Voorzieningenrechter Rechtbank Den Haag
Zitting van 18 februari 2015, te 11.00 uur
Rolnr. 14/1575

Staat der Nederlanden/Stichting Privacy First e.a.

Pleitnota C.M. Bitter en R.J.M. van den Tweel

1 Inleiding

1.1 Dataretentie is een actueel onderwerp in de maatschappelijke discussie over de privacy van burgers. Deze discussie kent vele aspecten en alleen al de technische kant van het onderwerp is complex. Er worden soms grote woorden gebruikt die niet steeds de lading dekken van het onderwerp waar het om gaat. Ook de juridische discussie over de met dataretentie verband houdende vraagstukken is complex. Er moet voor worden gewaakt dat er te snel conclusies worden getrokken, zo ook in deze zaak.

1.2 Privacy van de burger is een groot goed, de effectieve opsporing en vervolging van ernstige misdrijven ook. De overheid heeft de publieke taak om misdrijven op te sporen en op te lossen. Telecommunicatiegegevens spelen bij de opsporing en vervolging van ernstige strafbare feiten een cruciale rol.

1.3 Met betrekking tot de bewaarplicht heeft de wetgever in de wetgeving een balans tussen het belang van privacy en het belang van opsporing aangebracht. Het gaat dan om méér dan alleen de Wet bewaarplicht telecommunicatiegegevens, en dat betekent dat – anders dan wellicht op het eerste gezicht lijkt – het arrest van het Hof van Justitie over de Dataretentierichtlijn géén consequenties heeft in de Nederlandse context. Mede daarom hebben we op voorhand een conclusie van antwoord ingediend om de feiten en het recht helder op een rij te zetten.

1.4 Er moet behoedzaam met dit onderwerp worden omgegaan, juist omdat niet alleen de belangen maar ook de opvattingen zo verschillen, niet alleen in Nederland, maar ook in de andere lidstaten van de EU en tussen de lidstaten en de EU-instellingen. Op dat niveau is de discussie ook niet uitgekristalliseerd. Behoedzaamheid is met name ook geboden omdat eisers in dit kort geding de buitenwerkingstelling van een wet in formele zin vorderen. Buiten toepassing laten van een wet in formele zin kan alleen bij een *onmiskenbare* onverbindendheid wegens strijd met een ieder verbindende

bepaling van hoger internationaal recht. De vaste rechtspraak van de Hoge Raad geldt hier onverkort.

> Zie bijvoorbeeld recent Voorzieningenrechter Rb Den Haag, 11 januari 2013 inzake de Wet normering topinkomens (ECLI:NL:RBDHA:2013:BY8165).

1.5 Eisers vorderen de buitenwerkingstelling van de Wet bewaarplicht telecommunicatiegegevens (hierna: Wbt) en beroepen zich daarbij in hoofdzaak op het arrest van het Hof van Justitie van 8 april 2014, waarbij de Dataretentierichtlijn ongeldig is verklaard.

1.6 De ongeldigverklaring van de Richtlijn door het Hof van Justitie betekent echter niet automatisch dat de Wbt evenzeer ongeldig is. De Wbt zal overeenkomstig artikel 15, lid 1 van de e-Privacyrichtlijn weliswaar in overeenstemming dienen te zijn met algemene beginselen van het Unierecht, waaronder de artikelen 7 en 8 van het Handvest van de grondrechten van de EU, en met art. 8 EVRM. De Wbt zal echter op de eigen merites moeten worden getoetst. Vanzelfsprekend worden de overwegingen van het Hof daarbij betrokken.

1.7 Naar het oordeel van de Staat is van een onverbindendheid van de Wbt wegens strijd met deze verdragsbepalingen geen sprake, nog daargelaten dat er van onmiskenbare onverbindendheid sprake zou zijn. De inbreuk op de privacy is met voldoende waarborgen omgeven en bovendien gerechtvaardigd. Daarbij mag ook het doel dat met de dataretentie is beoogd niet uit het zicht worden verloren.

2 De bewaarplicht en het belang voor de opsporing en vervolging

2.1 In de conclusie van antwoord is uiteengezet waartoe de Wbt strekt. De Wbt stelt zeker dat telecommunicatiegegevens een half jaar respectievelijk een jaar worden bewaard, zodat deze gegevens – alleen in de daarvoor nader in het Wetboek van Strafvordering (hierna: Sv) omschreven gevallen en onder de voorgeschreven voorwaarden - beschikbaar zijn voor de opsporing. De gegevens worden bewaard door de aanbieders van de diensten zelf; zij zijn dus niet bij politie/justitie opgeslagen. Politie en justitie beschikken dus niet over een grote databak met gegevens waaruit zij naar believen kunnen putten. Op grond van de regeling van Sv kan de officier van justitie de gegevens uitsluitend in een concreet geval van verdenking van bepaalde, ernstige en zeer ernstige misdrijven, in het belang van het onderzoek vorderen. Dit betekent dat technieken als 'mass surveillance', datamining en profiling technisch niet mogelijk en ook niet aan de orde zijn. Voor andere doeleinden dan opsporing en vervolging, in de omschreven gevallen, mogen de gegevens niet worden gebruikt. Als de bewaartermijn voorbij is, moeten ze zonder meer worden vernietigd. Het Agentschap Telecom houdt daar toezicht op. Ook het Cbp houdt toezicht op de verwerking van de gegevens. Van belang is bovendien dat de Wbt geen betrekking heeft op de inhoud van de

communicatie. Dat is relevant, omdat beide onder het toepassingsbereik van art. 8 EVRM vallen, maar de aard en ernst van de inmenging ingeval van verkeersgegevens veel kleiner is dan ingeval van het verwerken van de inhoud van de communicatie. Deze rechtbank heeft dat nog recent vastgesteld (Rb. Den Haag 23 juli 2014, ECLI:NL:RBDHA:2014:8966).

