

Rechtbank Den Haag, Team Handel
Kort geding 7 juni 2018, 10.00 uur
Voorzienenrechter mr. G.P. van Ham
Zaaknummer: C/09/553023 KG ZA 18-476

PLEITAANTEKENINGEN

inzake:

1. Stichting Bits of Freedom
2. Stichting Free Press Unlimited
3. Stichting Greenpeace Council
4. Vereniging Nederlands Juristen Comité voor de Mensenrechten (NJCM)
5. Vereniging Nederlandse Vereniging van Strafrechtadvocaten (NVSA)
6. Stichting Platform Bescherming Burgerrechten
7. Stichting Privacy First
8. Stichting Waag Society
9. BIT B.V.
10. Mijndomein Hosting B.V.
11. SpeakUp B.V.
12. VOYS B.V.

EISERS

advocaten: mr. O.M.B.J. Volgenant, mr. F.F. Blokhuis
en mr. R.H.W. Lamme

tegen:

De Staat der Nederlanden

GEDAAGDE

advocaat: mr. C.M. Bitter en mr. R.W. Veldhuis

I. Inleiding: de Wiv2017 is een lekke boot die gerepareerd moet worden

1. De Wiv2017 moet een zeewaardige, stevige boot zijn, maar het is nu een boot met gaten in de romp. Een boot met constructiefouten. In plaats van gaten in de boot te dichten en pas daarna de boot te water te laten, heeft het kabinet ervoor gekozen vanaf 1 mei te gaan varen. Er zijn wat papieren proppen in de gaten gestopt. Dat zou dan voorlopig genoeg moeten zijn.
2. Er is al wel aangekondigd dat er 'na de zomer' een reparatie zal plaatsvinden middels een wetswijziging. Wat die reparatie in gaat houden en wanneer dit precies gaat gebeuren is onduidelijk. Tot die tijd moeten we het doen met toezeggingen in brieven, met verwijzingen naar moties en met beleidsregels, die deels slechts intern en niet publiekelijk toegankelijk zijn. Dat is een rommelige oplossing. Die oplossing voldoet niet. De keuze van het kabinet voor deze volgorde is onlogisch, onwenselijk en juridisch onjuist.
3. Waar het gaat om zo'n belangrijk onderwerp als de bevoegdheden van de geheime diensten is dat onaanvaardbaar. Zo'n wet moet 'particularly precise' zijn en elke bevoegdheid van de Diensten moet met voldoende waarborgen zijn omgeven. Volgens het Europees recht moet de boot solide, zeewaardig en onzinkbaar zijn. Dat is op dit moment niet het geval.
4. De oplossing is simpel. De lekkende boot van de Wiv2017 vaart al, en in deze procedure vorderen Eisers dat de boot door mag varen als de gaten dan wel voorlopig stevig worden dichtgestopt door een vonnis van de rechter. Dat is een tijdelijk lapmiddel, totdat de wetgever een reparatie heeft uitgevoerd en de boot zeewaardig heeft gemaakt. De boot maakt dan met hulp van het vonnis voorlopig geen water meer. Dat geeft de wetgever de gelegenheid om de benodigde reparatie zorgvuldig uit te voeren.

II. Plan van aanpak

5. Welke onderwerpen komen aan de orde in ons pleidooi? We beginnen met het juridisch kader. [Hoofdstuk III]. In de dagvaarding hebben we uitgelegd op welke onderdelen de Wiv2017 in strijd is met de grondrechten. In dit kort geding zijn vier bevoegdheden aan de orde:
 - A. grootschalig verzamelen van gegevens via ongerichte bulkinterceptie;
 - B. grootschalig verzamelen van gegevens via informanten;
 - C. grootschalig verzamelen van gegevens via hacken van derden; en
 - D. het doorgeven van die gegevens aan buitenlandse diensten.

6. We zullen vandaag nader toelichten wat de Diensten onder de nieuwe Wiv2017 mogen, en wat de gebreken zijn van deze bepalingen [Hoofdstuk IV]. Daarna bespreken we of er grootschalig gegevens verzameld worden en waarom daar zoveel weerstand tegen is [Hoofdstuk V]. Dan bespreken we de Conclusie van Antwoord van de Staat. Daar zit een aantal erkenningen in die voor het kort geding van vandaag zeer relevant zijn [Hoofdstuk VI]. Vervolgens zullen we toelichten wat Eisers aan Uw Rechtbank vragen, en waarom Eisers niet kunnen wachten op de benodigde wetswijziging [Hoofdstuk VII]. We sluiten af met een duidelijke conclusie [Hoofdstuk VIII].

III. Juridisch kader: quality of the law: bepalingen moeten *'particularly precise'* zijn

7. We hebben het juridisch kader uitgebreid geschetst in de dagvaarding. We zullen dat nu niet herhalen. Zoals we in de dagvaarding hebben uitgelegd, vereist het Europees recht dat in de Wiv2017 zowel de bevoegdheid die leidt tot een inbreuk op grondrechten als de daarbij geldende waarborgen *'particularly precise'* omschreven zijn.

8. De Wiv2017 is een complex bouwwerk geworden waarbij de waarborgen deels gezocht moeten worden in de parlementaire geschiedenis, in moties en in beleidsregels.

9. Wat niet in de wet zelf staat heeft uiteraard een andere waarde dan de tekst van de wet. Minister Ollongren heeft daar zelf onlangs een staaltje van laten zien, in de recente discussie met de Eerste Kamer over de inwerkingtredingsprocedure van de Wiv2017 na het raadgevend referendum. Op een vraag vanuit de Eerste Kamer antwoordt minister Ollongren dat wat in de Memorie van Toelichting op de Wet op het Raadgevend Referendum staat niet van toepassing is.¹ De wettekst is volgens de minister leidend. Deze zelfde minister, of één van haar opvolgers, kan met hetzelfde gemak een beleidsregel terzijde schuiven. Hieruit blijkt hoe belangrijk het is dat de waarborgen in de wet staan.

