprätthåller en databas med beteckningen Prism (se Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection av den 27 november 2013).

36. Av de omfattande handlingar som i det nationella målet har ingetts tillsammans med förklaringar avgivna under ed, framgår det enligt High Court att riktigheten i många av Edward Snowdens avslöjanden är ostridig. Utifrån detta har High Court dragit slutsatsen att när personuppgifter har överförts till Förenta staterna, kan NSA och andra amerikanska säkerhetsorgan såsom Federal Bureau of Investigation (FBI) komma åt dessa uppgifter inom ramen för godtyckliga och storskaliga övervaknings- och uppfångandeåtgärder.

37. High Court har understrukit att de grundlagsfästa rättigheterna till ett privatliv och till respekt för hemmets okränkbarhet är så betydelsefulla i irländsk rätt att varje ingrepp i dessa rättigheter måste uppfylla de lagstadgade kraven och vara proportionerligt. Storskalig och godtycklig åtkomst till personuppgifter uppfyller enligt High Court absolut inte kravet på proportionalitet och torde därför strida mot den irländska grundlagen. [19]

38. För att avlyssning av elektroniska kommunikationer ska kunna anses vara grundlagsenlig, är det enligt High Court nödvändigt att visa att specifik avlyssning av kommunikationer och övervakning av specifika personer eller grupper av personer är objektivt motiverad med hänvisning till intresset av att upprätthålla den nationella säkerheten och bekämpa brottslighet samt att det finns tillräckliga och kontrollerbara garantier.

39. Därför anser High Court att om det nationella målet skulle prövas enbart mot bakgrund av irländsk rätt, skulle en viktig fråga uppkomma angående huruvida Förenta staterna ”garanterar en adekvat skyddsnivå för privatlivet och för de grundläggande fri- och rättigheterna” i den mening som avses i section 11.1 i dataskyddslagen. Av detta följer att ombudsmannen på grundval av irländsk rätt, i synnerhet de krav som slås fast i grundlagen, inte hade kunnat avslå Maximillian Schrems klagomål utan skulle ha varit skyldig att pröva den frågan.

40. High Court har emellertid också noterat att det nationella målet rör tillämpningen av unionsrätten i den mening som avses i artikel 51.1 i stadgan, vilket betyder att lagenligheten av ombudsmannens beslut ska prövas mot bakgrund av unionsrätten.

41. Det problem som ombudsmannen ställdes inför har av High Court förklarats som följer. Enligt section 11.2 a i dataskyddslagen är ombudsmannen skyldig att pröva frågan huruvida skyddet i ett tredjeland är adekvat ”i överensstämmelse med” ett konstaterande från unionens sida som kommissionen har gjort med stöd av artikel 25.6 i direktiv 95/46. Av detta följer att ombudsmannen inte kunde avvika från ett sådant konstaterande. Eftersom kommissionen i beslut 2000/520 hade konstaterat att Förenta staterna garanterar en adekvat skyddsnivå såvitt avser databehandling som utförs av bolag som har anslutit sig till *safe harbor*-principerna, måste ombudsmannen nödvändigtvis avslå ett klagomål i vilket det gjordes gällande att detta skydd inte var adekvat.

42. High Court har i detta sammanhang noterat att ombudsmannen därigenom strikt efterlevde direktiv 95/46 och beslut 2000/520 men har också framhållit att vad Maximillian Schrems i realiteten har motsatt sig är villkoren för *safe harbor*-systemet som sådant snarare än ombudsmannens tillämpning därav. Samtidigt har High Court framhållit att Maximillian Schrems inte direkt har bestritt giltigheten av vare sig direktiv 95/46 eller beslut 2000/520.

43. Enligt High Court är den centrala frågan således huruvida ombudsmannen, mot bakgrund av unionsrätten och särskilt med beaktande av artiklarna 7 och 8 i stadgan (vilka trädde i kraft efter ombudsmannens aktuella beslut), är helt bunden av kommissionens konstaterande i beslut 2000/520 enligt vilket Förenta staternas rätt och praxis i fråga om skydd för personuppgifter är adekvat.

19 — Härvid har High Court framför allt hänvisat till respekten för människans värdighet och den enskildes frihet (ingressen), den personliga självbestämmanderätten (artikel 40.3.1 och 40.3.2), hemmets okränkbarhet (artikel 40.5) och skyddet för familjelivet (artikel 41).

44. High Court har också tillagt att det i det nationella målet inte har framställts någon invändning avseende Facebook USA:s och Facebook Irelands handlande som sådant. Artikel 3.1 b i beslut 2000/520 – som ger de behöriga nationella myndigheterna rätt att förelägga ett företag att upphöra med överföring av uppgifter till ett tredjeland – är emellertid enligt High Court tillämplig endast när ett klagomål rör det berörda företagets handlande, vilket alltså inte skulle vara fallet här.

45. High Court har därför framhållit att den verkliga invändningen inte avser Facebook USA:s handlande som sådant, utan i stället den omständigheten att kommissionen har gjort bedömningen att Förenta staternas rätt och praxis i fråga om uppgiftsskydd garanterar ett adekvat skydd trots att Edward Snowdens avslöjanden tydligt visar att amerikanska myndigheter på ett storskaligt och godtyckligt sätt kan komma åt personuppgifter om personer bosatta inom unionen. [20]

46. Därvid har High Court svårt att se hur beslut 2000/520 i praktiken skulle kunna uppfylla kraven enligt artiklarna 7 och 8 i stadgan, särskilt med beaktande av de principer som domstolen angav i sin dom i målet Digital Rights Ireland m.fl. [21]. I synnerhet skulle den garanti som ges i artikel 7 i stadgan, och som också följer av de grundläggande värderingar som är gemensamma för medlemsstaternas traditioner, komma att urholkas om offentliga myndigheter hade rätt att godtyckligt och generellt få åtkomst till elektroniska kommunikationer utan att behöva anföra sakliga skäl avseende nationell säkerhet eller brottsbekämpning med direkt koppling till de berörda individerna och helt utan tillräckliga och kontrollerbara garantier. Eftersom Maximillian Schrems talan gav vid handen att beslut 2000/520 betraktat fristående från sitt sammanhang skulle kunna vara oförenligt med artiklarna 7 och 8 i stadgan, skulle domstolen kunna tänkas göra bedömningen att det är möjligt att tolka direktiv 95/46, i synnerhet artikel 25.6 i detta, och beslut 2000/520 så, att de nationella myndigheterna får göra egna utredningar i syfte att avgöra huruvida de krav som följer av artiklarna 7 och 8 i stadgan är uppfyllda vid överföring av personuppgifter till ett tredjeland och lagring av personuppgifter i ett tredjeland.

47. Mot denna bakgrund har High Court beslutat att vilandeförklara det nationella målet och ställa följande tolkningsfrågor till domstolen:

”Är ombudsmannen, när han ska pröva ett klagomål rörande överföring av personuppgifter till ett tredjeland (i det aktuella fallet Förenta staterna) vars rätt och praxis enligt klaganden inte garanterar ett adekvat skydd för den berörda personen, helt bunden av det konstaterande från unionens sida med motsatt innebörd som återfinns i beslut 2000/520, mot bakgrund av artiklarna 7, 8 och 47 i stadgan och trots bestämmelserna i artikel 25.6 i direktiv 95/46?

Om så inte är fallet, får eller ska ombudsmannen göra en egen utredning och undersöka hur de faktiska omständigheterna har utvecklats sedan beslut 2000/520 först offentliggjordes?”

## II – **Bedömning**

48. High Court har genom sina båda frågor uppmanat domstolen att slå fast vilka befogenheter de nationella tillsynsmyndigheterna har när de tar emot ett klagomål som rör en överföring av personuppgifter till ett företag i ett tredjeland och det till stöd för klagomålet görs gällande att det berörda tredjelandet inte garanterar en adekvat skyddsnivå för de överförda uppgifterna, trots att kommissionen med stöd av artikel 25.6 i direktiv 95/46 har antagit ett beslut i vilket det tredjelandets skyddsnivå förklaras vara adekvat.

20 — I detta sammanhang har High Court påpekat att Maximillian Schrems som huvudsaklig grund för sin talan i det nationella målet har gjort gällande att ombudsmannen inte hade giltiga skäl för att dra slutsatsen att skyddsnivån för personuppgifter i Förenta staterna var adekvat, mot bakgrund dels av Edward Snowdens avslöjanden på senare tid, dels av den omständigheten att personuppgifter har ställts till förfogande för de amerikanska underrättelseorganen i stor skala.

21 — C-293/12 och C-594/12, EU:C:2014:238, punkterna 65–69.

49. Här ska det påpekas att Maximillian Schrems klagomål till ombudsmannen har två dimensioner. Genom detta klagomål ifrågasätts överföringen av personuppgifter från Facebook Ireland till Facebook USA. Maximillian Schrems har yrkat att denna överföring ska upphöra, eftersom Förenta staterna enligt hans uppfattning inte garanterar en adekvat skyddsnivå för personuppgifter som överförs inom ramen för *safe harbor*-systemet. Närmare bestämt har han kritiserat Förenta staterna för införandet av Prism-programmet, som ger NSA möjlighet att fritt komma åt stora mängder data som finns lagrade på servrar i Förenta staterna. Klagomålet avser således specifikt överföring av personuppgifter från Facebook Ireland till Facebook USA samtidigt som det också innebär ett mer allmänt ifrågasättande av nivån på skyddet för sådana uppgifter inom ramen för *safe harbor*-systemet.

50. Ombudsmannen gjorde bedömningen att den omständigheten att det förelåg ett beslut av kommissionen i vilket Förenta staterna förklarades garantera en adekvat skyddsnivå inom ramen för *safe harbor*-systemet i sig hindrade honom från att utreda detta klagomål.

51. Det är således lämpligt att på en och samma gång ta upp båda frågorna, vilka i huvudsak rör huruvida artikel 28 i direktiv 95/46 jämförd med artiklarna 7 och 8 i stadgan ska tolkas så, att förekomsten av ett beslut som kommissionen har antagit med stöd av artikel 25.6 i direktivet medför att en nationell tillsynsmyndighet hindras dels från att utreda ett klagomål i vilket det görs gällande att ett tredjeland inte garanterar en adekvat skyddsnivå för överförda personuppgifter, dels från att i förekommande fall tillfälligt förbjuda överföringen av dessa uppgifter.

52. Artikel 7 i stadgan garanterar rätten till respekt för privatlivet medan artikel 8 uttryckligen avser rätten till skydd av personuppgifter. I artikel 8.2 och 8.3 anges att personuppgifter ska behandlas lagenligt, för bestämda ändamål och på grundval av den berörda personens samtycke eller på någon annan legitim och lagenlig grund, att var och en har rätt att få tillgång till insamlade uppgifter som rör honom eller henne och att få rättelse av dem, och att en oberoende myndighet ska kontrollera att dessa regler efterlevs.

### A – *De nationella tillsynsmyndigheternas befogenheter i fall där kommissionen har antagit ett beslut om adekvat skyddsnivå*

53. Kärnan i det klagomål som är i fråga i det nationella målet är, som Maximillian Schrems har påpekat i sitt yttrande, överföringen av personuppgifter från Facebook Ireland till Facebook USA mot bakgrund av den allmänna åtkomst till uppgifter lagrade hos Facebook USA som NSA och andra amerikanska säkerhetsorgan ges rätt till i den amerikanska lagstiftningen.

54. När en nationell tillsynsmyndighet tar emot ett klagomål vars syfte är att ifrågasätta konstaterandet att ett visst tredjeland garanterar en adekvat skyddsnivå för överförda uppgifter, har denna myndighet enligt Maximillian Schrems befogenhet att, under förutsättning att den förfogar över uppgifter som tyder på att påståendena i klagomålet är välgrundade, förordna om tillfälligt förbud för den överföring av uppgifter som genomförs av det företag som avses i klagomålet.

55. Maximillian Schrems har, med hänvisning till ombudsmannens skyldighet att skydda hans grundläggande rättigheter, gjort gällande att det åligger ombudsmannen inte endast att utreda klagomålet utan även att, om detta bifalls, utnyttja sina befogenheter att tillfälligt förbjuda överföringen av uppgifter mellan Facebook Ireland och Facebook USA.

56. Ombudsmannen avslog emellertid klagomålet med hänvisning till de bestämmelser i dataskyddslagen där hans befogenheter räknas upp. Det beslutet fattade ombudsmannen utifrån sin bedömning att han var bunden av beslut 2000/520.

57. Av detta följer att det centrala problemet i förevarande mål är huruvida kommissionens bedömning att nivån på det skydd som beskrivs i beslut 2000/520 är adekvat helt binder en nationell tillsynsmyndighet och hindrar denna från att utreda påståenden som innebär att kommissionens bedömning ifrågasätts. Tolkningsfrågorna rör således hur omfattande undersökningsbefogenheter de nationella dataskyddsmyndigheterna har när det föreligger ett kommissionsbeslut om adekvat skyddsnivå.

58. Kommissionen anser det viktigt att beakta sambandet mellan kommissionens och de nationella dataskyddsmyndigheternas befogenheter. De nationella myndigheternas befogenheter är enligt kommissionen koncentrerade till tillämpningen av dataskyddslagstiftningen i enskilda fall, medan det faller inom kommissionens befogenhetsområde att göra en allmän översyn av tillämpningen av beslut 2000/520, inbegripet att anta eventuella beslut om att tills vidare inte tillämpa beslutet eller upphäva beslutet.