2.2 Bij de opsporing van misdrijven spelen gegevens die bij derden beschikbaar zijn een onmisbare rol. Deze rol neemt steeds meer toe. De samenleving is de afgelopen twintig jaar ingrijpend gewijzigd. Naast de fysieke, analoge wereld is een geheel nieuwe, virtuele wereld ontstaan. Belangrijke delen van het sociale en economische leven hebben zich naar die virtuele wereld verplaatst. Veel economische activiteiten zijn sterk afhankelijk van het internet en de moderne communicatiemiddelen. Die snelle ontwikkeling van telecommunicatie en internet is ook gepaard gegaan met nieuwe vormen van criminaliteit: cybercrime, internetoplichting en DDOS-aanvallen, die de samenleving ernstig kunnen ontwrichten, maar ook zedendelicten als kinderporno en grooming (het via internet benaderen van kinderen voor seksuele doeleinden). Deze vormen van criminaliteit laten nagenoeg uitsluitend op het internet hun sporen achter en zijn dan ook alleen op te sporen met behulp van het internet, in veel gevallen alleen door een analyse te maken van wat er voorafgaand aan het delict is gebeurd, ofwel van historische gegevens.

> Zo is een hacker binnengedrongen in de infrastructuur van een grote communicatieaanbieder en had daar enorme schade kunnen toebrengen. De hacker is tijdig aangehouden dankzij onderzoek aan de hand van historische gegevens van de gebruikte IP-adressen.
>
> In veel gevallen van fraude met internetbankieren, digitale diefstal, kinderporno, ronselen of rekruteren van personen voor de jihad, is het IP-adres van de computer die de verdachte heeft gebruikt het enige spoor. Zijn de internetgegevens niet meer beschikbaar, dan is een strafrechtelijk onderzoek onmogelijk.

Kan met klassieke opsporingsmethoden onderzoek worden gedaan naar de zichtbare, fysieke sporen die de pleger van het misdrijf heeft achtergelaten – bijv. vingerafdrukken, voetsporen, bloedsporen – dat is bij internetcriminaliteit niet mogelijk. De sporen zijn dan uitsluitend of in relevante mate in digitale vorm beschikbaar, bij de aanbieders van telecommunicatie en de serviceproviders.

2.3 Ook meer klassieke vormen van criminaliteit worden in toenemende mate gepleegd met behulp van het internet en (mobiele) telecommunicatie. Misdrijven waarbij communicatie centraal staat: stalking, verspreiding van kinderporno, bedreiging en de opruiing tot terroristische misdrijven. De opsporing van deze misdrijven is in toenemende mate afhankelijk geworden van de beschikbaarheid van internet- en

verkeersgegevens, al dan niet samen met klassieke opsporingsmethoden. Zo kan met verkeersgegevens een verdachte met een bepaalde locatie worden verbonden, of kan uit telefonische contacten blijken dat verdachten elkaar kennen. Er kunnen ook (belastende, maar ook ontlastende) contacten met slachtoffers en derden blijken.

> Misdrijven in de persoonlijke sfeer, geweldsdelicten en zedendelicten, stalking, die diep ingrijpen in het leven van het slachtoffer, kunnen vaak alleen succesvol worden opgespoord en vervolgd als verkeersgegevens beschikbaar zijn.
>
> De zaak Benaouf A. is illustratief. Benaouf A., die werd verdacht van medeplichtigheid aan een liquidatie, beriep zich tegenover het OM lange tijd op zijn zwijgrecht. Pas zeven maanden na zijn aanhouding legde hij een verklaring af, waarin hij een alternatief scenario schetste en waarin hij een inmiddels overleden derde als dader aanwees. Met behulp van historische telefoongegevens kon het OM vaststellen dat het alternatieve scenario niet juist was. Benaouf A. is inmiddels veroordeeld. De rechtbank heeft de telefoongegevens expliciet benoemd in haar uitspraak (rechtbank Amsterdam 1 december 2014, ECLI:NL:RBAMS:2014:8047).
>
> In de zaak Robert M. zijn de historische verkeersgegevens van cruciaal belang geweest om bewijs te verzamelen voor het grootschalige misbruik, maar ook om slachtoffers en medeverdachten in beeld te krijgen. Tot op heden zijn in Nederland en in het buitenland meer dan honderdvijftig verdachten aangehouden. Meer dan honderd kinderen konden uit een actuele misbruiksituatie worden bevrijd. Met uitzondering van een (zeer) beperkt aantal gevallen was een gebruikt IP-adres de enige aanwijzing die kon leiden tot de identiteit van een verdachte of slachtoffer.
>
> Op 12 februari 2015 heeft de rechtbank Amsterdam een man veroordeeld tot een meerjarige gevangenisstraf, omdat hij gedurende een periode van meer dan zeven jaren met misleiding en bedreiging met zeer grote regelmaat jonge kinderen er toe had gebracht voor de webcam seksuele poses aan te nemen en seksuele handelingen te verrichten (ECLI:NL:RBAMS:2015:673). De opnames die hij daarvan maakte, heeft hij bewaard en verspreid, ook naar andere kinderen. De rechtbank beschrijft hoe de man, die voor zijn contacten een hotmail adres op naam van een ander gebruikte, is opgespoord (r.o. 4.1): onderzoek naar het IP adres gebruikt door verdachte in dreigende chats met een kind van twaalf leidde naar zijn woning, waar bij een doorzoeking in zijn computer veel belastend materiaal werd gevonden. De rechtbank overweegt ook nog (r.o. 8.4): "De enkele filmfragmenten die de rechtbank ter terechtzitting kort heeft besproken zijn echter ronduit schokkend te noemen en geven een kort inzicht in de afschuwelijke wereld

van de kinderporno-industrie. De rechtbank onderstreept dat het verwerven van kinderporno, relatief gemakkelijk vanachter een computer thuis en zogenaamd op afstand, krachtig moet worden bestreden."
Op het moment van de eerste aangifte waren zelfs de laatste chatcontacten al meer dan een maand oud, zodat zonder bewaarplicht niet gewaarborgd is dat de gegevens nog beschikbaar zijn.

In de afgelopen twee weken zijn nog twee andere uitspraken gedaan, waarin telecommunicatiegegevens een prominente rol spelen. Op 6 februari 2015 heeft de rechtbank Limburg een man tot vijftien jaar cel veroordeeld voor doodslag en diefstal (ECLI:NL:RBLIM:2015:999) en op 13 februari 2015 heeft de rechtbank Den Haag meerdere leden van de Trailer Trash Travellers veroordeeld voor afpersing met geweld (ECLI:NL:RBDHA:2015:1460). Dit onderstreept hoe veelvuldig er bij de opsporing gebruik wordt gemaakt van telecommunicatiegegevens en dat het om een effectief opsporingsmiddel gaat.
De memorie van toelichting bij het conceptwetsvoorstel en het door de Staat overgelegde rapport van de Europese Commissie van maart 2013 (productie 2 bij de conclusie van antwoord) geven talloze andere voorbeelden van gevallen waarin de bewaarplicht een belangrijke rol in de opsporing en vervolging heeft gespeeld.

