



Datum van
inontvangstneming

:

26/08/2014

Zaak C-362/14

Verzoek om een prejudiciële beslissing

Datum van indiening:

25 juli 2014

Verwijzende rechter:

High Court of Ireland (Ierland)

Datum van de verwijzingsbeslissing:

17 juli 2014

Verzoekende partij:

Maximillian Schrems

Verwerende partij:

Data Protection Commissioner

DE HIGH COURT

(Omissis)

In de zaak tussen

MAXIMILLIAN SCHREMS

(Omissis)

EN

DATA PROTECTION COMMISSIONER

(Omissis)

VERZOEK OM EEN PREJUDICIELE BESLISSING

ARTIKEL 267 VWEU

(Omissis)

Hierbij verzoekt de High Court of Ireland (omissis) het Hof van Justitie (hierna: „het Hof”) krachtens artikel 267 VWEU om een prejudiciële beslissing aangaande de in punt 22 hierna uiteengezette vragen.

[OR. 1]

Inleiding

- 1 De prejudiciële vragen zijn gerezen in een hoger beroepsprocedure voor de High Court waarin verzoeker, van Oostenrijkse nationaliteit, opkomt tegen het besluit van de Data Protection Commissioner (verweerder; hierna „Commissioner”) om krachtens artikel 10, lid 1, sub b, van de Data Protection Act 1988 (wet op de gegevensbescherming; hierna: „wet van 1988”) zijn klacht niet in behandeling te nemen. (Omissis).
- 2 Alle gebruikers in Europa van het grootste sociale netwerk, Facebook, dienen een overeenkomst te ondertekenen met Facebook Ireland Ltd (hierna: „Facebook Ireland”). In dat opzicht is Facebook Ireland onderworpen aan de bevoegdheid van de Commissioner uit hoofde van de Ierse wetgeving inzake gegevensbescherming. Facebook Ireland is een dochteronderneming van de in de Verenigde Staten gevestigde onderneming Facebook Inc. (hierna: „Facebook”). Schrems is sinds 2008 gebruiker van dit sociale netwerk geweest. Sommige of alle gegevens die verband houden met Facebookgebruikers binnen de Europese Unie/Europese Economische Ruimte worden in de praktijk doorgezonden naar en bewaard op servers die zich fysiek in de Verenigde Staten bevinden.
- 3 De klacht die Schrems op 25 juni 2013 indiende bij de Commissioner, kwam er in wezen op neer dat, in het licht van de onthullingen sinds mei 2013 van Edward Snowden over de activiteiten van de National Security Agency (nationale veiligheidsdienst; hierna: „NSA”) van de Verenigde Staten, de wetgeving en de praktijk in de Verenigde Staten (hierna ook: „VS”) geen effectieve bescherming boden op het punt van de toegang tot de aldus aan de VS doorgezonden gegevens.
- 4 Bij brieven van 25 en 26 juli 2013 maakte de Commissioner gebruik van zijn bevoegdheid onder artikel 10, lid 1, sub a, van de wet van 1988 om deze klacht niet nader te onderzoeken op de grond dat deze „lichtzinnig en onredelijk” („frivolous and vexatious”) was (omissis). Naar Iers recht en in dit specifieke wettelijke kader wordt met deze uitdrukking eenvoudig bedoeld dat de Commissioner meende dat de klacht rechtens ongegrond was. Met name moeten hieraan niet de door verzoeker aangevoerde andere betekenissen worden verbonden (omissis).

[OR. 2-3]

- 5 De Commissioner kwam tot dit oordeel op de grond dat i) er geen bewijzen waren dat de NSA (of andere veiligheidsdiensten van de VS) zich toegang had verschaft

