Datum van inontvangstneming	:	05/03/2013

Zaak C-46/13

Verzoek om een prejudiciële beslissing

Datum van indiening:

28 januari 2013

Verwijzende rechter:

Datenschutzkommission (Oostenrijk)

Datum van de verwijzingsbeslissing:

18 januari 2013

Verzoekende partij:

H

Verwerende partij:

E

(omissis)

De Datenschutzkommission (commissie voor gegevensbescherming) heeft (omissis) op haar zitting van 18 januari 2013 in de beroepsprocedure [redacted] tegen Orange Austria Telecommunication Gesellschaft m.b.H. (omissis) betreffende een in het kader van het recht op gegevensbescherming ingesteld beroep wegens schending van het recht op inlichtingen over eigen gegevens als gevolg van het onvolledig verstrekken van gegevens, beslist:

- Het Hof van Justitie van de Europese Unie wordt overeenkomstig artikel 267 VWEU verzocht om een prejudiciële beslissing over de volgende vragen met betrekking tot richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van richtlijn 2002/58/EG (PB L 105, blz. 54; hierna: richtlijn 2006/24/EG), 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 **[Or. 2];** hierna: richtlijn 95/46/EG) en het Handvest van de grondrechten van de Europese Unie (PB C 83, blz. 389; hierna: „Handvest"):

1. Moet artikel 7, sub c, van richtlijn 2006/24/EG aldus worden uitgelegd dat een natuurlijke persoon op wie een gegevensbewaring in de zin van de richtlijn betrekking heeft, niet behoort tot de kring van „speciaal daartoe bevoegde personen" in de zin van deze bepaling, en die persoon geen recht kan worden toegekend om van de aanbieder van een openbare communicatiedienst of de exploitant van een openbaar communicatienetwerk inlichtingen te verkrijgen over zijn eigen gegevens?

2. Moet artikel 13, lid 1, sub c en d, van richtlijn 95/46/EG aldus worden uitgelegd dat het recht van een natuurlijke persoon op wie een gegevensbewaring in de zin van richtlijn 2006/24/EG betrekking heeft, om op grond van artikel 12, sub a, van eerstgenoemde richtlijn van de aanbieder van een openbare communicatiedienst of de exploitant van een openbaar communicatienetwerk inlichtingen te verkrijgen over zijn eigen gegevens, kan worden uitgesloten of beperkt?

3. Indien de eerste vraag, op zijn minst, gedeeltelijk bevestigend wordt beantwoord, is dan artikel 7, sub c, van richtlijn 2006/24/EG verenigbaar met het fundamentele recht van artikel 8, lid 2, tweede zin, van het Handvest en dus geldig?

Motivering:

A) Rechtvaardiging van het beroep bij de Datenschutzkommission

De Datenschutzkommission is de op grond van nationaal Oostenrijks recht [§§ 35-40 van het Datenschutzgesetz (Oostenrijkse wet inzake gegevensbescherming; hierna: „DSG 2000")] overeenkomstig artikel 28 van richtlijn 95/46/EG ingestelde controlerende instantie. Zij is tegelijk de in artikel 22 van richtlijn 95/46/EG voorziene toezichthoudende autoriteit, die enkel is onderworpen aan rechterlijk toezicht door de hoogste publiekrechtelijke gerechtshoven (Verwaltungsgerichtshof en Verfassungsgerichtshof). Zij is een onafhankelijke, collegiale instantie, overeenkomstig artikel 20, lid 2, punten 3 en 8, en artikel 133, punt 4, van het Oostenrijkse Bundes-Verfassungsgesetz (Oostenrijkse federale grondwet). De Datenschutzkommission kan worden aangemerkt als een rechterlijke instantie in de zin van het recht van de Unie (Verwaltungsgerichtshof, 27 september 2007), (omissis).

In de onderhavige procedure heeft verzoeker als persoon van wie de gegevens zijn verwerkt door een exploitant van openbare communicatiediensten en openbare communicatienetwerken (hierna: verweerster) overeenkomstig § 26 **[Or. 3]**, lid 1, DSG 2000 (artikel 12, sub a, van richtlijn 95/46/EG) verzocht om inlichtingen,

welke onvolledig zijn verstrekt (hetgeen niet wordt betwist). Als het beroep gegrond wordt verklaard, dan dient de Datenschutzkommission verweerster door middel van een uitvoerbaar bevel op te dragen volledige inlichtingen te verstrekken (§ 31, lid 7, DSG 2000).

