De Wiv 2017: sleepnet, aftapconsultancy en twijfelachtig toezicht

*Dorien Verhulst**

Na een lang wetgevingstraject is een nieuwe Wet op de inlichtingen en veiligheidsdiensten aangenomen. Dit artikel geeft een schets van de herziene wet, bezien vanuit het perspectief van burgers en aanbieders van elektronische communicatiediensten. Nieuw zijn met name de bevoegdheid voor 'onderzoeksopdrachtgerichte interceptie', een scala behulpzaamheidsverplichtingen voor (allerlei) aanbieders van communicatiediensten en een complex, diffuus systeem van toezicht. Daarop volgen enkele kritische noten. Bij de critici van de nieuwe wet ontbreekt het vooralsnog aan een moraalridder met de voeten in de klei. Intussen verspeelt de overheid echter iedere goodwill voor gemoderniseerde bevoegdheden door op allerlei punten grote zorgvuldigheid te suggereren, maar harde waarborgen te schuwen.

De Wiv 2017

Totstandkoming

De herziene Wet op de inlichtingen en veiligheidsdiensten is op 17 augustus 2017 in het *Staatsblad* gepubliceerd.[1] Een succesvolle protestactie heeft ertoe geleid dat op 21 maart 2018 een raadgevend referendum over de nieuwe wet zal worden gehouden. Het kabinet zal de uitkomst daarvan 'zorgvuldig in overweging nemen', maar gaat tegelijkertijd uit van inwerkingtreding op 1 mei 2018.[2] Het referendum lijkt daarmee een laatste stuiptrekking na een langdurig wetgevend proces. Dat begon in 2015, met een consultatie van een conceptversie. Daarop volgden ruim 500 kritische reacties, afkomstig van maatschappelijke organisaties, technologie- en communicatiebedrijven, wetenschappers en – vermoedelijk dankzij de inspanningen van Bits of Freedom – een groot aantal individuele burgers.[3] In het voorjaar van 2016 lekte een aangepaste versie van het wetsvoorstel en de memorie van toelichting,[4] die vervolgens in het najaar naar de Tweede Kamer werden gestuurd.[5] Het wetsvoorstel werd op 14 februari 2017 door de Tweede Kamer in gewijzigde vorm aangenomen en op 11 juli 2017 door de Eerste Kamer.[6]

Onderzoeksopdrachtgerichte interceptie (bulkinterceptie)

Meest controversieel is zonder twijfel de nieuwe bevoegdheid die bulkinterceptie van elektronische communicatie mogelijk maakt, eufemistisch aangeduid als 'onderzoeksopdrachtgerichte interceptie' (art. 48-50 Wiv 2017). De nieuwe bevoegdheid maakt het mogelijk om alle telecommunicatie en datatransmissie af te tappen, ongeacht de plaats waar de communicatie plaatsvindt en met alle technische middelen, op basis van een 'onderzoeksopdracht'.[7] De nieuwe bevoegdheid vormt een enorme uitbreiding van de bestaande bevoegdheid ten aanzien van kabelgebonden communicatie, om specifieke personen, organisaties en nummers (gericht) af te tappen (art. 47 Wiv 2017).[8] Bulkinterceptie wordt mogelijk op basis van een drie-trapsmodel: verzameling (art. 48 Wiv

* Mr. D. Verhulst is advocaat te Amsterdam (Brinkhof).

1 Wet van 26 juli 2017, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 2017), *Stb.* 2017, 317. Een aantal bepalingen inzake de (noodzakelijke benoemingen voor de) toezichthoudende organen TIB en de CTIVD zijn op 1 september 2017 al in werking getreden, *Stb.* 2017, 318. Zie voor eerdere besprekingen van het wetsvoorstel o.a. W. Muller& W. Voermans, 'Nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten. Een nieuw evenwicht tussen veiligheid en waarborgen', *NJB* 2017/95; E.J. Eskens, 'Ongerichte interceptie, of het verwerven van bulkcommunicatie, en waarom de Grondwet en het EVRM onvoldoende tegenwicht bieden', *Computerrecht* 2015/85.

