

# ECLI:NL:RBDHA:2015:2498

Instantie	Rechtbank Den Haag
Datum uitspraak	11-03-2015
Datum publicatie	11-03-2015
Zaaknummer	C/09/480009 / KG ZA 14/1575
Rechtsgebieden	Civiel recht
Bijzondere kenmerken	Kort geding
Inhoudsindicatie	

De kortgedingrechter in Den Haag heeft de Wet bewaarplicht telecommunicatiegegevens buiten werking gesteld. Deze wet verplicht aanbieders van telefoon- en internetdiensten de verkeers- en locatiegegevens van gebruikers op te slaan. De wet maakt een inbreuk op het recht op eerbiediging van privé-leven en het recht op bescherming van persoonsgegevens. De rechter is van oordeel dat deze inbreuk niet is beperkt tot het strikt noodzakelijke.

Vindplaatsen	Rechtspraak.nl
--------------	----------------

## Uitspraak

### Rechtbank den haag

Team Handel - voorzieningenrechter

zaak- / rolnummer: C/09/480009 / KG ZA 14/1575

### Vonnis in kort geding van 11 maart 2015

in de zaak van

1. de stichting

**Stichting Privacy First,**

gevestigd te Amsterdam,

2. de vereniging

**Nederlands Juristen Comité voor de Mensenrechten,**

gevestigd te Leiden,

3. de vereniging

**Nederlandse Vereniging van Strafrechtadvocaten,**

gevestigd te Goirle,

4. de vereniging

**Nederlandse vereniging van Journalisten,**

gevestigd te Amsterdam,

5. de besloten vennootschap met beperkte aansprakelijkheid

**BIT B.V.,**

gevestigd te Ede,

6. de besloten vennootschap met beperkte aansprakelijkheid

**SpeakUp B.V.,**

gevestigd te Enschede,

7. de besloten vennootschap met beperkte aansprakelijkheid

**VOYS B.V.,**

gevestigd te Groningen,

eiseressen,

advocaat mr. F.F. Blokhuis te Amsterdam,

tegen:

**de Staat der Nederlanden** (het Ministerie van Economische Zaken en het Ministerie van Veiligheid en Justitie),

zetelend te Den Haag,

gedaagde,

advocaat mr. R.J.M. van den Tweel te Den Haag.

Partijen worden hierna respectievelijk aangeduid als 'Privacy First cs' en 'de Staat'.

## **1 De feiten**

Op grond van de stukken en het verhandelde ter zitting van 18 februari 2015 wordt in dit geding van het volgende uitgegaan.

- 1.1. Privacy First cs zijn organisaties die ten doel hebben mensenrechten, waaronder het recht op privacy, te beschermen (eiseressen sub 1 en 2), verenigingen van beroepsgroepen met een recht op geheimhouding (eiseressen sub 3 en 4) en aanbieders van telecommunicatiediensten en openbare telecommunicatienetwerken (eiseressen sub 5, 6 en 7).
- 1.2. Op 15 maart 2006 is de richtlijn 2006/24/EG bekendgemaakt in het Publicatieblad van de Europese Unie, 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 (hierna: de Dataretentierichtlijn). De Dataretentierichtlijn is twintig dagen daarna in werking getreden.
- 1.3. In de Dataretentierichtlijn staat onder meer vermeld:

*"Artikel 1*

***Onderwerp en werkingssfeer***

1. Deze richtlijn heeft tot doel een harmonisatie tot stand te brengen van de nationale bepalingen van de lidstaten waarbij aan aanbieders van elektronische communicatiediensten of een openbaar communicatienetwerk verplichtingen worden opgelegd inzake het bewaren van bepaalde gegevens die door hen gegenereerd of door hen worden verwerkt, teneinde te garanderen dat die gegevens beschikbaar zijn voor het onderzoeken, opsporen en vervolgen van ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten.

2. Deze richtlijn heeft betrekking op verkeers- en locatiegegevens van natuurlijke en rechtspersonen, evenals op de daarmee verband houdende gegevens die nodig zijn om de abonnee of geregistreerde gebruiker te identificeren. Zij is niet van toepassing op de inhoud van elektronische communicatie, de informatie die wordt geraadpleegd met behulp van een elektronisch communicatienetwerk daaronder begrepen."

1.4. Implementatie van de Dataretentierichtlijn in de Nederlandse wetgeving heeft geleid tot de Wet van 18 juli 2009 tot wijziging van de Telecommunicatiewet en de Wet op de economische delicten in verband met de implementatie van Richtlijn 2006/24/EG van het Europees Parlement en de Raad van de Europese Unie betreffende de bewaring van gegevens die zijn verwerkt in verband met het aanbieden van openbare elektronische communicatiediensten en tot wijziging van Richtlijn 2002/58/EG (Wet bewaarplicht telecommunicatiegegevens, vindplaats: Stb. 2009, 333, hierna: de Wbt). De Wbt is in werking getreden op 1 september 2009. In de Wbt staat onder meer vermeld:

#### **"ARTIKEL 1**

*De Telecommunicatiewet wordt als volgt gewijzigd:*

(...)