2.4 Zonder historische verkeersgegevens is de kans op een positieve identificatie van de dader van het strafbare feit met name bij de misdrijven die met behulp van of op het internet worden gepleegd erg klein tot nihil. Bovendien zal het bij gebreke van historische verkeersgegevens vaker noodzakelijk zijn om zwaardere middelen in te zetten, met een verdergaande inbreuk op de privacy ten gevolge, zoals het tappen van het telefoonverkeer. In sommige gevallen is het misdrijf dus niet op te lossen. Uit het al genoemde rapport van de Europese Commissie van maart 2013 blijkt ook dat in Duitsland, waar op enig moment is gestopt met het bewaren van historische verkeersgegevens, een substantieel deel van de onderzoeken vastliep vanwege het ontbreken van historische verkeersgegevens. Dat is zorgwekkend.

2.5 De Staat meent dat de noodzaak van een bewaarplicht voor de opsporing hiermee meer dan voldoende is aangetoond. Alternatieven zijn er niet. Zoals ook het WODC heeft geconcludeerd,[1] is bijvoorbeeld het gericht bevriezen van gegevens geen reëel alternatief. Hiermee kunnen immers geen gegevens worden opgevraagd die in het verleden zijn vastgelegd, terwijl deze gegevens cruciaal zijn om het strafbare feit te kunnen opsporen en/of de gedragingen van betrokkenen in de juiste context te kunnen plaatsen. Met deze gegevens kunnen relaties (netwerken) van betrokkenen in beeld worden gebracht en gegevens over de plaats delict (in samenhang met andere

[1] WODC-rapport p. 146

opsporingsmethoden) in kaart worden gebracht. Het beperken van de bewaarplicht tot gegevens van personen die verdacht worden of zijn geweest van strafbare feiten is geen reëel alternatief, daargelaten hoe dat er in de praktijk uit zou moeten zien. Op die manier kunnen bijv. 'first offenders' immers niet worden opgespoord. Ook kunnen alibi's van verdachten waarin niet-verdachte personen en slachtoffers een rol spelen, niet worden nagetrokken. Geen van de hiervoor genoemde voorbeelden had kunnen worden opgelost als de bewaarplicht zou moeten worden beperkt tot personen die worden of zijn verdacht (geweest) van strafbare feiten. Zonder bewaarplicht kunnen ernstige en zeer ernstige misdrijven niet of te vaak niet worden opgelost, waardoor slachtoffers in de kou blijven staan. Opsporing en vervolging kunnen in het huidige digitale tijdperk niet meer zonder een bewaarplicht. Toewijzing van de vorderingen zou dus voor de opsporing zeer ernstige gevolgen hebben.

2.6 In de strafrechtpraktijk is door de verdediging een beroep gedaan op het arrest van het Hof van Justitie van 8 april 2014 en de onverbindendheid van de Wbt. De strafrechter heeft zich inmiddels expliciet uitgelaten over de rechtsgeldigheid van de Wbt, en overwogen in het arrest van het Hof van Justitie geen aanleiding te zien voor het oordeel dat de Wbt onverbindend zou zijn, en voor het buiten beschouwing laten van bewijs dat is verkregen met behulp van verkeers- en/of gebruikersgegevens die worden bewaard op grond van de Wbt (Gerechtshof Amsterdam 27 mei 2014, ECLI:NL:GHAMS:2014:2028 en Gerechtshof Amsterdam 9 mei 2014, ECLI:NL:GHAMS:2014:1835). Reeds gezien dit oordeel van de strafrechter kan bezwaarlijk worden geconcludeerd dat sprake zou zijn van onmiskenbare onverbindendheid van de Wbt.

3 Het oordeel van het HvJ EU over artikel 7 en 8 Handvest

3.1 Algemene opmerkingen

3.1.1 Uit het arrest van het Hof van Justitie van 8 april 2014 over de ongeldigheid van de Dataretentierichtlijn kan hoe dan ook niet de conclusie worden getrokken dat de Wbt op dezelfde gronden in strijd is met de artikelen 7 en 8 van het Handvest.

3.1.2 Het is van belang om te beseffen dat het Hof van Justitie zich enkel heeft uitgesproken en heeft kunnen uitspreken over de ongeldigheid van de richtlijn. Het Hof van Justitie heeft géén bevoegdheid tot de uitleg of toetsing van nationale regelgeving. Bovendien gaat het hier om een richtlijn die niet rechtstreeks toepasselijk is in de rechtsorde van de lidstaten. De richtlijn laat aan de lidstaten de ruimte en de bevoegdheid om in lijn met het nationale systeem de concrete wijze van implementatie van de richtlijn in hun rechtsorde te kiezen (artikel 288 VWEU). Ook de Dataretentierichtlijn laat de lidstaten op tal van onderdelen de ruimte om concrete, nadere invulling te geven aan diverse

onderdelen. Het gaat om minimumharmonisatie en *niet* om volledige harmonisatie.[2] Het Hof van Justitie heeft zich niet uitgelaten over de concrete invulling van de lidstaten maar was wel kritisch over de ruimte die de richtlijn in dit verband aan de lidstaten liet. Die ruimte was te groot.[3]

3.1.3 Nederland heeft deze ruimte echter niet ten volle benut. In ieder geval moet de Wbt op zijn eigen merites én in samenhang met alle overige waarborgen, zoals onder meer de waarborgen uit Sv (en die uit de Wet bescherming persoonsgegevens) worden beoordeeld. Als we daarbij de overwegingen van het Hof van Justitie tot richtsnoer nemen, moet de conclusie zijn dat de Wbt niet in strijd is met de artikelen 7 en 8 van het Handvest en geen ongerechtvaardigde inbreuk vormt op het privé-leven of de privacy.[4]

3.2 De inmenging is geregeld bij wet, dient een doel van algemeen belang en is geschikt

3.2.1 In de eerste plaats is van belang te constateren dat het Hof de aard en ernst van de inmenging (van de bewaarplicht en de toegang tot de bewaarde gegevens) nuanceert door er op te wijzen dat de voorgeschreven bewaring van gegevens niet raakt aan de inhoud van die gegevens. De richtlijn biedt niet de mogelijkheid om kennis te nemen van de inhoud zelf van de elektronische communicaties (punt 39 van het arrest).