59. Enligt kommissionen har Maximillian Schrems inte lagt fram några specifika argument som ger vid handen att han löpte överhängande risk att drabbas av allvarlig skada till följd av överföringen av uppgifter mellan Facebook Ireland och Facebook USA. De abstrakta och allmänna farhågor som Maximillian Schrems har gett uttryck för på tal om de övervakningsprogram som de amerikanska säkerhetsorganen har genomfört är tvärtom identiska med de farhågor som har föranlett kommissionen att inleda en översyn av beslut 2000/520.

60. Kommissionen anser att om de nationella tillsynsmyndigheterna vidtar åtgärder på grundval av klagomål som uteslutande avser strukturella och abstrakta farhågor, inkräktar de därigenom på kommissionens behörighet att omförhandla villkoren för nämnda beslut med Förenta staterna eller vid behov tills vidare upphöra med att tillämpa detta beslut.

61. Jag delar inte kommissionens åsikt. Enligt min uppfattning kan förekomsten av ett beslut som kommissionen har antagit med stöd av artikel 25.6 i direktiv 95/46 inte omintetgöra eller ens inskränka de befogenheter som de nationella tillsynsmyndigheterna har med stöd av artikel 28 i det direktivet. Tvärtemot vad kommissionen har gjort gällande, hindrar ett sådant beslut, som jag ser det, inte en nationell tillsynsmyndighet som får in enskilda klagomål från att i enskilda ärenden, med stöd av sina undersökningsbefogenheter och sitt oberoende, bilda sig en egen uppfattning om den allmänna skyddsnivån i ett tredjeland och därefter vidta vederbörliga åtgärder.

62. Enligt domstolens fasta rättspraxis ska vid tolkningen av en unionsbestämmelse inte bara lydelsen beaktas, utan också sammanhanget och de mål som eftersträvas med de föreskrifter som bestämmelsen ingår i. [22]

63. Av skäl 62 i direktiv 95/46 framgår att det ”[f]ör skyddet av enskilda personer med avseende på behandlingen av personuppgifter är … av avgörande betydelse att medlemsstaterna inrättar oberoende tillsynsmyndigheter”.

64. Enligt artikel 28.1 första stycket i samma direktiv ska ”[v]arje medlemsstat … tillse att det utses en eller flera myndigheter som har till uppgift att inom dess territorium övervaka tillämpningen av de bestämmelser som medlemsstaterna antar till följd av detta direktiv”. I artikel 28.1 andra stycket i direktivet föreskrivs att ”[d]essa myndigheter … fullständigt oberoende [ska] utöva de uppgifter som åläggs dem”.

22 — Se, bland annat, dom Koushkaki (C-84/12, EU:C:2013:862, punkt 34 och där angiven rättspraxis).

65. Artikel 28.3 i direktiv 95/46 innehåller en uppräkning av de befogenheter som varje tillsynsmyndighet förfogar över: undersökningsbefogenheter, effektiva befogenheter att ingripa – bland annat att besluta om tillfälligt eller slutligt förbud mot behandling – och befogenhet att inleda rättsliga förfaranden i samband med överträdelser av de nationella bestämmelser som har antagits till följd av direktivet eller att uppmärksamma de rättsliga myndigheterna på sådana överträdelser.

66. Enligt artikel 28.4 första stycket i direktiv 95/46 kan dessutom ”[v]ar och en … vända sig till tillsynsmyndigheten med begäran om skydd för sina fri- och rättigheter med avseende på behandling av personuppgifter”. I artikel 28.4 andra stycket anges vidare att ”[v]ar och en … i samband med tillämpningen av de nationella bestämmelser som har antagits med stöd av artikel 13 i detta direktiv till tillsynsmyndigheten [kan] ge in en begäran om att få kontrollera om en behandling är tillåten”. Härvid ska det förtydligas att nämnda artikel 13 ger medlemsstaterna rätt att genom lagstiftning vidta åtgärder för att begränsa omfattningen av ett antal skyldigheter och rättigheter som anges i direktiv 95/46 i fall då en sådan begränsning är en nödvändig åtgärd med hänsyn till bland annat statens säkerhet, försvaret, allmän säkerhet och förebyggande av, undersökning av, avslöjande av eller åtal för brott.

67. Kravet på en oberoende myndighet som övervakar efterlevnaden av de unionsrättsliga bestämmelserna om skydd för enskilda personer med avseende på behandling av personuppgifter följer även, som domstolen redan tidigare har slagit fast, av unionens primärrätt, bland annat av artikel 8.3 i stadgan och av artikel 16.2 FEUF.[23] Domstolen har också påpekat att ”[i]nrättandet av oberoende tillsynsmyndigheter i medlemsstaterna … således [är] av avgörande betydelse för skyddet av enskilda personer med avseende på behandlingen av personuppgifter”[24].

68. Vidare har domstolen funnit att ”artikel 28.1 andra stycket i direktiv 95/46 ska tolkas så, att de tillsynsmyndigheter som är behöriga i fråga om övervakning av behandling av personuppgifter ska åtnjuta ett sådant oberoende att de kan utöva sina uppgifter utan påverkan utifrån. Detta oberoende utesluter bland annat varje åläggande eller all annan påverkan utifrån, direkt eller indirekt, som kan inverka på deras beslutsfattande och som kan hindra nämnda myndigheter från att fullgöra sin uppgift att säkerställa en riktig avvägning mellan skyddet för rätten till privatliv och ett fritt flöde av personuppgifter”[25].

69. Domstolen har också påpekat att ”[g]arantin för de nationella tillsynsmyndigheternas oberoende är avsedd att säkerställa en effektiv och tillförlitlig övervakning av att bestämmelserna om skydd för enskilda personer med avseende på behandling av personuppgifter följs”[26]. Denna garanti för myndigheternas oberoende har införts ”för att förstärka skyddet av de personer och organ som berörs av [de nationella tillsynsmyndigheternas] beslut”[27].

70. Som framgår bland annat av skäl 10 och artikel 1 i direktiv 95/46 är syftet med detta direktiv att inom unionen ”säkerställa en hög skyddsnivå i fråga om grundläggande fri- och rättigheter med avseende på behandling av personuppgifter”.[28] Domstolen anser därvid att ”[d]e tillsynsmyndigheter som avses i artikel 28 i direktiv 95/46 är … dessa grundläggande fri- och rättigheters väktare”.[29]

23 — Se dom kommissionen/Österrike (C-614/10, EU:C:2012:631, punkt 36) och dom kommissionen/Ungern (C-288/12, EU:C:2014:237, punkt 47).

24 — Se, bland annat, dom kommissionen/Ungern (C-288/12, EU:C:2014:237, punkt 48 och där angiven rättspraxis). Se även, för ett liknande resonemang, dom Digital Rights Ireland m.fl. (C-293/12 och C-594/12, EU:C:2014:238, punkt 68 och där angiven rättspraxis).

25 — Se, bland annat, dom kommissionen/Ungern (C-288/12, EU:C:2014:237, punkt 51 och där angiven rättspraxis).

26 — Dom kommissionen/Tyskland (C-518/07, EU:C:2010:125, punkt 25).

27 — Ibidem.

28 — Ibidem (punkt 22 och där angiven rättspraxis).

29 — Ibidem (punkt 23). Se även, för ett liknande resonemang, dom kommissionen/Österrike (C-614/10, EU:C:2012:631, punkt 52) och dom kommissionen/Ungern (C-288/12, EU:C:2014:237, punkt 53).

71. Med tanke på de nationella tillsynsmyndigheternas betydelsefulla roll i samband med skyddet för enskilda personer med avseende på behandling av personuppgifter, ska dessa myndigheters befogenheter att ingripa inte inskränkas ens i fall där kommissionen har antagit ett beslut med stöd av artikel 25.6 i direktiv 95/46.

72. Härvid noterar jag att det inte finns något som tyder på att system för överföring av personuppgifter till tredjeländer skulle falla utanför det materiella tillämpningsområdet för artikel 8.3 i stadgan, som på den högsta nivån i den unionsrättsliga normhierarkin slår fast vikten av den tillsyn som utövas av en oberoende myndighet när det gäller efterlevnaden av bestämmelserna om skydd för personuppgifter.

73. Om de nationella tillsynsmyndigheterna var helt bundna av kommissionens beslut skulle detta oundvikligen inskränka deras fullständiga oberoende. I sin roll som väktare av grundläggande rättigheter måste de nationella tillsynsmyndigheterna kunna genomföra helt oberoende utredningar av de klagomål som de får in, i det överordnade intresse som utgörs av skyddet för enskilda med avseende på behandling av personuppgifter.

74. Dessutom finns det, som den belgiska regeringen och Europaparlamentet framhöll vid den muntliga förhandlingen, inget hierarkiskt förhållande mellan kapitel IV i direktiv 95/46, som rör överföring av personuppgifter till tredjeländer, och kapitel VI i samma direktiv, som rör bland annat de nationella tillsynsmyndigheternas roll. Ingenting i kapitel VI tyder på att bestämmelserna om de nationella tillsynsmyndigheterna på något sätt skulle vara underordnade de separata bestämmelser om överföring som anges i kapitel IV.

75. Tvärtom framgår det uttryckligen av artikel 25.1 i direktiv 95/46, vilken återfinns i kapitel IV, att det är tillåtet att överföra personuppgifter till ett tredjeland som garanterar en adekvat skyddsnivå endast under förutsättning att de nationella bestämmelser som har antagits till följd av andra bestämmelser i direktivet iakttas.

76. Medlemsstaterna ska nämligen enligt artikel 25.1 i direktiv 95/46 föreskriva i nationell lagstiftning att överföring av personuppgifter som är under behandling eller som är avsedda att behandlas efter överföring till tredjeland endast får ske om ifrågavarande tredjeland – utan att detta påverkar tillämpningen av de nationella bestämmelser som har antagits till följd av de andra bestämmelserna i direktiv 95/46 – säkerställer en adekvat skyddsnivå.

77. Enligt artikel 28.1 i direktiv 95/46 har de nationella tillsynsmyndigheterna till uppgift att inom respektive medlemsstats territorium övervaka tillämpningen av de bestämmelser som medlemsstaterna antar till följd av det direktivet.

78. Utifrån en jämförelse av dessa båda bestämmelser är det möjligt att dra slutsatsen att den regel som anges i artikel 25.1 i direktiv 95/46 – att överföring av personuppgifter får ske endast om det tredjeland som uppgifterna ska överföras till garanterar en adekvat skyddsnivå för dem – är en av de regler vilkas tillämpning de nationella tillsynsmyndigheterna ska övervaka.

79. De nationella tillsynsmyndigheternas befogenhet att helt oberoende utreda klagomål som de får in med stöd av artikel 28 i direktiv 95/46 ska, i överensstämmelse med artikel 8.3 i stadgan, tolkas extensivt. Denna befogenhet kan således inte inskränkas med stöd av den befogenhet att konstatera att ett tredjeland garanterar en adekvat skyddsnivå som unionslagstiftaren genom artikel 25.6 i direktivet har tilldelat kommissionen.

80. Med tanke på att de nationella tillsynsmyndigheterna har en så viktig roll för skyddet av personuppgifter, måste de kunna göra utredningar när de får in klagomål med upplysningar som skulle kunna göra det möjligt att ifrågasätta skyddsnivån i ett tredjeland, även när kommissionen genom ett beslut med stöd av artikel 25.6 i direktiv 95/46 har konstaterat att det berörda tredjelandet garanterar en adekvat skyddsnivå.

81. Om en nationell tillsynsmyndighet, efter att ha gjort en utredning, finner att den ifrågasatta överföringen av uppgifter undergräver det skydd som unionsmedborgarna ska åtnjuta med avseende på behandling av uppgifter rörande dem, har myndigheten befogenhet att tillfälligt förbjuda den aktuella överföringen av uppgifter, oavsett vilken allmän bedömning som kommissionen har gjort i sitt beslut.

82. Av artikel 25.2 i direktiv 95/46 följer nämligen att bedömningen av huruvida skyddsnivån i ett tredjeland är adekvat ska göras på grundval av en rad olika omständigheter av såväl faktisk som rättslig art. Om det i fråga om någon av dessa omständigheter sker en utveckling som förefaller vara ägnad att göra det möjligt att ifrågasätta huruvida ett tredjelands skyddsnivå är adekvat, måste en nationell tillsynsmyndighet som har fått in ett klagomål kunna dra vederbörliga slutsatser av detta när det gäller den ifrågasatta överföringen.

83. Det är förvisso riktigt, som Irland har framhållit, att ombudsmannen i likhet med alla andra statliga myndigheter är bunden av beslut 2000/520. Det framgår nämligen av artikel 288 fjärde stycket FEUF att ett beslut av en unionsinstitution är till alla delar bindande. Följaktligen ska beslut 2000/520 efterlevas av medlemsstaterna, till vilka det riktar sig.

84. Härvid ska det noteras att det i artikel 5 i beslut 2000/520 föreskrivs att ”[m]edlemsstaterna skall vidta alla åtgärder som är nödvändiga för att följa detta beslut senast nittio dagar efter det att beslutet har delgivits medlemsstaterna”. Dessutom bekräftas det i artikel 6 i nämnda beslut att ”[d]etta beslut riktar sig till medlemsstaterna”.