10. Dat onderkent ook Harm Brouwer, de voorzitter van de CTIVD (Productie 16): *Inmiddels zijn die waarborgen wel toegezegd, aldus Brouwer. "Maar het was beter geweest als dat in de wetstekst had gestaan."*²

¹ Brief van minister Ollongren aan de Eerste Kamer d.d. 27 april 2018: Productie 21, pagina 2: *In antwoord op deze vraag breng ik graag naar voren dat het woord 'tijdelijk' op deze plaats in de toelichting van de initiatiefwet niet aansluit op de wettekst van artikel 12 waarop de toelichting betrekking heeft.*

² Zie Productie 16. De CTIVD heeft dit standpunt ook ingenomen in de Eindbalans Wiv2017 (productie 2 van de Staat): '(4) *Is de Wiv 2017 in balans? Ja. De Wiv 2017 is niet volmaakt, maar wel in balans. In balans omdat het een werkbare basis biedt voor zowel de bescherming van de nationale veiligheid als de rechtsbescherming van de burger daarbij en voor effectief toezicht. Niet volmaakt omdat die basis weliswaar is verankerd in de wet, maar in niet onbelangrijke mate invulling krijgt in moties, toelichtingen en in de door de regering gedane toezeggingen omtrent de uitvoering van de nieuwe wet. Het zou de*

11. De Autoriteit Persoonsgegevens stelt in dit verband expliciet: *‘Juist omdat de diensten in de praktijk heimelijk opereren, moet in de wet duidelijk worden aangegeven wanneer bepaalde bevoegdheden mogen worden ingezet tegen burgers.’* (Productie 17)

IV. Grootschalige, ongerichte verzameling en (ongeëvalueerde) doorgifte voldoen niet aan de Weber/Zakharov-criteria

12. Bij de beoordeling van de Wiv2017 zijn volgens het EHRM³ alle omstandigheden van het geval relevant, waarbij in ieder geval nodig is dat duidelijk is afgebakend, zoals we in de dagvaarding hebben uitgelegd:

- a) voor welke doelen de bevoegdheden mogen worden ingezet;
- b) jegens welke categorieën van personen deze bevoegdheden mogen worden ingezet;
- c) gedurende welke periode deze bevoegdheden mogen worden ingezet;
- d) welke procedure moet worden gevolgd voor het onderzoeken, gebruiken en bewaren van onderschepte gegevens;
- e) welke waarborgen er gelden bij het aan derden verstrekken van de data; en
- f) welke waarborgen er gelden rondom het wissen of vernietigen van data.

13. We duiden deze eisen in de dagvaarding aan als de *‘Weber/Zakharov-criteria’*. Het *Zakharov*-arrest van de Grote Kamer van het EHRM van december 2015 is leidend. In aanvulling op de dagvaarding leggen we de vier bevoegdheden van de Wiv2017 waar dit kort geding over gaat langs de lat van deze criteria.

a. Voor welke doelen mogen de bevoegdheden worden ingezet? Dat is zeer ruim en vaag

14. De taakomschrijving van de Diensten is zeer ruim en vaag. De taken gaan veel verder dan alleen onderzoek naar bijvoorbeeld dreigend terrorisme. De taken van de Diensten staan in het belang van *‘de nationale veiligheid’*. Dat is een breed begrip, dat echter niet in de Wiv2017 is gedefinieerd, en ook nergens anders. Volgens de Memorie van Toelichting valt daar in ieder geval ook de *‘integriteit van de openbare sector’* onder, maar een nadere afbakening hiervan ontbreekt. De AIVD kan onderzoek doen bij een vermoeden van een *gevaar voor gewichtige belangen van de staat*, maar ook ter *beveiliging van vitale*

rechtszekerheid op de langere termijn gediend hebben als deze in de wet zelf waren opgenomen.’

³ EHRM 29 juni 2006, 54934/00, *Weber en Saravia t. Duitsland*, par. 95, en EHRM (Grote Kamer) 4 december 2015 nr. 47143/06 (*Zakharov t. Rusland*): 232. *‘The assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law. The Court has to determine whether the procedures for supervising the ordering and implementation of the restrictive measures are such as to keep the “interference” to what is “necessary in a democratic society” (see Klass and Others, cited above, §§ 49, 50 and 59; Weber and Saravia, cited above, § 106; Kvasnica v. Slovakia, no. 72094/01, § 80, 9 June 2009; and Kennedy, cited above, §§ 153 and 154).’*

*onderdelen van het bedrijfsleven.*⁴ Wat hier in de praktijk onder wordt verstaan is niet bekend. De Staat noemt als reden dat anders *'de ontvreemding van bedrijfsvertrouwelijke informatie en persoonsgegevens onopgemerkt blijft.'*⁵ Dat staat mijlenver af van een bedreiging van de nationale veiligheid.

15. De onderzoeksoopdrachten die de Diensten ter uitvoering van hun wettelijke taken moeten uitvoeren zijn gekoppeld aan een zogeheten Geïntegreerde Aanwijzing Inlichtingen- en Veiligheidsdiensten.⁶ De inhoud hiervan is staatsgeheim. De daadwerkelijke onderzoeksoopdrachten zijn ook geheim. Ze sluiten aan bij de prioriteiten van de AIVD en de MIVD, die in staatsgeheime jaarplannen zijn uitgewerkt.
16. Voor 2018 zijn voor de AIVD de volgende prioriteiten en accenten genoemd:⁷ geopolitieke ontwikkelingen, heimelijke politieke beïnvloeding, digitale spionage, cyberdreiging, terroristische dreiging, Jihadistisch terrorisme, radicalisering, links- en rechtsextremisme. Dat is dus ook ontzettend ruim.
17. De regering wees er in de Memorie van Toelichting op dat in de praktijk van samenwerking van inlichtingen- en veiligheidsdiensten bij de uitwisseling van informatie het beginsel van *quid pro quo* (voor wat hoort wat) een belangrijk element is.⁸ Hier wees ook Arnbak op in het Financieele Dagblad:⁹

'Aftapvoorstanders spelen steeds maar weer de terrorismekaart, maar machtspolitiek vormt een andere cruciale drijfveer achter de wet. Beschik je als land over waardevolle informatie, dan kun je deze data internationaal uitruilen en zo macht verwerven.'
18. De Wiv2017 voldoet op dit punt niet aan de *Weber/Zakharov*-criteria: de doelstellingen zijn veel té ruim en niet toetsbaar omdat dit goeddeels staatsgeheim is.

⁴ Artikel 8 lid 2 Wiv 2017.

⁵ Zie 4.5. CvA.

⁶ Artikel 6 lid Wiv2017.

⁷ TK 30 977, nr. 150, Brief over jaarplan AIVD, 19 december 2017,
<https://www.aivd.nl/publicaties/kamerstukken/2017/12/21/kamerbrief-over-jaarplan-aivd-2018>

⁸ TK 34 588, nr. 3, Memorie van Toelichting, p. 158.

⁹ <https://axelarnbak.nl/2018/01/26/44e-fd-column-machtspositie-nederland-belangrijke-drijfveer-voor-controversiele-internettap/>

b. Jegens wie mogen de bevoegdheden worden ingezet?