B) Aanhangige beroepsprocedure

Verzoeker is als klant van verweerster eindgebruiker van openbaar beschikbare communicatiediensten en beschikt over een abonnement voor mobiele telefonie. Op 12 juni 2012 richtte hij een verzoek om inlichtingen tot verweerster, waarin hij in het bijzonder ook inlichtingen verlangde over overeenkomstig § 102a van het Telekommunikationsgesetz 2003 (Oostenrijkse wet op de telecommunicatie; hierna: „TKG 2003") verwerkte en bewaarde gegevens. Daarop verstrekte verweerster op 4 juli 2012 aan verzoeker inlichtingen die in wezen enkel betrekking hadden op de aard van de verzamelde gegevens, doch geen inhoudelijke inlichtingen over de door verweerster verwerkte, bewaarde gegevens van verzoeker, noch over eventuele ontvangers van berichten (of kringen van ontvangers).

Daartegen heeft verzoeker op 26 juni 2012 beroep ingesteld bij de Datenschutzkommission. Hij stelt te zijn geschonden in zijn recht op inlichtingen. De aan hem verstrekte inlichtingen zijn gebrekkig, want onvolledig, aangezien hem met betrekking tot de over hem bewaarde gegevens zonder toereikende motivering geen inlichtingen zijn verstrekt.

Verweerster bracht hier tegenin – voor zover in casu van belang – dat de gewone wetgever de uit § 1 DSG 2000 voortvloeiende rechten ten aanzien van bewaarde gegevens, in het kader van de hem gelaten speelruimte heeft ingeperkt, om de doelstelling van de gegevensbewaring niet in gevaar te brengen. Een dergelijk gevaar is denkbaar, wanneer criminelen zich op elk moment op de hoogte zouden kunnen stellen van de stand van de voor hun strafvervolging dienende gegevens. Overeenkomstig § 102b TKG 2003, is het verstrekken van inlichtingen over bewaarde gegevens uitsluitend toelaatbaar op basis van een rechterlijk goedgekeurd bevel van de officier van justitie tot het oplossen en vervolgen van ernstige strafbare feiten. In het verstrekken van inlichtingen op grond van § 26 DSG 2000 heeft de wetgever in deze bepaling bewust niet voorzien.

Voor het overige staat ook § 26, lid 2, punt 5, DSG 2000 – krachtens welke bepaling geen inlichtingen behoeven te worden verstrekt wanneer sprake is van een hoger openbaar belang in verband met het voorkomen of vervolgen van strafbare feiten – aan het verstrekken van de door verzoeker verlangde inlichtingen in de weg, omdat richtlijn 2006/24/EG ervan uitgaat dat de gegevensbewaring een noodzakelijke maatregel in de zin van artikel 8 EVRM is in het belang van het voorkomen van wanordelijkheden en strafbare feiten of de bescherming van de rechten en vrijheden. **[Or. 4]**

C) Toe te passen bepalingen van nationaal recht (onderverdeeld naar rechtsgebied)

1) Recht op gegevensbescherming

De grondwettelijke bepaling § 1, lid 2, lid 3, punten 1 en 4, DSG 2000, luidt, inclusief opschrift:

„Fundamenteel recht op gegevensbescherming

§1. (1)[-]

(2) Voor zover het gebruik van persoongegevens niet van vitaal belang is voor de betrokkene dan wel met diens toestemming geschiedt, zijn beperkingen van het recht op geheimhouding toelaatbaar, zij het enkel ter bescherming van zwaarder wegende, gerechtvaardigde belangen van een ander en, in geval van inmenging door een overheidsinstantie, enkel op grond van wetten die om de in artikel 8, lid 2, van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) (BGBl. 210/1958) genoemde redenen noodzakelijk zijn. Dergelijke wetten mogen het gebruik van gegevens die naar hun aard bijzonder beschermenswaardig zijn enkel toelaten ter bescherming van belangrijke algemene belangen en moeten tegelijkertijd passende garanties vastleggen voor de bescherming van de geheim te houden belangen van de betrokkene. Ook in het geval van toelaatbare beperkingen dient de inmenging in het fundamentele recht steeds zo licht mogelijk en doelgericht te zijn.

