Heden, de achtste januari tweeduizendenvijftien, op verzoek van

1. de stichting Stichting Privacy First, gevestigd te (1091 GR) Amsterdam, aan de Wibautstraat 150, hierna ook te noemen '**Privacy First**';
2. de vereniging Nederlands Juristen Comité voor de Mensenrechten, gevestigd te (2311 GW) Leiden, aan de Sterrenwachtlaan 11, hierna ook te noemen '**NJCM**';
3. de vereniging Nederlandse Vereniging van Strafrechtadvocaten, gevestigd te (5051 RB) Goirle, aan de Kloosterstraat 17-19, hierna ook te noemen '**NVSA**';
4. de vereniging Nederlandse vereniging van Journalisten gevestigd te (1071 DR) Amsterdam, aan de Johannes Vermeerstraat 22, hierna ook te noemen '**NVJ**';
5. de besloten vennootschap BIT B.V., gevestigd te (6716 BP) Ede, aan de Galileïlaan 19, hierna ook te noemen '**BIT**';
6. de besloten vennootschap SpeakUp B.V., gevestigd te (7521 PK) Enschede, aan de Institutenweg 20 22, hierna ook te noemen '**SpeakUp**'; en
7. de besloten vennootschap VOYS B.V., gevestigd te (9723 ZA) Groningen, aan het Helperpark 292, hierna ook te noemen '**VOYS**';

voor deze zaak woonplaats kiezende te (1017 NA) Amsterdam aan de Leidsegracht 9, ten kantore van Boekx Advocaten, van welk kantoor mr. F.F. Blokhuis en mr. O.M.B.J. Volgenant tot advocaten worden gesteld en in deze zaak als zodanig zullen optreden, zulks met het recht van substitutie,

heb ik,

GEDAGVAARD

DE STAAT DER NEDERLANDEN (t.a.v. Ministerie van Economische Zaken en Ministerie van Veiligheid en Justitie), wier zetel gevestigd is te Den Haag, mijn exploit doende ten parkette van de Procureur-Generaal bij de Hoge Raad der Nederlanden aan de Kazemestraat 52 (2514 CV) te Den Haag, aldaar aan genoemd adres mijn exploit doende door afschrift dezes te laten aan:

OM

op woensdag de achttiende februari tweeduizendvijftien (10-2-2015), des voormiddags om 11.00 uur, in persoon of vertegenwoordigd door een advocaat te verschijnen ter terechtzitting van de rechtbank Den Haag, bij de Voorzieningenrechter die dan recht zal spreken in kort geding en deze zaak zal behandelen in één der zalen van het gerechtsgebouw in het Paleis van Justitie aan de Prins Clauslaan 60 te (2595 AJ) Den Haag;

MET AANZEGGING DAT:

a. indien gedaagde niet op de voorgeschreven wijze in het geding verschijnt, en de voorgeschreven termijnen en formaliteiten in acht zijn genomen, de rechter verstek tegen die gedaagde zal verlenen en de hierna omschreven vordering zal toewijzen, tenzij deze hem onrechtmatig of ongegrond voorkomt;
b. bij verschijning in het geding van gedaagde een griffierecht zal worden geheven, te voldoen binnen vier weken te rekenen vanaf het tijdstip van verschijning;
c. de hoogte van de griffierechten is vermeld in de meest recente bijlage behorend bij de Wet griffierechten burgerlijke zaken, die onder meer is te vinden op de website www.rechtspraak.nl en op de website van de Koninklijke Beroepsorganisatie van Gerechtsdeurwaarders: www.kbvg.nl/griffierechtentabel;
d. van een persoon die onvermogend is, een bij of krachtens de Wet vastgesteld griffierecht voor onvermogenden wordt geheven, indien hij op het tijdstip waarop het griffierecht wordt geheven heeft overgelegd:
    a. een afschrift van het besluit tot toevoeging, bedoeld in artikel 29 van de Wet op de rechtsbijstand, of indien dit niet mogelijk is ten gevolge van omstandigheden die redelijkerwijs niet aan hem zijn toe te rekenen, een afschrift van de aanvraag, bedoeld in artikel 24, tweede lid, van de Wet op de rechtsbijstand, dan wel:
    b. een verklaring van het bestuur van de raad voor de rechtsbijstand, bedoeld in artikel 7, derde lid, onderdeel 3 van de Wet op de rechtsbijstand, waaruit blijkt dat zijn inkomen niet meer bedraagt dan de inkomens, bedoeld in de algemene maatregel van bestuur krachtens artikel 35, tweede lid van die wet;

Boekx

TENEINDE

alsdan namens de in de aanhef genoemde partijen als eisers te horen eis doen op de volgende gronden.

INHOUDSOPGAVE

1. INLEIDING EN ACHTERGROND

1.1 Eisers, hierna verder gezamenlijk te noemen '**Eisers**', eisen dat de Wet Bewaarplicht Telecommunicatiegegevens[1] (hierna: '**de Wet**', **Productie 1**) buiten werking wordt gesteld.

1.2 De Wet is, na veel discussie en kritiek[2], geïmplementeerd naar aanleiding van de Dataretentierichtlijn 2006/24/EG[3] (hierna: '**de Dataretentierichtlijn**', **Productie 2**). De Dataretentierichtlijn is op 8 april 2014 door het Europese Hof van Justitie (hierna: '**het Hof**') ongeldig verklaard (**Productie 3**), omdat zij een bijzonder zware inbreuk maakt op de privacygrondrechten.[4] De Wet komt materieel grotendeels overeen met de Dataretentierichtlijn. De Raad van State, de vaste commissies van de Eerste Kamer en de regering vinden dat de Wet moet worden aangepast. De Raad van State (**Productie 4**) en de commissies van de Eerste Kamer (**Productie 5**) vinden dat de Wet ook direct moet opgeschort c.q. niet mag worden gehandhaafd.

---

[1] Voluit: 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), Kamerstukken II 2007-2008, 31 145, nrs. 1-14, Staatblad 2009/333. Na invoering per 1 september 2009 is deze wet nog gewijzigd – ter uitvoering van een toezegging aan de Eerste Kamer van die strekking – waarbij de termijn voor het bewaren van internetgegevens is verkort van 12 naar 6 maanden, Staatsblad 2011, 350, inwerkingtreding 16 juli 2011.

[2] Franken, toenmalige Eerste Kamerlid, was een fervent tegenstander, maar stemde toch voor de wet met de gevleugelde woorden dat politieke opportuniteit soms zwaarder weegt dan wetenschappelijke rationaliteit (Eerste Kamer, 6 juli 2009, p. 39-1807). Zie voorts bijv. H. Franken, '*Wie wat bewaart heeft wat*', RM Themis 2007/4, p. 125-126; '*Vrijwillig op weg naar de politiestaat*', NRC Handelsblad 2 april 2008; '*Niets verkeerd met bewaren van telefoongegevens*', NRC Handelsblad 7 april 2008; '*Dataretentie helpt nauwelijks*' NRC Handelsblad 10 april 2008, alsmede A.H.J. Schmidt & G-J. Zwenne, '*Recht en risico. Kanttekeningen bij het voorstel voor een richtlijn over de bewaring van telecommunicatie-verkeersgegevens*', Mediaforum 2005-9, p. 292-302 en het vervolg daarop G-J. Zwenne en A.H.J. Schmidt, '*Opmerkingen bij het wetsvoorstel Wet bewaarplicht telecommunicatiegegevens*', Mediaforum 2008/7-8, p. 278-285 en G-J. Zwenne en F. Simons, '*Duitse bewaarplicht ongrondwettig. En in Nederland?*', IR 2010, nr. 3, p. 87-94.

[3] Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006 betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG, PbEG 13 april 2006, L105/54-62.

[4] Hof van Justitie van de Europese Unie 8 april 2014, gevoegde zaken *Digital Rights Ireland* en *Seitlinger* (zaken C-293/12 en C294/12).

1.3 De Nederlandse regering weigert echter de Wet buiten werking te stellen, ondanks het feit dat de Wet onmiskenbaar in strijd is met Europese regelgeving. Handhaving van onrechtmatige wetgeving is onrechtmatig. Door de Wet wordt op massale schaal inbreuk gemaakt op de fundamentele grondrechten van burgers, door van iedereen (meta)data te bewaren, ongeacht of personen verdacht zijn of niet (**Productie 6**).[5] De Minister van Veiligheid en Justitie vindt het echter noodzakelijk, zelfs na het arrest van het Hof van 8 april 2014 (hierna ook: '**het Arrest'**), om alle metadata gegevens van burgers op te slaan, *'nu niet op voorhand bij de opslag al kan worden onderscheiden tussen verdachte en niet-verdachte burgers'* (**Productie 7**).[6]

1.4 De manier waarop de Staat de afgelopen jaren omgaat met grondrechten is zorgelijk. Met name waar het gaat om rechtsbescherming tegenover de overheid waait er een kille wind vanuit Den Haag. Bijvoorbeeld op het gebied van de journalistieke bronbescherming. De Staat is al drie keer door het Europees Hof voor de Rechten van de Mens (hierna: '**het EHRM**') veroordeeld, in 2007, 2010 en 2012. Na jaren van toezeggingen en stilzitten zijn in het najaar van 2014 eindelijk twee wetsvoorstellen verschenen. Maar deze wetsvoorstellen schieten op essentiële punten tekort en wijken af van het advies van de Raad van State. Een adequate wettelijke regeling voor journalistieke bronbescherming is nog ver weg. Wanneer de Nederlandse staat door de hoogste Europese rechter gedwongen wordt de Nederlandse wet aan te passen, doet de regering dat met veel tegenwerking en vertraging. Adviezen van de Raad van State slaat zij regelmatig in de wind.