*artikel 13.2a komt te luiden:*

#### **Artikel 13.2a**

1. In dit artikel wordt verstaan onder:

a. *gegevens: de verkeers- en locatiegegevens, (...) alsmede de daarmee verband houdende gegevens die nodig zijn om de abonnee of gebruiker te identificeren;*

b. *oproeping zonder resultaat: een communicatie waarbij een telefoonoproep wel tot een verbinding heeft geleid, maar onbeantwoord is gebleven of via het netwerkbeheer is beantwoord.*

2. *Aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten bewaren de in de bij deze wet behorende bijlage aangewezen gegevens, voorzover deze in het kader van de aangeboden netwerken of diensten worden gegenereerd of verwerkt, ten behoeve van het onderzoeken, opsporen en vervolgen van ernstige misdrijven.*

3. *De gegevens, bedoeld in het tweede lid, worden door de aanbieders bewaard gedurende een*

*periode van twaalf maanden, gerekend vanaf de datum van de communicatie.*

*4. De verplichting, bedoeld in het tweede lid, heeft betrekking op gegevens van oproepelingen zonder resultaat, voorzover deze gegevens door de aanbieders bij het aanbieden van openbare telecommunicatienetwerken of openbare telecommunicatiediensten worden gegenereerd, verwerkt en opgeslagen of gelogd."*

1.5. Bij wet van 6 juli 2011 is artikel 13.2a, derde lid, van de Telecommunicatiewet opnieuw gewijzigd. Dat artikellid luidt sindsdien (Stb. 2011, 350):

*"3. De gegevens, bedoeld in het tweede lid, worden door de aanbieders bewaard gedurende een periode van:*

*a. twaalf maanden voor gegevens in verband met telefonie over een vast of mobiel netwerk (...), of*

*b. zes maanden voor gegevens in verband met internettoegang, e-mail over het internet en internettelefonie, (...) gerekend vanaf de datum van de communicatie."*

1.6. Het Hof van Justitie van de Europese Unie (hierna: het Hof) heeft de Dataretentierichtlijn op 8 april 2014 met terugwerkende kracht ongeldig verklaard (HvJ EU 8 april 2014, gevoegde zaken C-293/12 en C-594/12, Digital Rights Ireland en Seitlinger ea). In zijn arrest heeft het Hof de geldigheid van de Dataretentierichtlijn getoetst aan de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie (hierna: het Handvest). Volgens het Hof vormt de Dataretentierichtlijn een zeer ruime en bijzonder zware inmenging in de door de artikelen 7 en 8 van het Handvest gewaarborgde rechten. Het Hof heeft voorts overwogen dat de Dataretentierichtlijn materieel tot doel heeft om tot de bestrijding van ernstige criminaliteit en aldus uiteindelijk tot de openbare veiligheid bij te dragen en dat de voorgeschreven bewaring van gegevens dus daadwerkelijk beantwoordt aan een doel van algemeen belang. Het Hof heeft geoordeeld dat de wetgever van de Europese Unie met de vaststelling van de Dataretentierichtlijn de door het evenredigheidsbeginsel gestelde grenzen heeft overschreden die hij in het licht van de artikelen 7, 8 en 52, lid 1, van het Handvest in acht dient te nemen. In het arrest staat ten aanzien daarvan, in de Nederlandse vertaling, onder meer vermeld:

*"49 Met betrekking tot de vraag of het door richtlijn 2006/24 nagestreefde doel kan worden verwezenlijkt door de bewaring van de gegevens, moet worden vastgesteld dat de gegevens die op grond van deze richtlijn moeten worden bewaard, gelet op het groeiende belang van elektronischemiddelende nationale strafvervolgingsautoriteiten extra mogelijkheden bieden om ernstige gevallen van criminaliteit op te helderen en in die zin dus een waardevol instrument vormen bij strafonderzoeken. De bewaring van dergelijke gegevens is derhalve geschikt voor de verwezenlijking van het door deze richtlijn nagestreefde doel.*

*(...)*

*51 Wat de noodzaak van de door richtlijn 2006/24 voorgeschreven bewaring van gegevens betreft, zij vastgesteld dat de bestrijding van zware criminaliteit, met name van georganiseerde misdaad en*

*terrorisme, weliswaar van primordiaal belang is om de openbare veiligheid te waarborgen, en dat de doeltreffendheid ervan in aanzienlijke mate kan afhangen van het gebruik van moderne onderzoekstechnieken, maar dat een dergelijke doelstelling van algemeen belang, hoe wezenlijk zij ook is, op zich niet kan rechtvaardigen dat een bewaringsmaatregel zoals die welke door richtlijn 2006/24 is ingevoerd, noodzakelijk wordt geacht voor het voeren van deze strijd.*

*52 Wat het recht op eerbiediging van het privéleven betreft, zij opgemerkt dat de bescherming van dit fundamentele recht volgens vaste rechtspraak van het Hof hoe dan ook vereist dat de uitzonderingen op de bescherming van persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven (...).*