(3) Eenieder heeft, voor zover de hem betreffende persoonsgegevens zijn bestemd voor computerondersteunde verwerking, of voor een handmatig, dat wil zeggen zonder computerondersteuning, bijgehouden gegevensbank, krachtens wettelijke bepalingen

1. het recht om te weten wie welke gegevens over hem verwerkt, waar de gegevens vandaan komen, waarvoor ze worden gebruikt en in het bijzonder ook aan wie zij worden doorgegeven;

2. [...].

(4) Beperkingen van de rechten uit hoofde van lid 3 zijn enkel toelaatbaar onder de in lid 2 genoemde voorwaarden.”

§ 26, leden 1 en 2, DSG 2000 luidt, inclusief opschrift:

„Recht op inlichtingen

§ 26, lid 1. Een opdrachtgever dient aan elke persoon of personengemeenschap die hierom schriftelijk verzoekt en zich op gepaste wijze identificeert, inlichtingen te vertrekken over de met betrekking tot die persoon of personengemeenschap

verwerkte gegevens. Met toestemming van de opdrachtgever kan het verzoek om inlichtingen ook mondeling worden gedaan. De inlichtingen dienen, in een algemeen begrijpelijke vorm informatie te verschaffen over de verwerkte **[Or. 5]** gegevens, de herkomst daarvan, eventuele ontvangers, of kringen van ontvangers, van berichten, het doel van de gegevensverwerking, alsook de rechtsgrondslagen hiervoor. Op verzoek van een betrokkene moeten ook namen en adressen van dienstverrichters bekend worden gemaakt, indien deze met de verwerking van zijn gegevens zijn belast. Wanneer over de persoon die om inlichtingen verzoekt geen gegevens voorhanden zijn, volstaat de bekendmaking van die omstandigheid (negatieve inlichting). Met toestemming van de persoon die om inlichtingen verzoekt, kan in plaats van schriftelijke inlichtingen ook mondeling inlichtingen worden verstrekt, met de mogelijkheid van inzage en verkrijging van een afschrift of fotokopie.

(2) Geen inlichtingen behoeven te worden verstrekt voor zover dit om bijzondere redenen noodzakelijk is ter bescherming van de persoon die om inlichtingen verzoekt of voor zover zwaarder wegende, gerechtvaardigde – inzonderheid ook openbare – belangen van de opdrachtgever of een derde, aan de gegevensverstrekking in de weg staan. Deze zwaarder wegende belangen kunnen voortvloeien uit de noodzaak van:

1. de bescherming van de grondwettelijke instellingen van de Republiek Oostenrijk, of

2. de veiligstelling van de inzetbaarheid van het Oostenrijkse leger, of

3. de veiligstelling van de belangen van een sluitende landsverdediging, of

4. de bescherming van essentiële belangen van economisch, buitenlands of financieel beleid van de Republiek Oostenrijk of de Europese Unie, of

5. het voorkomen of vervolgen van strafbare feiten.

De toelaatbaarheid van de weigering om inlichtingen te verstrekken op grond van de onder de punten 1 tot en 5 genoemde redenen is onderworpen aan toezicht door de Datenschutzkommission (§ 30, lid 3) en de bijzondere beroepsprocedure bij de Datenschutzkommission (§ 31, lid 4).

2) Telecommunicatierecht

De §§ 102a, 102b en 109, lid 1, punt 24, TKG 2003 luiden, inclusief opschriften:

„Bewaarde gegevens

§ 102a. (1) Naast de bevoegdheid tot het bewaren of verwerken overeenkomstig de §§ 96, 97, 99, 101 en 102, dienen aanbieders van openbare communicatiediensten volgens de leden 2 tot en met 4 daarenboven gegevens vanaf het tijdstip waarop zij zijn gegenereerd of verwerkt, tot zes maanden na beëindiging van de communicatie te bewaren. De bewaring vindt uitsluitend plaats ten behoeve van het onderzoeken, opsporen en vervolgen van strafbare feiten waarvan de ernst een bevel krachtens § 135, lid 2a, [Strafprozessordnung (Oostenrijks wetboek van strafvordering)] rechtvaardigt. **[Or. 6]**

(2) Aanbieders van internettoegangsdiensten zijn verplicht de volgende gegevens te bewaren:

1. naam, adres en identificatiecode van de abonnee aan wie op een bepaald tijdstip een openbaar IP-adres was toegewezen, onder vermelding van de tijdzone waarop dit is gebaseerd;

2. datum en tijdstip van de toewijzing en intrekking van een openbaar IP-adres bij een internettoegangsdienst, onder vermelding van de tijdzone waarop dit is gebaseerd;

3. telefoonnummer van de oproeper voor de toegang via een inbelverbinding;

4. de eenduidige identificatie van de aansluiting waarmee de internettoegang tot stand is gebracht.