1.5 De opstelling van de regering met betrekking tot de bewaarplicht past in dat beeld. Dat de rechter er nu aan te pas moet komen om de regering te dwingen deze schending van grondrechten te staken is een zorgelijke ontwikkeling. Het zou de Staat sieren zich sterk te maken voor de privacy van haar burgers en de belangen van geheimhouders, in plaats van zolang mogelijk vasthouden aan een regeling waarvan al in april 2014 door de hoogste Europese rechter is vastgesteld dat die in strijd met fundamentele rechten is.

1.6 Daarom verzoeken Eisers uw rechtbank hiertoe een voorziening te treffen en de Wet buiten

[5] In *De Correspondent* werd aangetoont wat je met metadata allemaal te weten kan komen over een persoon: *Metadata, het meest onderschatte woord van het jaar*, 20 december 2013, en *Hoe je onschuldige smartphone bijna je hele leven doorgeeft aan de geheime dienst*, 20 december 2013.
[6] Brief d.d. 17 november 2014 van Minister Opstelten aan Tweede Kamer.

werking te stellen totdat deze is ingetrokken of is aangepast.

2. PARTIJEN

2.1 Eisers zijn onder te verdelen in drie groepen:

a. organisaties die zich sterk maken voor privacybelangen en/of mensenrechten;
b. groepen die een recht op geheimhouding hebben, zoals advocaten en journalisten; en
c. aanbieders van telecommunicatiediensten en van openbare telecommunicatie-netwerken.[7]

2.2 Iedere groep heeft er via een eigen invalshoek belang bij dat de Wet buiten werking wordt gesteld.

Organisaties die de belangen van mensenrechten behartigen

2.3 De burgers en privacy-organisaties ageren tegen de zware inmenging op de fundamentele privacy-grondrechten, zoals beschermd in artikelen 7 en 8 Handvest en 8 EVRM.

2.4 Privacy First, opgericht op 26 maart 2008, heeft blijkens haar statuten (**Productie 8**) ten doel*: 'het behouden en bevorderen van het recht op privacy, alsmede de persoonlijke vrijheid van leefomgeving, op welke wijze dan ook, onder meer door het in rechte optreden voor alle burgers in Nederland ter bescherming van dit algemene belang en voorts al hetgeen met een en ander rechtstreeks of zijdelings verband houdt of daartoe bevorderlijk kan zijn, alles in de ruimste zin van het woord.'* In casu komt Privacy First op grond van artikel 3:305a BW op voor het algemeen belang bij handhaving van het recht op privacy van iedereen in Nederland die communiceert via telefoon of internet. Een eigen belang van Privacy First ex artikel 3:303 BW is daarbij niet vereist, zo is recent door zowel de rechtbank Den Haag als het Hof Den Haag in vergelijkbare rechtszaken van Privacy First bevestigd. Overigens is in onderhavige zaak wel een eigen belang van Privacy First bij toewijzing van de vorderingen aanwezig, aangezien bij voorzetting van de huidige bewaarplicht tevens sprake is van een onrechtmatige inbreuk op de communicatievrijheid van Privacy First zelf. Privacy First is dan ook zowel ontvankelijk op grond van artikel 3:305a BW als op grond van artikel 3:303 BW.

[7] als bedoeld in artikel 13.2a Tw jo artikel 1.1. sub i, ee, ff Tw.

2.5 Het NJCM is een organisatie die volgens haar statuten (**Productie 9**) als doelstellingen heeft: '*het ontwikkelen, versterken en beschermen van de fundamentele rechten en vrijheden van de mens op nationaal en internationaal niveau en in het bijzonder, onverminderd genoemde doelstellingen, het bevorderen en handhaven van de volgende beginselen:*

a. *De verplichting van de overheid de fundamentele rechten en vrijheden te erkennen en in haar handelen en nalaten te eerbiedigen;*

b. *De mogelijkheid van beroep op de fundamentele rechten en vrijheden tegen particulieren;*

2.6 PILP, Public Interest Litigation Project, is een project van het NJCM om strategische procedures te voeren omtrent mensenrechten. Het NJCM is de in rechte optredende rechtspersoon. PILP en het NJCM vinden privacy een belangrijk mensenrecht, en constateren dat dit grondrecht in Nederland onder druk staat. Het NJCM en PILP zijn bovendien van oordeel dat uitspraken van het Hof door de Staat goed opgevolgd moeten worden en zij maken zich zorgen nu dat in het onderhavige geval niet direct gebeurt. Wanneer een Europese regeling vernietigd wordt op grond van een grove schending van mensenrechten is het wenselijk dat de handhaving van de daarop gebaseerde wet geschorst wordt totdat er een nieuwe wet is. NJCM en PILP vinden het zorgelijk dat de regering niet uit zichzelf onmiddellijk overgegaan is tot schorsing van de handhaving.[8]

Geheimhouders

2.7 Voor de geheimhouders, zoals advocaten en journalisten, geldt dat zij een verschoningsrecht hebben. Het opslaan en afgeven van de communicatiegegevens schendt dat recht.

2.8 De vereniging NVSA stelt zich blijkens haar statuten (**Productie 10**) onder meer ten doel *'(…) al datgene, dat voor een goed functioneren van een verdediging in strafzaken dienstig is en zonodig daartoe in rechte op te treden.'* Bijna alle in Nederland gespecialiseerde strafrechtadvocaten zijn lid van de NVSA. Advocaten kunnen aangeven welke telefoonlijnen onder geheimhoudersnummers vallen, zodat die gesprekken niet getapt kunnen worden door justitie. Advocaten ontberen die mogelijkheid voor internetgegevens of metadata van

[8] Ter vergelijking, na het arrest HvJEU 10 april 2014, zaak C-435/12 (*ACI/ Thuiskopie*), verklaarde staatsecretaris Teeven een week later dat het arrest onmiddellijke werking had, zodat illegaal downloaden in Nederland verboden was. Ook daar waren privacyrechten in het geding, namelijk die van de downloaders.

telefonie. Daarmee wordt onrechtmatig jegens hen gehandeld. Daarmee hebben zij, naast een collectief belang, ook een eigen belang ex artikel 3:303 BW in deze procedure een voorziening te vragen.

2.9 De NVJ stelt zich blijkens haar statuten (**Productie 11**) onder meer tot doel: *'nationaal en internationaal te waken en waar nodig te strijden voor de persvrijheid en het recht op informatie van de burgers, welke vrijheid en welk recht zij beschouwt als haar wezenlijke grondslagen*'. De NJV tracht dat doel te realiseren via alle wettige middelen. Ook de NVJ was eerder ontvankelijk in een vergelijkbare procedure, '*aangezien de persvrijheid en het recht op informatie van burgers onderdeel zijn van het recht op bescherming van de vrijheid van meningsuiting en de NVJ met haar vorderingen op grond van dit grondrecht de bescherming van journalisten wier belangen zij behartigt, beoogt te bewerkstelligen*.'[9]

2.10 Het recht op journalistieke bronbescherming brengt met zich mee dat in ieder geval een rechterlijke toetsing plaats moet vinden voordat de overheid informatie opvraagt die kan leiden tot het identificeren van bronnen. De Staat is al drie maal door het EHRM veroordeeld in zaken over journalistiek brongeheim wegens schending van artikelen 8 en 10 EVRM.[10]

Collectief belang en overleg

2.11 Privacy First, het NJCM, de NVJ en de NVSA komen allen op voor een collectief belang, op grond van artikel 3:305a BW, welke belangen zij ieder afzonderlijk volgens hun statuten behartigen. Al deze eisers waren eerder ontvankelijk in een of meerdere procedures tegen de Staat.[11]

---

9 Rb. Den Haag 23 juli 2014 ECLI:NL:RBDHA:2014:8966.

10 EHRM, *Voskuil v. Nederland*, 22 november 2007, nr. 64752/01, EHRM, Grote Kamer, *Sanoma v. Nederland*, 14 september 2010, nr. 38224/03: *First and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial decision-making body. (…) It is clear, in the Court's view, that the exercise of any independent review that only takes place subsequently to the handing over of material capable of revealing such sources would undermine the very essence of the right to confidentiality.*, en EHRM, *Telegraaf v. Nederland*, 22 november 2012, nr. 39315/06: *Review post factum (…) cannot restore the confidentiality of journalistic sources once it is destroyed. The Court thus finds that the law did not provide safeguards appropriate to the use of powers of surveillance against journalists with a view to discovering their journalistic sources. There has therefore been a violation of Articles 8 and 10 of the Convention.*

11 Zie Rb. Den Haag 23 juli 2014, ECLI:NL:RBDHA:2014:8966 (*Burgers tegen Plasterk*), r.o. 5.3 en 5.4, waarin Privacy First, de NVJ en de NVSA ontvankelijk waren, en HR 9 april 2010 ECLI:NL:HR:2010:BK4549 (*Vrouwenkiesrecht SGP*) waarin het NJCM ontvankelijk was.