3.2.2 De bewaring van de verkeersgegevens doet naar het oordeel van het Hof ook geen afbreuk aan de wezenlijke inhoud het recht op bescherming van persoonsgegevens omdat de richtlijn de lidstaten verplicht om waarborgen te creëren met betrekking tot gegevensbescherming en – beveiliging (punt 40 van het arrest). Nederland heeft aan die verplichting voldaan; daar komen wij straks over te spreken (zie ook de conclusie van antwoord).

3.2.3 Verder is het Hof het met de Uniewetgever eens dat de inmenging voldoet aan een evident doel van algemeen belang, namelijk om te garanderen dat de gegevens beschikbaar zijn met het oog op het onderzoek, de opsporing en de vervolging van ernstige criminaliteit, en de bescherming van de openbare veiligheid (punten 41 t/m 44). Bewaring van gegevens is in de visie van het Hof een geschikt instrument voor de verwezenlijking van dat legitieme doel.

3.3 De inmenging van de bewaring en van de toegang hangen samen

3.3.1 Alleen met betrekking tot het sluitstuk van de evenredigheidstoets (is de inmenging ook noodzakelijk?) plaatst het Hof van Justitie enkele kritische opmerkingen. Die kritische opmerkingen moeten wel in hun onderlinge verband worden bezien. Uit niets

[2] Zie ook punt 42 e.v. van de conclusie van A-G Cruz Villalón in zaak C-293/12.
[3] Zie punten 113, 117 t/m 120 en 123 van de conclusie van A-G Cruz Villalón in zaak C-293/12.
[4] A-G Cruz Villalón lijkt daar ook expliciet rekening mee te houden, zie punt 157 van zijn conclusie.

blijkt dat de geconstateerde gebreken in de richtlijn ieder afzonderlijk reeds tot ongeldigheid leiden. Integendeel, het gaat juist om de combinatie van gebreken die het Hof tot dit oordeel brengt.

3.3.2 Zo constateert het Hof allereerst (in punten 57 t/m 59) dat de richtlijn zonder onderscheid van personen en zonder enige beperking van toepassing is. De richtlijn is dus ook van toepassing op personen ten aanzien van wie geen enkele aanwijzing bestaat dat hun gedrag een verband vertoont met zware criminaliteit. Ook wordt in de richtlijn geen enkel verband vereist tussen de gegevens die moeten worden bewaard en de bedreiging van de openbare veiligheid.

3.3.3 Dat leidt echter niet tot de conclusie dat een dergelijke ruime bewaarplicht ten algemene niet kan. Immers, in dat geval had het Hof al tot ongeldigheid kunnen concluderen, want als inmenging van de bewaarplicht niet kan worden gerechtvaardigd, komen we niet toe aan een toets van de inmenging als gevolg van de toegang tot de bewaarde gegevens. In plaats daarvan buigt het Hof zich vervolgens (in de punten 60 e.v.) over de vraag of de Dataretentierichtlijn voldoende waarborgen biedt voor die toegang. Hieruit moet worden afgeleid dat, wanneer ten aanzien van de toegang de noodzakelijke waarborgen en garanties worden geboden, óók de bewaring van de gegevens, zelfs zonder enig onderscheid, beperking of uitzondering, in overeenstemming moet worden geacht met de artikelen 7 en 8 van het Handvest. Met andere woorden, de garanties met betrekking tot de toegang kunnen tevens dienen als garanties voor de bewaring van gegevens waarmee van een ongerechtvaardigde, laat staan een onmiskenbaar ongerechtvaardigde, inbreuk geen sprake is.[5]

3.3.4 Bovendien, indien met betrekking tot het bewaren aan deze kritiek tegemoet zou moeten worden gekomen, zouden enkel bij een concrete verdenking en na een vordering van het OM gegevens kunnen worden bewaard en veilig gesteld voor onderzoek later. Zoals hiervoor is toegelicht, is het bevriezen van gegevens echter geen reëel alternatief voor de bewaarplicht.

3.3.5 Kernvraag in dit kort geding zal dus zijn of de garanties die in de Dataretentierichtlijn ontbraken, wél aanwezig zijn in de Nederlandse wetgeving. Dat is het geval.

3.4 De Nederlandse wet biedt voldoende garanties: de inmenging is gerechtvaardigd

3.4.1 Het Hof meent dat de richtlijn geen objectieve criteria bevat ter begrenzing van de toegang tot de bewaarde gegevens. Ook wordt het doel, de bestrijding van ernstige criminaliteit, onvoldoende duidelijk bepaald doordat in artikel 1 lid 1 van de richtlijn slechts wordt verwezen naar de nationale definities van ernstige criminaliteit. Dit laat ruimte, teveel ruimte voor een eigen invulling door de lidstaten. Daarmee is niet

[5] Zie ook uitdrukkelijk A-G Cruz Villalón in punten 121 en 122 van zijn conclusie in zaak C-293/12.

verzekerd dat de toegang tot de bewaarde gegevens strikt gebonden is aan het legitieme doel, namelijk om nauwkeurig afgebakende zware criminaliteit te voorkomen, op te sporen of strafrechtelijk te vervolgen.

3.4.2 De Wbt biedt die duidelijke afbakening wél, namelijk door de verwijzing naar de regeling voor de toegang tot de gegevens ten behoeve van de opsporing en vervolging van ernstige strafbare feiten in Sv. De raadpleging van de gegevens is beperkt tot de opsporing en vervolging van ernstige strafbare feiten waarvoor voorlopige hechtenis is toegestaan (misdrijven als bedoeld in artikel 67 Sv, waarop een gevangenisstraf van vier jaar of meer staat, en een aantal afzonderlijk benoemde misdrijven) of van terroristische misdrijven.

3.4.3 De door het Hof (in punten 60 t/m 62 van het arrest) gesignaleerde tekortkomingen bestaan dus in het geval van de Nederlandse regelgeving niet. De op de bewaarplicht toepasselijke Nederlandse regelgeving bevat – anders dan de richtlijn – wél de nodige objectieve criteria wat betreft de bewaring, beveiliging en toegang, en omschrijft het doel waarvoor de bewaarde gegevens mogen worden geraadpleegd, heel precies. Daar kan geen misverstand over bestaan.