tot de persoonsgegevens van Schrems (ontbreken van procesbelang), zodat de klacht louter hypothetisch en speculatief van aard was, en ii) de Europese Commissie in haar beschikking van 26 juli 2000 (2000/520/EG) overeenkomstig richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door de Veiligheidsbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende vaak gestelde vragen, die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd (PB L 215, blz. 7; hierna: „Veiligheidsbeschikking”) heeft vastgesteld dat de Verenigde Staten „worden geacht een passend beschermingsniveau te waarborgen voor (...) persoonsgegevens” in overeenstemming met artikel 25, lid 6, van richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB L 281, blz. 31; hierna: „richtlijn 95/46”). De Commissioner tekende aan dat de Veiligheidsbeschikking een „communautair besluit” was in de zin van artikel 11, lid 2, sub a, van de wet van 1988, zodat naar Iers recht ieder vraagstuk omtrent de toereikendheid van de gegevensbescherming in een derde land (in dit geval, de Verenigde Staten) waaraan gegevens worden doorgegeven, moet worden beslist „in overeenstemming met dat besluit”. Aangezien de klacht van verzoeker nu juist hierop betrekking had – dat persoonsgegevens werden doorgegeven naar een derde land waar zulke normen in de praktijk niet golden – stelde de Commissioner zich op het standpunt dat de aard van de Veiligheidsbeschikking een onderzoek naar die vraag uitsloot.

Het ontbreken van procesbelang

- 6 Volgens de Commissioner had Schrems geen belang bij de indiening van zijn klacht. Aangezien hij niet kon aantonen dat de NSA zich toegang tot zijn persoonsgegevens had verschaft, werd de klacht in wezen hypothetisch en speculatief geacht. [De High Court] aanvaardde (omissis) dat Schrems weliswaar niet kon zeggen of de autoriteiten van de VS zich ooit toegang tot zijn eigen persoonsgegevens hadden verschaft of dat op deze wijze zouden doen, maar dat zelfs wanneer dit onwaarschijnlijk geacht zou worden, hij „zeker gerechtigd was bezwaar te maken tegen een situatie waarin zijn gegevens worden doorgegeven naar een rechtsgebied dat, hoe men het ook bekijkt, slechts een beperkte bescherming lijkt te bieden tegen bemoeienis van de veiligheidsdiensten van de VS met die gegevens”. [De High Court] verwierp daarom de exceptie van ontbreken van procesbelang.

[OR. 3]

Beoordeling van het bewijs en vaststelling van de feiten

- 7 [De High Court] heeft met betrekking tot het onderscheppen van persoonsgegevens de volgende feiten als vaststaand aangenomen:
- a) Het langs elektronische weg volgen en onderscheppen van communicaties op de in de wet bepaalde wijze dient noodzakelijke en onontbeerlijke doelstellingen van algemeen belang, te weten de handhaving het bewaren van de nationale veiligheid en het voorkomen van ernstige criminaliteit. Het volgen en onderscheppen van persoonsgegevens die zijn doorgegeven van de Europese Unie („Unie”) aan de VS door de NSA (en andere vergelijkbare instanties, zowel in de VS als elders) dient legitieme en noodzakelijke doeleinden van terrorismebestrijding.
 - b) De onthullingen van Edward Snowden tonen echter aan dat die autoriteiten hierin veel te ver gingen. Weliswaar oefent de Foreign Intelligence Services Court (gerecht voor de beoordeling van verzoeken betreffende buitenlandse inlichtingendiensten) in de VS enig toezicht uit, maar dit dient voornamelijk de administratie en vindt plaats in het geheim. Burgers van de Unie beschikken in feite niet over een recht om gehoord te worden over het volgen en onderscheppen van hun gegevens en bovendien worden besluiten over de toegang tot zulke gegevens niet genomen op basis van het Unierecht.
 - c) Hoewel er tot op zekere hoogte verschil van mening bestaat over de reikwijdte en de omvang van sommige van de programma’s (die het volgen van gegevens betreffen) betwist kan worden, wordt uit de uitgebreide dossiers met bewijsstukken die in de onderhavige procedure zijn overgelegd duidelijk dat dit niet geldt voor de juistheid van een groot deel van de onthullingen van Snowden. [De High Court] constateerde dan ook dat de NSA (en andere federale instanties zoals de Federal Bureau of Investigation) toegang tot onder meer de door bedrijven als Facebook Ireland aan haar moederonderneming in de Verenigde Staten doorgegeven persoonsgegevens kunnen verkrijgen in het kader van een programma waaronder zulke gegevens op massale schaal zonder enige differentiatie worden gevolgd en onderschept. Na de onthullingen van Snowden liet het beschikbare bewijsmateriaal zelfs geen andere realistische conclusie toe (omissis).
 - d) Zowel Facebook als Facebook Ireland heeft zelfcertificeringsbrieven afgegeven in overeenstemming met de Veiligheidsbeschikking.