85. Jag anser emellertid, mot bakgrund av de ovannämnda bestämmelserna i direktiv 95/46 och i stadgan, att den bindande verkan av beslut 2000/520 inte är sådan att den helt utesluter att ombudsmannen utreder klagomål i vilka det hävdas att överföringar av personuppgifter till Förenta staterna inom ramen för det beslutet inte uppvisar de nödvändiga skyddsgarantier som krävs enligt unionsrätten. Med andra ord innebär den bindande verkan inte att sådana klagomål ska avslås summariskt, det vill säga omedelbart och helt utan prövning av huruvida de är välgrundade.

86. Till detta ska läggas att det följer av systematiken i artikel 25 i direktiv 95/46 att ett konstaterande enligt vilket ett tredjeland garanterar eller inte garanterar en adekvat skyddsnivå kan göras antingen av medlemsstaterna eller av kommissionen. Det rör sig således om en delad befogenhet.

87. Av artikel 25.6 i nämnda direktiv framgår att medlemsstaterna, när kommissionen har konstaterat att ett tredjeland garanterar en adekvat skyddsnivå i den mening som avses i artikel 25.2 i direktivet, ska vidta de åtgärder som är nödvändiga för att följa kommissionens beslut.

88. Eftersom ett sådant beslut gör det tillåtet att överföra personuppgifter till ett tredjeland vars skyddsnivå kommissionen finner adekvat, ska medlemsstaterna således i princip tillåta att företag inom deras territorium gör sådana överföringar.

89. Artikel 25 i direktiv 95/46 ger emellertid inte kommissionen ensam befogenhet att konstatera att nivån på skyddet av överförda personuppgifter är adekvat eller inte. Denna artikels systematik vittnar i stället om att även medlemsstaterna har en roll att spela i detta sammanhang. Ett beslut av kommissionen har förvisso en betydelsefull funktion när det gäller att skapa enhetliga villkor för överföring som gäller i medlemsstaterna, men dessa enhetliga villkor kan endast gälla så länge konstaterandet inte har ifrågasatts.

90. Argumentet att det är nödvändigt att skapa enhetliga villkor för överföring av personuppgifter till ett tredjeland har enligt min mening begränsad giltighet i en sådan situation som den i det nationella målet, där kommissionen inte endast har underrättats om att dess konstaterande är föremål för kritik utan faktiskt också själv har framfört sådan kritik och bedriver förhandlingar i syfte att avhjälpa situationen.

91. Bedömningen av huruvida ett tredjelands skyddsnivå är adekvat eller ej kan dessutom föranleda samarbete mellan medlemsstaterna och kommissionen. I artikel 25.3 i direktiv 95/46 föreskrivs nämligen att ”[m]edlemsstaterna och kommissionen skall informera varandra när de anser att ett tredje land inte erbjuder en adekvat skyddsnivå enligt punkt 2”. Som parlamentet har påpekat, visar detta tydligt att medlemsstaterna och kommissionen har likvärdiga roller när det gäller att hitta fall där tredjeländer inte garanterar en adekvat skyddsnivå.

92. Syftet med ett beslut om adekvat skyddsnivå är att tillåta överföring av personuppgifter till det berörda tredjelandet. Detta betyder inte att unionsmedborgarna inte längre kan vända sig till tillsynsmyndigheterna med en begäran avsedd att skydda deras personuppgifter. Härvid noterar jag att det i artikel 28.4 första stycket i direktiv 95/46, där det stadgas att ”[v]ar och en … [kan] vända sig till tillsynsmyndigheten med begäran om skydd för sina fri- och rättigheter med avseende på behandling av personuppgifter”, inte finns någon bestämmelse om undantag från den principen i fall där det föreligger ett beslut som kommissionen har antagit med stöd av artikel 25.6 i direktivet.

93. Ett beslut som kommissionen har antagit med stöd av sina genomförandebefogenheter enligt nämnda bestämmelse medför således att personuppgifter får överföras till ett tredjeland, men däremot medför ett sådant beslut inte att medlemsstaterna, och i synnerhet deras nationella tillsynsmyndigheter, helt fråntas sina befogenheter, eller ens får dessa befogenheter beskurna, i fall där det har framförts påståenden om ingrepp i grundläggande rättigheter.

94. En nationell tillsynsmyndighet måste kunna utöva befogenheterna enligt artikel 28.3 i direktiv 95/46, bland annat befogenheten att besluta om tillfälligt eller slutligt förbud mot en behandling av personuppgifter. I uppräkningen av befogenheter i denna bestämmelse hänvisas det förvisso inte uttryckligen till några befogenheter i förhållande till överföring från en medlemsstat till ett tredjeland, men en sådan överföring ska enligt min uppfattning anses utgöra en behandling av uppgifter.[30] Av den berörda bestämmelsens lydelse framgår dessutom att uppräkningen inte är uttömmande. Under alla omständigheter måste de nationella tillsynsmyndigheterna, med tanke på deras centrala roll i det system som införs genom direktiv 95/46, ha befogenhet att tillfälligt förbjuda en överföring av uppgifter i fall där det har konstaterats ett ingrepp i grundläggande rättigheter eller föreligger risk för ett sådant ingrepp.

95. Att frånta en nationell tillsynsmyndighet dess undersökningsbefogenheter under sådana omständigheter som i förevarande mål skulle dessutom strida inte endast mot principen om oberoende utan även mot det syfte som eftersträvas genom direktiv 95/46 såsom detta framgår av artikel 1.1 i nämnda direktiv.

96. Som domstolen har påpekat, ”framgår [det] av skälen 3, 8 och 10 i direktiv 95/46 att unionslagstiftaren hade för avsikt att underlätta den fria rörligheten för personuppgifter genom tillnärmning av medlemsstaternas lagstiftningar samtidigt som enskilda personers grundläggande rättigheter skyddas, särskilt rätten till skydd för privatlivet, och att garantera en hög skyddsnivå inom unionen. I artikel 1 i direktivet föreskrivs således att medlemsstaterna ska skydda fysiska personers grundläggande fri- och rättigheter, särskilt rätten till privatliv, i samband med behandling av personuppgifter.”[31]

30 — Se generaladvokaten Légers förslag till avgörande i målet parlamentet/rådet och kommissionen (C-317/04, EU:C:2005:710, punkterna 92–95). Se även dom parlamentet/rådet och kommissionen (C-317/04 och C-318/04, EU:C:2006:346, punkt 56).

31 — Se, bland annat, dom IPI (C-473/12, EU:C:2013:715, punkt 28 och där angiven rättspraxis).

97. Bestämmelserna i direktiv 95/46 ska följaktligen tolkas i överensstämmelse med det direktivets syfte att garantera en hög skyddsnivå för enskilda personers grundläggande fri- och rättigheter, särskilt rätten till skydd för privatlivet, i samband med behandling av personuppgifter inom unionen.

98. Vikten av detta syfte, liksom den roll som medlemsstaterna ska spela i strävan att förverkliga detta syfte, innebär att medlemsstaterna och därmed också deras nationella tillsynsmyndigheter inte kan vara helt bundna av ett beslut om adekvat skyddsnivå från kommissionens sida, när särskilda omständigheter föranleder allvarlig oro över huruvida de grundläggande rättigheter som garanteras i stadgan respekteras i samband med överföring av personuppgifter till ett tredjeland.

99. Domstolen har redan tidigare funnit att ”eftersom bestämmelserna i direktiv 95/46 reglerar behandling av personuppgifter som kan innebära intrång i de grundläggande friheterna och då särskilt i rätten till privatliv, måste bestämmelserna i fråga med nödvändighet tolkas mot bakgrund av de grundläggande rättigheterna, vilka enligt fast rättspraxis utgör en integrerad del av de allmänna rättsprinciper som domstolen ska säkerställa iakttagandet av och som numera är stadfästa i stadgan” [32].

100. Dessutom vill jag hänvisa till den rättspraxis enligt vilken ”medlemsstaterna inte endast ska tolka sin nationella rätt på ett sätt som står i överensstämmelse med unionsrätten, utan även se till att de inte grundar sig på en tolkning av en sekundärrättslig bestämmelse som skulle stå i strid med de grundläggande rättigheter som skyddas genom unionens rättsordning eller med andra allmänna unionsrättsliga principer” [33].

101. I domen i målet N. S. m.fl. [34] slog domstolen fast att ”det inte är förenligt med medlemsstaternas skyldighet att tolka och tillämpa förordning [(EG)] nr 343/2003 på ett sätt som överensstämmer med de grundläggande rättigheterna att tillämpa förordning nr 343/2003[ [35]] på grundval av en icke motbevisbar presumtion om att den asylsökandes grundläggande rättigheter kommer att respekteras i den medlemsstat som i normalfallet är behörig att pröva hans eller hennes ansökan” [36].

102. Härvid angav domstolen förvisso att det verkligen ska presumeras, mot bakgrund av medlemsstaternas ställning som säkra ursprungsländer i förhållande till varandra när det gäller rättsliga och praktiska frågor med koppling till asylrätten, att den behandling som asylsökande erhåller i varje medlemsstat överensstämmer med kraven i stadgan, i konventionen angående flyktingars rättsliga ställning, undertecknad den 28 juli 1951 i Genève, [37] och i Europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, undertecknad i Rom den 4 november 1950 [38]. Domstolen konstaterade emellertid också att ”det inte [kan] uteslutas att systemet i praktiken stöter på betydande funktionella svårigheter i en viss medlemsstat, och att det därför finns en allvarlig risk för att asylsökande som överförs till denna medlemsstat behandlas på ett sätt som inte är förenligt med deras grundläggande rättigheter” [39].

32 — Se, bland annat, dom Google Spain och Google (C-131/12, EU:C:2014:317, punkt 68 och där angiven rättspraxis).

33 — Se, bland annat, dom N. S. m.fl. (C-411/10 och C-493/10, EU:C:2011:865, punkt 77 och där angiven rättspraxis).

34 — C-411/10 och C-493/10, EU:C:2011:865.

35 — Rådets förordning av den 18 februari 2003 om kriterier och mekanismer för att avgöra vilken medlemsstat som har ansvaret för att pröva en asylansökan som en medborgare i tredje land har gett in i någon medlemsstat (EUT L 50, s. 1).

36 — Punkt 99 i domen.

37 — *Förenta nationernas fördragssamling*, volym 189, s. 150, nr 2545 (1954).

38 — Se dom N. S. m.fl. (C-411/10 och C-493/10, EU:C:2011:865, punkt 80).

39 — Ibidem (punkt 81).

103. Med ledning av detta slog domstolen fast att det ”ankommer … på medlemsstaterna, inbegripet de nationella domstolarna, att inte överföra en asylsökande till den ’ansvariga medlemsstaten’ i den mening som avses i förordning nr 343/2003, när de inte kan sväva i okunnighet om att de systembrister vad beträffar asylförfarandet och mottagningsvillkoren för asylsökande som finns i den medlemsstaten utgör allvarliga och klarlagda skäl att anta att den asylsökande löper en verklig risk att utsättas för omänsklig eller förnedrande behandling i den mening som avses i artikel 4 i stadgan” [40].

104. Det förefaller mig som om domstolens lösning i målet N. S. m.fl. [41] kan utvidgas till att omfatta en sådan situation som den som är i fråga i det nationella målet. En tolkning av unionens sekundärrätt som bygger på en icke motbevisbar presumtion om att de grundläggande rättigheterna kommer att respekteras – av en medlemsstat, av kommissionen eller av ett tredjeland – ska således anses oförenlig med medlemsstaternas skyldighet att tolka och tillämpa unionens sekundärrätt på ett sätt som överensstämmer med de grundläggande rättigheterna. Artikel 25.6 i direktiv 95/46 innebär följaktligen inte att kommissionens bedömning att ett tredjelands skyddsnivå är adekvat ger upphov till en sådan icke motbevisbar presumtion om att de grundläggande rättigheterna respekteras. Den presumtion, som ligger till grund för denna bestämmelse, om att överföringen av uppgifter till ett tredjeland sker med respekt för de grundläggande rättigheterna ska i stället anses som motbevisbar. [42] Detta betyder att den bestämmelsen inte ska tolkas så, att den undergräver de garantier avseende skyddet av personuppgifter och respekten för rätten till detta skydd som anges bland annat i artikel 28.3 i direktiv 95/46 och i artikel 8.3 i stadgan.

105. Utifrån nämnda dom drar jag således slutsatsen att medlemsstaterna måste kunna vidta nödvändiga åtgärder för att slå vakt om de grundläggande rättigheter som skyddas enligt artiklarna 7 och 8 i stadgan, när det har konstaterats systembrister i det tredjeland till vilket personuppgifter överförs.

106. Till yttermera visso får kommissionens antagande av ett beslut om adekvat skyddsnivå, som den italienska regeringen har påpekat i sitt yttrande, inte leda till att unionsmedborgarna får ett svagare skydd med avseende på behandling av uppgifter rörande dem om uppgifterna överförs till ett tredjeland än vad som skulle ha varit fallet om uppgifterna hade behandlats inom unionen. De nationella tillsynsmyndigheterna måste således kunna ingripa och utöva sina befogenheter med avseende på överföring av uppgifter till tredjeländer för vilka det antagits ett beslut om adekvat skyddsnivå. I annat fall får unionsmedborgarna ett sämre skydd än när uppgifter rörande dem behandlas inom unionen.

