



Datum van
inontvangstneming

:

06/12/2017

Zaak C-623/17

Samenvatting van het verzoek om een prejudiciële beslissing overeenkomstig artikel 98, lid 1, van het Reglement voor de procesvoering van het Hof van Justitie

Datum van indiening:

31 oktober 2017

Verwijzende rechter:

Investigatory Powers Tribunal - London (Verenigd Koninkrijk)

Datum van de verwijzingsbeslissing:

18 oktober 2017

Verzoekende partij:

Privacy International

Verwerende partijen:

Secretary of State for Foreign and Commonwealth Affairs

Secretary of State for the Home Department

Government Communications Headquarters (GCHQ)

Security Service (MI5)

Secret Intelligence Service (MI6)

Voorwerp van de procedure in hoofdgeding

Het hoofdgeding heeft betrekking op de verwerving en het gebruik van bulkcommunicatiegegevens door de veiligheids- en inlichtingendiensten van het Verenigd Koninkrijk. Deze omvatten gegevens over het „wie, wanneer, waar, hoe en met wie” van zowel het gebruik van de telefoon als het gebruik van het internet, met inbegrip van de locatie van mobiele en vaste telefoons waarmee gebeld wordt of waarmee oproepen ontvangen worden en de locatie van computers die gebruikt worden om toegang te krijgen tot het internet. De inhoud van dergelijke communicatie behoort niet tot bulkcommunicatiegegevens; deze mogen enkel verworven worden door middel van een rechterlijke beslissing.

Verzoekster heeft beroep ingesteld bij de verwijzende rechter en stelt dat de verwerving en het gebruik van bulkcommunicatiegegevens door de veiligheids- en inlichtingendiensten inbreuk maakt op het recht op eerbiediging van het privéleven bedoeld in artikel 8 EVRM en in strijd is met het Unierecht. Verweerders beweren dat het gebruik van dergelijke bevoegdheden wettig is en essentieel voor onder meer de bescherming van de nationale veiligheid.

Voorwerp en rechtsgrondslag van de prejudiciële vraag

Met zijn verzoek om een prejudiciële beslissing krachtens artikel 267 VWEU wenst de verwijzende rechter van het Hof te vernemen op welke basis het Unierecht van toepassing is op de activiteiten die de nationale veiligheid betreffen van de veiligheids- en inlichtingendiensten van een lidstaat, gelet op artikel 4 VEU, dat bepaalt dat de Europese Unie de essentiële staatsfunctie van bescherming van de nationale veiligheid moet eerbiedigen, waaruit volgt dat de nationale veiligheid de uitsluitende verantwoordelijkheid van elke lidstaat blijft. Indien het Unierecht van toepassing is, wordt het Hof verzocht te verduidelijken welke impact het arrest van 21 december 2016, *Tele2 Sverige en Watson e.a.*, C-203/15 en C-698/15 (EU:C:2016:970), heeft.

Prejudiciële vragen

Overwegende hetgeen volgt:

- a. de capaciteiten (van de veiligheids- en inlichtingendiensten) om de aan hen geleverde bulkcommunicatiegegevens te gebruiken zijn essentieel voor de bescherming van de nationale veiligheid van het Verenigd Koninkrijk, waaronder op het gebied van terrorismebestrijding, contraspionage en de bestrijding van nucleaire proliferatie;
- b. een fundamenteel element van het gebruik van bulkcommunicatiegegevens door de veiligheids- en inlichtingendiensten is om voorheen onbekende bedreigingen voor de nationale veiligheid te ontdekken door middel van niet-gerichte bulktechnieken die afhankelijk zijn van de aggregatie van bulkcommunicatiegegevens op één plaats. Het belangrijkste nut ervan ligt in een snelle identificatie en ontwikkeling van het doelwit, alsook het voorzien van een grond voor actie in geval van een onmiddellijke bedreiging;
- c. de leverancier van een elektronischecommunicatienetwerk is daarna niet verplicht om de bulkcommunicatiegegevens te bewaren (na de periode van hun gebruikelijke bedrijfsmatige vereisten); deze worden enkel bewaard door de Staat (veiligheids- en inlichtingendiensten);
- d. de nationale rechter heeft vastgesteld dat de waarborgen die betrekking hebben op het gebruik van bulkcommunicatiegegevens door de veiligheids- en