2.12 Aan de eisen van artikel 3:305a BW is voldaan. Eisers hebben getracht door overleg het in deze procedure gevorderde te bereiken. Genoemde vier Eisers zijn allen een vereniging of stichting en zij behartigen de belangen die hier in het geding zijn, op basis van toereikende statutaire doelomschrijvingen (3:305a lid 1 BW). Zij ontplooien allen activiteiten op het gebied van bescherming van privacy, bronbescherming of geheimhouding. De belangen zijn gelijksoortig en lenen zich bij uitstek voor bundeling. Zij hebben de Minister van Veiligheid en Justitie op maandag 8 december 2014 verzocht te overleggen (**Productie 12**). Bij monde van de landsadvocaat heeft de Minister aangegeven wel bereid te zijn tot overleg, maar niet tot wijziging van het standpunt, zoals verwoord in de brief van 17 november 2014 aan de Tweede Kamer (**Productie 13**). De poging van dezer Eisers om via overleg het in deze procedure gevorderde te bereiken heeft aldus geen resultaat gehad (**Productie 14**).

Algemeen belang en eigen belang

2.13 Zowel het belang van de bronbescherming als het belang van de geheimhouding zijn algemene belangen. Journalisten als publieke waakhond en advocaten vervullen immers elementaire rollen in de democratische rechtstaat. De journalisten die lid zijn van de NVJ hebben ook een eigen belang bij waarborgen voor bronbescherming. Ook de leden van de NVSA hebben een eigen belang bij waarborgen met betrekking tot de vertrouwelijkheid van communicatie met cliënten.

De aanbieders van openbare telecommunicatiediensten en telecommunicatienetwerken

2.14 De aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatie-diensten (hierna: '**de aanbieders**') zijn thans verplicht verkeers- en locatiegegevens op te slaan. Het onderhouden van die systemen kost uiteraard geld, hetgeen een beperking van hun recht op vrijheid van onderneming is in de zin van artikel 17 Handvest. De vergoeding die zij hiervoor ontvangen is niet kostendekkend. Zij slaan (op grond van de Wet) meer en langer gegevens op dan nodig is voor bedrijfsdoeleinden, zoals bijvoorbeeld facturatie. Veel aanbieders houden er twee systemen voor aan. Eén systeem voor de bewaarplicht en één voor bedrijfsdoeleinden.

2.15 De aanbieders moeten thans gegevens blijven opslaan, zonder dat daarvoor een rechtmatige grondslag is. Daarmee handelen ze in strijd met de Wet Bescherming Persoonsgegevens en

artikel 15 e-privacy richtlijn. De aanbieders zitten aldus in een onmogelijke spagaat. Voys, SpeakUp en BIT (**Producties 15, 16 en 17**) bewaren momenteel gegevens die zij – bij gebreke van de Wet – niet zouden bewaren. Zo zou Voys bijvoorbeeld de klant de keuze willen geven welke gegevens zij voor de klant bewaart. SpeakUp streeft naar een bewaartermijn voor bedrijfsdoeleinden van drie maanden. Langer bewaren zou een opt-in keuze van de klant kunnen zijn.

De Staat

2.16 Het Ministerie van Economische zaken is belast met toezicht en handhaving van de Telecommunicatiewet. Het Ministerie heeft die bevoegdheid gedelegeerd aan een aantal toezichthouders. Het toezicht op de naleving van de bewaarplicht ligt in handen van het Agentschap Telecom (hierna: '**AT**'), dat opereert als een onafhankelijke toezichthouder en toeziet op de naleving van de Wet. Het AT is onderdeel van het Ministerie van Economische Zaken, en legt rechtstreeks verantwoording af aan de Minister van Economische Zaken. Daarnaast ziet het College Bescherming Persoonsgegeven (hierna: '**CBP**') toe op alle wettelijke regelingen waarin sprake is van het bewaren, gebruiken of verwerken van persoonsgegevens.

3. ACHTERGROND EN FEITEN

De Dataretentierichtlijn

3.1 De Dataretentierichtlijn heeft de lidstaten opgedragen bepaalde categorieën gegevens gedurende ten minste zes maanden en ten hoogste twee jaar vanaf de datum van de communicatie te bewaren, op zodanige wijze dat de bewaarde gegevens en alle andere daarmee verband houdende relevante informatie onverwijld aan de bevoegde autoriteiten kunnen worden meegedeeld wanneer daarom wordt verzocht.

3.2 Het gaat om de volgende gegevens:

a) gegevens die nodig zijn om de bron van een communicatie te traceren en te identificeren:

1. in het geval van telefonie over een vast of mobiel netwerk:

i) het telefoonnummer van de oproeper,

ii) naam en adres van de abonnee of de geregistreerde gebruiker;

2. in het geval van internettoegang, email over het internet en internettelefonie:

i) de toegewezen gebruikersidentificatie(s),

ii) de gebruikersidentificatie en het telefoonnummer toegewezen aan elke communicatie die het publieke telefoonnetwerk binnenkomt,

iii) naam en adres van de abonnee of de geregistreerde gebruiker aan wie het IPadres, de gebruikersidentificatie of het telefoonnummer was toegewezen op het tijdstip van de communicatie;

b) gegevens die nodig zijn om de bestemming van een communicatie te identificeren:

1. in het geval van telefonie over een vast netwerk en mobiele telefonie:

i) het telefoonnummer (de telefoonnummers) die werden opgeroepen en, in het geval van aanvullende diensten zoals call forwarding of call transfer, het nummer (de nummers) waarnaar de verbinding is doorgeleid,

ii) naam (namen) en adres (adressen) van de abonnee(s) of de geregistreerde gebruiker(s);

2. in het geval van email over het internet en internettelefonie:

i) de gebruikersidentificatie of [het] telefoonnummer van de beoogde ontvanger(s) van een internettelefoonoproep,

ii) naam (namen) en adres (adressen) van de abonnee(s) of de geregistreerde gebruiker(s) en de gebruikersidentificatie van de beoogde ontvanger van de communicatie;

c) gegevens die nodig zijn om de datum, het tijdstip en de duur van een communicatie te bepalen:

1. in het geval van telefonie over een vast netwerk en mobiele telefonie: datum en tijdstip van aanvang en einde van de verbinding;

2. in het geval van internettoegang, email over het internet en internettelefonie:

i) datum en tijdstip van de login en logoff van een internetsessie gebaseerd op een bepaalde tijdzone, samen met het IPadres, hetzij statisch, hetzij dynamisch, dat door de aanbieder van een internettoegangsdienst aan een communicatie is toegewezen, en de gebruikersidentificatie van de abonnee of geregistreerde gebruiker,

ii) [...] datum en tijdstip van de login en logoff van een emaildienst over het internet of internettelefoniedienst gebaseerd op een bepaalde tijdzone;

d) gegevens die nodig zijn om het type communicatie te bepalen:

1. in het geval van telefonie over een vast netwerk en van mobiele telefonie: de gebruikte telefoondienst,

2. in het geval van email over het internet en internettelefonie: de gebruikte internetdienst;

e) gegevens die nodig zijn om de communicatieapparatuur of de vermoedelijke communicatieapparatuur van de gebruikers te identificeren:

1. in het geval van telefonie over een vast netwerk, het/de oproepende en opgeroepen nummer(s);

2. in het geval van mobiele telefonie:

i) het/de oproepende en opgeroepen nummer(s),

ii) de International Mobile Subscriber Identity (IMSI) van de oproepende deelnemer,

iii) de International Mobile Equipment Identity (IMEI) van de oproepende deelnemer,

iv) de IMSI van de opgeroepen deelnemer,

v) de IMEI van de opgeroepen deelnemer,

vi) in geval van vooraf betaalde anonieme diensten, datum en tijdstip van de eerste activering van de dienst en aanduiding (Cell ID) van de locatie waaruit de dienst is geactiveerd;

3. in het geval van internettoegang, email over het internet en internetdiensten:

i) het inbellende nummer voor een inbelverbinding,

ii) de digital subscriber line (DSL) of [een] ander eindpunt van de initiatiefnemer van de communicatie;

f) gegevens die nodig zijn om de locatie van mobiele communicatieapparatuur te bepalen:

1. de locatieaanduiding (Cell ID) bij het begin van de verbinding,

2. gegevens voor het identificeren van de geografische locatie van cells middels referentie aan hun locatieaanduidingen (Cell ID's) gedurende de periode dat communicatiegegevens worden bewaard.

2. Gegevens waaruit de inhoud van de communicatie kan worden opgemaakt, mogen krachtens deze richtlijn niet worden bewaard.

De Wet

3.3 De Wet implementeert de Dataretentierichtlijn vrij letterlijk. De Wet heeft betrekking op verkeers- en locatiegegevens. Onder verkeersgegevens worden de gegevens verstaan die worden verwerkt voor het overbrengen van communicatie over een elektronisch communicatienetwerk of voor de facturering ervan. Dit kunnen onder andere zijn het aansluitnummer, de datum, het tijdstip en de duur van de communicatie en het soort communicatie. Locatiegegevens betreffen gegevens over de geografische positie van het gebruikte apparaat, bijvoorbeeld van de mobiele telefoon.

3.4 De Wet verplicht aanbieders om metadata van telefoongesprekken en internetsessies voor respectievelijk 12 en 6 maanden te bewaren. In de Wet is dit vastgelegd in artikel 13.2a dat luidt:

Artikel 13.2a Tw

1. In dit artikel wordt verstaan onder:

a. gegevens: de verkeers- en locatiegegevens, bedoeld in artikel 11.1, onderdeel b respectievelijk onderdeel d, alsmede de daarmee verband houdende gegevens die nodig zijn om de abonnee of gebruiker te identificeren;

b. oproeppoging 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:

a. twaalf maanden voor gegevens in verband met telefonie over een vast of mobiel netwerk, bedoeld in de bij deze wet behorende bijlage, onder A, of

b. zes maanden voor gegevens in verband met internettoegang, e-mail over het internet en internettelefonie, bedoeld in de bij deze wet behorende bijlage, onder B, gerekend vanaf de datum van de communicatie.