(3) Aanbieders van openbare telefoondiensten, met inbegrip van internettelefoondiensten, zijn verplicht de volgende gegevens te bewaren: [...]

(4) Aanbieders van e-maildiensten zijn verplicht de volgende gegevens te bewaren: [...]

(5) De in lid 1 neergelegde verplichting tot bewaring geldt enkel voor gegevens die overeenkomstig de leden 2 tot en 4 als gevolg van het aanbieden van de desbetreffende communicatiediensten zijn gegenereerd of verwerkt.

In verband met oproeppogingen zonder resultaat geldt de in lid 1 neergelegde verplichting tot bewaring enkel voor zover die gegevens als gevolg van het aanbieden van de desbetreffende communicatiedienst zijn gegenereerd of verwerkt en worden bewaard of geprotocolleerd.

(6) De in lid 1 neergelegde verplichting tot bewaring geldt niet voor aanbieders waarvan de ondernemingen niet verplicht zijn tot betaling, overeenkomstig § 34 KommAustriaG [Oostenrijkse wet tot instelling van een communicatieautoriteit], van de financieringsbijdrage.

(7) De inhoud van de communicatie, en met name gegevens over op het internet opgeroepen adressen, mogen op grond van deze bepaling niet worden bewaard.

(8) De krachtens lid 1 te bewaren gegevens moeten, behoudens het bepaalde in § 99, lid 2, na het verstrijken van de bewaringstermijn zo spoedig mogelijk en uiterlijk een maand na afloop van de bewaringstermijn worden gewist. Het verstrekken van inlichtingen na afloop van de bewaringstermijn is ontoelaatbaar.

(9) Met betrekking tot bewaarde gegevens die overeenkomstig § 102b worden verstrekt, worden de aanspraken op informatie of inlichtingen over dit gegevensgebruik uitsluitend geregeld door de bepalingen van de Strafprozessordnung. **[Or. 7]**

Inlichtingen over bewaarde gegevens

§ 102b. (1) Het verstrekken van inlichtingen over bewaarde gegevens is uitsluitend toelaatbaar op basis van een rechterlijk goedgekeurd bevel van de officier van justitie tot het oplossen en vervolgen van strafbare feiten waarvan de ernst een bevel krachtens § 135, lid 2a, Strafprozessordnung rechtvaardigt.

(2) De krachtens § 102a te bewaren gegevens moeten zodanig worden bewaard dat zij zo spoedig mogelijk kunnen worden doorgegeven aan de autoriteiten die overeenkomstig de bepalingen van de Strafprozessordnung bevoegd zijn inzake het verstrekken van inlichtingen over de gegevens van een berichtendoorgave.

(3) Het doorgeven van de gegevens dient te geschieden in een geschikte, beschermde vorm, met inachtneming van § 94, lid 4, TKG 2003.

„Administratieve sancties

§ 109. (1) Een met een geldboete van maximaal 4 000 EUR te bestraffen administratieve overtreding begaat degene die

1. [...]23.[...]

24. in strijd met § 102b zonder rechterlijke goedkeuring inlichtingen over gegevens verstrekt”

3) Strafprocesrecht

§ 135, leden 1, 2 en 2a, Strafprozessordnung 1975, BGBl. 631/1975, in de in casu toepasselijke versie, luidt, inclusief opschrift:

„Inbeslagneming van brieven, inlichtingen over gegevens van een communicatie, inlichtingen over bewaarde gegevens en toezicht op de communicatie

§ 135. (1) Inbeslagneming van brieven is toelaatbaar wanneer dit noodzakelijk is voor de oplossing van een opzettelijk begaan strafbaar feit waarop een

vrijheidsstraf van meer dan een jaar is gesteld, en de verdachte vanwege een dergelijk feit is aangehouden, dan wel indien vanwege dat feit een bevel tot zijn voorgeleiding of aanhouding werd uitgevaardigd.