*(...)*

*54 De betrokken Unieregeling moet dus duidelijke en precieze regels betreffende de draagwijdte en de toepassing van de betrokken maatregel bevatten die minimale vereisten opleggen, zodat de personen van wie de gegevens zijn bewaard over voldoende garanties beschikken dat hun persoonsgegevens doeltreffend worden beschermd tegen het risico van misbruik en tegen elke onrechtmatige raadpleging en elk onrechtmatig gebruik van deze gegevens (...).*

*55 De noodzaak om over dergelijke garanties te beschikken is des te groter wanneer de persoonsgegevens, zoals is bepaald in richtlijn 2006/24, automatisch worden verwerkt en er een aanzienlijk risico bestaat dat deze gegevens op onrechtmatige wijze zullen worden geraadpleegd (...).*

*56 Met betrekking tot de vraag of de inmenging die richtlijn 2006/24 meebrengt, beperkt is tot het strikt noodzakelijke, zij opgemerkt dat artikel 3 van deze richtlijn, gelezen in samenhang met artikel 5, lid 1, ervan, voorschrijft om alle verkeersgegevens betreffende vaste en mobiele telefonie, internettoegang, e-mail over het internet en internettelefonie te bewaren. Deze richtlijn strekt zich dus uit tot alle wijdverspreide elektronischecomunicatiemiddelen, die een steeds belangrijker plaats innemen in het dagelijkse leven van de mensen. Bovendien ziet deze richtlijn ingevolge artikel 3 ervan op alle abonnees en geregistreeerde gebruikers. Zij leidt dus tot inmenging in de fundamentele rechten van bijna de gehele Europese bevolking.*

*57 Dienaangaande zij in de eerste plaats vastgesteld dat richtlijn 2006/24 algemeen van toepassing is op alle personen, alle elektronischecomunicatiemiddelen en alle verkeersgegevens, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het doel, zware criminaliteit te bestrijden.*

*58 Richtlijn 2006/24 is om te beginnen algemeen van toepassing op alle personen die gebruikmaken van elektronischecomunicatiediensten, zonder dat de personen van wie de gegevens worden bewaard zich echter, zelfs niet indirect, in een situatie bevinden die aanleiding kan geven tot strafrechtelijke vervolging. Zij is dus zelfs van toepassing op personen voor wie er geen enkele*

*aanwijzing bestaat dat hun gedrag – zelfs maar indirect of van ver – een verband vertoont met zware criminaliteit. Bovendien bevat de richtlijn geen uitzonderingen, zodat zij zelfs van toepassing is op personen van wie de communicaties volgens de nationale rechtsregels onder het zakengeheim vallen.*

*59 Voorts beoogt deze richtlijn weliswaar bij te dragen tot de strijd tegen zware criminaliteit, maar zij vereist geen enkel verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid. Zij beperkt met name de bewaring niet tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaalde geografische zone en/of een kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit, of op personen voor wie de bewaring van de gegevens om andere redenen zou kunnen helpen bij het voorkomen, opsporen of vervolgen van zware criminaliteit.*

*60 In de tweede plaats bevat richtlijn 2006/24 niet alleen geen beperkingen, maar ook geen objectieve criteria ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan met het oog op het voorkomen, opsporen of strafrechtelijk vervolgen van inbreuken die, gelet op de omvang en de ernst van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten, voldoende ernstig kunnen worden geacht om een dergelijke inmenging te rechtvaardigen. Integendeel, richtlijn 2006/24 verwijst in artikel 1, lid 1, ervan enkel op algemene wijze naar ernstige criminaliteit zoals gedefinieerd in de nationale wetgevingen van de lidstaten.*

*61 Bovendien bevat richtlijn 2006/24 geen materiële en procedurele voorwaarden betreffende de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan. Artikel 4 van deze richtlijn, dat de toegang van deze autoriteiten tot de bewaarde gegevens regelt, bepaalt niet uitdrukkelijk dat deze toegang en het latere gebruik van de betrokken gegevens strikt gebonden zijn aan het doel, nauwkeurig afgebakende zware criminaliteit te voorkomen, op te sporen of strafrechtelijk te vervolgen, maar bepaalt enkel dat elke lidstaat de procedure en de te vervullen voorwaarden vaststelt voor toegang tot de bewaarde gegevens overeenkomstig de vereisten inzake noodzakelijkheid en evenredigheid.*

*62 In het bijzonder bevat richtlijn 2006/24 geen objectieve criteria op basis waarvan het aantal personen dat de bewaarde gegevens mag raadplegen en vervolgens gebruiken, kan worden beperkt tot wat strikt noodzakelijk is voor de verwezenlijking van het nagestreefde doel. Maar bovenal is de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens niet onderworpen aan enige voorafgaande controle door een rechterlijke instantie of een onafhankelijke administratieve instantie waarvan de beslissing beoogt om de toegang tot de gegevens en het gebruik ervan te beperken tot wat strikt noodzakelijk is ter verwezenlijking van het nagestreefde doel en die uitspraak doet op een gemotiveerd verzoek van deze autoriteiten, ingediend in het kader van procedures ter voorkoming, opsporing of vervolging van strafbare feiten. Aan de lidstaten is evenmin enige specifieke verplichting opgelegd om dergelijke beperkingen vast te stellen.*

(...)