inlichtingendiensten (onder voorbehoud van enkele buiten beschouwing gelaten kwesties) in overeenstemming zijn met het EVRM; en

e. de nationale rechter heeft vastgesteld dat de oplegging van de vereisten die gespecificeerd zijn in de punten 119 tot en met 125 van het arrest [van 21 december 2016, *Tele2 Sverige en Watson e.a.*, C-203/15 en C-698/15 (EU:C:2016:970)], indien van toepassing, de maatregelen van de veiligheids- en inlichtingendiensten om de nationale veiligheid te beschermen zullen dwarsbomen en daardoor de nationale veiligheid van het Verenigd Koninkrijk in gevaar brengen;

1. Valt een vereiste in een aanwijzing van een minister aan een leverancier van een elektronisch communicatienetwerk dat bulkcommunicatiegegevens verstrekt worden aan de veiligheids- en inlichtingendiensten van een lidstaat, gezien artikel 4 VEU en artikel 1, lid 3, van richtlijn 2002/58/EG betreffende de persoonlijke levenssfeer en elektronische communicatie, binnen de werkingssfeer van het Unierecht en de e-privacyrichtlijn?

2. Indien het antwoord op de eerste vraag bevestigend is: zijn de in het arrest *Watson* geformuleerde vereisten of andere vereisten, naast de vereisten die worden opgelegd door het EVRM, van toepassing op een dergelijke aanwijzing van een minister? Zo ja, hoe en in welke mate zijn deze vereisten van toepassing, rekening houdende met de essentiële noodzaak voor de veiligheids- en inlichtingendiensten om bulkverwerving en automatische verwerkingstechnieken te gebruiken voor de bescherming van de nationale veiligheid en met de mate waarin dergelijke mogelijkheden op kritieke wijze belemmerd kunnen worden door dergelijke vereisten, voor zover zij verder in overeenstemming zijn met het EVRM?

Aangevoerde bepalingen van Unierecht

Artikelen 4, 5 en 6 VEU

Artikel 16 VWEU

Handvest van de grondrechten, artikelen 7, 8 en 51

Richtlijn 95/46/EG (hierna: „richtlijn gegevensbescherming”), overweging 13 en artikel 3

Richtlijn 2002/58/EG (hierna: „e-privacyrichtlijn”), overweging 11, artikelen 1 en 15

Advies 1/15 (PNR-overeenkomst EU-Canada) van 26 juli 2017 (EU:C:2017:592)

Arresten van 30 mei 2006, *Parlement/Raad en Commissie*, C-317/04 en C-318/04 (EU:C:2006:346); 10 februari 2009, *Ierland/Parlement*, C-301/06 (EU:C:2009:68); 15 december 2009, *Commissie/Italië*, C-387/05,

(EU:C:2009:781); 4 juni 2013, ZZ, C-300/11(EU:C:2013:363), en 21 december 2016, Remondis, C-51/15 (EU:C:2016:985)

Arrest van 8 april 2014, Digital Rights Ireland en Seitlinger e.a., C-293/12 en C-594/12 (EU:C:2014:238) (hierna: „arrest Digital Rights Ireland”)

Arrest van 21 December 2016, Tele2 Sverige and Watson e.a., C-203/15 en C-698/15 (EU:C:2016:970) (hierna: „arrest Watson”)

Conclusies van advocaat-generaal Mengozzi in de adviesprocedure krachtens artikel 218, lid 11, VWEU, bij advies 1/15, EU:C:2016:656 en in de zaak Remondis, C-51/15,(EU:C:2016:504

Mededeling van de Europese Raad (PB C 69I van 23.2.2016, blz. 1) (deel C, punt 5)

Aangevoerde bepalingen van nationaal recht

Telecommunications Act 1984 [telecommunicatiewet]

Data Retention and Investigatory Powers Act 2014 (hierna ook: „DRIPA”) [wet betreffende gegevensbewaring en onderzoeksbevoegdheden]