3.4.4 Ook het ontbreken van voldoende garanties dat de bewaarde gegevens doeltreffend worden beschermd, doet zich in Nederland niet voor. Op grond van het op artikel 13.5, leden 2 en 3 Tw gebaseerde Besluit beveiliging gegevens telecommunicatie (Bbgt) moeten de aanbieders een bijzonder hoog niveau van bescherming en beveiliging bieden. Aanbieders van telecommunicatiediensten moeten bepaalde beginselen van gegevensbescherming en –beveiliging respecteren. Zij zijn verplicht om ervoor te waken dat gegevens per ongeluk of onrechtmatig worden vernietigd dan wel per ongeluk verloren raken of worden gewijzigd (vgl. punt 40 van het arrest van het HvJ). Deze voorschriften zijn in Nederland gedetailleerd vastgelegd in het Bbgt. In dit Besluit zijn strikte voorschriften gesteld aan de personen die toegang tot de gegevens kunnen hebben en medewerking kunnen geven aan een vordering van het OM (zie par. 3.2.15 van de conclusie van antwoord). Het Agentschap Telecom en het College bescherming persoonsgegevens houden hier toezicht op.

3.4.5 Dat toezicht is adequaat, uit de jaarverslagen blijkt niet dat AT onvoldoende toezicht heeft kunnen houden. Slechts enkele kleine aanbieders bewaren hun gebruikersgegevens buiten het grondgebied van de EU. De zes grote aanbieders, die zelf al ruim 90% van de gegevens vertegenwoordigen, slaan de gegevens binnen de EU op. Om te kunnen waarborgen dat dit in de toekomst ook zo blijft, wordt in het conceptwetsvoorstel, conform het arrest van het Hof van Justitie, opslag binnen de EU verplicht gesteld.

3.4.6 De toegang tot de bewaarde gegevens is ook onderworpen aan een voorafgaande controle. Anders dan door eisers wordt betoogd, volgt duidelijk uit punt 62 van het

arrest dat deze voorafgaande controle niet uitsluitend een rechterlijke controle kan zijn, maar ook een controle door een onafhankelijke administratieve instantie mag zijn. Niet goed valt in te zien waarom het openbaar ministerie niet als een onafhankelijke administratieve instantie kan worden aangemerkt, als bedoeld in het arrest van het Hof.

3.4.7 In Sv is precies geregeld in welke gevallen een opsporingsambtenaar bepaalde telecommunicatiegegevens, de zogenaamde gebruikersgegevens, mag vorderen. Die bevoegdheid is beperkter dan de bevoegdheid van een officier van justitie (zie par. 3.2.6 t/m 3.2.11 van de conclusie van antwoord). In beide gevallen wordt niet lichtzinnig omgegaan met de bevoegdheden. Het gaat – bij het maken van een inbreuk op de privacy – steeds om een afweging tussen privacy - en opsporingsbelang. De officier van justitie maakt die afweging in het concrete geval en weegt daarbij die belangen steeds opnieuw af. Daarbij is steeds de vraag welk middel het meest resultaat heeft met zo min mogelijke inbreuken op de privacy of andere grondrechten. Er is sprake van gerichte bevraging in het concrete geval. Het opvragen van de gegevens gebeurt niet lichtvaardig, maar alleen als er redelijkerwijs geen andere, minder inbreuk makende mogelijkheden zijn om de waarheid omtrent ernstige misdrijven aan te tonen.

3.4.8 In elk geval kan er achteraf rechterlijke controle plaatsvinden bij een vervolging. Er zijn de Staat geen gevallen bekend waarin in het strafproces gebruikte telecommunicatiegegevens als onrechtmatig verkregen buiten beschouwing gebleven. Als voorbeeld kan op de al genoemde arresten van het Gerechtshof Amsterdam van 9 en 27 mei 2014 (ECLI:NL:GHAMS:2014:1835 en ECLI:NL:GHAMS:2014:2028) worden gewezen.

3.4.9 Om twijfels weg te nemen en extra waarborgen te creëren, is een conceptwetsvoorstel opgesteld dat inmiddels in consultatie is gegeven. Voorgesteld wordt om een differentiatie aan te brengen in de mate waarin een officier van justitie toegang heeft tot de telefoongegevens. Er wordt een onderscheid gemaakt tussen zeer ernstige misdrijven en ernstige misdrijven. Alleen in het eerste geval kunnen gegevens tot een jaar terug worden opgevraagd. In het tweede geval kunnen alleen gegevens tot zes maanden terug worden opgevraagd. Internetgegevens worden hoe dan ook maar zes maanden bewaard. Verder wordt voorgesteld dat historische verkeersgegevens kunnen worden gevorderd na een vooraf verkregen machtiging van de rechter-commissaris. Daarmee zou worden voorzien in de zwaarste vorm van voorafgaand toezicht, zwaarder dan is voorgeschreven voor ingrijpende opsporingsmiddelen als bijvoorbeeld infiltratie.

3.4.10 Ten slotte plaatst het Hof (in de punten 63 en 64) nog een opmerking over de bewaartermijn; op grond van de richtlijn geldt deze bewaartermijn zonder dat enig onderscheid wordt gemaakt tussen de categorieën van gegevens, en de termijn van

bewaring (maximaal 24 maanden) is bovendien niet bepaald op basis van objectieve criteria. Ook hier geldt dat de Nederlandse regelgeving wél is beperkt tot wat strikt noodzakelijk is, ook zonder de voorgestelde differentiatie. Op grond van de Wbt is de bewaartermijn voor de telefoongegevens twaalf maanden en voor internetgegevens zes maanden. Daarmee zit Nederland aan de onderzijde van de termijnen die de richtlijn noemt. En daarmee blijft Nederland ook binnen de bewaringsduur die A-G Cruz Villalón nog als noodzakelijk en evenredig aanmerkt.[6]

3.4.11 In de praktijk blijkt dat een bewaartermijn van twaalf maanden noodzakelijk is. Diverse zaken hadden niet kunnen worden opgelost, als een kortere bewaartermijn had gegolden.

> De hiervoor al genoemde zaak Benaouf A. is illustratief. Pas zeven maanden na zijn aanhouding legde hij een verklaring af, waarin hij een alternatief scenario schetste. Met behulp van historische telefoongegevens kon het OM vaststellen dat het alternatieve scenario niet juist was. Wanneer een bewaartermijn van zes maanden had gegolden, had het OM dit niet kunnen vaststellen.