19. In het *Zakharov-arrest*¹⁰ is bepaald dat grootschalige, niet-geïndividualiseerde surveillance niet te rechtvaardigen is onder het EVRM. Er moet een redelijk vermoeden zijn dat een individuele persoon een gevaar is voor de nationale veiligheid. Een ‘target’ in het jargon van de Diensten.
20. Maar vandaag hebben we het juist over bevoegdheden om grootschalig ongericht gegevens te verzamelen van burgers waartegen géén redelijk vermoeden bestaat. Die bevoegdheden zijn naar hun aard *niet* beperkt tot bepaalde categorieën van personen.
21. Het ongerichte karakter van de interceptie-bevoegdheid heeft juist als doel om grootschalig gegevens te verzamelen – waaronder per definitie ook gegevens van niet-verdachte burgers – om deze gegevens pas daarna te onderzoeken.

De beleidsregels

22. Artikel 5 van de Beleidsregels vult de inzet van de bijzondere bevoegdheden in.¹¹ De beleidsregels zeggen daarbij slechts dat toepassing van een bijzondere bevoegdheid, zoals ‘onderzoekopdrachtgerichte interceptie’, zo gericht mogelijk dient plaats te vinden. Dat is een woordenspel dat geen enkele extra waarborg biedt. Het is een cosmetisch lapmiddel.
23. De Staat erkent bovendien in 6.13 CvA dat de Diensten zich richten op een geografisch gebied of een bepaalde datastroom. Daarmee wordt erkend dat bulkinterceptie ex artikel 48 Wiv2017 zich niet richt op bepaalde personen waartegen een ‘*reasonable suspicion*’ is. In die betekenis van het woord is het dus ongericht. De instructie van de beleidsregels dat het ‘zo gericht mogelijk’ moet zijn betekent niet dat het alsnog op bepaalde personen wordt gericht.
24. De beleidsregels laten expliciet nog steeds toe dat er grootschalig gegevens worden verzameld middels bulkinterceptie van communicatie via de kabel en middels het hacken van derden. De bevoegdheid tot grootschalige verzameling van gegevens van iedereen is in

¹⁰ EHRM (Grote Kamer) 4 december 2015 nr. 47143/06 (*Zakharov t. Rusland*). Het EHRM stelt dat de instantie die toestemming geeft voor geheime surveillance (i.e. voorafgaand toezicht) “*must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security.*”

¹¹ Productie 7: Artikel 5: *De toepassing van bijzondere bevoegdheden door de dienst dient zo gericht mogelijk plaats te vinden. Bij het verzoek om toestemming als bedoeld in artikel 29 van de wet tot de inzet van een bijzondere bevoegdheid, wordt nadrukkelijk aangegeven op welke wijze aan de eis van gerichte inzet van de desbetreffende bijzondere bevoegdheid invulling wordt gegeven.*

strijd met het *Weber/Zakharov*-criterium van een redelijk vermoeden tegen een persoon.

Gebruik informanten – mag dat nu wel of niet tot grootschalige verzameling van persoonsgegevens leiden?

25. Ook bij het gebruik van informanten om grootschalig data te verzamelen zijn de categorieën van personen jegens wie deze bevoegdheid mag worden ingezet in de Wiv2017 niet beperkt. Burgers die geen risico zijn voor de nationale veiligheid, bronnen van journalisten en NGO's, vertrouwelijke gegevens van cliënten van advocaten: van *iedereen* zullen gegevens kunnen worden verzameld via een informant. Er is géén toetsing door de TIB.¹² Er is zelfs géén toestemming van de minister nodig.¹³ De eis dat eerst toestemming nodig is van de Rechtbank Den Haag voor de inzet van een bevoegdheid jegens een advocaat of een journalist¹⁴ geldt niet voor de inzet van informanten (omdat dit geen bijzondere bevoegdheid is). De beleidsregels regelen niets over deze *loophole* in de wet.
26. De Staat heeft in de CvA betoogd dat de bevoegdheid om te werken met informanten niet leidt tot kennisneming van grote hoeveelheden data. Dat is verrassend nieuws. Het is goed nieuws voor Eisers, die zich zorgen maakten om het gebruik van deze bevoegdheid. De Staat stelt in haar Conclusie van Antwoord letterlijk – en ik citeer het zorgvuldig zodat iedereen in de zaal ook precies weet welke bewoordingen de Staat gebruikt:

6.20 CvA: Onjuist is dus dat via informanten grote hoeveelheden data zouden kunnen worden vergaard, zonder dat deze gegevens zijn geëvalueerd. Daarvan is geen sprake.

6.21 CvA: Evenmin gaat het, als gezegd, om de mogelijkheid tot kennisneming van grote hoeveelheden ongeëvalueerde data, zoals eisers stellen. Willekeurige opvraging is niet mogelijk.

27. Eisers zijn blij met deze onvoorwaardelijke toezegging. Eisers zijn er ook wel verbaasd over. In de wettekst is deze beperking namelijk niet opgenomen.

¹² Artikel 39 Wiv2017 staat in paragraaf 3.2.4. van de Wiv2017. Het raadplegen van informanten wordt niet als 'bijzondere bevoegdheid' aangemerkt, waarover paragraaf 3.2.5. van de Wiv2017 gaat. Niet één van de waarborgen of beperkingen die gelden bij het middels bulkinterceptie binnenhalen van gegevens geldt voor het binnenhalen van gegevens via informanten. Er is daarom géén procedure voor het onderzoeken, gebruiken en bewaren van via informanten onderschepte gegevens opgenomen in de Wiv2017.

¹³ De Beleidsregels hebben géén betrekking op de gegevens die via informanten zijn binnengehaald. De artikelen 27 Wiv2017 (zo spoedig mogelijk op relevantie onderzoeken en vertrouwelijke communicatie tussen een advocaat en zijn cliënt weggooien), artikel 28 en 29 Wiv2017 zijn niet van toepassing op het werken met informanten. Artikel 20 Wiv2017 bevat geen concrete termijn.

¹⁴ artikel 30 Wiv2017.