Aangevoerde bepalingen van internationaal recht

Artikel 8 EVRM; arrest EHRM van 29 juni 2006, Weber en Saravia v Duitsland, verzoekschrift nr. 54934/00, ontvankelijkheidsbeschikking van 29 juni 2006

Korte uiteenzetting van de feiten en de procedure in het hoofdgeding

- 1 Verzoekster is Privacy International, een non-gouvernementele mensenrechtenorganisatie die zich inzet voor de bescherming van de mensenrechten op zowel nationaal als internationaal vlak. Verwerende partijen zijn de minister van Buitenlandse Zaken en Gemenebestzaken, de minister van Binnenlandse Zaken en de drie veiligheids- en inlichtingendiensten, te weten: de Government Communications Headquarters (GCHQ), de Secret Service [veiligheidsdienst] (MI5) en de Secret Intelligence Service [geheime inlichtingendienst] (MI6).
- 2 Krachtens Section 94 van de Telecommunications Act 1984 mag een minister aan een exploitant van een openbaar elektronischecomunicatienetwerk de algemene of specifieke aanwijzingen geven die hij noodzakelijk acht in het belang van de nationale veiligheid. De veiligheids- en inlichtingendiensten hebben bulkcommunicatiegegevens verkregen van openbare elektronischecomunicatienetwerken in overeenstemming met dergelijke aanwijzingen. De gegevens omvatten verkeers- en locatiegegevens die informatie

verstrekken over sociale, commerciële en financiële activiteiten en reizen. De bulkcommunicatiegegevens verworven van openbare elektronische communicatienetwerken worden veilig bewaard door de veiligheids- en inlichtingendiensten. Een fundamenteel kenmerk van veel van de technieken voor het zoeken van bulkcommunicatiegegevens door de inlichtingen- en veiligheidsdiensten is dat deze technieken (bijvoorbeeld filteren en matching) niet-gericht zijn, dat wil zeggen niet gericht op specifieke, bekende doelen.

- 3 De verwijzende rechter is van oordeel dat bulkcommunicatiegegevens zo uitgebreid mogelijk moeten zijn om de verwerving ervan effectief te laten zijn. Indien de extreem moeilijke taak van identificatie van mogelijke dreigingen door personen die op dit moment niet het doel van een onderzoek zijn, omschreven wordt als het zoeken naar een naald in een hooiberg, dan is deze taak onmogelijk zonder toegang tot die hooiberg. Het gebruik van dergelijke gegevens door de veiligheids- en inlichtingendiensten verschilt sterk van een onderzoek door de politie naar een strafbaar feit, waarin de politie wellicht een verdachte geïdentificeerd heeft die kan worden onderworpen aan een gericht onderzoek.
- 4 De verwijzende rechter is op grond van het voorliggende bewijs overtuigd dat bulkcommunicatiegegevens essentieel zijn voor het werk van veiligheids- en inlichtingendiensten bij het tegengaan van ernstige bedreigingen van de openbare veiligheid, onder meer op het gebied van terrorismebestrijding, contraspionage en bestrijding van proliferatie van kernwapens en dat de capaciteiten van veiligheids- en inlichtingendiensten met betrekking tot bulkcommunicatiegegevens, onder meer de capaciteit om bulkcommunicatiegegevens te verwerven en te gebruiken, essentieel zijn voor de bescherming van de nationale veiligheid van het Verenigd Koninkrijk. Dat bewijs betrof onder meer het gebruik van bulkcommunicatiegegevens na in het Verenigd Koninkrijk gepleegde terroristische aanslagen om de daders, die niet onder toezicht stonden, te identificeren. De operationele zaak voor het gebruik van bulkcommunicatiegegevens is beoordeeld in het rapport van de inlichtingen- en veiligheidscommissie van het parlement van het Verenigd Koninkrijk, „Privacy and Security: A modern and transparent legal framework”, 12 maart 2015 (<http://isc.independent.gov.uk/news-archive/12march2015>).
- 5 De verwijzende rechter heeft gedetailleerd bewijs en argumenten overwogen met betrekking tot de waarborgen die van toepassing zijn op de verwerving en het gebruik van bulkcommunicatiegegevens door de veiligheids- en inlichtingendiensten, waaronder de regeling voor het opslaan en bewaren van bulkcommunicatiegegevens en procedures voor de toegang tot en openbaarmaking van bulkcommunicatiegegevens buiten de veiligheids- en inlichtingendiensten, en heeft ook enkele bevindingen gedaan met betrekking tot de vereisten van het EVRM.
- 6 De verwerving van bulkcommunicatiegegevens en de automatische verwerking daarvan door de veiligheids- en inlichtingendiensten is minder indringend dan andere middelen om informatie te verkrijgen, en de mate van inbreuk als resultaat