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

3.5 Het voorgaande is nader uitgewerkt in een algemene maatregel van bestuur, het Besluit vorderen gegevens telecommunicatie[12] (hierna: '**het Besluit**', **Productie 18**) .

3.6 De in artikel 13.2a lid 2 bedoelde gegevens, die de aanbieders moeten bewaren, zijn als volgt uitgewerkt in een bij de Wet behorende bijlage (**Productie 19**), waarbij vrij letterlijk de tekst van de Dataretentierichtlijn is gevolgd:

In deze bijlage wordt verstaan onder:

a. telefoondienst: oproepen (met inbegrip van spraak, voicemail, conference call of call-gegevens), aanvullende diensten (met inbegrip van call forwarding en call transfer), messaging- en multimediadiensten (met inbegrip van short message service (SMS), enhanced media service (EMS) en multimedia service (MMS);

b. gebruikersidentificatie: een unieke identificatie die aan een persoon wordt toegewezen wanneer deze zich abonneert op of registreert bij een internettoegangsdienst of internetcommunicatiedienst;

c. celidentiteit (Cell ID): de unieke code van een cel van waaruit een mobiele telefoonoproep werd begonnen of beëindigd.

In deze bijlage worden als gegevens, bedoeld in artikel 13.2a van de wet, aangewezen de volgende gegevens:

A. Bij telefonie over een mobiel of een vast netwerk:

a. het telefoonnummer van de oproeper en het telefoonnummer (de telefoonnummers) die werden opgeroepen en, in het geval van aanvullende diensten zoals call forwarding of call transfer, het nummer (de nummers) waarnaar de verbinding is doorgeleid.

b. namen en adressen van de betrokken abonnees of geregistreerde gebruikers;

[12] Stb. 2004, 394, laatstelijk gewijzigd Stb. 2006, 730.

c. datum en tijdstip van aanvang en einde van de verbinding;

d. de gebruikte telefoondienst;

e. bij mobiele telefonie:

– de International Mobile Subscriber Identity (IMSI) van de oproepende en van de opgeroepen deelnemer;

– de International Mobile Equipment Identity (IMEI) van de oproepende en de opgeroepen deelnemer;

– in geval van vooraf betaalde anonieme diensten, datum en tijdstip van de eerste activering van de dienst en aanduiding (Cell ID) van de locatie waaruit de dienst is geactiveerd;

– de locatieaanduiding bij het begin van de verbinding;

– gegevens voor het identificeren van de geografische locatie van cells middels referentie aan hun locatieaanduidingen gedurende de periode dat communicatiegegevens worden bewaard.

B. Bij internettoegang, e-mail over het internet en internettelefonie:

a. de toegewezen gebruikersidentificatie(s) en de gebruikersidentificatie of telefoonnummer van de beoogde ontvanger(s) van een internettelefoonoproep;

b. de gebruikersidentificatie en het telefoonnummer toegewezen aan elke communicatie die het publieke telefoonnetwerk binnenkomt;

c. naam en adres van de abonnee of de geregistreerde gebruiker aan wie het IP-adres, de gebruikersidentificatie of het telefoonnummer was toegewezen op het tijdstip van de communicatie en naam (namen) en adres (adressen) van de abonnee(s) of de geregistreerde gebruiker(s) en de gebruikersidentificatie van de beoogde ontvanger van communicatie;

d. datum en tijdstip van de log-in en log-off van een internetsessie gebaseerd op een bepaalde tijdzone, samen met het IP-adres, hetzij statisch, hetzij dynamisch, dat door de aanbieder van een internettoegangsdienst aan een communicatie is toegewezen, en de gebruikersidentificatie van de abonnee of geregistreerde gebruiker;

e. datum en tijdstip van de log-in en log-off van een e-maildienst over het internet of internettelefoniedienst gebaseerd op een bepaalde tijdzone;

f. de gebruikte internetdienst;

g. het inbellende nummer voor een inbelverbinding;

h. de digital subscriber line (DSL) of ander eindpunt van de initiatiefnemer van de communicatie.

Het arrest van 8 april 2014

3.7 Het Europese Hof verklaarde op 8 april 2014 de Dataretentierichtlijn met terugwerkende kracht ongeldig. Het Hof was van oordeel dat de Dataretentierichtlijn een buitengewoon zware inmenging *('wide-ranging […] and particularly serious interference'*) op de eerbiediging van het privéleven en bescherming van persoonsgegevens vormde, wegens schending van artikelen 7

en 8 Handvest van de Grondrechten (hierna ook: '**het Handvest**'):[13]

> '57 Dienaangaande zij in de eerste plaats vastgesteld dat richtlijn 2006/24 algemeen van toepassing is op alle personen, alle elektronischecommunicatiemiddelen 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 elektronischecommunicatiediensten, 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,

[13] Handvest van de grondrechten van de Europese Unie, PbEU 2007/C 303/01.

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.

63 Wat in de derde plaats de termijn betreft gedurende welke de gegevens worden bewaard, bepaalt artikel 6 van richtlijn 2006/24 dat deze gedurende ten minste zes maanden moeten worden bewaard, zonder dat enig onderscheid wordt gemaakt tussen de in artikel 5 van deze richtlijn genoemde categorieën van gegevens naargelang van het nut ervan voor het nagestreefde doel of naargelang van de betrokken personen.

64 Bovendien varieert de bewaringstermijn van ten minste zes maanden tot ten hoogste vierentwintig maanden, zonder dat wordt gepreciseerd dat deze termijn op basis van objectieve criteria moet worden vastgesteld om te waarborgen dat hij beperkt is tot wat strikt noodzakelijk is.

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.'

De regering handhaaft niettemin de Wet

3.8 Na het Arrest heeft de Nederlandse regering meerdere keren expliciet verklaard de Wet te blijven handhaven (**Productie 20**).[14] Staatssecretaris Teeven heeft dit begin april in het mondelinge vragenuurtje gesteld. De Minister van Economische Zaken Kamp heeft daarnaar verwezen in zijn brief van 16 mei 2014 aan de Tweede Kamer (**Productie 21**):

'Het agentschap zal de komende toezichtperiode inzetten op een verbetering in de naleving van deze verplichtingen en is daarbij bevoegd boetes op te leggen oplopend tot € 450.000,= per overtreding.
(…)
De staatssecretaris van Veiligheid en Justitie heeft aangegeven dat de nationale regelgeving van kracht blijft.

(…)
Handhaving van bestaande wettelijke normen blijft onverminderd van belang en dan met name het toezicht op niet te lang en niet te veel bewaren van gegevens van klanten/gebruikers.'

3.9 In de brief van 17 november 2014 heeft de Minister van Veiligheid en Justitie Opstelten een aanpassingswet voorgesteld. Totdat die nieuwe wet in werking is getreden zal de huidige Wet gehandhaafd worden.

3.10 Op 1 december 2014 heeft het kabinet in reactie op een artikel op de website van Bits of Freedom (bof.nl) bericht aan de redacties van tweakers en Nu.nl dat zij het opschorten van de

[14] http://webwereld.nl/overheid/82140-agentschap-telecom-blijft-bewaarplicht-handhaven.

Wet niet nodig vindt, omdat de Wet op termijn zal worden aangepast (**Productie 22**).[15] Hoe en wanneer de Wet aangepast zal worden, is nog de vraag. Het debat daarover zal in het parlement en in de maatschappij gevoerd worden. Iedereen kan via een internetconsultatie zijn visie op het voorstel aan de wetgever laten weten. Deze ingestuurde reacties zijn zonder uitzondering zeer kritisch. Een aantal grote marktpartijen heeft bovendien nog tot eind januari 2015 de tijd gekregen om input te geven aan de Minister. De Minister maakt geen haast.

3.11 Het is waarschijnlijk dat het nog meer dan een jaar zal duren voordat een aanpassingsvoorstel van kracht wordt. Ondertussen gaat de grootschalige *mass surveillance* door, zonder dat de door het Hof vastgestelde gebreken zijn verholpen. De vaste commissies Immigratie en Asiel/JBZRaad en voor Veiligheid en Justitie van de Eerste Kamer hebben op 10 december 2014 de Minister hierop aangesproken:

> *'De commissies stellen vast dat de regering als gevolg van het arrest van het Hof van Justitie met een nieuw voorstel komt, dat overeenkomstig de voorlichting van de Raad van State een aantal beperkingen bevat ten opzichte van de Wet bewaarplicht telecommunicatiegegevens. De commissies stellen voorts vast dat de Raad van State in haar voorlichting ook heeft aangegeven dat de wet in zijn huidige vorm niet in stand kan blijven. Het zal echter enige tijd duren voordat het nieuwe voorstel, dat onlangs in consultatie is gegaan, in werking zal treden. De regering kan er daarom niet mee volstaan om tot dat tijdstip de oude wet ongewijzigd te handhaven. Zij zou op zijn minst de voorgestelde beperkingen al moeten gaan toepassen. De commissies verzoeken of de regering hiertoe bereid is.'* (onderstreping advocaat)

3.12 Of de door het Ministerie van Veiligheid en Justitie voorgestelde aanpassingen voldoende zijn, is geen onderwerp van deze procedure. Partijen wensen daarover de dialoog aan te gaan buiten de rechtszaal, ondermeer via de internetconsultatie. Aanleiding voor deze procedure is het feit dat de Wet vooralsnog onverkort van kracht blijft en gehandhaafd zal worden, ondanks kennelijke strijd met hogere Europese regelgeving.