107. Att kommissionen antar ett beslut med stöd av artikel 25.6 i direktiv 95/46 medför således uteslutande att det allmänna förbudet upphävs vad gäller export av personuppgifter till tredjeländer vilka erbjuder en skyddsnivå som är jämförbar med den som nämnda direktiv garanterar. Med andra ord skapas det inte någon särskild undantagsordning där unionsmedborgarna åtnjuter ett svagare skydd än vad de gör enligt den allmänna ordning som i nämnda direktiv föreskrivs såvitt avser behandling av uppgifter inom unionen.

40 — Ibidem (punkt 94).

41 — C-411/10 och C-493/10, EU:C:2011:865.

42 — Punkt 104 i denna dom.

108. Domstolen har förvisso slagit fast, i punkt 63 i sin dom i målet Lindqvist,[43] att det ”[g]enom kapitel IV i direktiv 95/46, vari artikel 25 ingår, införs en särreglering”. Detta innebär emellertid enligt min uppfattning inte att särregleringen ska erbjuda ett svagare skydd. I artikel 25 i nämnda direktiv anges det nämligen en rad skyldigheter som medlemsstaterna och kommissionen ska fullgöra[44] för att det mål om skydd av uppgifter som slås fast i artikel 1.1 i direktivet ska kunna förverkligas, och i artikel 25 slås det också fast en princip med innebörden att om ett tredjeland inte garanterar en adekvat skyddsnivå, ska överföring av personuppgifter till det tredjelandet förbjudas.[45]

109. När det mer specifikt gäller *safe harbor*-systemet har kommissionen inte avsett att nationella tillsynsmyndigheter ska kunna ingripa och tillfälligt förbjuda överföring av uppgifter annat än inom ramen för artikel 3.1 b i beslut 2000/520.

110. Enligt skäl 8 i detta beslut är det ”[f]ör att värna om öppenhet och för att bevara förmågan hos de behöriga myndigheterna i medlemsstaterna att garantera skydd av enskilda med avseende på behandlingen av deras personuppgifter … nödvändigt att i detta beslut specificera vilka omständigheter som i undantagsfall bör medföra att vissa dataflöden avbryts, trots att skyddsnivån befunnits vara adekvat”.

111. I förevarande mål är det närmare bestämt tillämpningen av artikel 3.1 b i nämnda beslut som har diskuterats. Enligt den bestämmelsen får nationella tillsynsmyndigheter besluta om tillfälligt förbud mot överföring av uppgifter i de fall då ”det är i hög grad sannolikt att principerna överträds, det finns välgrundad anledning att tro att den berörda instansen för handläggning av klagomål inte vidtar och inte i rätt tid kommer att vidta de åtgärder som behövs för att lösa problemet, en fortsatt överföring av uppgifterna skulle innebära en överhängande risk för allvarlig skada för registrerade, och de behöriga myndigheterna i medlemsstaten har gjort vad som under rådande omständigheter rimligtvis kan krävas för att anmärka mot organisationen och ge den tillfälle att gå i svaromål”.

112. I nämnda bestämmelse anges ett flertal villkor som i förevarande mål har blivit föremål för olikartade tolkningar från parternas sida.[46] Utan att gå närmare in på dessa tolkningar kan jag konstatera att det framgår av dem att de aktuella villkoren strikt anger gränserna för de nationella tillsynsmyndigheternas befogenhet att tillfälligt förbjuda överföring av uppgifter.

113. I motsats till vad kommissionen har gjort gällande, ska artikel 3.1 b i beslut 2000/520 tolkas i överensstämmelse med det syfte att skydda personuppgifter som eftersträvas genom direktiv 95/46, och mot bakgrund av artikel 8 i stadgan. Kravet på en tolkning som står i överensstämmelse med de grundläggande rättigheterna talar för en extensiv tolkning av nämnda bestämmelse.

114. Av detta följer att de villkor som anges i artikel 3.1 b i beslut 2000/520 enligt min uppfattning inte kan hindra en nationell tillsynsmyndighet från att på ett fullständigt oberoende sätt utöva sina befogenheter enligt artikel 28.3 i direktiv 95/46.

43 — C-101/01, EU:C:2003:596.

44 — Punkt 65.

45 — Punkt 64.

46 — Maximillian Schrems anser att det första villkoret – att det är ”i hög grad sannolikt att principerna överträds” – inte är uppfyllt. Det har nämligen inte hävdats att Facebook USA, i egenskap av självcertifierad organisation till vilken uppgifter har överförts, själv skulle ha överträtt *safe harbor*-principerna i och med att de amerikanska myndigheterna har fått storskalig och godtycklig åtkomst till de uppgifter som Facebook USA innehar. *Safe harbor*-principerna begränsas i själva verket uttryckligen av amerikansk rätt, som i fjärde stycket i bilaga I till beslut 2000/520 definieras genom hänvisning till lagar, myndighetsföreskrifter och rättspraxis.

115. Som den belgiska och den österrikiska regeringen påpekade vid den muntliga förhandlingen, är den ”nödutgång” som utgörs av artikel 3.1 b i beslut 2000/520 så trång att den är svår att använda i praktiken. Det krävs att flera olika kriterier är uppfyllda samtidigt, och kraven är för högt ställda. Mot bakgrund av artikel 8.3 i stadgan är det emellertid inte möjligt att inskränka de nationella tillsynsmyndigheternas handlingsutrymme i fråga om deras befogenheter enligt artikel 28.3 i direktiv 95/46 till den grad att dessa befogenheter inte länge kan utövas.

116. Härvid har parlamentet på goda grunder framhållit att det är unionslagstiftaren som har bestämt vilka befogenheter de nationella tillsynsmyndigheterna ska ha. De genomförandebefogenheter som unionslagstiftaren genom artikel 25.6 i direktiv 95/46 har tilldelat kommissionen påverkar inte de befogenheter som samma lagstiftare genom artikel 28.3 i det direktivet har tilldelat de nationella tillsynsmyndigheterna. Med andra ord saknar kommissionen befogenhet att inskränka de nationella tillsynsmyndigheternas befogenheter.

117. Detta innebär att de nationella tillsynsmyndigheterna, för att kunna säkerställa ett lämpligt skydd av enskilda personers grundläggande rättigheter med avseende på behandling av personuppgifter, måste ha befogenhet att utreda påståenden om ingrepp i dessa rättigheter. Om en sådan myndighet efter en sådan utredning anser att det i ett tredjeland som omfattas av ett beslut om adekvat skyddsnivå finns tydliga indikationer på åsidosättande av unionsmedborgarnas rätt till skydd för sina personuppgifter, måste den tillfälligt kunna förbjuda överföring av uppgifter till en mottagare i det tredjelandet.

118. Med andra ord måste de nationella tillsynsmyndigheterna kunna genomföra utredningar och i förekommande fall tillfälligt förbjuda en överföring av uppgifter, oberoende av de restriktiva villkoren enligt artikel 3.1 b i beslut 2000/520.

119. Dessutom måste de nationella tillsynsmyndigheterna, i kraft av sin befogenhet enligt artikel 28.3 i direktiv 95/46 att inleda rättsliga förfaranden vid överträdelse av nationella bestämmelser som har antagits till följd av det direktivet eller att uppmärksamma de rättsliga myndigheterna på sådana överträdelser, kunna väcka talan vid nationell domstol när de får kännedom om faktiska omständigheter som visar att ett tredjeland inte garanterar en adekvat skyddsnivå, varvid den nationella domstolen i förekommande fall kan besluta att begära förhandsavgörande av EU-domstolen i syfte att få till stånd en prövning av giltigheten av ett kommissionsbeslut om adekvat skyddsnivå.

120. Av det ovan anförda följer att artikel 28 i direktiv 95/46 jämförd med artiklarna 7 och 8 i stadgan ska tolkas så, att förekomsten av ett beslut som kommissionen har antagit med stöd av artikel 25.6 i nämnda direktiv inte hindrar en nationell tillsynsmyndighet från att utreda ett klagomål i vilket det görs gällande att ett tredjeland inte garanterar en adekvat skyddsnivå för överförda personuppgifter och inte heller från att i förekommande fall tillfälligt förbjuda överföringen av dessa uppgifter.

121. High Court har förvisso framhållit i begäran om förhandsavgörande att Maximillian Schrems i det nationella målet formellt sett inte har bestritt giltigheten av vare sig direktiv 95/46 eller beslut 2000/520, men det framgår likafullt av nämnda begäran att hans huvudsakliga kritik syftar till att ifrågasätta konstaterandet att Förenta staterna inom ramen för *safe harbor*-systemet garanterar en adekvat skyddsnivå för överförda personuppgifter.

122. Det framgår dessutom av ombudsmannens yttrande att Maximillian Schrems klagomål utgör ett direkt ifrågasättande av beslut 2000/520. Hans syfte med att lämna in detta klagomål var nämligen att framföra kritik mot villkoren och funktionssättet för *safe harbor*-systemet som sådant, med hänvisning till att den storskaliga övervakningen av personuppgifter som hade överförts till Förenta staterna enligt honom visade att det inte fanns något reellt skydd för dessa uppgifter enligt gällande rätt och praxis i detta tredjeland.

123. Vidare har High Court själv påpekat att den garanti som följer av artikel 7 i stadgan och av de grundläggande värderingar som är gemensamma för medlemsstaternas grundlagstraditioner skulle komma att urholkas om offentliga myndigheter hade rätt att godtyckligt och generellt få åtkomst till elektroniska kommunikationer utan att behöva anföra sakliga skäl avseende nationell säkerhet eller brottsbekämpning med direkt koppling till de berörda individerna och helt utan tillräckliga och kontrollerbara garantier.[47] High Court har således indirekt uttryckt tvivel rörande giltigheten av beslut 2000/520.

124. Bedömningen av huruvida Förenta staterna, inom ramen för *safe harbor*-systemet, garanterar en adekvat skyddsnivå för överförda personuppgifter gör det således nödvändigt att se närmare på frågan om det beslutets giltighet.

125. Härvid ska det påpekas att domstolen, inom ramen för det instrument för dess samarbete med nationella domstolar som har införts genom artikel 267 FEUF, under vissa särskilda omständigheter får pröva sekundärrättsliga bestämmelsers giltighet även om begäran om förhandsavgörande uteslutande avser en fråga om unionsrättens tolkning.

126. Domstolen har också vid ett flertal tillfällen på eget initiativ ogiltigförklarat en rättsakt som den endast hade blivit ombedd att tolka.[48] Dessutom har den slagit fast att ”[o]m domstolen kommer fram till att de frågor som ställts av en nationell domstol gäller giltigheten snarare än tolkningen av [unions]rättsakter, ankommer det på domstolen att omedelbart upplysa den nationella domstolen härom, utan att påtvinga denna formalia som enbart skulle försena förfarandet enligt artikel [267 FEUF] och strida mot dess karaktär”[49]. Till yttermera visso har domstolen redan tidigare funnit att när en hänskjutande domstol uttrycker tvivel om huruvida en sekundärrättslig rättsakt är förenlig med bestämmelserna om skyddet för de grundläggande rättigheterna, ska detta anses som ett ifrågasättande av rättsaktens giltighet mot bakgrund av unionsrätten.[50]

127. Det följer vidare av domstolens praxis att de rättsakter som antas av unionens institutioner, organ och byråer presumeras vara giltiga, vilket innebär att de har rättsverkan så länge de inte har återkallats eller förklarats vara ogiltiga inom ramen för en talan om ogiltigförklaring, till följd av en begäran om förhandsavgörande eller till följd av en invändning om rättsstridighet. Domstolen har exklusiv behörighet att förklara en unionsrättsakt ogiltig, och denna exklusiva behörighet har till syfte att upprätthålla rättssäkerheten genom att säkerställa unionsrättens enhetliga tillämpning. Så länge det aktuella beslutet inte har förklarats ogiltigt och kommissionen inte har ändrat eller upphävt det, har det tvingande verkan i alla sina delar och är direkt tillämpligt i samtliga medlemsstater.[51]

128. Därför anser jag att domstolen, för att kunna ge High Court ett fullständigt svar och för att kunna skingra de tvivel rörande giltigheten av beslut 2000/520 som har uttryckts i förevarande mål, ska pröva det beslutets giltighet.

129. Det är därvid viktigt att förtydliga att bedömningen av huruvida beslut 2000/520 är giltigt eller ogiltigt ska inskränkas till de anmärkningar som har diskuterats i förevarande mål. Alla aspekter av *safe harbor*-systemets funktionssätt har nämligen inte diskuterats i detta sammanhang, varför det inte förefaller mig möjligt att här göra en uttömmande granskning av detta systems tillkortakommanden.

47 — Punkt 24 i begäran om förhandsavgörande.

48 — Se, bland annat, dom Strehl (62/76, EU:C:1977:18, punkterna 10–17), dom Roquette Frères (145/79, EU:C:1980:234, punkt 6) och dom Schutzverband der Spirituosen-Industrie (C-457/05, EU:C:2007:576, punkterna 32–39).

49 — Dom Schwarze (16/65, EU:C:1965:117, s. 1094).

50 — Se dom Hauer (44/79, EU:C:1979:290, punkt 16).

51 — Se, bland annat, dom CIVAD (C-533/10, EU:C:2012:347, punkterna 39–41 och där angiven rättspraxis).

130. Frågan huruvida de amerikanska underrättelseorganens generella och ospecifika åtkomst till överförda uppgifter kan påverka lagenligheten av beslut 2000/520 har emellertid diskuterats inför domstolen i förevarande mål, varför beslutets giltighet kan prövas ur den synvinkeln.