van het elektronisch zoeken van bulkcommunicatiegegevens mag niet worden overschat.

- 7 De regeling van Section 94 verschilt van de bepalingen van de Data Retention and Investigatory Powers Act 2014, de nationale wet van het Verenigd Koninkrijk die onderzocht werd in het arrest Watson, krachtens welke een openbaar telecommunicatiebedrijf door een minister verplicht kan worden om commerciële gegevens te bewaren, zodat deze indien nodig beschikbaar zijn voor veiligheids- en inlichtingendiensten en andere overheidsinstanties. Anders dan de DRIPA vereist Section 94 van de 1984 Act dat communicatiegegevens geleverd worden door de exploitant aan de veiligheids- en inlichtingendiensten, zodat zij als bulkcommunicatiegegevens door de veiligheids- en inlichtingendiensten worden bewaard.

Belangrijkste argumenten van partijen in het hoofdgeding

Argumenten van verzoekende partij

- 8 Gelet op het arrest Watson is de verwerving van (en toegang tot en gebruik van) bulkcommunicatiegegevens volgens het Unierecht onwettig. De vereisten die van toepassing zijn op bewaarde communicatiegegevens, gespecificeerd door het Hof in de punten 119 tot en met 125 van het arrest Watson (hierna: „Watson-vereisten”), zijn van toepassing in deze nationale veiligheidscontext.
- 9 Nationale veiligheid vormt noch een grond om jurisdictie uit te sluiten, noch een kader dat buiten het Verdrag valt, maar een afwijking. Indien een uitzondering wordt gebruikt om af te wijken van of nadere voorwaarden te stellen aan de rechten en verplichtingen van artikel 5 van de e-privacyrichtlijn, moet deze in overeenstemming zijn met de minimumstandaarden die door het EU-recht worden voorgeschreven. De bewoordingen van artikel 4 VEU dat de Unie de essentiële staatsfuncties moet eerbiedigen, met name de bescherming van de nationale veiligheid, en in het bijzonder dat de nationale veiligheid de uitsluitende verantwoordelijkheid blijft van elke lidstaat, moeten zo worden gelezen dat daarbij enkel administratieve en uitvoerende verantwoordelijkheden worden verleend.
- 10 De activiteiten van de veiligheidsdiensten van de lidstaten vallen hoe dan ook enkel buiten de werkingssfeer van de Verdagen in zoverre zij de bij het Unierecht vastgestelde rechten en plichten niet doorkruisen, met als gevolg dat de Europese Unie noch bevoegd is om te werken aan de nationale veiligheid van een lidstaat, noch om commentaar te leveren op de toereikendheid of ontoereikendheid van de inspanningen van een lidstaat, noch kan eisen dat in dat opzicht bepaalde stappen worden genomen (zie de behandeling van afwijkingen betreffende de nationale veiligheid in de arresten Commissie/Italië, C-387/05, punt 45, en ZZ, C-300/11, punt 38).