Uit het WODC-rapport volgt dat in 2012 34,6% van de opgevraagde telecommunicatiegegevens ouder was dan zes maanden.[7]

3.4.12 De conclusie is dat de diverse tekortkomingen die het Hof van Justitie met betrekking tot de richtlijn constateert, zich in de Nederlandse regelgeving niet voordoen. Daarin zijn de nodige duidelijke en precieze regels en garanties opgenomen, waarmee voldoende is gewaarborgd dat de inmenging op de privacy daadwerkelijk beperkt is tot het strikt noodzakelijke. De stapeling van gebreken die het Hof heeft geleid tot de ongeldigverklaring van de richtlijn, doet zich in de Nederlandse situatie niet voor. Voor een buitenwerkingstelling van de Wbt bestaat dus geen aanleiding.

3.4.13 Het arrest van het Hof heeft veel discussie en hernieuwd verzet tegen de bewaarplicht opgeroepen, waarbij soms nuances uit het oog worden verloren. In Nederland is de discussie onder meer beïnvloed door de voorlichting van de Raad van State. De nuance dat de Raad van State zich primair heeft uitgesproken over de Wbt en niet zozeer over het geheel van samenhangende waarborgen in Sv en de Tw, is daarbij uit het zicht geraakt. Ook is weinig aandacht besteed aan het feit dat de Raad van State heeft vastgesteld dat het in de eerste plaats aan de wetgever en in de tweede plaats aan de rechter is om zich uit te laten over de geldigheid van de Wbt. Om een einde te maken aan alle discussie en buiten twijfel te stellen dat de nationale wetgeving in

[6] Zie punt 149 van zijn conclusie in zaak C-293/12
[7] WODC-rapport, p. 120 en 125.

overeenstemming is met het Handvest, is spoedig het genoemde conceptwetsvoorstel tot wijziging van Sv en de Tw opgesteld.

3.4.14 Ook in andere lidstaten is de discussie over de bewaarplicht opgelaaid. Zoals is toegelicht in de conclusie van antwoord, heeft de discussie tot verschillende uitkomsten in de lidstaten geleid. In enkele lidstaten is de bewaarplicht buiten werking gesteld, maar in verreweg de meeste lidstaten geldt de bewaarplicht nog steeds. Dit kan onder meer worden verklaard door het feit dat de lidstaten verschillend zijn omgegaan met de implementatieruimte in de richtlijn (zie productie 1 bij de conclusie van antwoord).

3.4.15 Tot slot is ook op Europees niveau discussie ontstaan over de bewaarplicht. Zo heeft bondskanselier Merkel in januari, naar aanleiding van de aanslagen in Parijs, bekendgemaakt dat zij bedrijven weer wil kunnen verplichten om hun telecomgegevens op te slaan. Daarnaast overdenkt de Europese Commissie nieuwe regels inzake een bewaarplicht. Mede gelet hierop is het naar mening van de Staat niet wenselijk de bewaarplicht nu overhaast op te schorten.

4 Ook geen schending artikel 8 EVRM

4.1 Aangezien artikel 7 van het Handvest een equivalent is van artikel 8 EVRM en het Hof van Justitie zich bij de toetsing van de Dataretentierichtlijn mede heeft laten leiden door de rechtspraak van het Europese Hof voor de Rechten van de Mens (EHRM), volgt uit het vorenstaande al dat eveneens geen sprake kan zijn van een schending van artikel 8 EVRM. Maar ook als we preciezer naar die casuïstische rechtspraak kijken, kan de conclusie geen andere zijn. Dit is al toegelicht in de conclusie van antwoord.

4.2 Net als het Hof van Justitie onderkent het EHRM het nut en de noodzaak van het bewaren van bepaalde privacygevoelige gegevens. Bij de toetsing van de noodzakelijkheid en evenredigheid daarvan neemt het EHRM in ogenschouw dat de verdragsstaten hier een "margin of appreciation" hebben.[8] En die marge is ruimer naar mate over het onderwerp minder overeenstemming bestaat en de uitvoeringspraktijken in de verdragsstaten onderling afwijken. Het is niet aan het EHRM om daar zijn eigen oordeel voor in de plaats te stellen. Verder neemt het EHRM in ogenschouw dat de toets anders kan uitpakken al naar gelang de aard en ernst van de inmenging. In de casuïstiek van het EHRM, waar eisers zich ook op beroepen, gaat het om uiteenlopende inbreuken, variërend van het voor onbepaalde duur bewaren van DNA-gegevens waartoe de betreffende overheid ongeclausuleerd toegang had, tot het strategisch monitoren van gesprekken zonder wettelijke basis.

[8] Idem punt 145 van de conclusie van A-G Cruz Villalón in zaak C-293/12.

4.3 Uit de rechtspraak van het EHRM, waarbij in het bijzonder nog eens het arrest K.U. tegen Finland wordt genoemd, volgt dat staten een fair balance moeten vinden tussen het algemene belang van opsporing en voorkoming van misdrijven, mede ter bescherming van de fundamentele rechten van het slachtoffer, en het individuele belang van burgers bij privacy. Volgens de Staat voorziet de Nederlandse wetgeving in de juiste balans. De Wbt levert een wezenlijke bijdrage aan de opsporing en vervolging van ernstige strafbare feiten, terwijl de inbreuk op de privacy van burgers beperkt is door de waarborgen in Sv en de Tw. In het conceptwetsvoorstel worden daar nog extra waarborgen aan toegevoegd.

4.4 Eisers hebben in hun dagvaarding niet aangegeven op welke onderdelen de Nederlandse wetgeving tekort zou schieten in het licht van de rechtspraak van het EHRM. Anders dan eisers lijken te betogen, volgt uit artikel 8 EVRM niet een absoluut verbod op het bewaren en raadplegen van telecommunicatiegegevens. De in de conclusie van antwoord opgenomen citaten uit de diverse uitspraken van het EHRM geven onmiskenbaar blijk van een genuanceerde visie van het Hof. In het licht van de relatief beperkte aard en ernst van de inmenging die hier aan de orde is, het feit dat de inmenging bij wet is voorzien en dus voor een ieder kenbaar is, en gelet op de waarborgen en garanties die in de Wbt, de Tw en het Sv zijn opgenomen, moet de conclusie zijn dat de Wbt niet onverbindend, en al helemaal niet onmiskenbaar onverbindend is wegens strijd met artikel 8 van het EVRM.