*65 Uit het bovenstaande volgt dat richtlijn 2006/24 geen duidelijke en precieze regels bevat betreffende de omvang van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten. Vastgesteld moet dus worden dat deze richtlijn een zeer ruime en bijzonder zware inmenging in deze fundamentele rechten in de rechtsorde van de Unie impliceert, zonder dat deze inmenging nauwkeurig is omkaderd door bepalingen die kunnen waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke.”*

1.7. Op 17 november 2014 heeft het kabinet schriftelijk gereageerd op de ongeldigverklaring van de Dataretentierichtlijn. In die brief heeft het kabinet gemeld dat de Wbt aangepast moet worden in het licht van het arrest van het Hof. In de brief staat onder meer vermeld:

*“De regering is aldus voornemens de nationale wetgeving inzake de bewaarplicht voor telecommunicatiegegevens aan te passen, zodat:*

*- de vordering van de officier van justitie tot het verstrekken van telecommunicatiegegevens slechts kan worden gegeven na een voorafgaande machtiging door de rechter-commissaris. Dit betekent dat de regeling van artikel 126n/u van het Wetboek van Strafvordering wordt gewijzigd;*

*- de toegang tot de gegevens ten behoeve van de opsporing en vervolging van ernstige misdrijven wordt gedifferentieerd aan de hand van de ernst van het misdrijf. Dit betekent dat de regeling van artikel 126n/u van het Wetboek van Strafvordering wordt gewijzigd;*

*- onderzocht zal worden of de telecommunicatiegegevens, die worden bewaard ten behoeve van de opsporing en vervolging van ernstige misdrijven, kunnen worden versleuteld zodat deze zijn afgeschermd van inzage door onbevoegden. Dit kan leiden tot wijziging van het Besluit beveiliging telecommunicatiegegevens;*

*- de aanbieders worden verplicht de te bewaren gegevens op het grondgebied van de Europese Unie te bewaren. Dit betekent dat de regeling van de artikelen 13.2a en 13.5 van de Telecommunicatiewet wordt gewijzigd;*

*- AT Agentschap Telecom, toevoeging voorzieningenrechter) als toezichhoudende autoriteit inzage kan verkrijgen in telecommunicatiegegevens die door de aanbieders worden bewaard of verstrekt, met het oog op een beter toezicht op de verwerking van de te bewaren gegevens, en de vernietiging daarvan. Dit betekent dat artikel 18.7, tweede lid, van de Telecommunicatiewet wordt gewijzigd;*

*Deze aanpassingen zullen worden opgenomen in een voorstel tot wijziging van de Telecommunicatiewet en het Wetboek van Strafvordering, dat binnenkort in consultatie zal worden gegeven.”*



## 2 Het geschil

### 2.1. Privacy First cs vorderen, na wijziging van eis, zakelijk weergegeven:

#### primair:

I. de Wbt, althans artikel 13.2a en/of artikel 13.2b en/of artikel 13.4 van de Telecommunicatiewet buiten werking te stellen, althans de Staat daartoe te veroordelen;

II. de Staat te verbieden gegevens als bedoeld in artikel 13.2a Telecommunicatiewet op te vragen bij aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten, voor zover één en ander in strijd is met de uitgangspunten die het Hof in het arrest van 8 april 2014 heeft geformuleerd;

#### subsidiar:

de Staat te verbieden de Wbt of onderdelen daarvan te handhaven en gegevens als bedoeld in artikel 13.2a Telecommunicatiewet op te vragen bij de aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten, voor zover één en ander in strijd is met de artikelen 7, 8 en 11 van het Handvest, 8 en 10 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), 10 van de Grondwet, 15 van de e-privacyrichtlijn en/of 6, lid 1 en 2 van het Verdrag betreffende de Europese Unie;

#### meer subsidiar:

de Staat te verbieden de Wbt te handhaven en aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten te dwingen gegevens als bedoeld in artikel 13.2a Telecommunicatiewet op te slaan en deze gegevens op te vragen, zolang de Wbt niet is gewijzigd zoals door de regering bij brief van 17 november 2014 voorgesteld of een intrekkingwet van de Wbt is aangenomen.

### 2.2. Daartoe voeren Privacy First cs het volgende aan. De Wbt is onmiskenbaar in strijd met Europese regelgeving en kan dan ook niet in stand blijven. De Wbt implementeert de Daretentierichtlijn vrij letterlijk. Het Hof heeft de Daretentierichtlijn op 8 april 2014 met terugwerkende kracht ongeldig verklaard. De Wbt schendt de artikelen 7 en 8 van het Handvest op gelijke wijze als de Daretentierichtlijn dat deed.