[OR. 4]

Nationaal recht

- 8 De nationale Ierse wet verbiedt het doorgeven van persoonsgegevens naar het buitenland, behalve wanneer de andere staat „met betrekking tot de verwerking van persoonsgegevens, met inachtneming van alle omstandigheden van die doorgifte, een passende bescherming van de privacy en de fundamentele rechten en vrijheden van betrokkenen waarborgt”. [De High Court] stelde vast dat het hier gaat om een verwijzing naar de maatstaven van de Ierse grondwet van 1937 (omissis).
- 9 Zodra een overheidsinstantie zich toegang verschafft tot privécommunicaties door deze te volgen of te onderscheppen, is volgens het Ierse recht het constitutionele recht op privacy in het geding. Voorts is de toegang van overheidsinstanties tot privécommunicaties vanuit de woning – of dit nu gaat om toegang tot telefoongesprekken, internetgebruik of privépost – een duidelijke inbreuk op de onschendbaarheid van de woning, die wordt gewaarborgd in artikel 40, lid 5, van de Ierse grondwet (omissis).
- 10 [De High Court] oordeelde voorts dat de enkele omstandigheid dat deze rechten in het geding zijn, niet betekent dat het onderscheppen van communicaties door overheidsinstanties per definitie of altijd onwettig is. De preambule van de Ierse grondwet spreekt van een „werkelijke sociale orde” waarin de „waardigheid en de vrijheid van het individu verzekerd wordt”, zodat zowel vrijheid als veiligheid op waarde geschat worden. [De High Court] oordeelde dat het langs elektronische weg volgen en onderscheppen van communicaties in een moderne samenleving onontbeerlijk is voor de handhaving van de staatsveiligheid. Het achtte het dan ook duidelijk dat wetgeving van deze algemene aard ten dienste staat van belangrijke, en zelfs essentiële en onontbeerlijke doeleinden en belangen van de staat, zoals ook blijkt uit het arrest van het Duitse Constitutionele Hof (Bundesverfassungsgericht) inzake de database tegen het terrorisme [arrest van 24 april 2013, „Antiterrordatei” – 1 BvR 1215/07] (omissis) en de overwegingen van het Hof in zijn arrest van 8 april 2014, Digital Rights Ireland Ltd (gevoegde zaken C-293/12 en C-594/12, punten 42 tot en met 44).

[OR. 5]

- 11 [De High Court] oordeelde voorts dat het belang van deze constitutionele rechten niettemin zodanig is dat ieder ingrijpen in de genoemde privacyrechten moet berusten op de wet en tevens proportioneel moet zijn. Dit geldt in het bijzonder met betrekking tot het onderscheppen en volgen van communicaties binnen de woning. Ook al hoeft de in artikel 40, lid 5, van de grondwet voor de privacy van de woning gebruikte term „onschendbaar” niet helemaal letterlijk te worden genomen (in de zin dat het recht niet absoluut is noch aan geen enkele beperking kan onderworpen), geeft de verwijzing naar onschendbaarheid in dit verband toch wel aan dat de woning het hoogste beschermingsniveau geniet dat in een democratische samenleving redelijkerwijs kan worden verleend.