2 Aldus minister Ollongren in een brief aan de Tweede Kamer van 1 november 2017 (kenmerk 8de9137e-or1-3.0).

3 Zie: https://www.internetconsultatie.nl/Wiv/details.

4 H. Modderkolk, 'Kabinet houdt vast aan massaal aftappen internetverkeer', *de Volkskrant* 29 april 2016. Volledige tekst gelekte versie hier: goo.gl/R8SSzd.

5 *Kamerstukken II* 2016/17, 34 588, nrs. 2-3.

6 In de Tweede Kamer stemden PvdA, Van Vliet, 50PLUS, Houwers, Monasch, VVD, SGP, ChristenUnie, CDA, Groep Bontes/Van Klaveren en PVV voor het wetsvoorstel. In de Eerste Kamer stemden SGP, ChristenUnie, VVD, PvdA, CDA, 50PLUS, OSF en PVV voor. Zie voor een bespreking van de belangrijkste amendementen: J.J. Oerlemans, 'Nieuwe Wiv door de Tweede Kamer aangenomen', *Computerrecht* 2017/87.

7 Met de term 'onderzoeksopdrachtgericht' wordt een koppeling beoogd met de 'Geïntegreerde Aanwijzing' (GA) voor de inlichtingendiensten, kort gezegd de door het kabinet opgestelde taakomschrijving voor de diensten voor een periode van vier jaar. In de GA zijn concrete onderzoeksopdrachten voor de diensten opgenomen, zie: *Kamerstukken II* 2016/17, 34 588, nr. 3 (MvT), p. 90. Daarnaast zijn echter ook aanvullende, vooraf geaccordeerde onderzoeksopdrachten mogelijk. Art. 26 Wiv 2017 bevat verder in het algemeen eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. De door de Tweede Kamer aangenomen motie-Recourt verduidelijkte dat de inzet van bevoegdheden ook zo gericht mogelijk moet zijn, zie: *Kamerstukken II* 2016/17, 34 588, nr. 66.

8 Op basis van art. 27 van de Wiv 2002 hebben de diensten daarnaast de bevoegdheid om (alleen) niet-kabelgebonden communicatie (ongericht) te scannen en analyseren.

2017), vooronderzoek (art. 49 Wiv 2017) en, ten slotte, de uiteindelijke selectie en (geautomatiseerde) analyse (art. 50 Wiv 2017). Voor iedere stap is voorafgaande toestemming van de relevante minister (van Binnenlandse Zaken of Defensie) vereist, die zal worden getoetst door een nieuw op te richten Toetsingscommissie Inzet Bevoegdheden.[9] Toestemming wordt verleend voor een periode van ten hoogste een jaar, maar kan (in theorie: oneindig) worden verlengd voor eenzelfde periode.[10]

In de toelichting wordt in populaire taal benadrukt dat de bevoegdheid niet overmatig of lichtvaardig zal worden ingezet.[11] De memorie van toelichting vermeldt verder dat tussen 2017 en 2020 vier 'access locaties' gereed zullen worden gemaakt voor onderzoeksopdrachtgerichte interceptie.[12] In een parlementair debat sloot minister Plasterk de mogelijkheid uit dat de Amsterdam Internet Exchange (AMS IX) in zijn geheel zou worden afgetapt.[13] De voorgestelde bevoegdheden bevatten een dergelijke beperking echter niet. Veelzeggend was de uitgelekte brief van de minister aan verschillende telecomaanbieders met het verzoek om een kostenraming van een aantal theoretische aftapscenario's. Volgens de NOS refereerde de brief daarbij aan het aftappen van alle communicatie tussen een stad met 400.000 inwoners en één bepaalde applicatie (conservatief geschat op 200 gebruikers) en het aftappen van wifihotspots.[14]