Argumenten van verwerende partijen

- 11 De conclusies in het arrest Watson met betrekking tot de DRIPA hebben geen effect op de verwerving van bulkcommunicatiegegevens voor de doeleinden van nationale veiligheid; deze moeten afzonderlijk worden behandeld van de doeleinden met betrekking tot ernstig strafbare feiten die aan de orde zijn in het arrest Watson.
- 12 Indien het arrest Watson van toepassing zou zijn op de nationale veiligheid, zou het niet in overeenstemming zijn met het VEU, aangezien het in strijd is met de artikelen 4 en 5 van het VEU, omdat de nationale veiligheid de uitsluitende verantwoordelijkheid van de lidstaten blijft en zij geen essentiële staatsfuncties aan de Unie hebben toegewezen. De activiteiten van de lidstaten met betrekking tot de nationale veiligheid, door middel van het vereisen van de levering en daarna de toegang tot en het gebruik van bulkcommunicatiegegevens zijn geen afwijkingen van de verplichtingen van de lidstaten krachtens het Verdrag, die strikte uitlegging en beperking vereisen, maar vallen buiten de competentiegrens van het Verdrag.
- 13 Het arrest Watson is in strijd met eerdere rechtspraak van het Hof, met name met het arrest Parlement/Raad en Commissie, C-317 en C-318/04.
- 14 De waarborgen in artikel 8 EVRM zijn in elk geval voldoende om de activiteiten van de lidstaten en de veiligheids- en inlichtingendiensten te controleren, en zorgen voor voldoende evenwicht tussen de bescherming van het publiek en de privacy. Daarnaast zijn de Watson-vereisten niet van toepassing dan wel zouden ze niet van toepassing moeten zijn op bulkcommunicatiegegevens.

Korte uiteenzetting van de motivering van de verwijzing

- 15 Hoewel de verwerking en de overdracht van gegevens in de zaak die aanleiding heeft gegeven tot het arrest Parlement/Raad en Commissie werd verricht door een commerciële onderneming, waarvan de activiteiten onderworpen waren aan de richtlijn gegevensbescherming, heeft het Hof in dat arrest geoordeeld dat de verwerking van dergelijke gegevens plaatsvond in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen, zoals wordt bepaald bij artikel 3, lid 2, van die richtlijn. Het is impliciet in de redenering in het arrest Parlement/Raad en Commissie dat het Hof gekozen heeft voor een teleologische uitlegging: aangezien het doel van het verwerken en de overdracht van gegevens aan de regering van de Verenigde Staten de bevordering van activiteiten van de Staat was, viel de activiteit van de gegevensverwerker buiten de werkingssfeer van het Unierecht.
- 16 Naar analogie daarvan is het uitoefenen van een wettelijke bevoegdheid door de regering van een lidstaat die erin bestaat van telecommunicatiebedrijven te eisen dat zij gegevens overdragen aan de Staat om de nationale veiligheid te beschermen (verwerving) een activiteit van de Staat die niet binnen de

werkings sfeer van het Unierecht valt. Op dezelfde basis valt ook het gebruik door een staat van dergelijke gegevens om de nationale veiligheid te beschermen (gebruik) buiten de werkingssfeer van het Unierecht. Ook het verwerken en overdragen van gegevens voor dergelijke doeleinden door commerciële ondernemingen, zoals vereist door het nationale recht (overdracht), moet buiten de werkingssfeer van het Unierecht vallen.