3.13 Zolang de Wet niet is ingetrokken of aangepast worden de privacyrechten van burgers massaal geschonden om een ineffectieve en achterhaalde Wet te handhaven. Voor geheimhouders zijn er onvoldoende waarborgen dat hun communicatie vertrouwelijk blijft. En de aanbieders zitten tussen twee vuren. Als zij blijven bewaren handelen zij in strijd met de fundamentele

[15] http://tweakers.net/nieuws/99985/bewaarplicht-moet-worden-opgeschort.html.

grondrechten van burgers en geheimhouders, en als zij stoppen met bewaren overtreden zij de Wet.

3.14 Door de Wet sinds 8 april 2014 niet buiten werking te stellen, handelt de Staat onmiskenbaar onrechtmatig jegens Eisers.

4. DE WET MOET BUITEN WERKING WORDEN GESTELD

4.1 Er zijn diverse redenen waarom de Wet in de huidige vorm niet in stand kan blijven, en op zo kort mogelijke termijn buiten werking moet worden gesteld. De belangrijkste argumenten volgen uit het Arrest en het daaropvolgende advies van de Raad van State. Daarbij is van belang dat de regering in haar brief van 17 november 2014 heeft erkend dat de Wet moet worden aangepast.

Argumenten uit het Arrest

4.2 De Ierse High Court en het Oostenrijkse Verfassungsgerichtshof hadden prejudiciële vragen gesteld aan het Hof. Zij verzochten het Hof de geldigheid van de Dataretentierichtlijn te toetsen aan onder andere de artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie, die zien op respectievelijk het recht op eerbiediging van het privé-leven (inclusief familie- en gezinsleven) en het daaraan verwante recht op bescherming van persoonsgegevens.

4.3 Het Hof stelt eerst vast (r.o. 28) dat de in artikel 11 Handvest gewaarborgde vrijheid van meningsuiting door dataretentie beïnvloed kan worden, ook al bestaat er geen recht om de inhoud van de communicatie te bewaren en in te zien. Er is dus gevaar voor een '*chilling effect*.'

4.4 Het Hof oordeelt dat de bewaarplicht op zichzelf een inmenging is in het recht op privacy (artikel 7 Handvest) (r.o. 34). Dit ongeacht de vragen of de gegevens gevoelig zijn, of dat personen er enig nadeel van ondervonden hebben. Het bewaren is immers een verwerking van persoonsgegevens in de zin van artikel 8 Handvest (r.o. 29).

4.5 De toegang tot die gegevens door de overheid is een *aanvullende* inmenging.[16] Ook is de verwerking van persoonsgegevens een inmenging van het in artikel 8 Handvest beschermde recht op bescherming van persoonsgegevens.

4.6 Het Hof oordeelt dat de Dataretentierichtlijn een zeer ruime en bijzonder zware inmenging vormt in de door de artikelen 7 en 8 van het Handvest gewaarborgde fundamentele rechten (r.o. 37). De omstandigheid dat de gegevens worden bewaard en later worden gebruikt zonder dat de betrokkenen worden ingelicht, kan bij de betrokken personen het gevoel opwekken dat hun privéleven constant in de gaten wordt gehouden, aldus het Hof.

4.7 Dat alles neemt niet weg dat het doel van de Dataretentierichtlijn (het bestrijden van internationaal terrorisme en ernstige criminaliteit) in beginsel een dergelijke inmenging kan rechtvaardigen. Echter, het Hof acht de wijze waarop de bewaarplicht in de Dataretentierichtlijn is geregeld om twee redenen in strijd met het evenredigheidsbeginsel.

4.8 Daarbij is van belang dat artikel 52 Handvest eist dat beperkingen op de uitoefening van de in het Handvest erkende rechten en vrijheden bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen. Er kunnen, met inachtneming van het evenredigheidsbeginsel, alleen beperkingen worden gesteld indien die noodzakelijk zijn en daadwerkelijk aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen beantwoorden.

Onvoldoende duidelijke en precieze regels en criteria

4.9 In de eerste plaats bevat de Dataretentierichtlijn volgens het Hof onvoldoende duidelijke en precieze regels en criteria betreffende de omvang van de inmenging in de door de genoemde fundamentele rechten. Dat geldt in ieder geval voor (i) de reikwijdte van de bewaarplicht zelf, (ii) voor de begrenzing van de toegang tot de gegevens door bevoegde autoriteiten en (iii) voor de termijn waarvoor de gegevens moeten worden bewaard.

[16] De toegang van de bevoegde nationale autoriteiten tot de gegevens is een aanvullende inmenging in dat fundamentele recht (zie met betrekking tot artikel 8 EVRM, arresten EHRM, *Leander/Zweden*, 26 maart 1987, reeks A nr. 116, § 48; *Rotaru/Roemenië*, Grote kamer, nr. 28341/95, § 46, CEDH 2000V, en *Weber en Saravia/Duitsland* (dec.), nr. 54934/00, § 79, CEDH 2006XI). De artikelen 4 en 8 van richtlijn 2006/24, die de toegang van de bevoegde nationale autoriteiten tot de gegevens regelen, vormen dus eveneens een inmenging in de door artikel 7 van het Handvest gewaarborgde rechten.

4.10 Wat betreft de reikwijdte van de bewaarplicht overweegt het Hof dat die betrekking heeft op gegevens betreffende alle eindgebruikers van telecomnetwerken (d.w.z. nagenoeg iedereen), met inbegrip van al degenen tegen wie geen enkele verdenking van ernstige criminaliteit bestaat (r.o. 58):

> 'Richtlijn 2006/24 is om te beginnen algemeen van toepassing op alle personen die gebruikmaken van elektronische communicatiediensten, 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.'

4.11 In dat verband wijst het Hof er ook op dat de bewaarplicht zich zelfs uitstrekt tot de communicatie van degenen met een beroepsgeheim ('zakengeheim'), zoals advocaten en artsen.

4.12 Voorts constateert het Hof dat de Dataretentierichtlijn geen verband eist tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid (r.o. 59). Er is geen afbakening van de '*gegevens met betrekking 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*'.

4.13 De Dataretentierichtlijn liet dus de ruimte om gegevens van iedereen te bewaren. In de Wet is van die ruimte gebruik gemaakt. Het Hof sanctioneert het ongericht bewaren van gegevens van alle burgers, zonder onderscheid naar persoon, locatie of gegevens. Het bewaren van alle verkeers-en locatiegegevens voor 6 tot 12 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 huidige Wet.

Toegang - onvoldoende bescherming tegen misbruik en onrechtmatige toegang

4.14 Daarnaast bevat de Dataretentierichtlijn geen '*objectieve criteria ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens',* aldus het Hof (r.o. 60). Ook zijn er geen materiële of procedurele voorwaarden voor de toegang tot die gegevens of objectieve criteria voor de kring van personen die kennis kunnen nemen van de gegevens. Er

gelden op dit moment voor de overheid geen beperkingen wie er kennis kan nemen van de gegevens, wanneer toegang tot die gegevens is verkregen.

4.15 Het Hof tilt er zwaar aan dat er geen voorafgaande rechterlijke controle is. De regering deelt dit oordeel kennelijk, want op dit punt is een voorstel gedaan. Echter, op dit moment 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.

Bezwaren ten aanzien van de bewaartermijnen

4.16 In r.o. 63 en 64 somt het Hof enkele bezwaren tegen de termijn op:

a. er wordt geen onderscheid gemaakt naargelang het nut daarvan, het nagestreefde doel of betrokken personen; en
b. er worden geen objectieve criteria genoemd om de bewaartermijn te beperken tot wat strikt noodzakelijk is.

4.17 De conclusie van het Hof luidt dat er sprake is van een zeer ruime en bijzonder zware inmenging in de fundamentele rechten, zonder dat deze inmenging nauwkeurig is omkaderd door bepalingen die kunnen waarborgen dat zij daadwerkelijk beperkt is tot het strikt noodzakelijke (r.o. 65).

4.18 Voorts stelt het Hof vast (r.o. 66) dat er onvoldoende garanties zijn dat de gegevens beschermd worden tegen misbruik, zoals artikel 8 van het Handvest eist. Lidstaten hebben ook geen verplichting daar regels voor te stellen.

4.19 In r.o. 67 overweegt het Hof:

> 'Artikel 7 van richtlijn 2006/24, gelezen in samenhang met artikel 4, lid 1, van richtlijn 2002/58 en artikel 17, lid 1, tweede alinea, van richtlijn 95/46, waarborgt niet dat bovengenoemde aanbieders via technische en organisatorische maatregelen een bijzonder hoog niveau van bescherming en beveiliging bieden, maar verleent deze aanbieders met name de mogelijkheid om bij de vaststelling van het door hen geboden beschermingsniveau rekening te houden met economische overwegingen, meer bepaald met de kosten voor het uitvoeren van de veiligheidsmaatregelen. In het bijzonder waarborgt richtlijn 2006/24 niet dat de gegevens na de bewaarperiode onherroepelijk worden vernietigd.'

4.20 Tot slot maakt het Hof er gewag van dat er geen verplichting is om de gegevens op Europees grondgebied te bewaren, zodat de toezichthouders, zoals het CBP en AT, effectief toezicht

kunnen houden.