5 Kort: positie van de geheimhouders (artikelen 10/11 EVRM)

5.1 Eisers hebben een beroep gedaan op schending van art. 10 en 11 EVRM, maar dat beroep niet uitgewerkt. Voor bijzondere eisen in verband met art. 10 en/of 11 EVRM of een andere uitkomst van de afweging in het kader van wetgeving in verband met die bepalingen ziet de Staat ook geen grond, zodat deze stelling verder onbesproken kan blijven.

5.2 Eisers hebben zich er verder nog op beroepen dat in de Wbt onvoldoende rekening zou worden gehouden met de bijzondere positie van geheimhouders. Er zou ook sprake zijn van een “chilling effect”. Eisers hebben deze stellingen niet nader uitgewerkt. Dat sprake zou zijn van een “chilling effect” ligt alleen al niet voor de hand, omdat geen sprake is van een bewaarplicht ten aanzien van de *inhoud* van de communicatie. Dat het bij de Wbt niet gaat om de inhoud van de communicatie is in het algemeen relevant voor de beoordeling van de positie van geheimhouders. Zo heeft de Hoge Raad bij arrest van 20 september 2011 geoordeeld dat verkeersgegevens van telefoonverkeer tussen de verdachte en zijn advocaat niet hoeven te worden vernietigd, zoals dat (in art. 126aa Sv) is voorgeschreven voor de inhoud van die gesprekken in verband met het verschoningsrecht van de professionele geheimhouders als geregeld in art. 218 Sv (HR 20 september 2011, NJ 2011, 437,

ECLI:NL:HR:2011:BP6016). De Hoge Raad citeert mede uit de wetsgeschiedenis van de Wet vorderen gegevens telecommunicatie:

> "2.5.1 (..) "(..) Er is echter geen reden ook de bevoegdheid tot het vorderen van verkeersgegevens van bijzondere waarborgen te voorzien. Deze bevoegdheid heeft een ander karakter dan de even genoemde bevoegdheden. Gegevens betreffende het telecommunicatieverkeer van de geheimhouder kunnen namelijk — anders dan de gegevens die bij de even genoemde bevoegdheden in het geding kunnen zijn — geen betrekking hebben op "hetgeen waarvan de wetenschap aan hen als zodanig is toevertrouwd" (artikel 218 Sv). Verkeersgegevens hebben geen betrekking op de inhoud van hetgeen geheimhouder en cliënt uitwisselen. Zij geven hooguit inzicht in de contacten die er geweest zijn tussen geheimhouder en cliënt, zoals dat bijvoorbeeld ook het geval kan zijn bij de bevoegdheid tot stelselmatige observatie. Bij de bevoegdheid tot stelselmatige observatie (en ander bevoegdheden) is niet voorzien in bijzondere waarborgen voor geheimhouders. Ook de huidige regeling van de bevoegdheid tot het vorderen van verkeersgegevens (artikel 126n en 126u Sv) kent geen bijzondere waarborgen."
> (Kamerstukken II 2001/02, 28 059, nr. 3, p. 19–20)"

5.3 Ook in het convenant tussen de Staat en de Nederlandse Orde van Advocaten over het systeem van automatische nummerherkenning (dat er heel kort gezegd toe strekt dat telefoongesprekken met advocaten niet worden getapt) is vastgelegd dat verkeersgegevens wel worden bewaard.

5.4 Hierbij kan in dit kort geding worden aangesloten. Het ligt niet voor de hand daarover in dit kader anders te oordelen.

6 Consequenties van een voorziening voor opsporing / reactie op vorderingen

6.1 Op grond van al het voorgaande concludeert de Staat dat er geen grond is voor de conclusie dat de Wbt onmiskenbaar onverbindend zou zijn. Daarop stuit toewijzing van de vordering tot buitenwerkingstelling van de Wbt af.

6.2 Toewijzing zou ook geen voorlopige voorziening inhouden: buitenwerkingstelling van de Wbt zou immers inhouden dat er geen verplichting, en dus ook geen grondslag, meer is voor de aanbieders van telecommunicatiediensten om de verkeersgegevens te bewaren. Dat zou betekenen dat zij ingeval van toewijzing van de vorderingen vanaf dat moment geen gegevens op grond van de Wbt meer bewaren, maar dan bestaat ook het risico dat de aanbieders de gegevens die zij tot dan toe op grond van de Wbt hebben bewaard – dat wil zeggen tot een jaar terug – vernietigen. Zou het oordeel in appel anders komen te luiden, dan zijn de gegevens al vernietigd en dus meer

beschikbaar voor de opsporing. Dat betekent onherstelbare schade voor de opsporing, maar het past ook niet bij het voorlopige karakter van het kort geding. Bovendien roept een toewijzing wezenlijke vragen op over de gevolgen daarvan voor de in lopende of afgeronde strafzaken gebruikte gegevens die dankzij de bewaarplicht nog beschikbaar waren en hebben bijgedragen aan de opsporing en vervolging van die zaken. Ook daarop moet toewijzing afstuiten.

6.3 Als alternatief voor de buitenwerkingstelling van de Wbt vorderen eisers een buitenwerkingstelling van de artikelen 13.2a, 13.2b en 13.4 van de Tw (primaire vordering, onder I). Deze artikelen zijn met de Wbt gewijzigd. De toewijzing van deze vordering stuit daarom op dezelfde redenen af als de buitenwerkingstelling van de Wbt. Bovendien moet in het oog worden gehouden, dat deze artikelen al bestonden voordat de Wbt in werking is getreden. De tekst van art. 13.2a en 13.2b is vervangen, terwijl art. 13.4 Tw door de Wbt is gewijzigd en aangevuld. Voor zover de artikelen al bestonden voordat de Wbt in werking trad of meer omvatten dan is aangevuld door de Wbt, kunnen zij in dit kort geding niet buiten werking worden gesteld. De vordering is dus ook onvoldoende bepaald en houdt geen rekening met dit soort consequenties.

6.4 Eisers vorderen bovendien een verbod op het opvragen van telecommunicatiegegevens als bedoeld in artikel 13.2a Tw (primaire vordering, onder II). Kennelijk gaan eisers ervan uit dat de buitenwerkingstelling van de Wbt alleen gevolgen zal hebben voor de toekomst en niet voor de reeds bewaarde gegevens. Met deze vordering beogen zij de toegang tot de reeds bewaarde gegevens op grond van Wbt te beperken.