- 12 [De High Court] oordeelde vervolgens dat de massale en ongedifferentieerde toegang tot persoonsgegevens die wellicht juist hun oorsprong binnen de woning hebben – zoals e-mails, sms'en, internetgebruik en telefoongesprekken – een toetsing op enkel deze grond aan het evenredigheidsbeginsel of aan de grondwet niet zou doorstaan. De kans op misbruik in zulke gevallen is enorm en het gevaar bestaat zelfs dat geen enkel aspect van het huiselijk of privéleven veilig zou zijn voor de onderzoekende blik van de staat. Een dergelijke situatie zou volstrekt indruisen tegen de grondslagen en de fundamentele waarden van de grondwet: eerbied voor de menselijke waardigheid en de vrijheid van het individu (genoemd in de preambule van de grondwet); de persoonlijke integriteit (artikel 40, lid 3, ten eerste en ten tweede); de onschendbaarheid van de woning (artikel 40, lid 5) en de bescherming van het gezinsleven (artikel 41). Met een beroep op oudere Ierse rechtspraak merkte [de High Court] op dat artikel 40, lid 5, van de grondwet veronderstelt dat „in een vrije samenleving de woning wordt afgeschermd als een plaats om te bekomen van de beslommeringen van de buitenwereld” en „de burger verzekert dat zijn of haar privacy, persoon en veiligheid beschermd wordt tegen alle indringers”, behoudens in de door de wet bepaalde gevallen en met inachtneming van het wezen van deze constitutionele waarborg.

[OR. 6]

- 13 [De High Court] oordeelde vervolgens dat de woning niet werkelijk een „plaats om te bekomen van de beslommeringen van de buitenwereld” kan zijn wanneer de bewoners bij voorbeeld niet een e-mail of een brief kunnen schrijven of zelfs een telefoongesprek kunnen voeren zonder beschermd te zijn tegen „het vooruitzicht dat de staat op massale en ongedifferentieerde schaal zulke communicaties altijd of naar willekeur volgt”. [De High Court] overwoog vervolgens:

„Deze algemene bescherming van de privacy, de persoon en de veiligheid in artikel 40, lid 5, [van de Ierse grondwet] zou volstrekt worden uitgehouden wanneer de overheid op massale en ongedifferentieerde schaal binnenshuis plaatsvindende gesprekken en communicaties kon volgen. Het onderscheppen van zulke communicaties kan grondwettelijk slechts aanvaardbaar zijn wanneer wordt aangetoond dat dit onderscheppen van communicaties en het volgen van personen of groepen van personen objectief wordt gerechtvaardigd door de belangen van misdaadbestrijding en van nationale veiligheid, en voorts dat al zulke activiteiten worden omringd met passende en controleerbare waarborgen.”

[OR. 7]

- 14 [De High Court] oordeelde voorts dat het, indien deze materie geheel werd beheerst door het Ierse recht, gemeten aan deze specifieke grondwettelijke normen op zijn minst een belangrijke strijdvraag zou zijn of de VS „een passende bescherming van de privacy en de fundamentele rechten en vrijheden” waarborgen in de zin van artikel 11, lid 1, sub a, van de wet van 1988, op grond

waarvan de doorgifte van gegevens aan dat land zou zijn toegestaan. Gezien de (kennelijk) beperkte bescherming van betrokkenen bij de huidige stand van het recht en de praktijk in de VS waar het de staatsinmenging betreft, zou de Commissioner inderdaad verplicht zijn geweest deze zaak te onderzoeken.

- 15 Indien de zaak enkel beoordeeld diende te worden volgens de Ierse grondwettelijke normen, zou de Commissioner zijn bevoegdheid krachtens artikel 10, lid 1, sub a, dan ook niet naar behoren hebben kunnen uitoefenen met de summiere vaststelling dat er niets te onderzoeken viel.