4.21 Op grond van het voorgaande heeft Hof de Dataretentierichtlijn met terugwerkende kracht ongeldig verklaard.

Voldoet de Wet momenteel aan de daaraan te stellen eisen?

4.22 De Wet moet aan artikelen 7, 8 en 52 van het Handvest voldoen, en bovendien aan artikel 15 e-privacyrichtlijn. [17] De regering heeft dit ook al bevestigd in de brief van Minister van Veiligheid en Justitie van 17 november 2014.

Artikel 15 e-privacyrichtlijn

4.23 Artikel 15, eerste lid, van de e-privacyrichtlijn luidt:

> 'De lidstaten kunnen wettelijke maatregelen treffen ter beperking van de reikwijdte van de in artikelen 5 en 6, artikel 8, leden 1, 2, 3 en 4, en artikel 9 van deze richtlijn bedoelde rechten en plichten, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van de nationale, dat wil zeggen de staatsveiligheid, de landsverdediging, de openbare veiligheid, of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten of van onbevoegd gebruik van het elektronische communicatiesysteem als bedoeld in artikel 13, lid 1, van richtlijn 95/46/EG. Daartoe kunnen de lidstaten onder andere wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode te bewaren om de redenen die in dit lid worden genoemd. 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. (onderstreping advocaat)'

4.24 De Raad van State is door de Minister van Justitie om advies gevraagd over wat de gevolgen voor de Nederlandse regelgeving zijn van het Arrest. De Raad van State redeneert als volgt:

> 'Met de ongeldigverklaring van de Dataretentierichtlijn wordt de bevoegdheid van EUlidstaten om een bewaarplicht voor telecommunicatiegegevens te regelen opnieuw beheerst door artikel 15, eerste lid, van de e-privacyrichtlijn. De regeling in de Wet bewaarplicht telecommunicatiegegevens moet voldoen aan het bepaalde in artikel 15, eerste lid, van de e-privacyrichtlijn en de daarin genoemde voorwaarden. '[18]

4.25 Artikel 15 van de e-privacyrichtlijn eist dat maatregelen die tot doel hebben dat

[17] Artikel 15, eerste lid, van richtlijn 2002/58/EG van12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (e-privacyrichtlijn). Artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie verwijzen naar de rechten, vrijheden en beginselen die zijn vastgesteld in het Handvest van de grondrechten van de Europese Unie en verklaart dat dit Handvest dezelfde juridische waarde heeft als de Verdragen.

[18] Adies Raad van State d.d. 17 juli 2014, W03.14.0161/II/Vo, Kamerstukken II 2014/2015, 33 542, nr. 16.

telecommunicatiegegevens worden bewaard voor opsporing van strafbare feiten voldoen aan de algemene beginselen van het Gemeenschapsrecht. De bescherming van grondrechten, zoals vastgelegd in de artikelen 7 en 8 Handvest en 8 EVRM zijn 'algemene beginselen'. De Wet schendt artikelen 7 en 8 van het Handvest en 8 EVRM, op gelijke wijze als de Dataretentierichtlijn dat deed.

4.26 De Raad van State concludeert dat de Wet moet voldoen aan artikelen 7 en 8 Handvest:

> 'Toetsing van de Wet bewaarplicht telecommunicatiegegevens aan het Handvest leidt tot de conclusie dat de Wet bewaarplicht telecommunicatiegegevens net als de Dataretentierichtlijn in strijd is met de artikelen 7 en 8 van het Handvest. Aan deze conclusie liggen dezelfde redenen ten grondslag als die leidden tot de ongeldigverklaring van de Dataretentierichtlijn. Voor zover de Wet bewaarplicht telecommunicatiegegevens de door het Hof gewraakte bepalingen uit de Dataretentierichtlijn heeft omgezet, heeft de Wet immers vrijwel dezelfde inhoud als de Dataretentierichtlijn.'

4.27 De regering heeft in de brief van 17 november 2014 erkend dat de Wet in strijd is met de e-privacyrichtlijn. Ook heeft zij erkend dat de Wet aan artikel 15 e-privacyrichtlijn moet voldoen. De Minister van Veiligheid en Justitie formuleerde dat als volgt:

> 'Vervolgens is de vraag aan de orde of de Wet bewaarplicht telecommunicatiegegevens aangepast moet worden, in het licht van de uitspraak van het Hof van Justitie. De regering beantwoordt deze vraag eveneens bevestigend. Nationale regels over de bewaring van telecommunicatiegegevens zijn relevant voor het vrije verkeer van diensten binnen de Europese Unie en vallen, nu de richtlijn dataretentie ongeldig is verklaard, onder de reikwijdte van richtlijn 2002/58/EG (e-privacyrichtlijn). Op grond van deze richtlijn kunnen de lidstaten regels stellen voor het bewaren van telecommunicatiegegevens, indien dat in een democratische samenleving noodzakelijk, redelijk en proportioneel is ter waarborging van legitieme belangen, waaronder het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten. Daartoe kunnen lidstaten onder andere wetgevingsmaatregelen treffen om gegevens gedurende een beperkte periode voor die doelen te bewaren. Deze maatregelen dienen in overeenstemming te zijn met het gemeenschapsrecht, met inbegrip van de beginselen, bedoeld in het Handvest van de grondrechten en het EVRM. Omdat een dergelijke bewaarplicht binnen de werkingssfeer van de e-privacyrichtlijn valt (artikel 15, eerste lid, e-privacyrichtlijn) en dus binnen de werkingssfeer van het recht van de Europese Unie, valt deze tevens onder de werkingssfeer van het Handvest van de grondrechten. De Afdeling advisering stelt vast dat de Wet bewaarplicht telecommunicatiegegevens de door het Hof van Justitie gewraakte bepalingen van de richtlijn dataretentie omzet en dat toetsing van de Wet bewaarplicht telecommunicatiegegevens aan het Handvest van de grondrechten tot de conclusie leidt dat deze wet, net als de richtlijn dataretentie, in strijd is met de artikelen 7 en 8 van het Handvest van de grondrechten. Hieruit vloeit voort dat de nationale wetgeving moet worden aangepast voor zover deze niet in overeenstemming is met het Handvest van de grondrechten. De Nederlandse regering kan deze zienswijze onderschrijven.'

4.28 De Wet kan daarom niet in stand blijven wegens strijd met het Unierecht. De Raad van State wijst op het *Van Gelder Papier*-arrest waarin de Hoge Raad vaststelde dat sprake is van

onrechtmatig handelen van de Staat wanneer de Staat een met een hogere regeling strijdig en mitsdien onverbindend voorschrift handhaaft.[19] Artikel 94 Grondwet staat de rechter toe de Wet, als formele wet, te toetsen aan de artikelen 7, 8 en 11 Handvest, artikel 15 e-privacyrichtlijn en aan de artikelen 8 en 10 EVRM.[20] Die toetsing leidt tot het oordeel dat de Wet onmiskenbaar onverbindend is.

De Wet is niet effectief en achterhaald

4.29 De Wet is bovendien nauwelijks effectief, zo wordt bevestigd door een onderzoek van het Wetenschappelijk Onderzoeks- en Documentatie Centrum (**Productie 23**).[21] Volgens dat onderzoek is de Wet achterhaald:

> 'Door de voortschrijdende technische ontwikkelingen is de huidige bewaarplicht voor internetgegevens grotendeels achterhaald. De wet is geschreven in een tijdperk dat men inlogde op het internet met een modem, terwijl veel mensen tegenwoordig 24 uur per dag, 7 dagen in de week online zijn. De lijst van te bewaren gegevens in de bijlage behorende bij artikel 13.2a Tw is gedateerd, waardoor gegevens van burgers worden opgeslagen die niet of nauwelijks door opsporingsdiensten worden gebruikt. Dit is een onwenselijke situatie.' (p. 149)

4.30 Vele andere lidstaten in Europa schaften de op basis van de Dataretentierichtlijn geïmplementeerde wetten al af, of stelden de bewaarplicht buiten werking. In Bulgarije, Roemenië, Cyprus, Duitsland en Tsjechië oordeelden de constitutionele rechtscolleges dat de nationale wetten en implementatie onhoudbaar waren wegens strijd met privacy-grondrechten. Het Oostenrijkse Constitutionele Hof heeft op 27 juni 2014 bepaald dat de Oostenrijkse wet ongeldig was. Op 23 april 2014 heeft het Constitutionele Hof van Slowakije de Slowaakse wet opgeschort. En op 3 juli 2014 heeft ook het Sloveense Constitutionele Hof een soortgelijke uitspraak gedaan. In Roemenië is op 8 juli 2014 de Roemeense bewaarplicht ongrondwettelijk verklaard. Dat Hof schorste de wet voor 45 dagen. Binnen die termijn kreeg de wetgever de tijd de wet te repareren. Na het verstrijken van de termijn zou de wet permanent buiten werking worden gesteld. Doordat de aanbieders in Nederland nog wel verplicht zijn om gegevens te bewaren, ontstaat er oneerlijke concurrentie in Europa.

---

[19] HR van 9 mei 1986, ECLI:NL:HR:1986:AC0867.

[20] Zie ook Hof Den Haag, 28 januari 2014; ECLI:NL:GHDHA:2014:72 over aansprakelijkheid van de staat voor niet juist invoeren van Richtlijn 2003/88/EG m.b.t. recht op vakantie tijdens ziekte.

[21] Bijlage bij de brief Minister van Veiligheid en Justitie van 12 februari 2014 inzake Evaluatie van de Wet bewaarplicht telecommunicatie- en internetgegevens (Kamerstuk 33 870, nr.1).