(2) Het verstrekken van inlichtingen over gegevens van een communicatie is toelaatbaar

1. wanneer en zolang er een ernstige verdenking bestaat dat een persoon op wie de inlichting **[Or. 8]** betrekking heeft een andere persoon heeft ontvoerd of anderszins van diens vrijheid heeft beroofd, en de inlichting enkel betrekking heeft op gegevens van een dergelijke communicatie, waarvan kan worden aangenomen dat zij ten tijde van de vrijheidsberoving door de verdachte is doorgegeven, ontvangen of verzonden,

2. wanneer te verwachten valt dat daardoor de oplossing kan worden bevorderd van een opzettelijk begaan strafbaar feit waarop een vrijheidsstraf van meer dan zes maanden is gesteld en de houder van de technische voorziening die de oorsprong of het doel was, of zal worden, van een communicatie, uitdrukkelijk instemt met het verstrekken van de inlichtingen, of

3. wanneer te verwachten valt dat daardoor de oplossing kan worden bevorderd van een opzettelijk begaan strafbaar feit waarop een vrijheidsstraf van meer dan een jaar is gesteld en op grond van bepaalde feiten kan worden aangenomen dat daardoor gegevens van de verdachte kunnen worden opgespoord,

4. wanneer op grond van bepaalde feiten kan worden aangenomen dat daardoor het verblijf kan worden opgespoord van een voortvluchtige of afwezige verdachte tegen wie een ernstige verdenking bestaat van het opzettelijk plegen van een strafbaar feit waarop een vrijheidsstraf van meer een jaar is gesteld.

(2a) Het verstrekken van inlichtingen over bewaarde gegevens (§§ 102a en 102b TKG) is in de gevallen genoemd onder de leden 2, punten 2 tot en met 4, toelaatbaar."

Daarnaast bestaan er nadere bepalingen die de politie en het openbaar ministerie bevoegdheid verlenen om ook zonder rechterlijke goedkeuring gegevens door te geven [zie onder andere § 53, lid 3a, Sicherheitspolizeigesetz (Oostenrijkse wet betreffende de veiligheidspolitie), BGBl. 566/1991, in de in casu toepasselijke versie].

De Datenschutzkommission dient, in overeenstemming met de rechtspraak van het Hof van Justitie van de Europese Unie, de bepalingen van het DSG 2000 en het TKG 2003 inzake het verstrekken van inlichtingen zo veel mogelijk uit te leggen

conform de bepalingen van richtlijn 2006/24/EG en richtlijn 95/46/EG (arrest van 7 december 1995, C-472/93, Luigi Spano e.a., Jurispr. blz. 1-4321 en aldaar aangehaalde rechtspraak), respectievelijk het Handvest in acht te nemen. De vraag van uitlegging en geldigheid van de richtlijn en de vraag naar de uitlegging van het Handvest vormen derhalve een wezenlijke grondslag voor de beslissing van de Datenschutzkommission. **[Or. 9]**

D) Toe te passen bepalingen van het recht van de Europese Unie:

1) Handvest van de grondrechten

„Artikel 8

Bescherming van persoonsgegevens

„1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.

2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.

3. Een onafhankelijke autoriteit ziet erop toe dat deze regels worden nageleefd."

2) Richtlijn 2006/24/EG:

„Artikel 7

Gegevensbescherming en gegevensbeveiliging

Onverminderd de bepalingen die zijn goedgekeurd ingevolge de richtlijnen 95/46/EG en 2002/58/EG zorgt iedere lidstaat ervoor dat de aanbieders van elektronische communicatiediensten of de aanbieders van een publiek communicatienetwerk ten minste de volgende beginselen van gegevensbeveiliging respecteren met betrekking tot gegevens die bewaard worden overeenkomstig deze richtlijn:

c) de gegevens worden onderworpen aan passende technische en organisatorische maatregelen om te waarborgen dat toegang tot de gegevens slechts geschiedt door speciaal daartoe bevoegde personen, [...]