De Daretentierichtlijn liet de ruimte om gegevens van iedereen te bewaren. In de Wbt is van die ruimte gebruik gemaakt. Het Hof keurt het ongericht bewaren van gegevens van alle burgers, zonder onderscheid naar persoon, locatie of gegevens af. Het bewaren van alle verkeers- en locatiegegevens voor zes tot twaalf maanden, ongeacht het doel, gaat dus te ver. Er moet sprake zijn van een beperkte en doelgerichte selectie van gegevens. Die is er niet in de Wbt. Verder tilt het Hof er zwaar aan dat er geen voorafgaande rechterlijke controle is. Onder de Wbt is het nog steeds mogelijk voor opsporingsambtenaren en officieren van justitie om toegang tot de gegevens te verkrijgen, zonder dat de rechter dat vooraf toetst. Het Hof heeft voorts bezwaren geuit tegen de bewaartermijnen, zoals

voorgeschreven in de Dataretentierichtlijn, nu geen onderscheid wordt gemaakt naargelang het nut daarvan, het nagestreefde doel of betrokken personen en geen objectieve criteria worden genoemd om de bewaartermijnen te beperken tot wat strikt noodzakelijk is. Ook heeft het hof vastgesteld dat er onvoldoende garanties zijn dat de gegevens worden beschermd tegen misbruik.

De Wbt is daarnaast in strijd met artikel 8 EVRM. De *opslag* van de verkeers- en locatiegegevens en de *toegang* van de nationale autoriteiten tot die gegevens vormen beide zelfstandige inbreuken op het recht op bescherming van de persoonlijke levenssfeer. De opslag vormt ook een inbreuk indien slechts een beperkt deel van de opgeslagen informatie daadwerkelijk wordt gebruikt. De retentie van de grote hoeveelheid data over onschuldige personen die de Wbt bestrijkt, vormt een zware inbreuk op artikel 8 EVRM. Uit de gegevens kunnen immers zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals ook het Hof aangeeft. De Wbt biedt onvoldoende waarborgen tegen misbruik en willekeur en onvoldoende duidelijk en precies is onder welke omstandigheden en voorwaarden de autoriteiten de maatregelen mogen inzetten. Zo wordt in de Wbt niet geregeld dat elk individueel verzoek tot toegang tot de gegevens aan het toezicht van de autoriteiten wordt onderworpen. Bovendien is de Wbt niet 'noodzakelijk in een democratische samenleving'. De zware inbreuk op de privacy is niet proportioneel ten opzichte van het te bereiken doel, namelijk de opsporing van zware criminaliteit.

De Wbt maakt ook inbreuk op de vrijheid van meningsuiting (artikel 10 EVRM en artikel 11 van het Handvest). Het feit dat gegevens van journalisten opgevraagd kunnen worden, leidt tot het risico dat zij bepaalde onderwerpen gaan mijden of dat bronnen zich niet meer tot journalisten durven te wenden. Ook zullen cliënten zich minder vrij voelen om met hun advocaat te overleggen. Er is dus gevaar voor een "chilling effect". De overheid dwingt aanbieders van telecommunicatiediensten de grondrechten van hun cliënten massaal te schenden. Bovendien wordt hun contractsvrijheid en vrijheid van onderneming aangetast.

In de brief van 17 november 2014 heeft de Minister van Veiligheid en Justitie weliswaar een aanpassingswet voorgesteld, maar totdat die wet in werking is getreden zal de Wbt in de huidige vorm gehandhaafd worden. Dat de Wbt met de huidige inhoud niet langer kan worden gehandhaafd, wordt breed gedragen. De Afdeling Advisering van de Raad van State heeft dit glashelder verwoord. Dit wordt eveneens onderschreven door de Commissie Bescherming Persoonsgegevens (CBP) en gezaghebbende wetenschappers.

Daarbij komt dat de Wbt nauwelijks effectief is en door voortschrijdende technische ontwikkelingen grotendeels is achterhaald. De noodzaak en effectiviteit van de Wbt zijn na ruim vijf jaar dataretentie niet aangetoond. Veel andere lidstaten in Europa schaften de op basis van de Dataretentierichtlijn geïmplementeerde wetten al af of stelden de bewaarplicht buiten werking.