Nationaal recht opzijgezet door Unierecht; de Veilighavenbeschikking

- 16 Partijen zijn het echter eens, dat de kwestie slechts gedeeltelijk wordt beheerst door het Ierse recht en dat wat dit cruciale vraagstuk van de toereikendheid van het recht en de praktijk inzake de gegevensbescherming in derde landen betreft, het Ierse recht moet wijken voor het algemene Unierecht op dit gebied. Artikel 11, lid 1, sub a, van de wet van 1988 (zoals vervangen bij artikel 12 van de wet van 2003 tot wijziging van de Data Protection Act) verwijst deze bredere kwestie namelijk naar het Unierecht. Artikel 11, lid 2, sub b, van de wet van 1988 bepaalt met name dat de Commissioner de vraag of de bescherming in de derde staat toereikend is, moet beslissen „in overeenstemming” met een communautair besluit van de Europese Commissie volgens artikel 25, lid 6, van richtlijn 95/46.
- 17 [De High Court] oordeelde voorts dat, aangezien de geldigheid van het administratieve besluit van de Commissioner om de zaak niet nader te onderzoeken, afhangt van de juiste uitlegging en toepassing van richtlijn 95/46 alsmede van het inderdaad overeenkomstig die richtlijn genomen besluit van de Europese Commissie, het hier een aangelegenheid betreft waarin een lidstaat het Unierecht tot uitvoering brengt in de zin van artikel 51, lid 1, van het Handvest van de grondrechten van de Europese Unie, hetgeen volstaat – althans wat dit onderdeel van de onderhavige zaak betreft – voor de toepasselijkheid van het Handvest: zie bij voorbeeld het arrest van het Hof, N.S. e.a. (gevoegde zaken C-411/10 en C-493/10, EU:C:2011:865, punten 64 tot en met 69) (omissis).

[OR. 8]

- 18 [De High Court] oordeelde vervolgens (in de punten 64 tot en met 70 van zijn tussenvonnissen):

„64. Dit brengt ons bij de kern van de vraag voor de Commissioner. Hij is vanzelfsprekend gebonden aan de bepalingen van richtlijn 95/46 en de Veilighavenbeschikking van de Commissie van 2000. Aangezien deze beschikking een ‚communautair besluit’ is inzake de toereikendheid van de gegevensbescherming in het land waaraan de gegevens worden doorgegeven, schrijft artikel 11, lid 2, sub a, van de wet van 1988 (zoals gewijzigd) bovendien voor, dat het vraagstuk van de toereikendheid van de

gegevensbescherming in het land waaraan de gegevens worden doorgegeven, moet worden beslist ,in overeenstemming met dat besluit'. In dit opzicht volgt artikel 11, lid 2, sub a, van de wet van 1988 getrouw de bepalingen van artikel 25, lid 6, van richtlijn 95/46.

65. Dit alles betekent dat de Commissioner geen besluit kan nemen dat niet met dat communautaire besluit valt te verenigen, en dat de Commissioner derhalve, wanneer het communautaire besluit de strekking heeft dat de gegevensbeschermingswetgeving van een bepaalde derde staat toereikend en doeltreffend is, niet mag beslissen dat dit niet het geval is. Het communautaire besluit in kwestie had, zoals reeds gezegd, de strekking dat de VS de betrokkenen toereikende gegevensbescherming bieden met betrekking tot gegevens die beheerd of verwerkt worden door bedrijven (zoals Facebook Ireland en Facebook) die de Veiligheidsbeginselen toepassen.

66. Hieruit volgt dat wanneer de Commissioner niet verder mag kijken dan de Veiligheidsbeschikking van de Europese Commissie van juli 2000, dat het onderhavige beroep moet falen. De reden hiervoor is – op het gevaar af in herhalingen te vervallen – dat de Commissie heeft besloten dat de VS een toereikend niveau van gegevensbescherming bieden, en zoals zojuist gezegd, artikel 11, lid 2, sub a, van de wet van 1998 (dat op zijn beurt artikel 25, lid 6, van richtlijn 95/46 volgt) de Commissioner bindt aan het besluit van de Commissie. In die omstandigheden is iedere klacht bij de Commissioner over het doorgeven van persoonsgegevens aan de VS door Facebook Ireland (of Facebook zelf) op de grond dat de gegevensbescherming van de VS niet toereikend is, tot mislukken gedoemd.

[OR. 9]

67. Het besluit van de Commissie is ongetwijfeld nog altijd juist wat de consumentenbescherming betreft, maar, zoals wij hebben gezien, is er sinds juli 2000 veel gebeurd. De ontwikkelingen bestonden onder meer in een toenemende bedreiging van de nationale en internationale veiligheid door staten die zich niet aan het recht houden, terroristische groeperingen en de georganiseerde misdaad, onthullingen betreffende het massale en ongedifferentieerde volgen van persoonsgegevens door de veiligheidsdiensten van de VS, de opkomst van de sociale media en, uit juridisch oogpunt niet het minst belangrijk, de verhoogde en thans in artikel 8 van het Handvest verankerde bescherming van persoonsgegevens.