Artikel 8 EVRM

4.31 Eisers beroepen zich voorts op artikel 8 EVRM. Eisers stellen zich op het standpunt dat de Wet in strijd is met het recht op eerbiediging van privéleven en correspondentie zoals neergelegd in artikel 8 EVRM. Uit het Arrest, dat de artikelen 7 en 8 Handvest in nauwe samenhang leest met artikel 8 EVRM en met de jurisprudentie van het EHRM, wordt duidelijk dat de Dataretentierichtlijn op een aantal punten in strijd is met artikel 8 EVRM. Dat geldt tevens voor diverse aspecten van de Nederlandse wetgeving die op de Dataretentierichtlijn is gebaseerd.

4.32 De *opslag* van de betreffende verkeers- en locatiegegevens en de *toegang* die de nationale autoriteiten tot die gegevens hebben 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.[22] De retentie van de grote hoeveelheid data over onschuldige personen die de Wet bestrijkt, vormt een zware inbreuk op artikel 8 EVRM. Zoals het Hof aangeeft (r.o. 26-27), kunnen uit de betreffende gegevens *'zeer precieze conclusies worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren.*'

Wettelijke grondslag

4.33 Om te beoordelen of deze inbreuken in overeenstemming met de wet zijn ('*in accordance with the law*' zoals vereist door artikel 8 lid 2 EVRM), is niet alleen het bestaan van toepasselijke wetgeving maar ook de kwaliteit daarvan relevant: de wet moet voldoende waarborgen tegen misbruik en willekeur bevatten en moet voldoende duidelijk en precies zijn om individuen een adequate indicatie te geven van de omstandigheden en voorwaarden waaronder de autoriteiten de maatregelen mogen inzetten.[23] Het resultaat van die beoordeling hangt onder meer af van *'the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind*

[22] Zie EHRM *Leander t. Zweden*, 26 maart 1987, appl.nr. 9248/81, par. 48; EHRM (GK) *S en Marper t. VK*, 4 december 2008, appl.nrs. 30562/04 en 30566/04, par. 73; EHRM *Rotaru t. Roemenië*, 4 mei 2000, appl.nr. 28341/95, par. 43; Advies Raad van State d.d. 17 juli 2014, W03.14.0161/II/Vo, onder 4a.
[23] EHRM *Khan t. VK*, 12 mei 2000, appl.nr. 35394/97, par. 26; EHRM *Uzun t. Duitsland*, 2 september 2010, appl.nr.35623/05, par. 63; EHRM *Weber en Saravia* (n-o), 29 juni 2006, 54934/00, par. 93; EHRM *Liberty and others t. VK*, 1 juli 2008, appl.nr. 58243/00, par. 62-63.

of remedy provided by the national law.'[24] Het EHRM vereist daarbij gedetailleerde regels: *'the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity'.*[25]

4.34 Het Europese Hof van Justitie legt de jurisprudentie van het EHRM aldus uit dat er minimumregels moeten bestaan om te zorgen *'dat 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'*, met name wanneer de gegevens automatisch worden verwerkt en het risico dat ze op onrechtmatige wijze worden geraadpleegd aanzienlijk is.[26]

4.35 Advocaat-Generaal Cruz-Villalón concludeerde in zijn conclusie voorafgaande aan het Arrest dat de kwaliteit van de Uniewetgeving onvoldoende is in de zin van artikel 52 lid 1 Handvest. Hij stelde hierbij onder meer dat de Dataretentierichtlijn de toegang tot verzamelde en bewaarde gegevens slechts had mogen toestaan aan de gerechtelijke of tenminste onafhankelijke autoriteiten, of dat de richtlijn had moeten regelen dat elk individueel verzoek tot toegang tot die gegevens aan het toezicht van die autoriteiten wordt onderworpen.[27] Ook onder het EVRM vormt het bestaan van zo'n rechterlijke toets een belangrijke waarborg bij zware inbreuken op het recht op privéleven.[28] Het gebrek aan een dergelijke toets in de Nederlandse wetgeving omtrent toegang tot de gegevens heeft tot gevolg die wetgeving niet aan het vereiste '*in accordance with the law*' voldoet.

Noodzakelijk in een democratische samenleving

4.36 Bovendien is de Wet niet 'noodzakelijk in een democratische samenleving'. Er moet sprake zijn van een '*pressing social need*' en de inbreuk op de privacy moet proportioneel zijn ten

[24] EHRM *Uzun t. Duitsland*, 2 september 2010, appl.nr.35623/05, par. 63; EHRM *Weber en Saravia (n-o)*, 29 juni 2006, 54934/00, par. 106.
[25] EHRM *Weber en Saravia (n-o)*, 29 juni 2006, 54934/00, par. 94; EHRM *Liberty and others t. VK*, 1 juli 2008, appl.nr. 58243/00, par. 62-63.
[26] Arrest, r.o. 54; EHRM (GK) *S en Marper t. VK*, 4 december 2008, appl.nrs. 30562/04 en 30566/04, par. 103; EHRM *M.K. t. Frankrijk*, 18 april 2013, appl.nr. 19522/09, par. 35.
[27] Conclusie A-G Cruz-Villalón, *Digital Rights Ireland en Seitlinger*, 12 december 2013, C-293/12 en C594/12, par. 127.
[28] EHRM *Huvig t. Frankrijk*, 24 april 1990, 11105/84, par. 33; EHRM *Uzun t. Duitsland*, 2 september 2010, appl.nr.35623/05, par. 71-72.

opzichte van het te bereiken doel, in casu het opsporen van ernstige criminaliteit. De Staat heeft op dit punt slechts een beperkte beoordelingsmarge omdat de bescherming van persoonsgegevens van groot belang is voor het recht op bescherming van het privéleven, terwijl de maatregelen een ernstige inbreuk maken op dit recht,[29] zowel wat betreft de opslag van als de toegang tot de gegevens.

4.37 Toegang tot de gegevens en het gebruik van de gegevens door de nationale autoriteiten moet strikt noodzakelijk zijn ten opzichte van het te bereiken doel.[30] Daarbij moeten adequate garanties bestaan tegen onrechtmatig gebruik. Een voorafgaande rechterlijke toets vormt een belangrijke waarborg bij zware inbreuken op het recht op privéleven.[31] De Wet bevat niet zo'n rechterlijke toets, zodat deze regeling in strijd is met artikel 8 EVRM.

De vrijheid van meningsuiting – Artikel 10 EVRM en 11 Handvest

4.38 Tot slot maakt de Wet inbreuk op de vrijheid van meningsuiting. Het feit dat gegevens van journalisten opgevraagd kunnen worden, brengt het risico met zich mee dat zij bepaalde onderwerpen gaan mijden of dat bronnen zich niet meer tot journalisten durven wenden. Er is dus gevaar voor een '*chilling effect*', zoals het Hof al vaststelde (r.o. 28).

Tussenconclusie

4.39 Het onverkort handhaven van de Wet is onrechtmatig (6:162 BW) jegens alle Eisers en jegens eenieder wier belangen zij vertegenwoordigen, waaronder alle in Nederland telefonerende en internettende burgers, geheimhouders zoals advocaten en journalisten, en aanbieders.

5. MOGELIJKE VERWEREN

5.1 Eisers zijn niet bekend met een verweer van de Staat, anders dan het standpunt van de Minister van Veiligheid en Justitie zoals uiteengezet in zijn brief van 17 november 2014, dat hierboven is besproken.

---

[29] Arrest, r.o. 48; EHRM (GK) *S en Marper t. VK*, 4 december 2008, appl.nrs. 30562/04 en 30566/04, par. 102; EHRM *M.K. t. Frankrijk*, 18 april 2013, appl.nr. 19522/09, par. 31.
[30] EHRM *M.K. t. Frankrijk*, 18 april 2013, appl.nr. 19522/09.
[31] EHRM *Huvig t. Frankrijk*, 24 april 1990, 11105/84, par. 33; EHRM *Uzun t. Duitsland*, 2 september 2010, appl.nr.35623/05, par. 71-72; EHRM *Rotaru t. Roemenië*, 4 mei 2000, appl.nr. 28341/95, par. 59.

5.2 Voor zover de Staat zou betogen dat de Voorzieningenrechter niet bevoegd is om een formele wet en Amvb buiten werking te stellen, wijzen Eisers erop dat uit de jurisprudentie[32] volgt dat de rechter hiertoe bevoegd is als de regelgeving onmiskenbaar onverbindend is. Het komt regelmatig voor dat een wet wegens strijd met Unierecht buiten werking wordt gesteld. In 2012 gebood uw Rechtbank in kort geding de Staat een wet buiten werking te stellen.[33] Op 28 januari 2014 oordeelde Hof Den Haag dat de Staat een richtlijn niet goed had geïmplementeerd.[34] En op 29 januari 2014 werd een artikel uit de Telecommunicatiewet onverbindend verklaard door Rechtbank Den Haag.[35] En in mei 2014 werd de Wet Verbod Pelshouderij buiten werking gesteld wegens strijd met hogere regelgeving.[36]

5.3 Voor zover de Staat zou betogen dat Eisers niet ontvankelijk zijn omdat er een andere rechtsgang open zou staan wijzen Eisers op het volgende. Burgers hebben geen mogelijkheid zich te verzetten tegen de bewaarplicht, en ook voor de geheimhouders is er geen andere rechtsgang. Op basis van vaste jurisprudentie van de Hoge Raad kan van de aanbieders niet gevergd worden dat zij de Wet overtreden om uit te lokken dat zij een strafrechtelijke sanctie krijgen of dat zij bestuursdwang opgelegd te krijgen, waartegen zij vervolgens tegen zouden kunnen ageren.[37]

6. TOELICHTING VORDERINGEN

6.1 De Staat kan volgens vaste jurisprudentie worden bevolen zich te onthouden van gedragingen die gebaseerd zijn op een onmiskenbaar onverbindende wet, oftewel: de Wet kan buiten werking worden gesteld.[38] Deze buitenwerkingstelling – wegens de onverbindendheid van de Wet gelet op de strijdigheid met hogere regelgeving – is van kracht tot in een eventuele bodemprocedure uitspraak is gedaan, dan wel totdat is voldaan aan een in een toepassingsverbod op te nemen voorwaarde, zoals aanpassing of intrekking van de Wet.