28. Eisers zijn er ook verbaasd over omdat in het recente verleden juist wél via informanten grootschalig persoonsgegevens zijn verzameld. Het ging toen om een dataset met gegevens van meer dan honderd miljoen personen, van wie relatief veel Nederlandse ingezetenen. Hier ging CTIVD-rapport nr. 55 van eind december 2017 over, dat de Staat zelf ook noemt (4.17 CvA en voetnoot 14). Onder de Wiv2002 gebruikten de Diensten informanten dus wél om grote datasets te bemachtigen en te bewaren.
29. De CTIVD heeft dit op onderdelen als onrechtmatig beoordeeld, en niet als rechtmatig zoals de Staat abusievelijk schrijft in de Conclusie van Antwoord (4.17 CvA).¹⁵
30. Uit het CTIVD-rapport blijkt dat de Diensten in het verleden de data niet vernietigden, maar juist bewaren voor toekomstige raadpleging. De Diensten hebben daar een systeem voor verzonden dat ze ‘buitenbak-binnenbak’ noemen. Dat systeem is vanuit het oogpunt van grondrechten onvoldoende. Ook de ‘buitenbak’ wordt door de Diensten zelf beheerd. De interne regels die de Diensten opstelden schoten tekort volgens de CTIVD, en deze interne regels zijn bovendien niet openbaar kenbaar.¹⁶
31. In het *Liberty*-arrest¹⁷ oordeelde het EHRM dat niet-openbare interne beleidsregels een inbreuk op de grondrechten opleveren. Een wet waarbij waarborgen in geheime beleidsregels zijn verstopt is onmiskenbaar onverbindend.
32. Kortom, onder de oude Wiv2002 gebruikten de Diensten wel degelijk informanten om grootschalig persoonsgegevens binnen te halen. Ook onder de Wiv2017 is dat op basis van de huidige tekst van de wet nog steeds mogelijk.
33. Nu de Staat stelt dat deze bevoegdheid tot het maken van een inbreuk op grondrechten niet bestaat, zal de Wiv2017 op dit punt moeten worden aangepast. De Wiv2017 moet op dit belangrijke punt ‘*particularly precise*’ zijn.

¹⁵ Toezichtsrapport CTIVD, nr. 55, 28 december 2017, Over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD: ‘De verwerving van de tweede dataset wordt als onrechtmatig beoordeeld. De reden daarvoor is dat de minister(s), bij het vaststellen van de interne beleidsnotities, niet alsnog om toestemming is gevraagd. Dit had wel moeten, omdat de gegevens in de bulkdataset zeer algemeen van aard zijn. De dataset bevat gegevens van meer dan honderd miljoen personen, van wie relatief veel Nederlands ingezetenen. De verwerving van een zodanige hoeveelheid persoonsgegevens brengt een ernstige privacy-inmenging met zich mee.’ (...) ‘Bij het ongericht verwerven gaat het doorgaans om zeer grote hoeveelheden gegevens (bulk). Op voorhand kan dikwijls worden ingeschat dat de bulkgegevens in overgrote meerderheid informatie bevatten die niet relevant is voor de goede taakuitvoering van de diensten, gegeven de aard van het te verwerven volume aan gegevens.’ <https://www.ctivd.nl/documenten/rapporten/2018/02/13/index>

¹⁶ CTIVD, rapport nr. 55: ‘Een kanttekening daarbij is wel dat een deel van de procedurele waarborgen niet publiekelijk toegankelijk is en daarmee niet kenbaar is, omdat zij alleen in intern beleid staan beschreven.’

¹⁷ EHRM *Liberty and others* t. VK, 1 juli 2008, appl.nr. 58243/00.

Hacken: mag dat nou wel of niet tot grootschalige verzameling persoonsgegevens leiden?

34. De Staat stelt (in 4.24 CvA) dat artikel 45 Wiv2017 niet zal worden gebruikt om derden te hacken om daarmee bulkgegevens te verkrijgen. Volgens de Staat worden derden uitsluitend gehackt om als ‘stepping stone’ te dienen om gericht binnen te kunnen dringen in het geautomatiseerde werk van een target. De Staat stelt dat deze bevoegdheid *gericht* is en niet leidt tot de vergaring van grote hoeveelheden data van willekeurige burgers.

35. De Staat stelt (in 6.26 CvA) expliciet – en ik citeer het zodat iedereen in de zaal het ook goed kan horen:

‘Evenmin worden door het hacken van derden, zoals eisers lijken te stellen, zelfstandig gegevens vergaard. (...) Derden zijn slechts een middel om bij het target te komen en fungeren alleen als stepping stone. Onjuist is dus dat bij toepassing van deze bevoegdheid de kans zou worden vergroot dat de diensten toegang krijgen tot bestanden bij die derden met gegevens van burgers die geen risico vormen, geheimhouders en bronnen van journalisten en NGO’s.’

36. Eisers zijn blij met deze interpretatie van de Staat. Eisers maakten zich namelijk flink zorgen over het gebruik van de hack-bevoegdheid om grootschalig persoonsgegevens te verzamelen. De Staat stelt in deze procedure dat die zorg onterecht is.

37. De Staat stelt dat het vastleggen of opnemen van gegevens bij het hacken van een derde in artikel 45 lid 5 Wiv2017 zou zijn uitgesloten.¹⁸ De Staat vergist zich. Dat staat daar helemaal niet.¹⁹ De bevoegdheid tot ‘*het overnemen van de gegevens opgeslagen of verwerkt in het geautomatiseerde werk*’ van artikel 45 lid 2 sub **d** is juist niet uitgesloten in lid 5.

38. De waarborg die de Staat in deze procedure noemt is dus *niet in de wet* te vinden. Eisers lezen in artikel 45 Wiv2017 de mogelijkheid dat er wél grootschalig persoonsgegevens worden verzameld middels het hacken. Dat zou een inbreuk op grondrechten zijn die de wet op dit punt onmiskenbaar onverbindend maakt.

¹⁸ 6.27 CvA: ‘Op grond van artikel 45 lid 5 Wiv2017 is het gebruik van de bevoegdheden ex artikel 40 lid 1 Wiv2017 (observeren en vastleggen van gegevens of volgen en daarbij vastleggen van gegevens van natuurlijke personen of zaken) en artikel 47 lid 1 Wiv2017 (aftappen, ontvangen, opnemen en afluisteren van communicatie) dan ook uitgesloten ten aanzien van het geautomatiseerde werk van een derde.’

¹⁹ Artikel 45 lid 5 luidt: Indien bij de uitoefening van de in het eerste lid, onder b, bedoelde bevoegdheid het binnendringen via het geautomatiseerd werk van een derde plaatsvindt, is met betrekking tot het geautomatiseerde werk van die derde, het derde en vierde lid van overeenkomstige toepassing. De uitoefening van de bevoegdheid, bedoeld in het tweede lid, onder c, is daarbij uitgesloten.

39. Nu de Staat stelt dat deze bevoegdheid tot het maken van een inbreuk op grondrechten niet bestaat, zal de Wiv2017 op dit punt moeten worden aangepast. De Wiv2017 moet op ook dit belangrijke punt '*particularly precise*' zijn.

c. Gedurende welke periode mogen de bevoegdheden worden ingezet?

40. Deze bevoegdheid tot grootschalige bulkinterceptie mag gedurende een zeer lange periode worden ingezet: gedurende maximaal een jaar met een verlenging van nog eens een jaar.²⁰ De periode dat informanten mogen worden ingezet is zelfs helemaal niet wettelijk beperkt. De periode dat er mag worden gehackt is drie maanden, en dit kan steeds worden verlengd. Dit is in strijd met de *Weber/Zakharov*-criteria.

d. Wat is de procedure voor het onderzoeken, gebruiken en bewaren van gegevens?