B – *Giltigheten av beslut 2000/520*

1. Aspekter att beakta vid prövningen av giltigheten av beslut 2000/520

131. Här ska erinras om den rättspraxis som innebär att en rättsakts lagenlighet inom ramen för en talan om ogiltigförklaring ska bedömas med hänsyn till de faktiska och rättsliga omständigheter som förelåg vid den tidpunkt då rättsakten antogs och att kommissionen inte kan lastas för sin bedömning annat än om denna framstår som uppenbart felaktig mot bakgrund av de uppgifter som kommissionen förfogade över när den antog den berörda rättsakten. [52]

132. I sin dom i målet Gaz de France – Berliner Investissement [53] erinrade domstolen vidare om principen att ”den bedömning av en rättsakts giltighet som domstolen har att göra i mål om förhandsavgörande [ska normalt] grundas på den situation som rådde då rättsakten antogs” [54]. Därvid föreföll domstolen emellertid godta att ”en rättsakts giltighet i vissa fall skulle kunna bedömas utifrån nya omständigheter som inträtt efter det att den antogs”. [55]

133. Den öppning som domstolen på detta sätt antydde förefaller mig vara särskilt relevant i förevarande mål.

134. De beslut som kommissionen antar med stöd av artikel 25.6 i direktiv 95/46 uppvisar nämligen särskilda kännetecken. Ett sådant beslut är avsett att vara en bedömning av huruvida skyddsnivån för personuppgifter i ett tredjeland är att betrakta som adekvat eller ej. En sådan bedömning torde komma att variera över tid beroende på de faktiska och rättsliga omständigheterna i tredjelandet.

135. Med tanke på att beslut om adekvat skyddsnivå utgör en särskild kategori av beslut, är det i detta fall nödvändigt att nyansera den regel som säger att ett besluts giltighet endast kan prövas mot bakgrund av de omständigheter som förelåg vid dess antagande. Annars skulle den regeln medföra att det vid domstolens prövning av ett sådant beslut om adekvat skyddsnivås giltighet flera år efter antagandet skulle vara omöjligt att beakta händelser som hade inträffat sedan dess, trots att det inte finns någon begränsning i tiden för en begäran om förhandsavgörande angående giltigheten av rättsakter och trots att det som föranleder en sådan begäran kan vara just händelser som har inträffat sedan beslutet antogs och visar på dettas tillkortakommanden.

136. Kommissionen har i det aktuella fallet låtit beslut 2000/520 förbli i kraft i ungefär 15 år. Detta vittnar om att kommissionen implicit har bekräftat sin bedömning från år 2000. När domstolen inom ramen för en begäran om förhandsavgörande ska pröva giltigheten av en bedömning som kommissionen har låtit förbli gällande över tid, är det därför inte endast möjligt utan också lämpligt att domstolen kan ställa den bedömningen i relation till de nya omständigheter som har tillkommit sedan kommissionsbeslut om adekvat skyddsnivå antogs.

52 — Se, bland annat, dom BVGD/kommissionen (T-104/07 och T-339/08, EU:T:2013:366, punkt 291), där det hänvisas till dom IECC/kommissionen (C-449/98 P, EU:C:2001:275, punkt 87).

53 — C-247/08, EU:C:2009:600.

54 — Punkt 49 och där angiven rättspraxis.

55 — Punkt 50 och där angiven rättspraxis. Se, för ett liknande resonemang, Lenaerts, K., Maselis, I., och Gutman, K., *EU Procedural Law*, Oxford University Press, 2014, där det sägs att ”in certain cases, the validity of the particular Union measure can be assessed by reference to new factors arising after that measure was adopted, depending on the determination of the Court” (punkt 10.16, s. 471).

137. Beslut om adekvat skyddsnivåens särskilda karaktär medför att kommissionen regelbundet ska se över dessa beslut. Om händelser som har inträffat under mellantiden inte föranleder kommissionen att ändra sitt beslut vid en översyn, innebär detta att kommissionen – implicit, men nödvändigtvis – bekräftar sin ursprungliga bedömning. Kommissionen upprepar således på det sättet sitt konstaterande att det berörda tredjelandet garanterar en adekvat skyddsnivå för överförda personuppgifter. Det ankommer på domstolen att bedöma huruvida det fortfarande finns giltig grund för det konstaterandet trots de händelser som sedermera har inträffat.

138. För att beslut av denna typ ska kunna bli föremål för en effektiv domstolskontroll, ska bedömningen av deras giltighet enligt min uppfattning göras mot bakgrund av det rådande faktiska och rättsliga sammanhanget.

2. Begreppet adekvat skyddsnivå

139. Artikel 25 i direktiv 95/46 bygger helt och hållet på principen att överföring av personuppgifter till ett tredjeland får ske endast om det tredjelandet garanterar en adekvat skyddsnivå för sådana uppgifter. Syftet med den artikeln är således att se till att det skydd som direktivet ger vidmakthålls vid överföring av personuppgifter till tredjeländer. Härvid ska det erinras om att nämnda direktiv garanterar unionsmedborgarna en hög skyddsnivå med avseende på behandling av deras personuppgifter.

140. Med tanke på hur viktigt skyddet av personuppgifter är för den grundläggande rätten till respekt för privatlivet, måste en sådan hög skyddsnivå garanteras även i fall där personuppgifter överförs till ett tredjeland.

141. Detta är skälet till att jag anser att kommissionen inte kan konstatera, med stöd av artikel 25.6 i direktiv 95/46, att ett tredjeland garanterar en adekvat skyddsnivå annat än om kommissionen efter en samlad bedömning av det tredjelandets rätt och praxis kan slå fast att detta land garanterar en skyddsnivå som i allt väsentligt är likvärdig med den som garanteras genom nämnda direktiv, även om detta skydd till sina närmare kännetecknen kan skilja sig från vad som allmänt är brukligt inom unionen.

142. Det engelska ordet ”adequate” kan förvisso rent språkligt förstås som att det syftar på en skyddsnivå som är nätt och jämnt tillfredsställande eller tillräcklig, och har således ett annat betydelseomfång än det franska ordet ”adéquat”. Tolkningen av ordet ”adekvat” ska emellertid uteslutande vägledas av det i direktiv 95/46 föreskrivna syftet att uppnå en hög skyddsnivå för de grundläggande rättigheterna.

143. Bedömningen av den skyddsnivå som ett tredjeland garanterar ska avse två huvudsakliga aspekter, nämligen innehållet i de gällande bestämmelserna och instrumenten för att säkerställa att dessa bestämmelser efterlevs. [56]

144. För att *safe harbor*-systemet – som till stor del bygger på att företag som frivilligt deltar i detta system certifierar och kontrollerar sig själva – ska kunna anses uppnå en skyddsnivå som i allt väsentligt är likvärdig med den som råder inom unionen, skulle detta system enligt min uppfattning behöva kompletteras med adekvata garantier och en tillräcklig tillsynsordning. Skyddet vid överföring av personuppgifter till tredjeländer bör nämligen inte vara svagare än skyddet vid behandling inom unionen.

56 — Se s. 5 i kommissionens arbetsdokument WP 12 med rubriken ”Överföring av personuppgifter till tredje land: tillämpning av artiklarna 25 och 26 i EU:s dataskyddsdirektiv”, antaget den 24 juli 1998 av Arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter.

145. Härvid ska det inledningsvis påpekas att den vedertagna uppfattningen inom unionen är att en extern kontrollapparat i form av en oberoende myndighet utgör en nödvändig beståndsdel i varje system som är avsett att garantera efterlevnaden av bestämmelserna om skydd av personuppgifter.

146. Om artikel 25.1–25.3 i direktiv 95/46 inte ska fråntas sin ändamålsenliga verkan är det vidare nödvändigt att beakta att svaret på frågan huruvida skyddsnivån i ett tredjeland är adekvat kan variera över tid och beror på en rad faktorer. Därför måste medlemsstaterna och kommissionen ständigt vara uppmärksamma på varje förändring i omständigheterna som kan föranleda en ny bedömning av huruvida ett tredjeland garanterar en adekvat skyddsnivå. Det är inte möjligt att göra en sådan bedömning av skyddets adekvata nivå en gång för alla och sedan låta denna bedömning gälla på obestämd tid, oberoende av förändringar i omständigheterna som visar att skyddsnivån i själva verket inte längre är adekvat.

147. Kravet på att tredjelandet ska garantera en adekvat skyddsnivå är således en fortgående skyldighet. Även om beslutet förvisso fattas vid en viss specifik tidspunkt kräver vidhållandet av beslutet att det inte finns några omständigheter som har tillkommit sedan tidpunkten för kommissionens ursprungliga bedömning som gör det möjligt att ifrågasätta den bedömningen.

148. Det är viktigt att hålla i minnet att syftet med artikel 25 i direktiv 95/46 är att undvika att personuppgifter överförs till ett tredjeland som inte garanterar en adekvat skyddsnivå, i strid med den grundläggande rätt till skydd av personuppgifter som garanteras i artikel 8 i stadgan.

149. Vidare ska det understrykas att befogenheten att konstatera att ett tredjeland garanterar en adekvat skyddsnivå – vilken unionslagstiftaren genom artikel 25.6 i direktiv 95/46 har tilldelat kommissionen – endast får utövas på det uttryckliga villkoret att tredjelandet i fråga verkligen garanterar en sådan nivå i den mening som avses i artikel 25.2 i direktivet. Om det framkommer nya omständigheter som kan föranleda en ändring av den ursprungliga bedömningen, ska kommissionen ändra sitt beslut med ledning därav.

### 3. Bedömning

150. Jag erinrar om att kommissionen enligt artikel 25.6 i direktiv 95/46, ”i enlighet med det i artikel 31.2 angivna förfarandet, [kan] 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”. Jämförd med artikel 25.2 i samma direktiv innebär artikel 25.6 att kommissionen, för att kunna konstatera att ett tredjeland garanterar en adekvat skyddsnivå, ska göra en samlad bedömning av de gällande rättsreglerna i det berörda tredjelandet och dessas tillämpning.

151. Att kommissionen, trots att det har framkommit nya faktiska och rättsliga omständigheter, har valt att vidmakthålla sitt beslut 2000/520 ska, som jag redan har slagit fast, ses som ett uttryck för kommissionens vilja att bekräfta sin ursprungliga bedömning.

152. Det ankommer inte på domstolen att inom ramen för en begäran om förhandsavgörande bedöma sakomständigheterna i det mål där den nationella domstolen har sett sig föranlåten att begära förhandsavgörande. [57]

57 — Se, bland annat, dom Fallimento Traghetti del Mediterraneo (C-140/09, EU:C:2010:335, punkt 22 och där angiven rättspraxis).

153. Därför kommer jag att utgå från de sakomständigheter som High Court har angett i begäran om förhandsavgörande. Dessa omständigheter har för övrigt till stor del godtagits av kommissionen som fastställda. [58]

154. De argument som inför domstolen har åberopats till stöd för ifrågasättande av kommissionens bedömning att *safe harbor*-systemet garanterar en adekvat skyddsnivå för personuppgifter som överförs från unionen till Förenta staterna kan beskrivas enligt följande.

155. I begäran om förhandsavgörande har High Court utgått från två konstateranden avseende sakomständigheter. Till att börja med har High Court utgått från att personuppgifter, efter att ha överförts av företag som Facebook Ireland till deras moderbolag i Förenta staterna, kan läsas av NSA och andra amerikanska säkerhetsorgan inom ramen för storskalig och ospecifik övervaknings- och uppfångandeverksamhet. Efter Edward Snowdens avslöjanden är detta enligt High Court den enda slutsats som för närvarande är möjlig att dra av den tillgängliga bevisningen. [59] Vidare har High Court utgått från att unionsmedborgare i praktiken inte har någon rätt att yttra sig om att NSA och andra amerikanska säkerhetsorgan övervakar och fångar upp uppgifter om dem. [60]

156. Dessa konstateranden avseende sakomständigheter från High Courts sida får stöd av konstateranden som kommissionen själv har gjort.

157. I sitt ovannämnda meddelande om hur principerna om integritetsskydd (*safe harb*[*o*]*r*) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU, utgick kommissionen exempelvis från konstaterandet att information om omfattningen och räckvidden av amerikanska övervakningsprogram under 2013 hade gett anledning till oro över kontinuiteten i skyddet för personuppgifter som har överförts lagligt till Förenta staterna inom ramen för *safe harbor*-systemet. Kommissionen påpekade därvid att det verkade som om alla företag som deltog i Prism-programmet, och således gav de amerikanska myndigheterna tillgång till uppgifter som lagras och behandlas i Förenta staterna, var *safe harbor*-certifierade. Detta hade enligt kommissionen gjort *safe harbor* -systemet till en av de kanaler genom vilka de amerikanska underrättelseorganen kan samla in personuppgifter som ursprungligen har behandlats inom unionen. [61]

158. Av ovanstående följer att Förenta staternas rätt och praxis gör det möjligt att i stor skala samla in personuppgifter om unionsmedborgare som har överförts inom ramen för *safe harbor*-systemet utan att dessa unionsmedborgare därvid åtnjuter ett effektivt domstolsskydd.