- 17 Deze kwesties worden niet bepaald door te analyseren of de activiteit in kwestie krachtens de bepalingen van de richtlijn gegevensbescherming en de e-privacyrichtlijn het verwerken van gegevens vormt, maar door te analyseren of het doel van een dergelijke activiteit, qua inhoud en effect, het bevorderen van een essentiële staatsfunctie (artikel 4, lid 2, VEU) is; in dit geval de bescherming van de nationale veiligheid „binnen een door de overheid ingesteld kader dat betrekking heeft op de openbare veiligheid” (arrest Parlement/Raad en Commissie, punt 58).
- 18 Artikel 1, lid 3, van de e-privacyrichtlijn bepaalt dat de richtlijn niet van toepassing is op activiteiten die betrekking hebben op onder andere de openbare veiligheid en de staatsveiligheid, die buiten de werkingssfeer van het Verdrag vallen. Die bewering wordt niet nader uitgewerkt. Artikel 15 van de e-privacyrichtlijn verwijst naar wettelijke maatregelen die lidstaten kunnen treffen ter waarborging van onder andere de nationale veiligheid. De laatste zin van artikel 15, lid 1, bepaalt: *„alle in dit lid bedoelde maatregelen dienen in overeenstemming te zijn met de algemene beginselen van het gemeenschapsrecht, met inbegrip van de beginselen als bedoeld in artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie”*. Deze zin heeft het Hof in het arrest Watson tot de slotsom gebracht dat de maatregelen in artikel 15 binnen de werkingssfeer van de e-privacyrichtlijn en het Handvest vallen. In het kader van de impact van artikelen 4 en 5 VEU en de noodzaak om de richtlijn zo te uit te leggen dat zij in overeenstemming is met de Verdragen heeft die zin wellicht niet die betekenis. Die had hij zeker niet toen de richtlijn werd vastgesteld, omdat artikel 6, leden 1 en 2, toen (vóór het Verdrag van Lissabon) anders was verwoord.
- 19 De laatste zin van artikel 15, lid 1, van de e-privacyrichtlijn moet worden uitgelegd als niets meer dan een herhaling van overweging 11 van die richtlijn (waarmee het anders in conflict is). Daarnaast is het EVRM van toepassing op de activiteiten die bij de artikelen 4 en 5 VEU worden uitgesloten; het Unierecht en het Handvest zijn dat niet.
- 20 Deze analyse kan wellicht het anders ogenschijnlijke conflict oplossen tussen de uitlegging van artikel 15 door het Hof in het arrest Watson en artikel 4, lid 2, VEU en overweging 11 en artikel 1, lid 3, van de e-privacyrichtlijn, die een positief voorbehoud van soevereiniteit door de lidstaten met betrekking tot activiteiten die verband houden met de nationale veiligheid lijken in te houden.

- 21 Als het Unierecht, niettegenstaande het bovenvermelde, wel van toepassing is op zaken met betrekking tot de nationale veiligheid en in het bijzonder op de verwerving en het gebruik van bulkcommunicatiegegevens door veiligheids- en inlichtingendiensten, zijn de vier Watson-vereisten, zoals afgeleid uit de punten 119 tot en met 125 van het arrest Watson:
- i. er is een beperking op elke **niet-gerichte toegang** tot bulkcommunicatiegegevens, onder voorbehoud van verduidelijking van de gevolgen van punt 119 van het arrest;
 - ii. er moet **voorafgaande toestemming** zijn (behalve in gevallen van naar behoren gerechtvaardigde spoedeisendheid) vóór enige toegang tot gegevens (punt 120);
 - iii. er moet worden gezorgd voor **voorafgaande kennisgeving** aan de betrokken personen (punt 121), en
 - iv. alle gegevens moeten worden bewaard **op het grondgebied van de Europese Unie** (punten 122 en 125).

Niet-gerichte toegang

- 22 De nadruk ligt in het arrest Watson op een strafrechtelijk onderzoek, niet op de nationale veiligheid. Punt 119 van het arrest Watson verklaart: *„In bijzondere situaties, zoals die waarin vitale belangen van nationale veiligheid, landsverdediging of openbare veiligheid door terroristische activiteiten worden bedreigd, zou echter ook toegang tot de gegevens van andere personen kunnen worden verleend, wanneer op grond van objectieve elementen kan worden geoordeeld dat deze gegevens in het concrete geval een daadwerkelijke bijdrage tot de bestrijding van dergelijke activiteiten zouden kunnen leveren. ”*
- 23 De verwijzingen naar een „bijzondere situatie” en „in het concrete geval” zijn niet passend wanneer uit het bewijs blijkt dat de beschikbaarheid van automatische verwerking in bulkvorm, dat wil zeggen niet-specifieke automatische verwerking in het belang van de nationale veiligheid, noodzakelijk is. De verwijzing naar „objectieve elementen” is ook ontoereikend en verwijst kennelijk naar wat het Hof in punt 111 verklaard heeft over het gebruik van geografische criteria die in de praktijk niet toegepast kunnen worden bij internationaal terrorisme.