41. De procedure die moet worden gevolgd voor het onderzoeken, gebruiken en bewaren van onderschepte gegevens staat toe dat de gegevens vele jaren lang worden bewaard.
42. Voor gegevens die middels bulkinterceptie zijn verzameld wordt onderscheid gemaakt tussen gegevens die op relevantie zijn beoordeeld en ongeëvalueerde gegevens, en er is een apart regime voor versleutelde data. Gegevens mogen drie jaar worden bewaard ten behoeve van het doen van onderzoek.²¹ Die termijn van drie jaar gaat lopen op het moment van verwerving óf pas later, namelijk na het ongedaan maken van de versleuteling. Voor versleutelde gegevens kan de bewaartermijn worden verlengd tot maximaal zes jaar.²²
43. Voor gegevens die nog niet op relevantie zijn beoordeeld geeft artikel 4 van de beleidsregels een specifieke regeling: die mogen steeds een jaar worden bewaard met mogelijkheid tot verlenging door de minister tot maximaal drie jaar. Die toestemming van de minister is niet onderworpen aan een toets door de TIB.
44. Gegevens die op relevantie zijn onderzocht en relevant blijken te zijn mogen bewaard worden voor de duur van het onderzoek (zolang ze relevant blijven). Dat kan dus vele jaren zijn. Zijn ze voor geen enkel onderzoek van de AIVD of de MIVD relevant, dan moeten ze verwijderd worden.

²⁰ artikel 48 lid 2 Wiv2017. De Staat suggereert in 4.12 CvA dat de bevoegdheid tot bulkinterceptie voor ten hoogste vier weken kan worden verleend, maar dat is onjuist.

²¹ Lid 5 van artikel 48 Wiv2017.

²² lid 6 van artikel 48 Wiv2017.

45. De minister geeft steeds toestemming voor het doen van onderzoek voor een periode van ten hoogste een jaar, en die periode kan *telkens* worden verlengd voor eenzelfde periode.²³ Het onderzoek zélf kan in theorie dus oneindig doorlopen.
46. Samengevat worden gegevens die zijn verzameld door grootschalige ongerichte interceptie gedurende *vele jaren* bewaard door de Diensten.²⁴ Ik breng in herinnering dat het HvJEU een bewaartermijn voor telecomdata van tussen de 6 maanden en 2 jaar al te lang vond.
47. Er is geen wettelijke bewaartermijn voor gegevens die middels informanten. De procedures voor het onderzoeken, gebruiken en bewaren zijn grotendeels gebaseerd op intern beleid van de Diensten, dat niet openbaar kenbaar is. Dat heeft de CTIVD geconstateerd in het eerder genoemde Toezichtsrapport 55.
48. De procedures voor het onderzoeken, gebruiken en bewaren voldoen niet aan de *Weber/Zakharov*-criteria.

e. Welke waarborgen gelden bij het wissen of vernietigen van data?

49. De Wiv2017 geeft geen adequate waarborgen over het wissen of vernietigen van gegevens die op grond van de bevoegdheid tot bulkinterceptie zijn verzameld. Alleen gegevens waarvan *vastgesteld* is dat ze niet relevant zijn voor *enig onderzoek van de AIVD of de MIVD* moeten worden vernietigd.²⁵ De toets zou natuurlijk andersom moeten zijn: alle gegevens moeten binnen korte tijd worden weggegooid *tenzij* is vastgesteld dat ze relevant zijn. Van het vernietigen van gegevens wordt geen verslag gedaan. Er is geen enkele controle hierop.
50. Omdat het werken met informanten niet als ‘bijzondere bevoegdheid’ wordt aangeduid zijn de Diensten hierbij niet aan specifieke beperkingen gebonden. Uit het kritische CTIVD-rapport over het vergaren van grote datasets met persoonsgegevens via informanten weten we dat de inzet van de Diensten niet is om deze gegevens weg te gooien, maar om ze te bewaren.

²³ artikel 49 lid 4.

²⁴ HvJ EU 8 april 2014, C 293/12 en C 594/12 (*Digital Rights Ireland*): 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.*

²⁵ artikel 48 lid 5 Wiv2017.

51. Langs de lat van de *Weber/Zakharov*-criteria schieten de waarborgen bij het wissen van data in de Wiv2017 tekort.

f. Doorgifte aan buitenlandse inlichtingen- en veiligheidsdiensten²⁶

52. Eisers hebben ernstige bezwaren tegen het doorgeven van grootschalig verzamelde gegevens van burgers die geen risico vormen voor de nationale veiligheid, gegevens van bronnen van journalisten en NGO's en vertrouwelijke gegevens van cliënten van advocaten. De Diensten hebben ook de bevoegdheid gegevens door te geven *zonder* dat er is onderzocht om welke gegevens het precies gaat.

53. Bijvoorbeeld vanuit het oogpunt van journalistieke bronbescherming is dat zeer bezwaarlijk. Communicatiegegevens waaruit een bron van een journalistieke onthulling kenbaar is, kunnen worden doorgegeven aan een buitenlandse dienst zonder dat de Nederlandse Dienst dat überhaupt weet. De bescherming die een verplicht oordeel van de Rechtbank beoogt te bieden wordt zo buitenspel gezet.

54. De Autoriteit Persoonsgegevens heeft expliciet gewezen op de risico's van het verstrekken van gegevens aan buitenlandse diensten, en dan met name ongeëvalueerde gegevens.²⁷ Ook de Raad van State was bijzonder kritisch hierover.²⁸ Ondanks deze scherpe kritiek is de bevoegdheid tot het verstrekken van ongeëvalueerde gegevens in de Wiv2017 opgenomen.

²⁶ 64 lid 1 en 89 lid 1 Wiv2017.