159. Dessa konstateranden avseende sakfrågor visar enligt min uppfattning att beslut 2000/520 inte innehåller tillräckliga garantier. Denna avsaknad av garantier har medfört att nämnda beslut har genomförts på ett sätt som inte uppfyller kraven enligt stadgan och enligt direktiv 95/46.

160. Syftet med ett beslut som kommissionen antar med stöd av artikel 25.6 i direktiv 95/46 är att konstatera att ett tredjeland ”har” en adekvat skyddsnivå. Verbet ”har”, i presens, innebär att ett sådant beslut, för att kunna vidmakthållas, ska avse ett tredjeland som även efter antagandet av nämnda beslut fortsätter att garantera en adekvat skyddsnivå.

161. De åberopade avslöjandena om NSA:s verksamhet och dess användning av uppgifter som har överförts inom ramen för *safe harbor*-systemet har belyst svagheterna i den rättsliga grund som beslut 2000/520 utgör.

58 — Se det meddelande från kommissionen som nämns i fotnot 2 och kommissionens meddelande till Europaparlamentet och rådet om hur principerna om integritetsskydd (*safe harb*[*o*]*r*) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU (COM(2013) 847 final).

59 — Punkt 7 c i begäran om förhandsavgörande.

60 — Punkt 7 b i begäran om förhandsavgörande.

61 — Sid 19 i kommissionens meddelande.

162. De tillkortakommanden som lyfts fram i förevarande mål står i synnerhet att finna i fjärde stycket i bilaga I till det beslutet.

163. Jag erinrar om att det i den bestämmelsen föreskrivs att ”[e]fterlevnaden av [*safe harbor* -]principerna kan begränsas a) till vad som är nödvändigt för att uppfylla krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden eller b) av lagar, myndighetsföreskrifter eller rättspraxis som skapar motstridiga skyldigheter eller ger explicita befogenheter, förutsatt att organisationen då den utövar dessa befogenheter kan visa att avvikelsen från principerna begränsar sig till vad som är nödvändigt för att de övergripande legitima intressen som är beroende av dessa befogenheter skall kunna tillgodoses”.

164. Problemet härrör väsentligen från det sätt på vilket de amerikanska myndigheterna utnyttjar de undantag som föreskrivs i denna bestämmelse. Eftersom dessa undantag är alltför allmänt hållna, begränsas myndigheternas tillämpning av dem inte till vad som är strikt nödvändigt.

165. Till denna alltför allmänt hållna formulering kommer också den omständigheten att unionsmedborgarna inte har tillgång till effektiva rättsmedel i fall där deras personuppgifter behandlas för andra ändamål än de för vilka de ursprungligen samlades in och för vilka de därefter överfördes till Förenta staterna.

166. De undantag från tillämpningen av *safe harbor*-principerna som anges i beslut 2000/520, vilka bland annat motiveras med krav i fråga om nationell säkerhet, borde ha åtföljts av en oberoende tillsynsordning som gjorde det möjligt att förhindra de konstaterade ingreppen i rätten till privatliv.

167. Avslöjandena om de amerikanska underrättelseorganens verksamhet i fråga om generell övervakning av uppgifter överförda inom ramen för *safe harbor*-systemet har alltså belyst vissa tillkortakommanden i beslut 2000/520.

168. De påståenden som har gjorts i förevarande mål kan inte föranleda slutsatsen att Facebook skulle ha brutit mot *safe harbor*-principerna. Om ett certifierat företag som Facebook USA ger de amerikanska myndigheterna åtkomst till uppgifter som har överförts till det företaget från en medlemsstat, kan företaget nämligen anses göra detta för att efterleva den amerikanska lagstiftningen. Med tanke på att en sådan situation uttryckligen är tillåten enligt beslut 2000/520, på grund av den allmänna lydelsen av de undantag som anges i det beslutet, är det i praktiken frågan huruvida sådana undantag är förenliga med unionens primärrätt som är aktuell i förevarande mål.

169. Härvid ska det påpekas att det följer av domstolens fasta praxis att iakttagandet av de mänskliga rättigheterna utgör ett villkor för att unionsrättsakter ska vara lagenliga och att det inom unionen är förbjudet att vidta åtgärder som strider mot de mänskliga rättigheterna. [62]

170. Det följer också av domstolens praxis att överlämnande av insamlade personuppgifter till – privat eller offentlig – tredje part utgör ett ingrepp i rätten till respekt för privatlivet ”oavsett hur de uppgifter som sålunda har lämnats används därefter” [63]. I sin dom i målet Digital Rights Ireland m.fl. [64] slog domstolen vidare fast att om behöriga nationella myndigheter ges rätt att få åtkomst till sådana uppgifter, utgör detta ett ytterligare, separat, ingrepp i denna grundläggande rättighet. [65] Domstolen fann också att alla former av behandling av personuppgifter omfattas av artikel 8 i stadgan och utgör

62 — Se, bland annat, dom Kadi och Al Barakaat International Foundation/rådet och kommissionen (C-402/05 P och C-415/05 P, EU:C:2008:461, punkt 284 och där angiven rättspraxis).

63 — Dom Österreichischer Rundfunk m.fl. (C-465/00, C-138/01 och C-139/01, EU:C:2003:294, punkt 74).

64 — C-293/12 och C-594/12, EU:C:2014:238.

65 — Punkt 35.

ingrepp i rätten till skydd för sådana uppgifter.[66] Den åtkomst som de amerikanska underrättelseorganen åtnjuter till de överförda uppgifterna utgör således också ett ingrepp i den grundläggande rätt till skydd för personuppgifter som garanteras i artikel 8 i stadgan, eftersom en sådan åtkomst ska ses som en behandling av dessa uppgifter.

171. I likhet med vad domstolen konstaterade i den domen, är det aktuella ingreppet långtgående och måste anses som synnerligen grovt, med tanke på det stora antalet berörda användare och den stora mängden överförda uppgifter. Tillsammans med den hemliga karaktären av de amerikanska myndigheternas åtkomst till personuppgifter som har överförts till företag i Förenta staterna gör detta att ingreppet är ytterst allvarligt.

172. Till detta ska läggas att de unionsmedborgare som använder Facebook inte underrättas om att deras personuppgifter kommer att vara generellt åtkomliga för de amerikanska säkerhetsorganen.

173. Vidare ska det framhållas att High Court har konstaterat att unionsmedborgare i praktiken saknar rätt att i Förenta staterna yttra sig om övervakningen och uppfångandet av deras uppgifter. FISC utövar tillsyn, men förfarandet inför FISC är hemligt och inte kontradiktoriskt.[67] Detta utgör som jag ser saken ett ingrepp i unionsmedborgarnas rätt enligt artikel 47 i stadgan till ett effektivt rättsmedel.

174. Det är således fastställt att de undantag från *safe harbor*-principerna som anges i fjärde stycket i bilaga I till beslut 2000/520 utgör ett ingrepp i de grundläggande rättigheter som skyddas genom artiklarna 7, 8 och 47 i stadgan.

175. Nästa steg i bedömningen är att kontrollera huruvida detta ingrepp är motiverat eller ej.

176. Enligt artikel 52.1 i stadgan ska varje begränsning i utövningen av de fri- och rättigheter som erkänns i nämnda stadga vara föreskriven i lag och vara förenlig med det väsentliga innehållet i dessa fri- och rättigheter. Sådana begränsningar får, med beaktande av proportionalitetsprincipen, endast göras om de är nödvändiga och faktiskt svarar mot mål av allmänt samhällsintresse som erkänns av unionen eller mot behovet av skydd för andra människors fri- och rättigheter.

177. Mot bakgrund av dessa villkor för att begränsningar i utövningen av de fri- och rättigheter som skyddas genom stadgan ska kunna godtas, betvivlar jag starkt att de begränsningar som är i fråga i förevarande mål skulle kunna anses vara förenliga med det väsentliga innehållet i artiklarna 7 och 8 i stadgan. De amerikanska underrättelseorganens åtkomst till de överförda uppgifterna förefaller nämligen avse även innehållet i elektroniska kommunikationer, vilket skulle strida mot det väsentliga innehållet i den grundläggande rättigheten till respekt för privatlivet och de övriga rättigheter som stadfästs i artikel 7 i stadgan. Dessutom skulle det, med tanke på att begränsningarna enligt fjärde stycket i bilaga I till beslut 2000/520 är så allmänt hållna att det i princip är möjligt att underlåta att tillämpa samtliga *safe harbor*-principer, kunna anses att dessa begränsningar strider mot det väsentliga innehållet i den grundläggande rätten till skydd av personuppgifter.[68]

178. När det gäller huruvida det konstaterade ingreppet svarar mot ett mål av allmänt samhällsintresse, ska det inledningsvis erinras om att efterlevnaden av *safe harbor*-principerna enligt fjärde stycket b i bilaga I till beslut 2000/520 kan begränsas ”av lagar, myndighetsföreskrifter eller rättspraxis som skapar motstridiga skyldigheter eller ger explicita befogenheter, förutsatt att organisationen då den utövar dessa befogenheter kan visa att avvikelsen från principerna begränsar sig till vad som är nödvändigt för att de övergripande legitima intressen som är beroende av dessa befogenheter skall kunna tillgodoses”.

66 — Punkt 36.

67 — Punkt 7 b i begäran om förhandsavgörande.

68 — Se dom Digital Rights Ireland m.fl. (C-293/12 och C-594/12, EU:C:2014:238, punkterna 39 och 40).

179. De ”legitima intressen” som det hänvisas till i denna bestämmelse preciseras inte närmare. Detta ger upphov till osäkerhet i fråga om – det potentiellt extremt vittomfattande – tillämpningsområdet för detta undantag från de anslutna företagens tillämpning av *safe harbor*-principerna.

180. Detta intryck bekräftas av de förklaringar som ges i avdelning B – med rubriken ”Uttryckliga befogenheter i lag” – i bilaga IV till beslut 2000/520. I synnerhet gäller detta påpekandet att ”amerikanska organisationer, om de i amerikansk lag har en motstridig skyldighet, oberoende av om de anslutit sig till *safe harbor* eller inte, [självklart måste] följa lagen”. Dessutom framhålls det, på tal om explicita befogenheter, att ”målsättningen med *safe harbor* [är] att överbrygga skillnaderna mellan det amerikanska och det europeiska sättet att hantera integritetsskydd, men vi måste respektera den lagstiftande makt våra valda politiska ombud har”.

181. Av detta följer enligt min uppfattning att nämnda undantag strider mot artiklarna 7, 8 och 52.1 i stadgan, eftersom det inte har ett tillräckligt preciserat mål av allmänt samhällsintresse.

182. Det lättvindiga och generella sätt på vilket det anges i fjärde stycket b i bilaga I och i punkt B i bilaga IV till beslut 2000/520 att amerikanska rättsregler kan medföra att det ska ges avkall på *safe harbor*-principerna är under alla omständigheter oförenligt med villkoret att undantag från bestämmelserna om skydd för personuppgifter ska begränsas till vad som är strikt nödvändigt. Nödvändighetsvillkoret nämns förvisso, men utöver att det framgår att det ankommer på det berörda företaget att bedöma huruvida detta villkor är uppfyllt, kan jag inte heller se hur ett företag skulle kunna undandra sig en skyldighet att avstå från att tillämpa *safe harbor*-principerna som följer av rättsregler som företaget är skyldigt att tillämpa.

183. Följaktligen anser jag att beslut 2000/520 ska förklaras ogiltigt, eftersom förekomsten av ett undantag som på ett så allmänt och ospecifikt sätt medger att avsteg görs från *safe harbor*-systemets principer i sig utgör hinder för att det systemet ska kunna anses garantera en adekvat skyddsnivå för personuppgifter som överförs från unionen till Förenta staterna.

184. När det därefter gäller den första kategorin av begränsningar enligt fjärde stycket a i bilaga I till beslut 2000/520, nämligen att efterlevnaden av *safe harbor*-principerna kan begränsas till vad som är nödvändigt för att uppfylla krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden, är det endast det första av dessa ändamål som jag anser vara tillräckligt precist för att kunna utgöra ett av unionen erkänt mål av allmänt samhällsintresse i den mening som avses i artikel 52.1 i stadgan.

185. Nästa steg i bedömningen är att kontrollera huruvida det konstaterade ingreppet är proportionerligt.

186. Härvid ska det erinras om att ”enligt [domstolens fasta] praxis, kräver proportionalitetsprincipen att unionsinstitutionernas åtgärder ska vara ägnade att uppnå de legitima mål som eftersträvas med bestämmelserna i fråga och att de inte går utöver vad som är lämpligt och nödvändigt för att uppnå dessa mål” [69].

187. När domstolsprövningen av huruvida dessa villkor är uppfyllda ”[rör ingrepp i grundläggande rättigheter], kan unionslagstiftarens utrymme för skönsmässig bedömning … vara begränsat på grund av ett antal omständigheter, såsom bland annat det område som berörs, beskaffenheten av den rättighet som garanteras genom stadgan, ingreppets beskaffenhet och allvar samt ingreppets syfte” [70].

69 — Dom Digital Rights Ireland m.fl. (C-293/12 och C-594/12, EU:C:2014:238, punkt 46 och där angiven rättspraxis).

70 — Ibidem (punkt 47 och där angiven rättspraxis).

188. Jag anser att de beslut som kommissionen antar med stöd av artikel 25.6 i direktiv 95/46 kan bli föremål för fullständig kontroll från domstolens sida med avseende på det proportionerliga i kommissionens bedömning av huruvida det skydd som ett tredjeland garanterar ”genom sin interna lagstiftning eller på grund av de internationella förpliktelser som … åligger landet” är av adekvat nivå.