2.3. De Staat voert gemotiveerd verweer, dat hierna, voor zover nodig, zal worden besproken.

### 3 De beoordeling van het geschil

- 3.1. Vooropgesteld wordt dat de vordering zich richt tegen de Staat als wetgever en strekt tot het buiten toepassing doen verklaren van een deel van een wet in formele zin. De burgerlijke rechter kan (onderdelen van) een wet in formele zin in kort geding slechts buiten toepassing verklaren indien en voor zover deze *onmiskenaar onverbindend* is wegens strijd met eenieder verbindende bepalingen van verdragen en besluiten van volkenrechtelijke organisaties. Dit criterium vloeit voort uit artikel 94 van de Grondwet en vaste jurisprudentie (vgl. HR 1 juli 1983, NJ 1984, 360) en wijst op grote terughoudendheid, te meer nu in een kortgedingprocedure als de onderhavige slechts een voorlopig oordeel kan worden gegeven. De in acht te nemen terughoudendheid vindt haar grondslag in de op de Grondwet berustende verdeling van bevoegdheden van de verschillende staatsorganen – de scheiding der machten. Wetten in formele zin worden vastgesteld door de wetgever. Het is bij uitstek de taak van de wetgever om alle in het geding zijnde argumenten en belangen tegen elkaar af te wegen, waarbij aan hem een grote mate van beleidsvrijheid toekomt. Er is dan ook geen plaats voor een eigen “volle” toetsing door de burgerlijke rechter.
- 3.2. De Staat heeft betoogd dat de strafrechter zich reeds expliciet heeft uitgelaten over de rechtsgeldigheid van de Wbt (Gerechtshof Amsterdam 9 mei 2014, ECLI:NL:GHAMS:2014:1835 en Gerechtshof Amsterdam 27 mei 2014, ECLI:NL:GHAMS:2014:2028), zodat bezwaarlijk kan worden geconcludeerd dat sprake is van onmiskenaar onverbindendheid van de Wbt. Dat betoog slaagt niet. De strafrechter heeft immers getoetst of een vormverzuim op grond van artikel 359a lid 1 van het Wetboek van Strafvordering heeft plaatsgevonden en of de belangen van de verdachten door toepassing van de (gewijzigde) Telecommunicatiewet zijn geschonden. De civielrechtelijke toets of de Wbt strijdig is met eenieder verbindende bepalingen van verdragen en besluiten van volkenrechtelijke organisaties heeft in genoemde arresten niet plaatsgevonden.
- 3.3. Privacy First cs hebben ter onderbouwing van hun vorderingen een beroep gedaan op de overwegingen in het arrest van het Hof van 8 april 2014, waarin de Dataretentierichtlijn ongeldig is verklaard. Niet in geschil is evenwel dat de ongeldigverklaring van de Dataretentierichtlijn door het Hof niet zonder meer meebrengt dat de Wbt eveneens ongeldig is. De Wbt is door de ongeldigverklaring van de Dataretentierichtlijn autonome wetgeving geworden die op de eigen merites moet worden getoetst, waarbij de overwegingen van het Hof moeten worden betrokken. Daarbij wordt nog opgemerkt dat de voorgestelde wijzigingen van de Wbt zoals verwoord in de brief 17 november 2014 geen rol spelen in de beoordeling, aangezien enkel de huidige van toepassing zijnde regelgeving dient te worden getoetst.
- 3.4. Artikel 51 van het Handvest bepaalt dat het Handvest van toepassing is indien de lidstaten het recht van de Unie ten uitvoer brengen. Uit jurisprudentie van het Hof volgt dat het begrip “uitvoering van Unierecht” in de zin van dit artikel aldus moet worden verstaan dat het gaat om optreden van de lidstaten binnen het toepassingsgebied van het recht van de Unie (onder meer: HvJ EU 30 april 2014,

C-390/12, Pflieger). Aangezien de Wbt een invulling vormt van de zogenoemde e-privacyrichtlijn (richtlijn 2002/58/EG) en een belemmering van het vrij verkeer van diensten meebrengt, valt deze wet onder de werkingssfeer van het Handvest. Getoetst dient dan ook te worden of de Wbt – zoals Privacy First cs stellen – een ontoelaatbare inbreuk maakt op de artikelen 7 en 8 van het Handvest. De Staat heeft in dit verband weliswaar niet weersproken dat de Wbt vrijwel dezelfde inhoud heeft als de Dataretentierichtlijn, maar zich – naar het oordeel van de voorzieningenrechter terecht – op het standpunt gesteld dat het geheel van relevante nationale wetgeving dient te worden betrokken bij de beoordeling van de vraag of de Wbt in overeenstemming is met de artikelen 7 en 8 van het Handvest. De bezwaren tegen de Dataretentierichtlijn die het Hof in het arrest van 8 april 2014 formuleert, hebben immers onder meer betrekking op de afwezigheid van bepaalde waarborgen voor veiligheid van en toegang tot de opgeslagen gegevens. Die bezwaren kunnen evenzeer worden ondervangen door toepasselijke bepalingen in andere nationale regelgeving.