Voorafgaande toestemming

- 24 De betekenis en gevolgen van deze vereiste in de verschillende omstandigheden van het gebruik van bulkcommunicatiegegevens door veiligheids- en inlichtingendiensten is onduidelijk. Is toestemming vereist (a) voorafgaand aan het aanvragen van een levering van de gegevens krachtens Section 94; (b) voorafgaand aan het elektronisch zoeken van de gegevens bij elk voorval (de bescherming van de nationale veiligheid is voortdurende en dezelfde gegevens

kunnen meerdere keren worden geraadpleegd zonder echte inbreuk op het privéleven van degenen wier gegevens worden bewaard, behalve voor diegenen die als gevolg van het automatisch verwerken van gegevens daadwerkelijk van belang kunnen zijn voor de veiligheids- en inlichtingendiensten); of (c) voorafgaand aan de eigenlijke toegang, hetzij gericht hetzij als resultaat van een eerder uitgevoerde elektronische zoekopdracht?

Kennisgeving

- 25 De context in het arrest Watson is die van een bepaald strafrechtelijk onderzoek dat beëindigd is. De noodzaak om de nationale veiligheid te beschermen is voortdurend, net zoals de voortdurende betrokkenheid van grote aantallen mensen bij de planning en uitvoering van terroristische activiteiten. Het gevaar van kennisgeving is niet alleen gerelateerd aan de omstandigheden van een bepaald onderzoek of een bepaald persoon die of dat betrokken is bij dat onderzoek, maar is ook gerelateerd aan verdere operaties, waaronder de methodologie voor de verwerving of het gebruik van de informatie en de identiteit van de betrokkenen.
- 26 De praktische moeilijkheden van kennisgeving ten aanzien van de verwerving of het gebruik van bulkcommunicatiegegevens zijn immens.

Bewaren van gegevens binnen de Europese Unie

- 27 Het is onduidelijk of er een absoluut verbod is op de overdracht van bulkcommunicatiegegevens buiten de Europese Unie, zoals lijkt te volgen uit het arrest Digital Rights Ireland. Daarnaast is het onduidelijk of dat verbod onderworpen is aan toetsing door een onafhankelijke autoriteit, gezien de bewoordingen van punt 123 van het arrest Watson.
- 28 Een absoluut verbod op de overdracht van bulkcommunicatiegegevens buiten de Europese Unie zou ernstige gevolgen hebben voor de soevereiniteit van de lidstaten en voor hun verplichtingen uit de Verdragen met betrekking tot het delen van de inlichtingen, wat van aanzienlijk belang kan zijn in geval van een bedreiging voor de territoriale integriteit (artikel 4, lid 2, VEU) van een lidstaat. Een dergelijke vereiste lijkt duidelijk in strijd met het arrest Parlement/Raad en Commissie, zoals bevestigd door het arrest Ierland/Parlement en het de conclusie van advocaat-generaal Mengozzi bij advies 1/15 over de ontwerpovereenkomst tussen Canada en de Europese Unie inzake de doorgifte en verwerking van gegevens van passagiers. Het lijkt ook inbreuk te maken op artikel 25 van de richtlijn gegevensbescherming, dat is opgenomen in hoofdstuk IV, „Doorgifte van gegevens naar derde landen”, dat uit hoofde van artikel 1, lid 2, van de e-privacyrichtlijn op die richtlijn van toepassing is..

Conclusie over de toepassing van de Watson-vereisten

- 29 Indien de Watson-vereisten van toepassing zijn op de maatregelen voor het beschermen van de nationale veiligheid, in het bijzonder op de regeling inzake

bulkcommunicatiegegevens, zouden zij die maatregelen op basis van het bewijs voor de verwijzende rechter dwarsbomen en het vermogen van de veiligheids- en inlichtingendiensten om de nationale veiligheid te beschermen op kritieke wijze ondermijnen en daarbij de nationale veiligheid van het Verenigd Koninkrijk in gevaar brengen.

- 30 Het Hof wordt verzocht deze gelegenheid te baat te nemen om, door heroverweging of verduidelijking van punt 119 van het arrest Watson of anderszins, te overwegen of de waarborgbepalingen van het EVRM met betrekking tot de verwerving en het gebruik van bulkcommunicatiegegevens door veiligheids- en inlichtingendiensten voldoende zijn om een passend evenwicht te vinden tussen de bescherming van het publiek en de privacy.