²⁷ Productie 17, paragraaf 3.3.2.2: *'het verstrekken van gegevens aan buitenlandse diensten – en dan met name ongeëvalueerde gegevens – in de praktijk bijzondere risico's met zich meebrengt voor individuele burgers en organisaties. Zo kan het gebeuren dat bijzondere persoonsgegevens, zoals gegevens over de seksuele geaardheid of gegevens over politieke of religieuze overtuigingen, worden verstrekt aan autoriteiten in landen waar mensenrechten niet (ten volle) worden gerespecteerd. Dit kan negatieve gevolgen hebben voor Nederlandse burgers wanneer zij deze landen bezoeken. Omdat met bulkinterceptie ook gegevens van niet-Nederlanders worden onderschept, kan het verstrekken van gegevens bovendien ingrijpende gevolgen hebben voor burgers die wonen in de landen waaraan deze gegevens worden verstrekt. Deze risico's zijn bij de verstrekking van ongeëvalueerde gegevens nog groter; op voorhand staat immers niet vast welke informatie besloten ligt in de verstrekte gegevens.'*

²⁸ Productie 18, p. 35: *'De overdracht van niet geëvalueerde gegevens, met name die gegevens die zijn verkregen uit grootschalige interceptie, vormt een ernstige inbreuk op het recht op bescherming van de persoonlijke levenssfeer van burgers. Dit geldt a fortiori indien deze gegevens worden overgedragen aan buitenlandse diensten, omdat daarmee effectieve controle van de Nederlandse toezichthouder op het gebruik van die gegevens ontbreekt.'*

Artikel 64 Wiv2017: verstrekking zonder samenwerkingsrelatie

55. De Diensten hebben de bevoegdheid tot het verstrekken van gegevens aan een buitenlandse dienst wanneer er sprake is van een dringende en gewichtige reden.²⁹ Er hoeft dan geen sprake te zijn van een samenwerkingsrelatie en dus ook niet van een ‘weging’. De beleidsregels gaan hier niet over. Het gaat hierbij niet alleen om geëvalueerde gegevens maar ook om ongeëvalueerde gegevens. Ministeriële toestemming volstaat. De TIB komt hier niet aan te pas. De Rechtbank Den Haag heeft geen rol hierin. De CTIVD wordt pas achteraf geïnformeerd.

Artikel 88 Wiv2017: verstrekking binnen een samenwerkingsrelatie

56. Als er wél een samenwerkingsrelatie is, is wél toestemming nodig van de minister als het gaat om ongeëvalueerde gegevens.³⁰ Maar voor gegevens die wel geëvalueerd zijn is geen toestemming van de minister nodig. Ook hier heeft de TIB geen rol, en de Rechtbank Den Haag ook niet. Ook hier wordt de CTIVD pas achteraf geïnformeerd.

57. Het kabinet zegt in de beleidsregels niet dat er voorlopig géén ongeëvalueerde bulkgegevens naar het buitenland gaan. Integendeel, die optie wordt juist nadrukkelijk opgehouden door de beleidsregels.³¹ Waar het gaat om via bulkinterceptie verkregen gegevens geldt als enige beperking dat het alleen naar landen mag waarbij een ‘wegingsnotitie’ aan de samenwerking ten grondslag ligt. Die beperking geldt dus niet voor ongeëvalueerde gegevens die middels een hack of middels een informant zijn verkregen. Die mogen ongeëvalueerd worden verstrekt aan een geheime dienst van een land waarmee geen wegingsnotitie aan de samenwerking ten grondslag ligt.

Gevaar van doorgeven door buitenlandse dienst aan derden

58. We hebben in de dagvaarding gewezen op het gevaar van het weer verder doorgeven van gegevens door de buitenlandse dienst. De Staat geeft ook op dit punt in deze procedure een expliciete en onvoorwaardelijke geruststelling (CvA 6.40): *‘De verstrekking van gegevens aan buitenlandse diensten vindt altijd plaats onder toepassing van de derde partij-regel (artikel 65 jo. artikel 62 lid 1 onder d Wiv2017.’*

²⁹ Artikel 64 lid1 Wiv2017. De Staat erkent in 4.31 CvA dat bij de verstrekking ex artikel 64 Wiv2017 geen weging als bedoeld in artikel 88 Wiv2017 heeft plaatsgevonden. Het kan daarbij ook gaan om verstrekking van ongeëvalueerde gegevens.

³⁰ artikel 89 lid 2 Wiv2017.

³¹ Artikel 2 van de beleidsregels luidt: *‘Ongeëvalueerde gegevens die met toepassing van de bijzondere bevoegdheid ex artikel 48, eerste lid, van de wet zijn verkregen, kunnen, voor zover het gegevens betreft die verkregen zijn uit toepassing van de bevoegdheid op de kabel, uitsluitend aan een partnerdienst worden verstrekt, indien aan de desbetreffende samenwerkingsrelatie een wegingsnotitie ten grondslag ligt.’*

59. Maar deze waarborg staat niet in de Wiv2017.³² Daar staat dat een dergelijke voorwaarde kán worden gesteld, maar die hóeft voor uitwisseling op grond van artikel 64 niet te worden gesteld.
60. Ook hier geldt weer dat de door de Staat genoemde waarborgen in de wet moeten staan. De wet moet aan kwaliteitseisen voldoen.
61. De waarborgen bij verstrekking van gegevens aan buitenlandse diensten schieten tekort en dat is in strijd met Europees recht.

V. Worden er grootschalig gegevens verzameld en waarom is daar zoveel weerstand tegen?

62. We hebben het vandaag over het *grootschalig* verzamelen van gegevens. De voorzitter van de CTIVD heeft de grootschaligheid bevestigd: *"Ja, het is grootschalig. Ga daar geen kiekeboe over spelen, kom daar nou toch voor uit"*. (Productie 16)
63. De regering heeft zelf het volgende voorbeeld van bulkinterceptie gegeven. In een fictieve stad met 400.000 inwoners zou al het internet-verkeer via een bepaalde chatdienst kunnen worden afgetapt (Productie 15). Nu die bevoegdheid daadwerkelijk in werking is getreden zou die stad zomaar Den Haag kunnen zijn, bijvoorbeeld om in kaart te brengen wie er via Whatsapp met personen in oorlogsgebieden contact heeft. Bij die appjes zitten dan ook berichten van alle Haagse burgers die geen enkel risico vormen voor de nationale veiligheid. Een ook het app-verkeer van alle in Den Haag werkzame journalisten, alle in Den Haag werkzame advocaten en zelfs alle Haagse rechters.
64. De wettelijke bevoegdheid is dus ruim, zeer ruim. Er mág op grote schaal gegevens worden verzameld.

³² Artikel 65 Wiv2017: 1. De verstrekking van gegevens kan geschieden onder de voorwaarde dat degene aan wie de gegevens worden verstrekt, deze gegevens niet aan anderen mag verstrekken.
2. De voorwaarde, bedoeld in het eerste lid, wordt in ieder geval gesteld, indien gegevens worden verstrekt aan een instantie als bedoeld in artikel 62, eerste lid, onder d.
3. Indien gegevens zijn verstrekt onder de voorwaarde dat deze niet aan anderen mogen worden verstrekt, kan door Onze betrokken Minister of namens deze het hoofd van de dienst alsnog toestemming worden verleend om deze aan andere personen of instanties te verstrekken. Aan de toestemming kunnen voorwaarden worden verbonden.