- 3.5. De artikelen 7 en 8 van het Handvest formuleren het recht op eerbiediging van privé-leven, familie- en gezinsleven, woning en communicatie en het recht op bescherming van persoonsgegevens. Privacy First cs hebben aangevoerd dat het enkele feit dat de Wbt voorschrijft dat telecommunicatiegegevens worden bewaard van personen al een ontoelaatbare inbreuk vormt op de artikelen 7 en 8 van het Handvest. Vaststaat dat, zoals het Hof ook overweegt onder punt 32 tot en met 37 van het arrest, de (in dit geval door de Wbt) opgelegde verplichting om gegevens over de communicaties van personen gedurende een bepaalde tijd te *bewaren* een inmenging vormt op de artikelen 7 en 8 van het Handvest. Dat is in lijn met de jurisprudentie van het Europees Hof voor de Rechten van de Mens, waar Privacy First cs zich op beroepen. Daarin wordt bijvoorbeeld met betrekking tot artikel 8 EVRM overwogen "*The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of article 8 (...). The subsequent use of the stored information has no bearing on that finding.*" (EHRM 4 december 2008, S. and Marper, appl.nos 30562/04 en 30566/04). Privacy First cs stellen dus terecht dat het *gebruik* van de gegevens een op zichzelf staande, verdergaande inmenging is in de genoemde rechten. Voor zover Privacy First cs evenwel betogen dat de inmenging in de genoemde rechten hoe dan ook ontoelaatbaar is, wordt dat betoog niet gevolgd. Beoordeeld dient immers te worden of de inmenging gerechtvaardigd en evenredig is.
- 3.6. Partijen twisten in dat kader over de noodzaak en effectiviteit van de bewaarplicht zoals die door de Wbt wordt voorgeschreven. Ten aanzien daarvan wordt vooropgesteld dat dit geschilpunt bij uitstek binnen de beleidsvrijheid van de wetgever valt, die alle argumenten en belangen tegen elkaar af dient te wegen, zodat de voorzieningenrechter dit punt slechts marginaal zal toetsen. Het Hof heeft overwogen dat de bestrijding van zware criminaliteit van primordiaal belang is om de openbare veiligheid te waarborgen, dat de doeltreffendheid ervan in aanzienlijke mate kan afhangen van het gebruik van moderne onderzoekstechnieken (punt 51) en dat de gegevens die moeten worden bewaard extra mogelijkheden bieden om ernstige gevallen van criminaliteit op te helderen (punt 49). Daarbij komt dat de Staat in deze procedure voldoende aannemelijk heeft gemaakt dat bepaalde vormen van criminaliteit nagenoeg uitsluitend zijn op te sporen door het gebruik van historische telecommunicatiegegevens, uitgaande van het gegeven dat steeds meer criminaliteit op of met behulp

van internet wordt gepleegd. De Staat heeft onweersproken aangevoerd dat enkele door hem genoemde omvangrijke strafzaken niet hadden kunnen worden opgelost zonder toepassing van de bewaarplicht. Uitgangspunt is dan ook dat de bewaarplicht noodzakelijk en effectief is.

- 3.7. Het geschil van partijen spitst zich voorts toe op de vraag of met de Nederlandse wetgeving voldoende wordt tegemoetgekomen aan de bezwaren die ertoe hebben geleid dat het Hof heeft geoordeeld dat de Dataretentierichtlijn ongeldig is. Evenals de Dataretentierichtlijn is de Wbt zonder enige beperking van toepassing op alle personen die gebruik maken van elektronische communicatiemiddelen en dus zelfs op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag een verband vertoont met zware criminaliteit. Ook wordt geen verband vereist tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid (punt 57 tot en met 59 van het arrest). Anders dan Privacy First cs betogen, kan uit het arrest van het Hof niet worden afgeleid dat een dergelijke ruime bewaarplicht hoe dan ook niet evenredig is ten opzichte van het beoogde doel. Het Hof beoordeelt immers vervolgens de vraag of de Dataretentierichtlijn voldoende waarborgen biedt voor de toegang tot de bewaarde gegevens. Indien het betoog van Privacy First cs juist zou zijn, zou het Hof niet meer aan die vraag zijn toegekomen. Daarbij komt dat het Hof "gelet op een en ander" ("*Having regard to all the foregoing considerations*", punt 69) oordeelt dat de wetgever de door het evenredigheidsbeginsel gestelde grenzen heeft overschreden. Daaruit volgt dat de opgesomde bezwaren in onderlinge samenhang beschouwd tot dat oordeel hebben geleid.
- 3.8. Het voorgaande laat onverlet dat dient te worden beoordeeld of de inmenging in de artikelen 7 en 8 van het Handvest voldoende nauwkeurig is omkaderd door bepalingen die waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke. In dat verband wordt opgemerkt dat een beperking van de gegevens die moeten worden opgeslagen tot de gegevens van verdachte burgers niet goed denkbaar is met het oog op het doel van de Wbt, de doeltreffende opsporing van zware criminaliteit. In geval van een *first offender* kan immers niet reeds op voorhand een onderscheid worden gemaakt tussen verdachte en niet-verdachte burgers. De noodzaak voor het bieden van waarborgen en garanties ten aanzien van de toegang tot die gegevens is evenwel des te groter nu het gaat om een zeer ruime inmenging, zodat daaraan hoge eisen dienen te worden gesteld.
- 3.9. De Staat heeft terecht aangevoerd dat aanbieders van telecommunicatiediensten in Nederland op grond van het Besluit beveiliging gegevens telecommunicatie een hoog niveau van bescherming en beveiliging moeten bieden en dat het Agentschap Telecom en het College bescherming persoonsgegevens daar toezicht op houden. In zoverre wordt dus tegemoetgekomen aan het bezwaar tegen de Dataretentierichtlijn dat het Hof onder punt 67 van het arrest vermeldt. Uit punt 69 moet echter worden afgeleid dat een voorschrift dat de betrokken gegevens op het grondgebied van de Unie moeten worden bewaard van wezenlijk belang ("*an essential component*") is voor de bescherming van personen bij de verwerking van persoonsgegevens, aangezien enkel met dat voorschrift ten volle is gewaarborgd dat een onafhankelijke autoriteit op basis van het Unierecht toezicht houdt op de vereisten inzake bescherming en beveiliging. Een dergelijk voorschrift ontbreekt in de Wbt. De Staat heeft ook erkend dat in de praktijk (enkele kleine) aanbieders hun gebruikersgegevens buiten het

grondgebied van de EU bewaren.