189. Härvid ska det noteras att domstolen i sin dom i målet Digital Rights Ireland m.fl.[71] fann att ”unionslagstiftarens utrymme för skönsmässig bedömning [är] begränsat med hänsyn till den stora betydelse som skyddet för personuppgifter har för den grundläggande rätten till respekt för privatlivet och med hänsyn till det långtgående och allvarliga ingrepp i denna rätt som [det aktuella] direktiv[et] … innebär. Det ska därför göras en strikt kontroll”.[72]

190. Ett sådant ingrepp måste vara ägnat att uppnå det mål som eftersträvas med den aktuella unionsrättsakten och måste vara nödvändigt för att detta mål ska kunna uppnås.

191. Härvid ska det noteras att ”[e]nligt domstolens fasta praxis kräver skyddet av den grundläggande rätten till respekt för privatlivet … att undantag från och begränsningar av skyddet för personuppgifter ska inskränkas till vad som är strängt nödvändigt”[73].

192. I sin kontroll ska domstolen också beakta att ”skyddet för personuppgifter, vilket följer av den uttryckliga skyldigheten i artikel 8.1 i stadgan, är av särskild betydelse för rätten till respekt för privatlivet i artikel 7 i stadgan”[74].

193. Enligt domstolen, som i detta fall hänvisar till praxis från Europeiska domstolen för de mänskliga rättigheterna, måste ”[d]en aktuella unionslagstiftningen … föreskriva tydliga och precisa bestämmelser som reglerar räckvidden och tillämpligheten av den aktuella åtgärden och som slår fast minimikrav, så att de personer vilkas uppgifter har lagrats har tillräckliga garantier som möjliggör ett effektivt skydd av deras personuppgifter mot riskerna för missbruk och otillåten tillgång eller användning”[75]. Domstolen anser i detta sammanhang att ”[n]ödvändigheten av sådana garantier är av än större betydelse när personuppgifterna … är föremål för automatisk behandling och risken för otillåten tillgång till uppgifterna är stor”[76].

194. Jag anser att det råder analogi mellan fjärde stycket a i bilaga I till beslut 2000/520 och artikel 13.1 i direktiv 95/46. I den förstnämnda bestämmelsen anges att efterlevnaden av *safe harbor*-principerna kan begränsas med hänvisning till ”krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden”. I den sistnämnda bestämmelsen föreskrivs att medlemsstaterna genom lagstiftning får vidta åtgärder för att begränsa omfattningen av de skyldigheter och rättigheter som anges i artiklarna 6.1, 10, 11.1, 12 och 21 i nämnda direktiv i fall då en sådan begränsning är en nödvändig åtgärd med hänsyn till bland annat statens säkerhet, försvaret, allmän säkerhet, förebyggande, undersökning eller avslöjande av brott eller åtal för brott.

195. Som domstolen fann i sin dom i målet IPI[77], framgår det av lydelsen av artikel 13.1 i direktiv 95/46 att medlemsstaterna får föreskriva sådana åtgärder som avses i den bestämmelsen endast när detta är nödvändigt. För att en medlemsstat ska få vidta en åtgärd med stöd av nämnda bestämmelse måste åtgärden således vara nödvändig.[78] När det gäller behandling av personuppgifter

71 — C-293/12 och C-594/12, EU:C:2014:238.

72 — Punkt 48.

73 — Dom Digital Rights Ireland (C-293/12 och C-594/12, EU:C:2014:238, punkt 52 och där angiven rättspraxis).

74 — Ibidem (punkt 53).

75 — Ibidem (punkt 54 och där angiven rättspraxis).

76 — Ibidem (punkt 55 och där angiven rättspraxis).

77 — C-473/12, EU:C:2013:715.

78 — Punkt 32.

inom unionen ska de begränsningar som anges i artikel 13 i direktivet förstås så, att de avser en inskränkning till vad som är strikt nödvändigt för att uppnå det eftersträvade målet. Enligt min uppfattning ska detsamma gälla såvitt avser de begränsningar för *safe harbor*-principerna som föreskrivs i fjärde stycket i bilaga I till beslut 2000/520.

196. Nödvändighetskriteriet nämns förvisso inte i alla språkversioner av fjärde stycket a i bilaga I till beslut 2000/520. Bland annat saknas detta kriterium i den franska versionen, som lyder ”[l]’adhésion aux principes peut être limitée par … les exigences relatives à la sécurité nationale, l’intérêt public et le respect des lois des États-Unis”, medan det exempelvis i den spanska, den tyska och den engelska versionen anges att de begränsningar som införs måste vara nödvändiga för att uppnå de aktuella målen.

197. Oaktat detta framgår det tydligt av de faktiska omständigheter som High Court har åberopat, och som kommissionen har hänvisat till i sina ovannämnda meddelanden, att tillämpningen av dessa begränsningar i praktiken inte inskränker sig till vad som är strikt nödvändigt för att uppnå de eftersträvade målen.

198. De amerikanska underrättelseorganens åtkomst till överförda personuppgifter omfattar nämligen generellt samtliga personer och samtliga elektroniska kommunikationsmedel liksom samtliga överförda uppgifter, inbegripet innehållet i meddelanden, helt utan åtskillnad, begränsningar eller undantag utifrån det mål av allmänt samhällsintresse som eftersträvas. [79]

199. De amerikanska underrättelseorganens åtkomst till överförda uppgifter omfattar i själva verket samtliga personer som använder elektroniska kommunikationstjänster, utan att det ställs något krav på att de berörda personerna ska utgöra ett hot mot den nationella säkerheten. [80]

200. En sådan storskalig och ospecifik övervakning är redan till sin natur oproportionerlig och utgör ett omotiverat ingrepp i de rättigheter som garanteras genom artiklarna 7 och 8 i stadgan.

201. Att det är omöjligt för unionslagstiftaren eller medlemsstaterna att anta lagbestämmelser som i strid med stadgan föreskriver en storskalig och ospecifik övervakning medför – som parlamentet på goda grunder har framhållit i sitt yttrande – med nödvändighet att det inte heller under några som helst omständigheter kan vara möjligt att ett tredjeland anses garantera en adekvat skyddsnivå för unionsmedborgarnas personuppgifter när det tredjelandets lagstiftning i praktiken tillåter att sådana uppgifter övervakas och uppfångas i stor skala och på ett ospecifikt sätt.

202. Dessutom ska det understrykas att *safe harbor*-systemet såsom detta definieras i beslut 2000/520 inte innehåller några garantier som är ägnade att förhindra storskalig och generell åtkomst till överförda uppgifter.

203. I sin dom i målet Digital Rights Ireland m.fl. [81] framhöll domstolen vikten av att föreskriva ”tydliga och precisa regler som reglerar räckvidden av ingreppet i de grundläggande rättigheter som är stadfästa i artiklarna 7 och 8 i stadgan” [82]. Ett sådant ingrepp måste enligt domstolen vara ”noggrant avgränsat genom bestämmelser som gör det möjligt att säkerställa att det verkligen är begränsat till vad som är

79 — Se, analogt, dom Digital Rights Ireland m.fl. (C-293/12 och C-594/12, EU:C:2014:238, punkt 57 och där angiven rättspraxis).

80 — Ibidem (punkterna 58 och 59).

81 — C-293/12 och C-594/12, EU:C:2014:238.

82 — Punkt 65.

strängt nödvändigt”[83]. I nämnda dom betonade domstolen också behovet av att föreskriva sådana ”tillräckliga garantier som krävs enligt artikel 8 i stadgan, vilka gör det möjligt att säkerställa ett effektivt skydd av [person]uppgifterna mot riskerna för missbruk och otillåten tillgång eller användning”[84].

204. Det måste konstateras att de privata klagomålsförfarandena och FTC, i och med att dess roll är begränsad till tvister av kommersiell art, inte kan utnyttjas för att ifrågasätta de amerikanska underrättelseorganens åtkomst till personuppgifter som har överförts från unionen.

205. FTC:s behörighet avser illojala eller bedrägliga handlingar och metoder i handeln och omfattar således inte insamling och användning av personuppgifter för ändamål som inte har med handel att göra.[85] Att FTC:s behörighetsområde är begränsat på detta sätt inskränker enskilda personers rätt till skydd för sina personuppgifter. Syftet med inrättandet av FTC var inte – som är fallet med de nationella tillsynsmyndigheterna i unionen – att skydda enskildas rätt till privatliv, utan att garantera konsumenterna en lojal och tillförlitlig handel. Denna omständighet begränsar *de facto* FTC:s förmåga att ingripa i frågor som rör skydd av personuppgifter. FTC har således inte en roll som är jämförbar med den som spelas av de nationella tillsynsmyndigheter som avses i artikel 28 i direktiv 95/46.

206. De unionsmedborgare vilkas uppgifter har överförts kan vända sig till specialiserade organ för klagomålshantering i Förenta staterna, exempelvis TRUSTe och BBBOnline, och begära närmare upplysningar om huruvida det företag som innehar deras personuppgifter bryter mot villkoren för systemet med självcertifiering. De privata klagomålsförfaranden som erbjuds av organ som TRUSTe kan emellertid inte avse ingrepp i rätten till skydd av personuppgifter som begås av andra organ eller myndigheter än självcertifierade företag. Dessa organ för klagomålshantering saknar helt behörighet att pröva frågor som rör lagenligheten av amerikanska underrättelseorgans verksamhet.

207. Både FTC och organen för klagomålshantering saknar således behörighet att pröva möjliga överträdelser av principerna för skydd av personuppgifter som begås av offentliga aktörer, såsom de amerikanska säkerhetsorganen. En sådan behörighet vore emellertid helt nödvändig för att rätten till ett effektivt skydd av sådana uppgifter skulle kunna garanteras fullt ut. Kommissionen saknade följaktligen grund för att konstatera, genom att anta beslut 2000/520 och genom att låta detta förbli i kraft, att det för samtliga personuppgifter som överförs till Förenta staterna föreligger ett adekvat skydd av rätten enligt artikel 8.3 i stadgan, det vill säga att det finns en oberoende myndighet som på ett effektivt sätt kontrollerar att kraven på skydd och säkerhet i fråga om dessa uppgifter efterlevs.

208. Det måste således konstateras att det inom ramen för det *safe harbor*-system som avses i beslut 2000/520 saknas en oberoende myndighet som kan kontrollera att tillämpningen av undantagen från *safe harbor*-principerna begränsas till vad som är strikt nödvändigt. Enligt unionsrätten utgör, som har påtalats ovan, en sådan tillsyn som utövas av en oberoende myndighet en grundläggande beståndsdel i skyddet för enskilda personer med avseende på behandling av personuppgifter.[86]

209. Härvid ska den roll som de nationella tillsynsmyndigheterna spelar i det system för skydd av personuppgifter som tillämpas inom unionen när det gäller att kontrollera de begränsningar som föreskrivs i artikel 13 i direktiv 95/46 framhållas. Enligt artikel 28.4 andra stycket i det direktivet kan ”[v]ar och en … i samband med tillämpningen av de nationella bestämmelser som har antagits med stöd av artikel 13 i detta direktiv till tillsynsmyndigheten ge in en begäran om att få kontrollera om en

83 — Ibidem.

84 — Ibidem (punkt 66).

85 — Se FoS 11 i bilaga II till beslut 2000/520, under rubriken ”Åtgärder från den federala konkurrensmyndighetens sida”, och bilagorna III, V och VII till nämnda beslut.

86 — Se dom Digital Rights Ireland m.fl. (C-293/12 och C-594/12, EU:C:2014:238, punkt 68 och där angiven rättspraxis).

behandling är tillåten”. Analogt borde det, med koppling till omnämnandet i fjärde stycket i bilaga I till beslut 2000/520 av begränsningar för tillämpningen av *safe harbor*-principerna, enligt min uppfattning ha inrättats en ordning för tillsyn som ombesörjdes av en oberoende myndighet specialiserad på skydd av personuppgifter.

210. Ingripanden av oberoende tillsynsmyndigheter är ett centralt inslag i det europeiska systemet för skydd av personuppgifter. Det är därför naturligt att förekomsten av sådana myndigheter redan från början har setts som ett av de villkor som måste vara uppfyllda för att nivån på det skydd som ett tredjeland garanterar ska kunna anses vara adekvat. Det rör sig således om ett villkor som måste vara uppfyllt för att överföring av uppgifter från medlemsstaterna till tredjeländer inte ska vara förbjuden enligt artikel 25 i direktiv 95/46.[87] Som påpekas i ett diskussionsunderlag framtaget av den arbetsgrupp som inrättas genom artikel 29 i direktivet, råder det i Europa bred enighet om att ”ett system med ’extern tillsyn’ genom en oberoende myndighet är ett nödvändigt inslag i en ordning för att säkerställa att bestämmelserna om skydd av personuppgifter efterlevs”[88].