---

[32] HR 1 juli 1983, NJ 1984, 360 (*LSV*), HR 16 mei 1986, NJ 1987, 251 (*Landbouwvliegers*) en HR 16 mei 1986, NJ 1987, 252 (*Van Gelder*).
[33] Rb. Den Haag 3 januari 2012, ECLI:NL:RBSGR:2012:BU9921 (*FNV Kiem- De Staat*), inhoudelijk bekrachtigd door Hof Den Haag 5 juni 2012.
[34] Hof Den Haag 28 januari 2014, ECLI:NL:GHDHA:2014:72, aansprakelijkheid Staat voor niet juist invoeren Richtlijn 2003/88/EG m.b.t. recht op vakantie tijdens ziekte.
[35] Rb. Den Haag 29 januari 2014, ECLI:NL:RBDHA:2014:1004.
[36] Rb. 's-Gravenhage 21 mei 2014, JB 2014/164, ECLI:NL:RBDHA:2014:6161.
[37] HR 11 oktober 1996 (*Leenders/Ubbergen*), LJN: ZC2169, NJ 1997/165, m.nt. Van der Scheltema, AB 1997/1, m.nt. Van der Drupsteen, JB 1996/241, m.nt. EvdL.
[38] HR 1 juli 1983, NJ 1984, 360 (*LSV*) en HR 16 mei 1986, NJ 1987, 251 (*Landbouwvliegers*).

6.2 Buitenwerkingstelling is ‘een in algemene termen vervat verbod’ aan de Staat om zich ‘te onthouden van gedragingen’ die op de werking van de regeling zijn gegrond, ‘met name het uitvoeren of doen uitvoeren daarvan’.[39] Buitenwerkingstelling houdt een absoluut toepassingsverbod in ten aanzien van alle ambten die behoren tot de veroordeelde overheidsrechtspersoon. In het onderhavige geval hebben het AT, de ACM (voorheen OPTA) en het CBP zich hier dus aan te houden. Ook het OM zal niet mogen handhaven en niet op basis van de Wet gegevens mogen opvragen bij de aanbieders.

6.3 De privacy van burgers moet voldoende gewaarborgd zijn. En de geheimhouders dienen de garantie te krijgen dat de Staat hun rechten respecteert. De primaire en subsidiaire vorderingen zijn er op gericht dat geen ongerichte bewaarplicht meer geldt voor de aanbieders, en dat de overheid niet langer op grond van de Wet toegang krijgt tot opgeslagen gegevens.

6.4 Meer subsidiair vorderen Eisers dat de zeer ruime en bijzonder zware inmenging in hun fundamentele rechten gestaakt wordt. Eisers vorderen dat de Staat de Wet niet langer handhaaft zolang de Wet die elementen (of een aantal daarvan) bevat die Hof hebben doen besluiten de Dataretentierichtlijn met terugwerkende kracht ongeldig te verklaren.

6.5 Meer subsidiair vorderen Eisers dat de Wet niet wordt gehandhaafd zolang die – naar Uw voorlopig oordeel – in strijd is met de toepasselijke grondrechten.

6.6 Nog meer subsidiair vorderen Eisers dat de Wet niet gehandhaafd mag worden tot de maatregelen die de regering bij brief van 17 november 2014 heeft voorgesteld zijn ingevoerd.

6.7 En uiterst subsidiair vragen Eisers UEA die maatregelen te treffen die UEA in goede justitie geraden acht.

6.8 Eisers vertrouwen erop dat de Staat het vonnis van uw Rechtbank zal opvolgen. Daarom wordt geen dwangsom gevorderd.

[39] HR 1 juli 1983, NJ 1984, 360 (*LSV*).

7. SPOEDEISENDHEID EN BEVOEGDHEID

7.1 Eisers en de partijen voor wie zij opkomen hebben er spoedeisend belang bij dat de Wet onverbindend wordt verklaard, althans niet langer wordt gehandhaafd. De regering heeft een wetsvoorstel ter consultatie voorgelegd. Er is geen concreet uitzicht op wijziging van de Wet. Dat kan nog maanden of zelfs jaren duren. Ondertussen duurt de grove schending van de rechten van Eisers en de door hun vertegenwoordigde achterban voort. Eisers hebben een spoedeisend belang bij het beëindigen van de zeer ruime en bijzonder zware inmenging in deze fundamentele rechten.

7.2 Uw Rechtbank is bevoegd kennis te nemen van dit geschil op grond van artikel 99 Rv.

MITSDIEN:

het de Voorzieningenrechter van de Rechtbank te 's-Gravenhage moge behagen bij vonnis, zoveel als mogelijk uitvoerbaar bij voorraad, met veroordeling van de Staat in de kosten van deze procedure, inclusief de nakosten:

primair

I. de Wet Bewaarplicht Telecommunicatie[40] buiten werking te stellen, althans de Staat daartoe te veroordelen;

subsidiair

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

meer subsidiair

III. de Staat te verbieden de Wet Bewaarplicht Telecommunicatie te handhaven en op basis daarvan gegevens 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 van Justitie in het arrest van 8 april 2014 heeft neergelegd, in het bijzonder door de Staat te verbieden die wet te handhaven, en die aanbieders te dwingen op basis daarvan gegevens op te slaan en deze gegevens op te vragen zolang die wet:

(i) algemeen van toepassing is op alle personen die gebruikmaken van elektronische communicatiediensten, zonder dat de personen van wie de gegevens worden bewaard zich, zelfs niet indirect, in een situatie bevinden die aanleiding kan geven tot strafrechtelijke vervolging; en

(ii) van toepassing is op personen voor wie er geen enkele aanwijzing bestaat dat hun gedrag – zelfs maar indirect of van ver – een verband vertoont met zware criminaliteit; en

(iii) geen uitzonderingen bevat, zodat zij zelfs van toepassing is op personen die vanuit hun functie een speciale positie als geheimhouder hebben (inclusief maar niet beperkt tot advocaten, artsen, notarissen en journalisten die hun bronnen moeten beschermen); en

[40] Stb. 333, 2009.

(iv) geen enkel verband legt tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid; en

(v) de bewaring niet beperkt 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; en

(vi) geen objectieve criteria bevat ter begrenzing van de toegang van de bevoegde 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; en

(vii) geen objectieve criteria bevat op basis waarvan het aantal personen dat de bewaarde gegevens mag raadplegen en vervolgens gebruiken, wordt beperkt tot wat strikt noodzakelijk is voor de verwezenlijking van het nagestreefde doel; en

(viii) de toegang van de bevoegde nationale autoriteiten tot de bewaarde gegevens niet onderwerpt 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; en

(ix) bepaalt dat gegevens deze gedurende een vaste termijn moeten worden bewaard, zonder dat enig onderscheid wordt gemaakt tussen bepaalde categorieën van gegevens naargelang van het nut ervan voor het nagestreefde doel of naargelang van de betrokken personen; en

(x) een bewaringstermijn bevat die niet op basis van objectieve criteria is vastgesteld om te waarborgen dat hij beperkt is tot wat strikt noodzakelijk is;

althans een door UEA in goede justitie vast te stellen aantal van bovengenoemde vereisten;

nog meer subsidiair

IV. de Staat te verbieden de Wet Bewaarplicht Telecommunicatie of onderdelen daarvan te handhaven en op basis daarvan gegevens op te vragen bij aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten voor zover één en ander in strijd is met:

(i) de artikelen 7, 8 en 11 van het Handvest van de Grondrechten; en/of

(ii) de artikelen 8 en 10 EVRM; en/of

(iii) artikel 10 Grondwet; en/of

(iv) artikel 15 van de e-privacyrichtlijn; en/of

(v) artikel 6, leden 1 en 2, van het Verdrag betreffende de Europese Unie;

en daarbij aan te geven op welke onderdelen deze wet naar het voorlopige oordeel van UEA daarmee in strijd is;

nog meer subsidiair

V. de Staat te verbieden de Wet Bewaarplicht Telecommunicatie te handhaven en aanbieders van openbare telecommunicatienetwerken of openbare telecommunicatiediensten te dwingen gegevens op te slaan en deze gegevens op te vragen zolang deze wet niet is gewijzigd zoals door de regering bij brief van 17 november 2014 voorgesteld, of een intrekkingswet van de Wet is aangenomen;

uiterst subsidiair

VI. zodanige voorzieningen te treffen als UEA in goede justitie geraden acht.

Deze zaak wordt behandeld door Boekx Advocaten
mr. F.F. Blokhuis en mr. O.M.B.J. Volgenant
Leidsegracht 9 (1017 NA) Amsterdam
T: 020 – 528 9532 | F: 020 – 528 9537
E: blokhuis@boekx.com | volgenant@boekx.com
www.boekx.com