Verzamelde gegevens mogen in principe drie jaar worden bewaard voor (latere) analyse (indien toepasselijk), gerekend vanaf het moment van decryptie (art. 48 lid 5 Wiv 2017). De relevantie van de gegevens moet 'zo snel mogelijk' worden onderzocht. Data waarvan de relevantie binnen een jaar na verzameling nog niet is onderzocht moeten, net als irrelevante gegevens, worden verwijderd (art. 27 lid 1 Wiv 2017).[15] Ongeevalueerde gegevens mogen worden uitgewisseld met buitenlandse diensten, onder daarvoor geldende voorwaarden en met toestemming van de minister.[16]

Nieuwe behulpzaamheidsverplichtingen

Op basis van de Wiv 2002, en de spiegelbepaling van artikel 13.2 van de Telecommunicatiewet, zijn aanbieders van traditionele telecommunicatiediensten en -netwerken verplicht om mee te werken aan (gericht) aftappen door de diensten.[17] De Wiv 2017 breidt deze behulpzaamheidsverplichting radicaal uit, met een nieuwe set verplichtingen om de diensten op allerlei manieren te helpen met (gericht en ongericht) aftappen en het verzamelen van gegevens. Deze verplichtingen rusten voortaan bovendien op iedere 'aanbieder van een communicatiedienst', een zeer ruime categorie die niet alleen aanbieders van besloten en openbare elektronische communicatiediensten omvat, maar ook aanbieders van allerlei verwante diensten zoals aanbieders van clouddiensten, web hosting en OTT-diensten.

Al deze aanbieders moeten op verzoek adviseren over de wijze waarop een tap het beste kan worden geplaatst (art. 52 Wiv 2017), meewerken met het plaatsen van een tap en technische voorzieningen gedurende een jaar na het staken van de tap in stand houden (art. 53 Wiv 2017),[18] informatie uit de cloud verstrekken (gekoppeld aan specifieke targets; art. 54 Wiv 2017); terstond historische en toekomstige metadata van een gebruiker, nummer of locatie verstrekken (art. 55 Wiv 2017), alsmede NAW-gegevens van gebruikers (art. 56 Wiv 2017) en meewerken aan decryptie, hetzij door het delen van kennis hetzij door informatie zelf te ontsleutelen (art. 57 Wiv 2017). Niet-meewerken is een strafbaar feit, waarvoor een gevangenisstraf tot twee jaar of een boete tot (voor een vennootschap) € 82.000 kan worden opgelegd (art. 143 Wiv 2017). Voor zover het verlenen van medewerking een verwerking van persoonsgegevens behelst, wordt de Wet bescherming persoonsgegevens in algemene termen niet van toepassing verklaard.[19] Op aanbieders rust een geheimhoudingsverplichting (art. 135 Wiv 2017).

Zoals (in ieder geval) KPN al tijdens de consultatiefase signaleerde, is het grote gevaar van deze regeling dat aanbieders eerst consultancy moeten bieden over de wijze waarop bepaalde verkeersstromen (kunnen) lopen, en hun rol daarin, om vervolgens in concrete gevallen daadwerkelijk verlengstuk van de inlichtingendiensten te zijn.[20] Met de mogelijkheid om medewerking te kunnen eisen van een onbenoemd groot aantal bedrijven is bovendien een principieel nieuw kader geschapen.[21] Aan al deze private spelers wordt een vergaande inbreuk op de bedrijfsvoering opgelegd, zonder inzicht in, en verantwoording van, de precieze feitelijke gevolgen daarvan.

Uitbreiding hackbevoegdheid

AIVD en MIVD hebben nu al de bevoegdheid om computersystemen binnen te dringen en daarin opgeslagen of verwerkte gegevens te kopiëren, met toestemming van de verantwoordelijk minister (art. 24 Wiv 2002). Daarbij kan eenieder die vermoed wordt kennis te hebben van de wijze van versleuteling bevolen worden om te assisteren met decryptie.

9 Toestemming is gekoppeld aan een specifieke 'onderzoeksopdracht', zie hiervoor ook voetnoot 8.

10 Art. 48 lid 2, 49 lid 4, art. 50 lid 4 Wiv 2017. Voor het selecteren van gegevens op grond van art. 50 Wiv 2017 geldt een kortere toestemmingstermijn van drie maanden, art. 50 lid 2 Wiv 2017.