211. Vidare erbjuder FISC inte någon effektiv möjlighet till rättslig prövning för unionsmedborgare vilkas personuppgifter har överförts till Förenta staterna. Det skydd mot övervakning från statliga myndigheter som ges inom ramen för section 702 i 1978 års lag om övervakning av utländska underrättelsetjänster tillämpas nämligen uteslutande på amerikanska medborgare och på utländska medborgare som är lagligen och varaktigt bosatta i Förenta staterna. Som kommissionen själv har påpekat, skulle tillsynen över de amerikanska programmen för insamling av underrättelseinformation kunna förbättras genom en förstärkt roll för FISC och genom införande av möjligheter till rättslig prövning för enskilda. Detta skulle kunna minska behandlingen av personuppgifter om unionsmedborgare som saknar betydelse för skyddet av den nationella säkerheten.[89]

212. Kommissionen har dessutom själv framhållit att unionsmedborgare saknar möjlighet att få tillgång till, rätta eller radera uppgifter liksom möjlighet till administrativ eller rättslig prövning med avseende på insamling och vidare behandling av deras personuppgifter som sker inom ramen för amerikanska övervakningsprogram.[90]

213. Avslutningsvis ska det också nämnas att det kan förekomma att de amerikanska bestämmelserna om skydd för privatlivet tillämpas olika på amerikanska medborgare och på utländska medborgare.[91]

214. Av det ovan anförda följer att det i beslut 2000/520 inte föreskrivs några tydliga och precisa regler som reglerar räckvidden av ingreppet i de grundläggande rättigheter som stadfästs i artiklarna 7 och 8 i stadgan. Det måste därför konstateras att nämnda beslut och det sätt på vilket detta tillämpas innebär ett ingrepp i dessa grundläggande rättigheter som är långtgående och synnerligen allvarligt, utan att detta ingrepp är noggrant avgränsat genom bestämmelser som gör det möjligt att säkerställa att det verkligen är begränsat till vad som är strikt nödvändigt.

215. Genom att anta beslut 2000/520 och därefter låta det förbli i kraft, har kommissionen följaktligen överskridit de begränsningar som följer av proportionalitetsprincipen såvitt avser artiklarna 7, 8 och 52.1 i stadgan. Till detta ska läggas att kommissionen därigenom också har gjort sig skyldig till ett omotiverat ingrepp i unionsmedborgarnas rätt till ett effektivt rättsmedel enligt artikel 47 i stadgan.

87 — Se Poullet, Y., ”L’autorité de contrôle: ’vues’ de Bruxelles”, *Revue française d’administration publique*, nr 89, januari–mars 1999, s. 69, särskilt s. 71.

88 — Se s. 6 i kommissionens arbetsdokument WP 12, som nämns i fotnot 56.

89 — Sidorna 10 och 11 i det meddelande från kommissionen som nämns i fotnot 2.

90 — Se punkt 7.2, s. 20 i det meddelande från kommissionen som nämns i fotnot 58.

91 — Se, såvitt avser denna fråga, Kuner, C., ”Foreign Nationals and Data Protection Law: A Transatlantic Analysis”, *Data Protection Anno 2014: How To Restore Trust*? Intersentia, Cambridge, 2014, s. 213, särskilt s. 216 och följande sidor.

216. Nämnda beslut ska därför förklaras ogiltigt, eftersom de ovan beskrivna kränkningarna av grundläggande rättigheter medför att det inte är möjligt att anse att det *safe harbor*-system som införs genom beslutet garanterar en adekvat skyddsnivå för personuppgifter som inom ramen för det systemet överförs från unionen till Förenta staterna.

217. Jag anser att kommissionen, när den konstaterade att unionsmedborgarnas grundläggande rättigheter kränktes på det ovan beskrivna sättet, tills vidare borde ha upphört att tillämpa beslut 2000/520.

218. Det beslutet gäller på obestämd tid. Förevarande mål visar emellertid att svaret på frågan huruvida skyddsnivån i ett tredjeland är adekvat kan ändras över tid, beroende på förändringar i de faktiska och rättsliga omständigheter som låg till grund för beslutet.

219. Beslut 2000/520 innehåller också bestämmelser som ger kommissionen möjlighet att anpassa beslutet efter omständigheterna.

220. Av skäl 9 i beslutet framgår exempelvis att ”[s]ystemet med *safe harbor* sådant det utformats enligt principerna och FoS kan behöva ses över i ljuset av erfarenheter från utveckling på integritetsskyddets område under förhållanden då tekniken ständigt gör det lättare att överföra och behandla personuppgifter och i ljuset av rapporter om genomförande av berörda tillsynsmyndigheter”.

221. Enligt artikel 3.4 i nämnda beslut gäller vidare att ”[o]m den information som inhämtats i enlighet med punkterna 1, 2 och 3 visar att någon av de myndigheter som har ansvar för att principerna tillämpade i överensstämmelse med FoS följs i Förenta staterna inte fullgör denna uppgift på ett effektivt sätt, skall kommissionen underrätta Förenta staternas handelsministerium om detta och vid behov lägga fram förslag till bestämmelser … i syfte att helt eller tills vidare upphäva detta beslut eller begränsa dess tillämpningsområde”.

222. Dessutom kan beslut 2000/520, enligt artikel 4.1 i detta, ”vid vilken tidpunkt som helst ändras på grundval av erfarenheter i samband med beslutets genomförande och/eller om det i Förenta staternas lagstiftning ställs krav på minst samma skyddsnivå, som den som uppnås genom principerna och FoS. Kommissionen skall under alla omständigheter utvärdera tillämpningen av detta beslut på grundval av tillgänglig information tre år efter det att beslutet delgivits medlemsstaterna och skall underrätta den kommitté som inrättats genom artikel 31 i direktiv [95/46] om alla iakttagelser av betydelse, däribland omständigheter som kan påverka den gjorda bedömningen att bestämmelserna i artikel 1 i detta beslut ger ett adekvat skydd i den mening som avses i artikel 25 i direktiv [95/46]”. Enligt artikel 4.2 i beslut 2000/520 ska vidare ”[k]ommissionen … om så behövs föreslå åtgärder i enlighet med det förfarande som föreskrivs i artikel 31 i direktivet”.

223. Kommissionen har i sitt yttrande påpekat att det är ”mycket sannolikt att efterlevnaden av *safe harbor*-principerna har inskränkts på ett sätt som inte längre motsvarar de strikt avgränsade villkoren för det föreskrivna undantaget i fråga om nationell säkerhet” [92]. I detta sammanhang anser kommissionen att de aktuella avslöjandena visar på storskalig och godtycklig övervakning i en omfattning som inte är förenlig med det nödvändighetskriterium som föreskrivs för detta undantag och inte heller, mer allmänt, med den rätt till skydd för personuppgifter som stadfästs i artikel 8 i stadgan. [93] Dessutom har kommissionen i annat sammanhang konstaterat att ”[r]äckvidden av … övervakningsprogram[men], i kombination med ojämlik behandling av [unions]medborgare, medför att den skyddsnivå som erbjuds genom [*safe harbor*]-systemet måste ifrågasättas” [94].

92 — Punkt 44.

93 — Ibidem.

94 — Se sid 5 i det meddelande från kommissionen som nämns i fotnot 2.

224. Vidare medgav kommissionen under den muntliga förhandlingen uttryckligen att det inom ramen för beslut 2000/520, såsom detta för närvarande tillämpas, inte finns någon garanti för att unionsmedborgarnas rätt till skydd för sina uppgifter säkerställs. Detta konstaterande är emellertid enligt kommissionens uppfattning inte av den arten att det gör nämnda beslut ogiltigt. Kommissionen håller förvisso med om att den ska agera när det framkommer nya omständigheter, men den anser sig ha vidtagit lämpliga och proportionerliga åtgärder genom att inleda förhandlingar med Förenta staterna i syfte att reformera *safe harbor*-systemet.

225. Jag delar inte den åsikten. Under tiden som förhandlingarna pågår, bör överföringar av personuppgifter till Förenta staterna nämligen tillfälligt kunna förbjudas på initiativ av de nationella tillsynsmyndigheterna eller med anledning av klagomål som kommer in till dessa.

226. Dessutom anser jag att kommissionen, när den gjorde de aktuella konstaterandena, tills vidare borde ha upphört att tillämpa beslut 2000/520. Det mål om skydd av personuppgifter som eftersträvas genom direktiv 95/46 och artikel 8 i stadgan medför nämligen skyldigheter inte endast för medlemsstaterna utan även för unionens institutioner, enligt vad som framgår av artikel 51.1 i stadgan.

227. I samband med sin bedömning av skyddsnivån i ett tredjeland ska kommissionen granska inte endast det tredjelandets inhemska lagstiftning och internationella åtaganden, utan även det sätt på vilket skyddet av personuppgifter säkerställs i praktiken. Om granskningen av den praktiska tillämpningen visar på brister i funktionen, ska kommissionen reagera och i förekommande fall utan dröjsmål tills vidare upphöra att tillämpa beslutet eller ändra det.

228. Som har framgått av resonemanget ovan, består den skyldighet som åvilar medlemsstaterna huvudsakligen i att de via sina nationella tillsynsmyndigheter ska se till att bestämmelserna i direktiv 95/46 följs.

229. Den skyldighet som åvilar kommissionen är att, i fall där det kan konstateras att ett tredjeland har åsidosatt sina skyldigheter, tills vidare upphöra att tillämpa ett beslut som den har antagit med stöd av artikel 25.6 i nämnda direktiv medan den förhandlar med det tredjelandet i syfte att få ett slut på åsidosättandena.

230. Syftet med beslut som kommissionen antar med stöd av nämnda bestämmelse är ju att konstatera att ett tredjeland ”har” en adekvat skyddsnivå för personuppgifter som överförs till det tredjelandet. Verbet ”har”, i presens, innebär att ett sådant beslut kan vidmakthållas endast om det berörda tredjelandet även efter antagandet av beslutet fortsätter att garantera en sådan adekvat skyddsnivå.

231. I skäl 57 i direktiv 95/46 anges att ”[o]m ett tredje land inte garanterar en adekvat skyddsnivå skall överföring av personuppgifter till det landet förbjudas”.

232. I artikel 25.4 i samma direktiv stadgas att ”[o]m kommissionen i enlighet med ett sådant förfarande som beskrivs i artikel 31.2 finner att ett tredje land inte erbjuder en sådan adekvat skyddsnivå som beskrivs i punkt 2 i denna artikel, skall medlemsstaterna vidta de åtgärder som är nödvändiga för att hindra överföring av uppgifter av samma slag till ifrågavarande tredje land”. Dessutom föreskrivs det i artikel 25.5 i nämnda direktiv att kommissionen ”[v]id lämpligt tillfälle skall … inleda förhandlingar för att avhjälpa den situation som uppstått när kommissionen kommit till den slutsats som anges i punkt 4”.

233. Av den sistnämnda bestämmelsen följer att förhandlingar med ett tredjeland som förs inom ramen för det system som införs genom artikel 25 i direktiv 95/46 syftar till att avhjälpa en avsaknad av adekvat skyddsnivå som har konstaterats i enlighet med det förfarande som anges i artikel 31.2 i direktivet. I förevarande fall har kommissionen inte formellt konstaterat, i enlighet med det förfarandet, att *safe harbor*-systemet inte längre garanterar en adekvat skyddsnivå. Trots detta var skälet till att kommissionen beslutade att inleda förhandlingar med Förenta staterna just att den dessförinnan hade kommit fram till att skyddsnivån i det tredjelandet inte längre var adekvat.

234. Kommissionen kände således till att tillämpningen av beslut 2000/520 inte fungerade som den skulle, men underlät ändå att upphöra att tillämpa det beslutet tills vidare eller att ändra det. Detta ledde till att ingreppet i de grundläggande rättigheterna för de personer vilkas personuppgifter har överförts och fortfarande överförs inom ramen för *safe harbor*-systemet kom att fortsätta.

235. Domstolen har – förvisso i ett annat sammanhang – redan tidigare funnit att det åligger kommissionen att se till att bestämmelser ändras i linje med nya insikter. [95]

236. En sådan underlåtenhet att agera från kommissionens sida som direkt undergräver de grundläggande rättigheter som skyddas genom artiklarna 7, 8 och 47 i stadgan utgör enligt min uppfattning ytterligare ett skäl till att förklara beslut 2000/520 ogiltigt inom ramen för förevarande begäran om förhandsavgörande. [96]

## III – **Förslag till avgörande**

237. Mot bakgrund av det ovan anförda föreslår jag att domstolen ska besvara High Courts frågor på följande sätt:

Artikel 28 i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter, jämförd med artiklarna 7 och 8 i Europeiska unionens stadga om de grundläggande rättigheterna, ska tolkas så, att förekomsten av ett beslut som Europeiska kommissionen har antagit med stöd av artikel 25.6 i direktiv 95/46 inte hindrar en nationell tillsynsmyndighet från att utreda ett klagomål i vilket det görs gällande att ett tredjeland inte garanterar en adekvat skyddsnivå för överförda personuppgifter och inte heller från att i förekommande fall tillfälligt förbjuda överföringen av dessa uppgifter.

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

95 — Se, för ett liknande resonemang, dom Agrarproduktion Staebelow (C-504/04, EU:C:2006:30, punkt 40).

96 — Domstolen fann förvisso i sin dom i målet T. Port (C-68/95, EU:C:1996:452) att ”fördraget inte innehåller några bestämmelser som gör det möjligt för en nationell domstol att vända sig till domstolen med en begäran om att denna skall meddela ett förhandsavgörande om en institutions passivitet” (punkt 53), men domstolen förefaller ha ställt sig mer positiv till denna möjlighet i sin dom i målet Ten Kate Holding Musselkanaal m.fl. (C-511/03, EU:C:2005:625, punkt 29).