65. De weerstand tegen deze nieuwe bevoegdheid tot grootschalige ongerichte interceptie is groot:

- a) in de consultatiefase gaf een record-aantal partijen kritisch commentaar op het wetsvoorstel. Meer dan duizend partijen deden dat.³³ Er was een stortvloed van kritiek;
- b) tijdens de parlementaire behandeling was er heel veel weerstand van de oppositie: het aantal moties en amendementen, vooral van oppositie-partij D66, was enorm;
- c) de drempel om over deze wet een referendum te houden werd snel en met gemak gehaald. Zo groot is de maatschappelijke onrust. De meerderheid van de stemmers sprak zich uit tégen de Wiv2017; en
- d) de partijen die vandaag procederen vertegenwoordigen een brede dwarsdoorsnede van de maatschappij:
 - het gaat om de privacy van gewone burgers,
 - het gaat om het belang van vertrouwelijkheid van communicatie van bronnen en journalisten en NGO's,
 - om het belang van de rechtspleging en de vertrouwelijkheid van communicatie met advocaten, en
 - het gaat om de belangen van communicatie-dienstverleners die door de Diensten gedwongen kunnen worden mee te werken.

66. Waarom maken Eisers zich zo druk over de nieuwe bevoegdheid tot het grootschalig verzamelen van gegevens? Omdat daarmee voor het eerst grote hoeveelheden data onder het bereik van de Diensten komen die pas dáárna worden onderzocht op relevantie. De *modus operandi* van de Diensten zal hierdoor fundamenteel veranderen. Van onderzoek dat zich richt op concrete bedreigingen voor de nationale veiligheid naar het binnenhalen van grote hoeveelheden data. Die data worden vervolgens geanalyseerd op patronen, afwijkingen, correlaties. Dát geeft het gevoel van een samenleving waarin de overheid middels digitale surveillance heel veel data gaat verzamelen, analyseren en bewaren.

67. De nieuwe werkwijze van de Wiv2017 legitimeert dat er op grote schaal gegevens worden verzameld en gebruikt van burgers die geen enkel risico vormen voor de nationale veiligheid.

³³ Bijvoorbeeld ook de Raad van State, de Raad voor de Rechtspraak, de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD), de Autoriteit Persoonsgegevens, en 29 vooraanstaande wetenschappers en alle betrokken marktpartijen waren uitermate kritisch op het wetsvoorstel.

68. Daarbij zullen ook gegevens zitten van bronnen van journalisten en NGO's. De Rechtbank Den Haag zou normaal gesproken vooraf toestemming moeten verlenen voor onderzoek naar bronnen,³⁴ maar bij bulkinterceptie stáán de gegevens al op de harde schijf van de Diensten. En als eenmaal de identiteit van een bron is onthuld, wat ook kan gebeuren zonder dat je daarnaar op zoek was, dan kan die informatie niet meer vergeten worden. Bronnen zullen er nooit meer op kunnen vertrouwen dat hun communicatie met een journalist in Nederland alleen wordt onderschept na voorafgaande rechterlijke toestemming, zoals het EHRM eist.
69. Hetzelfde bezwaar geldt voor de vertrouwelijke communicatie tussen advocaten en hun cliënten. Waar het huidige systeem van nummerherkenning er nu voor zorgt dat een tap afslaat als er met een nummer van een advocaat wordt gebeld, zit zo'n waarborg naar zijn aard niet in het grootschalig binnenhalen van communicatiegegevens.

VI. Bespreking van een aantal onderdelen van de Conclusie van Antwoord

70. We hebben een aantal onderdelen van de Conclusie van Antwoord van de Staat al besproken en zullen nog een paar opmerkingen over dat processtuk maken. De overige onderdelen ervan worden betwist voorzover in de dagvaarding niet eenzelfde standpunt wordt ingenomen.
71. In de dagvaarding is uitvoerig uitgelegd waarom het Handvest voor de Grondrechten en de EU-privacyregelgeving wel degelijk van toepassing is op de vergaande inbreuk op grondrechten die de regelgeving over inlichtingen- en veiligheidsdiensten maakt. Er ligt een prejudiciële vraag hierover bij het HvJEU.
72. De Staat beargumenteert in 6.5 CvA dat er voor de Wiv2017 'een grotere mate van beoordelingvrijheid' is, met verwijzing naar het *Weber*-arrest uit 2006. Die beoordelingsvrijheid is nadien flink beperkt, onder meer in het leidende *Zakharov*-arrest van de Grote Kamer uit 2015.³⁵

³⁴ artikel 30 lid 2 Wiv2017.

³⁵ *Zakharov*: 232. 'As to the question whether an interference was "necessary in a democratic society" in pursuit of a legitimate aim, the Court has acknowledged that, when balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse.'

73. De Staat stelt in 6.9 CvA dat het verzamelen en opslaan van gegevens als een geringe inbreuk zou moeten worden beschouwd. In de jurisprudentie van de hoogste Europese rechters wordt dit juist als een ernstige inbreuk aangemerkt. In *Digital Rights Ireland*³⁶ ging het vooral over het ontbreken van bepaalde specifieke waarborgen in de Dataretentierichtlijn en niet zozeer over de verzameling op zichzelf. In het recente *Tele2*-arrest³⁷ zijn algemene, strenge voorwaarden opgenomen voor de verzameling van data. Het HvJEU heeft de regels op het gebied van dataretentie sinds Uw vonnis uit 2015 in het kort geding over de Wet Bewaarplicht Telecommunicatie dus aangescherpt. Uitgangspunt is dat de verzameling van gegevens op zichzelf een inbreuk is op de persoonlijke levenssfeer.

74. Ad 8.10 CvA: De Eerste Kamer is wel degelijk buitenspel gezet. De Eerste Kamer had als medewetgever kunnen meebeslissen (a) wanneer het kabinet de Wiv2017 gewijzigd zou hebben vóór inwerkingtreding, en (b) wanneer het kabinet conform artikel 11 Wrr een wet had voorgelegd over de inwerkingtreding na de uitkomst van het raadgevend referendum.

VII. Nadere toelichting petitum en belangenafweging

75. Eisers zijn niet tegen de Wiv2017 in zijn geheel. Maar op een paar onderdelen is de Wiv2017 te ver doorgeschooten.

76. Eisers zijn tegen de bevoegdheden die grootschalige ongerichte dataverzameling mogelijk maken, omdat daarbij – naar de aard van de bevoegdheid – gegevens zullen zitten van gewone burgers die helemaal geen risico voor de nationale veiligheid vormen. En ook gegevens over bronnen van journalisten en NGO's, en vertrouwelijke gegevens van advocaten en hun cliënten. Die grootschalig verzamelde gegevens mogen aan buitenlandse diensten worden verstrekt, soms zelfs al vóóordat de Nederlandse Diensten daar zelf naar gekeken hebben. Dat gaat te ver. Dat is onderwerp van dit kort geding. Er bestaan overigens ook fundamentele bezwaren tegen andere onderdelen van de Wiv2017, maar die zijn vandaag niet aan de orde.