11 Zie bijv. par. 1.7 ('Wat gaan we nu wel en niet doen in de praktijk') van de MvT: "Wij gaan niet op zoek naar mensen die het woord 'bom' of 'ISIS' gebruiken in hum e-mails. Wij trekken niet in bulk internetverkeer naar binnen om te kijken welke mensen op zoek zijn naar kunstmest (…) Wat doen we wel? Onderzoekopdracht gerichte interceptie zal te allen tijde een zeer klein percentage betreffen van het totaal aan nationaal en internationaal dataverkeer (…)."

12 MvT, p. 16.

13 'Plasterk: AIVD gaat niet hele AMS-IX aftappen', Security.nl 11 februari 2015.

14 'Plasterk denkt na over aftappen chat-apps en wifi-hotspots', NOS 20 april 2016.

15 Voor (gegevens die betrekking hebben op) vertrouwelijke communicatie tussen een advocaat en cliënt geldt een strenger regime: die moeten in beginsel terstond worden verwijderd, tenzij verdere verwerking noodzakelijk is voor het onderzoek en de Rechtbank Den Haag daarvoor toestemming heeft verleend (art. 27 lid 2 Wiv 2017).

16 MvT, p. 102.

17 Daarnaast bevat art. 89 Wiv 2002 een specifieke strafbaarstelling voor de medewerkingsplicht aan decryptie en bevat art. 184 Sr een algemene strafbaarstelling van het niet opvolgen van een bevoegd gegeven ambtelijk bevel.

18 Volgens de memorie van toelichting zal voor (gerichte en ongerichte) interceptie in praktijk medewerking van de betreffende communicatieaanbieder nodig zijn. De tekst van de betreffende bevoegdheden sluit echter niet uit dat die zonder een dergelijke medewerking worden uitgeoefend. Zie: MvT, p. 97.

19 Art. 52 lid 4, 54 lid 5, 55 lid 5, 56 lid 5 jo. art. 39 lid 5 Wiv 2017. Zie voor een kritische bespreking van (de onmogelijkheid van) het wegwuiven van de wettelijke voorschriften voor verwerkingsverantwoordelijken de noot van M.E. Koning onder HvJ EU 21 december 2016, gev. zaken C-203/15 en C-698/15 (*Tele2 en Watson*), EHRC 2017, 79.

20 Zie de gedetailleerde kritische reactie van G.J.C. Wabeke en P.C. Knol namens KPN van 31 augustus 2015 op het geconsulteerde wetsvoorstel, zie: https://zoek.officielebekendmakingen.nl/blg-787330.pdf.

21 Het uitgangpunt van het huidige wettelijke kader – waarin de bevoegdheid van de diensten is geregeld in de Wiv 2002 en de verplichting tot medewerking van aanbieders van openbare telecommunicatiediensten daarop aansluitend in de Telecommunicatiewet – en de bovenliggende normatieve kaders van (o.a.) de Kaderrichtlijn (2002/21/EG) en Machtigingsrichtlijn (2002/20/EG) worden immers (grotendeels) verlaten.

Deze bestaande hackbevoegdheid wordt in de Wiv 2017 verruimd tot een bevoegdheid om ieder geautomatiseerd werk binnen te dringen of te verkennen, om vervolgens technische voorzieningen aan te brengen voor observatie en (gerichte) surveillance (art. 45 Wiv 2017). Daarmee komt waarschijnlijk een onvoorstelbaar grote hoeveelheid gegevens binnen het bereik van de diensten. Het aanhangige wetsvoorstel Computercriminaliteit III bevat namelijk een aanzienlijke verruiming van het begrip 'geautomatiseerd werk'. Daardoor zou met de nieuwe hackbevoegdheid voortaan niet alleen toegang kunnen worden verkregen tot opgeslagen gegevens, maar ook tot alle gegevens die worden uitgewisseld via daarmee verbonden communicatiekanalen alsmede gegevens opgeslagen in clouddiensten.[22] Voor gegevens die met de hackbevoegdheid zijn verkregen, geldt geen specifieke bewaartermijn; bepaald is slechts dat de relevantie van de gegevens zo snel mogelijk moet worden onderzocht en dat irrelevante gegevens en gegevens waarvan de relevantie na een jaar nog niet is vastgesteld, moeten worden vernietigd (art. 27 Wiv). Als de diensten malware installeren geldt slechts een inspanningsverplichting om die na gebruik te verwijderen (art. 45 lid 7 Wiv 2017).