68. Hoewel verzoeker betoogt dat de Commissioner het Unierecht onjuist heeft toegepast door de klacht als onhoudbaar te beschouwen, is in werkelijkheid het tegendeel waar: de Commissioner heeft juist blijk gegeven scrupuleus vast te houden aan de letter van richtlijn 95/46 en de Veiligheidsbeschikking.

69. In feite heeft verzoeker bezwaar tegen de Veiligehavenbeschikking zelf in plaats van tegen de wijze waarop de Commissioner deze heeft toegepast. Er valt wellicht veel voor te zeggen dat het Veiligehavenregiem achterhaald is door de ontwikkelingen. Aan de onthullingen van Snowden kan worden toegeschreven dat hierdoor gapende lacunes in de huidige wetgeving en praktijk van de VS op het gebied van gegevensbescherming aan het licht zijn gekomen, en het feit dat artikel 8 van het Handvest nadien in werking is getreden, vormt een aanwijzing dat een nieuwe evaluatie van de uitlegging van richtlijn 95/46 en de Veiligehavenbeschikking van 2000 wellicht geboden is. Er moet echter opnieuw op worden gewezen dat in de onderhavige procedure noch de geldigheid van richtlijn 95/46 noch die van Veiligehavenbeschikking als zodanig zijn bestreden.

70. Hoewel de geldigheid van de beschikking van 2000 niet rechtstreeks in twijfel wordt getrokken, doemt hier toch de wezenlijke vraag op of de Commissioner volgens het Unierecht, niettegenstaande artikel 25, lid 6, van richtlijn 95/46, zonder meer is gebonden aan die in de Veiligehavenbeschikking van 2000 neergelegde bevindingen van de Europese Commissie betreffende de toereikendheid van de gegevensbescherming in het recht en de praktijk van de Verenigde Staten, gezien met name de inwerkingtreding van artikel 8 van het Handvest sindsdien. Tenzij deze vraag wordt beantwoord op een wijze die de Commissioner in staat stelt de achterliggende redenen van dat communautaire besluit te onderzoeken of het naast zich neer te leggen, lijkt zowel de klacht van verzoeker bij de Commissioner als het onderhavige beroep te moeten falen om de reeds uiteengezette redenen.”

[OR. 10-11]

- 19 Aangezien het kernpunt in de onderhavige zaak is of het recht en de praktijk van de VS voldoende gegevensbescherming bieden,¹ en de handelwijze van Facebook Ireland/Facebook² zelf³ in de onderhavige procedure nooit is bestreden, is [de High Court] van oordeel dat de werkelijke vraag is of de Commissioner gebonden is aan de oudere bevindingen van de Europese Commissie dienaangaande in de Veiligehavenbeschikking. Met andere woorden, de onderhavige klacht heeft

- 1 – Zo was de voornaamste grond die verzoeker aanvoerde (omissis) in de Statement of Grounds (het stuk dat de grondslag vormt voor de hogerberoepsprocedure) van 21 oktober 2013, dat in het licht van de recente onthullingen van Snowden „en de terbeschikkingstelling op grote schaal van privégegevens aan de informatiediensten [van de VS]”, de Commissioner niet kon concluderen dat „in de Verenigde Staten van Amerika een passend niveau van bescherming bestond”.
- 2 – Schrems heeft 22 verschillende klachten bij de Commissioner ingediend over Facebook, maar geen enkele daarvan kwam aan de orde in de onderhavige procedure.
- 3 – Anders dan dat zij samenwerkten met de veiligheidsautoriteiten van de VS in het kader van het PRISM-programma, door de gegevens van hun gebruikers door te geven en „massale toegang” tot zulke gegevens te verstrekken zonder dat daarvoor gegronde redenen hoefden te worden aangevoerd (omissis) (omissis).