77. Het kabinet heeft naar aanleiding van de uitkomst van het referendum een wetswijziging aangekondigd. Wat Eisers vragen is dat dat in afwachting van de benodigde wetswijziging de bevoegdheden tot grootschalige ongerichte verzameling en het verstrekken daarvan aan buitenlandse diensten buiten werking worden gesteld. Dat is dus een *tijdelijke* maatregel.

³⁶ HvJ EU 8 april 2014, C 293/12 en C 594/12 (*Digital Rights Ireland*), punt 29.

³⁷ HvJ EU 21 december 2016, C 203/15 en C 698/15 (*Tele2*), punt 85.

78. Het vervangen van de Wiv2002 door de Wiv2017 heeft in totaal vijf jaar in beslag genomen. Een uitstel van vier maanden – omdat de sollicitatieprocedure voor de TIB niet soepel liep – was geen enkel probleem. Dan kunnen de Diensten nu ook nog wel even wachten totdat de wet gewijzigd is. Het kabinet heeft zelf in de hand voor hoe lang onderdelen van de Wiv2017 tijdelijk buiten werking zijn. Als het kabinet haast maakt met een wetswijziging kan die binnen een paar maanden worden doorgevoerd.
79. Het kabinet stelt dat het ‘voor de goede uitvoering van de operationele taak van de diensten noodzakelijk is dat de wet in haar geheel met ingang van 1 mei in werking treedt’.³⁸ Dat standpunt is niet nader onderbouwd of toegelicht. De Staat zou afzonderlijk voor iedere bevoegdheid waar we vandaag buitenwerkingstelling van vragen concreet moeten aangeven waarom die bevoegdheid niet kan wachten op de benodigde wetswijziging. Dat heeft de Staat niet gedaan.
80. Daarbij is van belang dat de Diensten over heel veel andere bevoegdheden beschikken onder de Wiv2017. De Diensten staan bepaald niet met lege handen als de vorderingen worden toegewezen. Ze mogen nog steeds gerichte onderzoeken doen en in dat kader kunnen ze afluisteren, aftappen, hacken, etc. etc.
81. Graag neem ik UEA mee door het petitum.
82. **Ad I.** De bevoegdheid tot bulkinterceptie is onmiskenbaar onverbindend wegens strijd met het Europese recht. De doelen zijn veel te ruim. Het *Zakharov*-arrest eist dat er een ‘reasonable suspicion’ is, en bulkinterceptie is naar zijn aard niet gericht op bepaalde personen. De overige waarborgen schieten tekort, onder meer doordat de interne beleidsregels van de Diensten over het gebruiken, bewaren en vernietigen niet publiekelijk beschikbaar zijn.
83. **Ad II.** De Staat stelt in deze procedure dat het werken met informanten niet tot grootschalige verzameling van persoonsgegevens leidt. Dat moet dan ook in de Wiv2017 komen te staan. Nu is de Wiv2017 op dit punt veel te ruim. Deze waarborg moet ‘*particularly precise*’ in de wet worden opgenomen.
84. De Staat zal overigens geen bezwaar kunnen hebben tegen de *tijdelijke maatregel* die Eisers vragen, namelijk dat artikel 39 Wiv2017 tot aan het moment dat de Wiv2017 gewijzigd is

³⁸ Productie 12.

niet wordt gebruikt om informanten te gebruiken voor zover de inzet van deze bevoegdheid leidt tot het grootschalig verzamelen, opslaan, gebruiken, bewaren en/of doorgeven van gegevens van burgers die geen risico vormen voor de nationale veiligheid en/of van cliënten van advocaten en/of van bronnen van journalisten en NGO's. Gedurende de tijdelijke buitenwerkingstelling kan de wetgever de Wiv2017 aanpassen. Hoe de wetgever dat precies wil doen is aan de wetgever. Daar zijn de vorderingen van Eisers niet op gericht. Vordering II van Eisers ligt voor toewijzing gereed.

85. **Ad III.** De Staat heeft gesteld dat met hacken niet grootschalig persoonsgegevens zullen worden verzameld. Ook dat moet '*particularly precise*' in de wet worden opgenomen. Ook op dit punt kan de Staat geen bezwaar hebben tegen de gevraagde tijdelijke maatregel die geldt tot het moment dat de wet is gewijzigd. Ook deze vordering kunt UEA toewijzen.
86. **Ad IV.** De door de Staat genoemde waarborg dat altijd als voorwaarde wordt gesteld dat een buitenlandse dienst de verstrekte gegevens niet verder doorgeeft staat niet in de wet. En het doorgeven van ongeëvalueerde gegevens is onmiskenbaar onverbindend wegens strijd met Europees recht. Ook deze vordering ligt voor toewijzing gereed.

VIII. Conclusie

87. De Wiv2017 moet een sterke boot zijn, een zeewaardige boot. Maar het huidige ontwerp deugt niet. Het is een boot die al voor de tewaterlating lek was. Met een lekke boot kún je nog een stukje doorvaren, maar de boot van de Wiv2017 maakt water. De Autoriteit Persoonsgegevens ziet het lek, wetenschappers en marktpartijen zien het lek, zelfs de toezichthouder op de Diensten ziet het lek. En de meerderheid van de stemmers bij het referendum zag het ook en adviseerde het kabinet de Wiv2017 niet ongewijzigd in te voeren. Het kabinet *zegt* daar naar te luisteren, maar doet dat in de praktijk niet. Het kabinet is aan het hozen in plaats van een grondige reparatie uit te voeren.
88. Het probleem zit in de grootschaligheid van de gegevens die de Diensten willen verzamelen. Die nieuwe *modus operandi* is in strijd is met Europese grondrechten. Dat is vanuit juridisch oogpunt het grootste gat in de romp van de Wiv2017. De Staat heeft in deze procedure – tot verrassing en blijdschap van Eisers – gesteld dat het werken met informanten en het hacken van derden niet zal leiden tot grootschalige verzameling van persoonsgegevens. Dat is goed nieuws, maar het staat niet in de wet. En daar hoort het wel thuis.

89. Een vonnis waarin u de vorderingen van Eisers toewijst geeft het kabinet de gelegenheid om de benodigde wetswijziging door te voeren, samen met het parlement. Dat kan heel snel of in alle rust, dat is aan het kabinet. Maar tot die wetswijziging is doorgevoerd maakt de boot dan geen water meer.
90. We verzoeken UEA daarom de vorderingen van Eisers toe te wijzen.