3) Richtlijn 95/46/EG:

„Artikel 12

Recht van toegang

De lidstaten waarborgen elke betrokkene het recht van de voor de verwerking verantwoordelijke te verkrijgen:

a) vrijelijk en zonder beperking, met redelijke tussenpozen en zonder bovenmatige vertraging of kosten:

- uitsluitsel omtrent het al dan niet **[Or. 10]** bestaan van verwerkingen van hem betreffende gegevens, alsmede ten minste informatie over de doeleinden van deze verwerkingen, de categorieën gegevens waarop deze verwerkingen betrekking hebben en de ontvangers of categorieën ontvangers aan wie de gegevens worden verstrekt;

- verstrekking, in begrijpelijke vorm, van de gegevens die zijn verwerkt, alsmede de beschikbare informatie over de oorsprong van de gegevens;

- mededeling van de logica die ten grondslag ligt aan de automatische verwerking van hem betreffende gegevens, in elk geval als het gaat om de geautomatiseerde besluiten als bedoeld in artikel 15, lid 1;

b) naar gelang van het geval, de rectificatie, de uitwissing of de afscherming van de gegevens waarvan de verwerking niet overeenstemt met de bepalingen van deze richtlijn, met name op grond van het onvolledige of onjuiste karakter van de gegevens;

c) kennisgeving aan derden aan wie de gegevens zijn verstrekt, van elke rectificatie, uitwissing of afscherming, uitgevoerd overeenkomstig punt b, tenzij zulks onmogelijk blijkt of onevenredig veel moeite kost.”

„Artikel 13

Uitzonderingen en beperkingen

De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in artikel 6, lid 1, artikel 10, artikel 11, lid 1, artikel 12 en artikel 21 bedoelde rechten en plichten indien dit noodzakelijk is ter vrijwaring van

[...]

d) de openbare veiligheid;

e) het voorkomen, het onderzoeken, opsporen en vervolgen van strafbare feiten of schendingen van de beroepscodes voor gereglementeerde beroepen;

[...]”

G) Rechtsvragen die dit verzoek om een prejudiciële beslissing motiveren

1) Uitlegging:

Verweerster heeft zich erop beroepen dat concrete bepalingen van nationaal recht overeenkomstig richtlijn 2006/24/EG eraan in de weg staan dat zij inlichtingen verstrekt aan de betrokkene. Daarmee rijst de vraag of artikel 7, sub c, van richtlijn 2006/24/EG aldus moet worden uitgelegd dat **[Or. 11]** het in de weg staat aan een verplichting voor een gegevensverwerker om inlichtingen te vertrekken betreffende de gegevensbewaring.

Artikel 7, sub c, van richtlijn 2006/24/EG bepaalt dat toegang tot de overeenkomstig artikel 5 van deze richtlijn bewaarde gegevens slechts geschiedt door „speciaal daartoe bevoegde personen”.

Dit maakt enerzijds de uitlegging mogelijk dat de voor bewaardoeleinden (dus voor een toekomstig, nog onbepaald doel binnen de sfeer van het veiligheidspolitierecht en het strafvervolgingsrecht) bewaarde gegevens uitsluitend voor bepaalde personen uit de kring van de met de tenuitvoerlegging van de desbetreffende wetten belaste autoriteiten toegankelijk gemaakt moeten worden. Daaronder dienen bijvoorbeeld, overeenkomstig de vereisten van de nationale wetgeving, te worden verstaan, ambtenaren van bepaalde politieautoriteiten, het openbaar ministerie en de rechtbanken. In dit geval kan de weigering om de betrokkene toegang te verschaffen tot zijn eigen gegevens kan daardoor worden gerechtvaardigd dat

a) de omvang van de desbetreffende gegevensbewaring wettelijk is vastgelegd en door de betrokkene, ook zonder kennis van de details, probleemloos kan worden nagetrokken, en

b) een aan een „potentiële” dader te verstrekken inlichting betreffende het daadwerkelijk verzoek door de veiligheids- of strafvervolgingsautoriteiten om bewaarde gegevens te verstrekken, dan wel betreffende het ontbreken van een dergelijk verzoek, het doel van een strafprocedure kan verijdelen of vervolging van de dader kan bemoeilijken.

Daartegenover kan uit de aanhef van artikel 7, van richtlijn 2006/24/EG, evenals uit punt 15 van de considerans van deze richtlijn de bedoeling van de Europese wetgever worden afgeleid om de door richtlijn 95/46/EG verleende rechten van de betrokkene niet verder in te perken. Artikel 7, sub c, van richtlijn 2006/24/EG zou dan aldus moeten worden verstaan dat het enkel ziet op het bevel om de daadwerkelijke toegang tot bewaarde gegevens – zowel bij de tot bewaring verplichte gegevensverwerker als bij de tot doorgave van deze gegevens

gemachtigde politie- en justitieautoriteiten – technisch en organisatorisch te beperken.