- 3.10. Voorts dient – aldus het Hof onder punt 60 van het arrest – de wetgeving objectieve criteria te bevatten ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan met het oog op het voorkomen, opsporen en strafrechtelijk vervolgen van inbreuken die voldoende ernstig kunnen worden geacht om de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten te rechtvaardigen. De voorzieningenrechter is van oordeel dat hier geen sprake van is in de Wbt. De Wbt biedt weliswaar een duidelijke afbakening omdat raadpleging van de gegevens is beperkt tot de opsporing en vervolging van strafbare feiten waarvoor voorlopige hechtenis is toegestaan of van terroristische misdrijven, maar deze categorie bevat eveneens strafbare feiten die niet voldoende ernstig zijn om de inmenging te rechtvaardigen. De bepalingen van de Dataretentierichtlijn waren immers een reactie op de terreuraanslagen in Londen en Madrid in 2004 en 2005. Het materiële doel van de Dataretentierichtlijn, en dus van de daarop gebaseerde Wbt, bestond er in te garanderen dat bepaalde gegevens beschikbaar zijn met het oog op de bestrijding van *ernstige* criminaliteit. Strafbare feiten waarvoor voorlopige hechtenis is toegestaan, zijn onder meer misdrijven waarop een gevangenisstraf van ten minste vier jaar staat. De Staat heeft aangevoerd dat niet lichtvaardig wordt overgegaan tot het opvragen van de gegevens en dat bijvoorbeeld in geval van een fietsendiefstal (ook een strafbaar feit waarvoor voorlopige hechtenis is toegestaan) geen gegevens zullen worden opgevraagd. Feit is echter dat de mogelijkheid daartoe wel bestaat en dat geen waarborgen bestaan om de toegang tot de gegevens daadwerkelijk te beperken tot hetgeen strikt noodzakelijk is voor de bestrijding van (enkel) ernstige criminaliteit.
- 3.11. Het voorgaande klemt temeer nu de Wbt en aanverwante regelgeving de toegang tot de bewaarde gegevens niet onderwerpen aan een voorafgaande controle door een rechterlijke instantie of onafhankelijke administratieve instantie. Anders dan de Staat betoogt, kan het openbaar ministerie niet als een onafhankelijke administratieve instantie worden aangemerkt. Dat het Hof dit als een zwaarwegend bezwaar beschouwt, kan worden afgeleid uit het gebruik van het woord “bovenal” (“*above all*”) onder punt 62 van het arrest.
- 3.12. Een en ander leidt tot de conclusie dat de Wbt in de huidige vorm een inbreuk maakt op de in de artikelen 7 en 8 van het Handvest gewaarborgde rechten die niet is beperkt tot het strikt noodzakelijke en dus als ontoelaatbaar dient te worden gekwalificeerd. Gelet hierop is de Wbt onmiskenbaar onverbindend. De voorzieningenrechter is zich ervan bewust dat buitenwerkingstelling van de Wbt ingrijpende gevolgen kan hebben voor de opsporing en vervolging van strafbare feiten. Dat rechtvaardigt evenwel niet dat voornoemde inbreuk blijft voortbestaan. Dat de gevolgen van een buitenwerkingstelling mogelijk onomkeerbaar zijn, staat op zichzelf evenmin in de weg aan het geven van de gevraagde voorziening. De primaire vordering van Privacy First cs, als geformuleerd onder I, zal dan ook worden toegewezen. Gelet hierop hebben Privacy First cs geen belang meer bij toewijzing van het onder II gevorderde. Buitenwerkingstelling van de Wbt leidt er immers toe dat de grondslag voor het opvragen van de bedoelde gegevens komt te vervallen.

3.13. De Staat zal, als de in het ongelijk gestelde partij, worden veroordeeld in de kosten van dit geding, alsmede (deels voorwaardelijk) in de nakosten.

#### **4 De beslissing**

De voorzieningenrechter:

- stelt de Wet bewaarplicht telecommunicatiegegevens buiten werking;
- veroordeelt de Staat in de kosten van dit geding, tot dusverre aan de zijde van Privacy First cs begroot op € 1.914,84, waarvan € 1.224,-- aan salaris advocaat, € 613,-- aan griffierecht en € 77,84 aan dagvaardingskosten;
- veroordeelt de Staat tevens in de nakosten, forfaitair begroot op € 131,-- aan salaris advocaat, te vermeerderen met € 68,-- aan salaris en met de exploitkosten gemaakt voor de betekening van dit vonnis indien tot betekening wordt overgegaan;
- verklaart dit vonnis tot zover uitvoerbaar bij voorraad;
- wijst af het meer of anders gevorderde.

Dit vonnis is gewezen door mr. G.P. van Ham en in het openbaar uitgesproken op 11 maart 2015.