6.5 In de eerste plaats moet worden opgemerkt dat de vordering voor dit doel te ruim is geformuleerd. Toewijzing van de vordering zou tot gevolg hebben dat in het geheel geen telecommunicatiegegevens als bedoeld in artikel 13.2a Tw meer kunnen worden opgevraagd. Er moeten echter nog wel vorderingen kunnen worden gedaan ten aanzien van de bedrijfsgegevens die aanbieders bewaren, ook al gaat het om dezelfde soort gegevens als waarop de bewaarplicht ziet. Dat gebeurde vóór de Wbt immers ook en dit kort geding gaat daar niet over. Overigens is het raadplegen van deze ten behoeve van de bedrijfsvoering bewaarde gegevens geen reëel alternatief voor de gegevens die op grond van de Wbt moeten worden bewaard, omdat ze veel minder (en steeds minder) omvattend zijn.

6.6 In de tweede plaats moet worden opgemerkt dat de vordering, zoals hier geformuleerd, praktisch onuitvoerbaar is. Het is onmogelijk om in ieder concreet geval te controleren of aan alle onder sub (i) tot en met (vii) cumulatief opgesomde voorwaarden is voldaan. Dat zou dus tot veel onzekerheid leiden en talloze uitlegkwesties opleveren, en alleen al daarom niet uitvoerbaar zijn. Dat is dus geen optie. Overigens zou het voldoen aan deze voorwaarden aan een bewaarplicht in de weg staan, omdat een bewaarplicht als hier aan de orde naar zijn aard betrekking

heeft – en moet hebben – op iedereen die gebruik maakt van de bedoelde communicatiemiddelen. Uit het arrest van het Hof van Justitie is in geen geval af te leiden dat een bewaarplicht ten aanzien van iedereen die gebruik maakt van de bedoelde telecommunicatiemiddelen onder alle omstandigheden onrechtmatig zou zijn. Dat is ook niet denkbaar, nu, zoals is toegelicht, de opsporing in de huidige tijd eenvoudigweg niet zonder kan. De Staat wijst er verder nogmaals op dat het Hof alleen in het samenstel van omstandigheden aanleiding ziet voor het oordeel dat de richtlijn niet voldeed aan art. 7 en 8 Handvest. Dat staat aan toewijzing van de vordering in de weg, omdat de Nederlandse regelgeving wél de nodige waarborgen kent.

6.7 De subsidiair geformuleerde vordering ten slotte is zodanig vaag en algemeen gesteld dat enigerlei toewijzing per definitie tot uitlegproblemen aanleiding zou geven, zodat deze vordering reeds daarom niet voor toewijzing in aanmerking komt. Nog daargelaten dat artikel 120 Gw in de weg staat aan een toets van de Wbt aan artikel 10 Gw en dat artikel 6, leden 1 en 2 (oud) VEU en artikel 15 van de e-Privacyrichtlijn niets toevoegen aan de algemene beginselen die reeds uit het Handvest en het EVRM voortvloeien.

7 Conclusie

7.1 Dataretentie is een actueel en gevoelig onderwerp waarbij diverse tegengestelde belangen een rol spelen. De bewaarplicht vormt een belangrijk instrument in de strijd tegen criminaliteit en terrorisme. Het is een geschikt en adequaat instrument waarmee een legitiem doel wordt nagestreefd. Daarover kan geen misverstand bestaan; de Europese rechters zijn het daarover eens. De wetgever heeft ook een goede balans getroffen tussen dit algemene belang en het belang van de privacy. Met de waarborgen zoals opgenomen in Wbt, Sv, Tw en de Wbp met betrekking tot de bewaartermijn, de opslag en beveiliging van de gegevens en de toegang tot en de vernietiging van de gegevens, is voldaan aan het noodzakelijkheids- en evenredigheidsbeginsel zoals dat voortvloeit uit zowel het Handvest als het EVRM.

7.2 De enkele omstandigheid dat de Wbt de nationale implementatie vormde van de door het Hof van Justitie ongeldig verklaarde Dataretentierichtlijn, doet aan deze conclusie niet af. De conclusie van het Hof van Justitie is gebaseerd op een combinatie van gebreken die het Hof in de richtlijn signaleerde. Kern van de kritiek is dat de Uniewetgever onvoldoende heeft gewaarborgd dat de lidstaten de rechten respecteren die uit het Handvest voortvloeien. Dat wil niet, althans niet automatisch zeggen dat alle lidstaten vervolgens ook daadwerkelijk in strijd met het Handvest handelen.

7.3 Het is aan de nationale rechter om de relevante regelgeving op dit vlak op de eigen merites te toetsen, met de nodige terughoudendheid die past bij toetsing van wetgeving in formele zin. En met de nodige terughoudendheid die past bij de huidige

fase waarin de maatschappelijke opvattingen sterk uiteenlopen en waarin de wetgever zich in het kader van de voorgestelde extra waarborgen nog moet uitspreken.

7.4 In het licht van de belangenafweging is niet zonder betekenis dat de bewaarplicht inmiddels al vijf jaar geldt. De providers hebben hun bedrijfsprocessen erop afgestemd en er zijn de nodige stappen gemaakt. Al die tijd is niet gebleken dat zaken zijn misgegaan, dat onbevoegden toegang hebben gekregen tot de bewaarde gegevens of dat gegevens zijn misbruikt e.d. Niet valt dan in te zien waarom niet op de uitkomst van de parlementaire discussie kan worden gewacht. Toewijzing van de gevraagde voorzieningen, welke dan ook, zou een belangrijke stap terug zijn, en verder terug dan tot het moment van inwerkingtreding van de Wbt.

7.5 Privacy is een groot goed, het verschoond blijven van inbreuken op privacy en het kunnen opsporen en vervolgen van ernstige misdrijven is dat ook. Het is de publieke taak van de overheid om de juiste balans te vinden en een juist antwoord te bieden op de grote uitdagingen in deze tijd. De gevraagde voorzieningen miskennen dat verschillende fundamentele rechten en uiteenlopende zwaarwegende belangen in het geding zijn en dat de weging ervan een uiterst complexe is, waarvoor een kort geding zich niet goed leent.

Wij concluderen tot afwijzing van de gevraagde voorzieningen, kosten rechtens.

behandeld door	R.J.M. van den Tweel
correspondentie	Postbus 11756, 2502 AT Den Haag
telefoon	(070) 515 38 01
fax	(070) 515 31 45
e-mail	rjm.vandentweel@pelsrijcken.nl
zaaknr	10044271