Anderzijds rijst ook de vraag of de unierechtelijke normen van richtlijn 95/46/EG, inzonderheid artikel 12 juncto artikel 13 daarvan, de lidstaten niet ook in gevallen waarin nog geen concrete strafrechterlijk relevante aanleiding bestaat verplichten om een recht op inlichtingen vast te leggen, dan wel of de gegevensbewaring in het algemeen binnen de werkingssfeer valt van de uitzonderingsbepaling van artikel 13 van richtlijn 95/46/EG [om redenen van openbare veiligheid (sub c) of met het oog op het voorkomen, onderzoeken, opsporen en **[Or. 12]** vervolgen van strafbare feiten (sub d)].

2) Subsidiaire vraag

De als subsidiair aan te merken derde vraag moet worden beantwoord in het geval dat artikel 7 van richtlijn 2006/24/EG, alleen of in samenhang met de artikelen 12 en 13 van richtlijn 95/46/EG (eerste en tweede vraag), in de weg zou staan aan het vastleggen van een recht op inlichtingen. Dan zou ook de vraag rijzen naar de rechtvaardiging van de bijzondere regelingen voor de gegevensbewaring in het licht van artikel 8 van het Handvest. Het met de gegevensbewaring nagestreefde doel van een uit voorzorg verrichte registratie van verkeers- en locatiegegevens van elektronische communicatie (zie artikel 2, lid 2, sub a) vormt een beperking van het fundamentele recht in de zin van artikel 8, lid 2, tweede zin, van het Handvest. Alle gegevens worden zonder uitzondering, preventief, zonder dat daar aanleiding voor bestaat en zonder dat er sprake is van een verdenking tegen de betrokkene, bewaard.

Het Oostenrijkse Verfassungsgerichtshof heeft in een verwijzingsbeschikking van 28 november 2012 (omissis) de volgende bezwaren geuit tegen het bevel tot het bewaren van verkeers- en locatiegegevens (punten 40-46):

„De richtlijn maakt een massale gegevensverzameling mogelijk, zowel met betrekking tot de kring van gegevens, zelfs al is die beperkt tot een catalogus van verkeersgegevens, als met betrekking tot de niet-limitatieve personenkring alsook in verband met de overheidstaken waarvoor die verzameling wordt bevolen. De ‚uitgestrektheid' van de inmenging overtreft daarmee alle inmengingen in het fundamentele recht op gegevensbescherming die tot nu toe in de rechtspraak van het Verfassungsgerichtshof zijn beoordeeld, waarbij ook rekening moet worden gehouden met de mogelijkheden om de in divers verband verzamelde gegevens te koppelen (omissis). De richtlijn gegevensbewaring omvat bovendien bijna uitsluitend personen die geen enkele aanleiding voor de gegevensbewaring hebben gegeven. Tegelijkertijd worden zij – onafhankelijk van hoe het gegevensgebruik concreet wordt ingericht – door de nationale wetgever – onvermijdelijk – aan een verhoogd risico blootgesteld, te weten het risico dat autoriteiten hun gegevens onderzoeken, kennis nemen van de inhoud daarvan, zich aldus op de hoogte stellen van privé gedrag van dergelijke personen en deze gegevens voor andere

doeleinden hergebruiken (bijvoorbeeld als gevolg van de toevallige aanwezigheid in een bepaalde cel op een tijdstip dat voor de onderzoekende autoriteit relevant is).” (Verfassungsgerichtshof, beschikking van 28 november 2012, punten 43 e.v.).

De Datenschutzkommission deelt deze bezwaren, die ook gelden voor de vraag of het door het Handvest gewaarborgde recht op inlichtingen over eigen gegevens door de desbetreffende rechtshandeling kan worden beperkt. De **[Or. 13]** Datenschutzkommission is bovendien van mening dat dit recht op inlichtingen, gelet op het fundamentele Unierecht op gegevensbescherming en ter eerbiediging van de rechten van de betrokkene (bijvoorbeeld om de omvang van de gegevensbewaring te controleren), bijzondere betekenis toekomt.

Voor de Datenschutzkommission

Wenen, 18 januari 2013

(omissis)