eigenlijk betrekking op de *inhoud* van die beschikking, en niet zozeer op de manier waarop de Commissioner *deze heeft toegepast* (omissis). Hoewel volgens artikel 3, lid 1, sub b, van de Veiligheidsbeschikking de nationale autoriteiten een organisatie kunnen bevelen de doorgifte van gegevens naar een bepaald derde land op te schorten, betreft dit omstandigheden waarin – anders dan hier – het probleem is gelegen in *het gedrag van die organisatie*. In deze zaak zijn de bezwaren niet gericht tegen het gedrag van Facebook zelf, als wel tegen het feit dat de Commissie reeds heeft bepaald dat het recht en de praktijk in de VS toereikende gegevensbescherming waarborgen terwijl over de desbetreffende omstandigheden na de onthullingen van Snowden in zoverre duidelijk is gebleken dat de autoriteiten van de VS op massale en ongedifferentieerde schaal toegang hebben tot de persoonsgegevens van burgers van de Unie die via Facebook aan de VS zijn doorgegeven.

- 20 Het zij benadrukt dat in de onderhavige procedure noch de geldigheid van richtlijn 95/46 noch die van de Veiligheidsbeschikking van 2000 zelf wordt bestreden. Evenmin is gesteld dat artikel 11, lid 2, sub a, van de wet van 1988 (zoals gewijzigd) geen getrouwe afspiegeling is van artikel 25, lid 6, van richtlijn 95/46.
- 21 Gelet hierop stelt [de High Court zich] op het standpunt dat het, met name gelet op [zijn] eerdere bevindingen inzake de onthullingen van Snowden, gevolgd door de inwerkingtreding van de artikelen 7 en 8 van het Handvest alsmede het recente arrest van het Hof in de zaak Digital Rights Ireland, passend is om over te gaan tot verwijzing van de vraag of de Commissioner is gebonden aan de eerdere beslissing in de Veiligheidsbeschikking van de Europese Commissie, dat het recht en de praktijk van de VS toereikende gegevensbescherming bieden.

[OR. 12]

De prejudiciële vragen

- 22 De [High Court] heeft het Hof daarom de volgende vragen gesteld:

„Wanneer bij een onafhankelijke ambtsdrager, aan wie bij de wet de toepassing en de uitvoering van de wetgeving inzake gegevensbescherming is opgedragen, een klacht wordt ingediend dat persoonsgegevens worden doorgegeven aan een derde land (in casu de Verenigde Staten van Amerika) waarvan het recht en de praktijk volgens de klager de betrokkenen geen passende bescherming bieden, is die ambtsdrager dan absoluut gebonden aan de communautaire bevinding van het tegendeel [in de beschikking van de Commissie van 26 juli 2000 (2000/520/EG)], gelet op de artikelen 7, 8 en 47⁴ van het Handvest van de grondrechten van de Europese Unie (PB 2000/C 364/01), niettegenstaande artikel 25, lid 6, van richtlijn

4 – Tijdens een latere zitting op 2 juli 2014 is afgesproken om in de conceptvraag ook artikel 47 op te nemen.

95/46/EG? Of kan en/of moet⁵ de ambtsdrager overgaan tot een eigen onderzoek van de zaak in het licht van de feitelijke ontwikkelingen die zich sinds de bekendmaking van die Commissiebeschikking hebben voorgedaan?”

Het standpunt van de verwijzende rechter inzake de gestelde vragen

- 23 In abstracto valt moeilijk in te zien hoe de Veiligehavenbeschikking in de praktijk kan voldoen aan de vereisten van de artikelen 7 en 8 van het Handvest, in het bijzonder in het licht van de beginselen die het Hof van Justitie heeft geformuleerd in het arrest *Digital Rights Ireland*.⁶ Volgens dat stelsel van zelfcertificering worden persoonsgegevens doorgezonden aan de Verenigde Staten, waar de veiligheidsdiensten van de VS zich op massale en ongedifferentieerde schaal toegang daartoe kunnen verschaffen. Het feit dat op Europese bodem geen toezicht wordt uitgeoefend, dat de betrokkene niet over een effectieve mogelijkheid beschikt om gehoord te worden of opmerkingen in te dienen en dat een toetsing, voor zover daarvan al sprake is, niet plaatsvindt volgens het Unierecht, zijn stuk voor stuk factoren die aanmerkelijke juridische problemen lijken op te werpen.
- 24 Voorts kan weliswaar worden toegegeven dat artikel 7 van het Handvest slechts „eerbiediging” van de woning waarborgt – en in dat opzicht wellicht niet zo ver gaat als artikel 40, lid 5, van de Ierse grondwet die de woning „onschendbaar” verklaart. Niettemin moet erop worden gewezen dat het beeld van de woning als toevluchtsoord en, in de bewoordingen van de Ierse rechter als „plaats om te bekomen van de beslommeringen van de buitenwereld”, een cruciaal element is van het waarborgen van de „eerbiediging” van de woning en de communicatie in artikel 7 van het Handvest, en in dat opzicht kernwaarden weerspiegelt die gemeen zijn aan de constitutionele tradities van de lidstaten. Deze waarborg wordt volledig uitgehold indien overheidsinstanties (hetzij vanaf het grondgebied van de Unie hetzij in een derde land) op een terloopse en veralgemeniseerde basis toegang konden krijgen tot elektronische communicaties, die dikwijls binnenshuis tot stand komen, zonder dat hiervoor een objectieve rechtvaardiging hoeft te worden aangevoerd die berust op overwegingen van nationale veiligheid of misdaadpreventie specifiek verband houdend met de betrokken persoon of personen, en zonder te worden omringd met passende en verifieerbare waarborgen (omissis).

[OR. 13-14]

- 25 Het moet echter worden benadrukt dat in de onderhavige procedure noch de geldigheid van richtlijn 95/46 noch die van de Veiligehavenbeschikking van de

5 – De woorden „en/of moet” zijn toegevoegd op verzoek van de verzoeker op de zitting van 2 juli 2014.

6 – Zie de punten 65 tot en met 69 van het tussenvonnissen.

Commissie als zodanig wordt bestreden. Evenmin is gesteld dat het Ierse recht geen juiste afspiegeling vormt van artikel 25, lid 6, van richtlijn 95/46 voor zover die wet voorschrijft dat de Commissioner is gebonden aan de bevindingen aangaande bepaalde landen in de Veiligheidsbeschikking van de Europese Commissie met betrekking tot de toereikendheid van de regeling van de gegevensbescherming in het derde land.

- 26 Gelet op wat wél wordt gesteld, namelijk de onverenigbaarheid in abstracto van de Veiligheidsbeschikking met de vereisten van de artikelen 7 en 8 van het Handvest, zou het Hof echter kunnen oordelen dat een uitlegging van richtlijn 95/46 in het algemeen (en van artikel 25, lid 6, ervan in het bijzonder) in combinatie met de Veiligheidsbeschikking van 2000 mogelijk is, zodat een nationale autoriteit zou kunnen overgaan tot een eigen onderzoek om vast te stellen of het doorgeven van persoonsgegevens aan een derde land in overeenstemming is met de vereisten van de artikelen 7 en 8 van het Handvest, in het licht van bij voorbeeld het arrest Digital Rights Ireland.

[OR. 14]

- 27 Zou het Hof echter oordelen dat een dergelijke uitlegging van richtlijn 95/46 en van de Veiligheidsbeschikking contra legem is of anderszins niet mogelijk is, dan lijken de nationale autoriteiten volledig te zijn gebonden aan de termen van de Veiligheidsbeschikking. Nu in het kader van deze specifieke klacht niet is gesteld dat Facebook Ireland of Facebook zelf in strijd met de Veiligheidsbeginselen hebben gehandeld, zou daaruit volgen dat de gevolgtrekking van de Commissioner dat deze klacht rechtens ongegrond is, geheel terecht was.

Tussenkoms van Digital Rights Ireland Ltd. als amicus curiae

- 28 Na de uitspraak van het tussenvonnis op 18 juni 2014 heeft Digital Rights Ireland Ltd („DRI”) (omissis) verzocht om tot de procedure te worden toegelaten als amicus curiae. Bij aanvullende beslissing van 16 juli 2014 heeft [de High Court] dit toegestaan (omissis).

(Omissis)

[OR. 15]

(Omissis)

17 juli 2014

Handtekening

Rechter Gerard Hogan

Rechter in de High Court of Ireland

[OR. 16]