Onduidelijk is ten slotte hoe de (aangevulde) hackbevoegdheid zich verhoudt tot de bevoegdheid tot onderzoeksopdrachtgerichte interceptie en de verschillende bevoegdheden om medewerking van aanbieders van communicatiediensten te bevelen. Dat laat bijvoorbeeld de vraag open of de verplichting om medewerking te verlenen aan bulkinterceptie (art. 53 Wiv 2017), vervolgens kan worden ingezet om de hackbevoegdheid uit te oefenen (art. 45 Wiv 2017). Andersom staat vast dat de hackbevoegdheid kan worden ingezet voor gerichte interceptie (art. 45 lid 2 sub c jo. art. 47 Wiv 2017). Dat suggereert, bij omissie, dat de hackbevoegdheid niet kan worden uitgeoefend voor onderzoeksopdrachtgerichte interceptie. Dat vermeldt de wettekst echter niet expliciet.

Rechtsmacht?

Gelet op de ruime, nieuwe aftapbevoegdheden en de ruime categorie 'aanbieders van een communicatiedienst' die daarbij behulpzaam moet zijn en verplicht kan worden allerhande gegevens aan de diensten te verstrekken, zullen vragen over rechtsmacht de komende jaren van cruciaal belang zijn. Veel aanbieders van in Nederland, en de rest van de wereld, populaire communicatiediensten zijn immers niet in Nederland gevestigd. De memorie van toelichting bevat op dat punt slechts een korte mededeling, in een subparagraaf 'capita selecta', met een diffuse boodschap. In de toelichting wordt eerst benadrukt dat de Wiv 2017, net als haar voorganger de Wiv 2002, geen extraterritoriale werking heeft, zodat de daarin vervatte medewerkingsplichten uitsluitend kunnen worden afgedwongen jegens aanbieders die binnen de Nederlandse jurisdictie vallen.[23] De toelichting vervolgt echter dat aanbieders die in Nederland persoonsgegevens verwerken, op grond van artikel 4 Wbp hier te lande een vestiging zullen moeten hebben, 'hetgeen een aanknopingspunt vormt voor het uitoefenen van rechtsmacht ook waar het gaat om (…) de Wiv 2002 of het huidige wetsvoorstel'.[24] Deze weergave is onjuist, artikel 4 Wbp eist namelijk niet dat buitenlandse verantwoordelijken een vestiging in Nederland hebben. Het is precies andersom: het artikel bepaalt dat als een buitenlandse verantwoordelijke een vestiging in Nederland heeft, de Wbp van toepassing is (en dat een verantwoordelijke zonder vestiging in Nederland, hier een vertegenwoordiger moet aanwijzen). De onderliggende, controversiële suggestie is echter glashelder: als een aanbieder onder de Nederlandse Wbp valt, dan zouden de diensten zich wel eens op het standpunt kunnen stellen dat ook de Wiv 2017 van toepassing is. Dat is temeer reden tot zorg, omdat de aankomende Algemene Verordening Gegevensbescherming (die per 25 mei 2018 van toepassing zal zijn) een nog veel ruimer toepassingsbereik heeft op – kort gezegd – multinationals die hun diensten in de Europese Unie aanbieden.

Geen onafhankelijk (rechterlijk) toezicht

De Wiv 2017 voorziet, op een beperkte uitzondering voor de inzet van inlichtingenmiddelen tegen advocaten en journalisten na, niet in een systeem van onafhankelijk, rechterlijk toezicht. Op grond van de nieuwe wet is voor inzet van de meest vergaande bevoegdheden voorafgaande toestemming van de betreffende minister vereist. De rechtmatigheid van die toestemming wordt *ex ante* getoetst door een nieuw op te richten Toetsingscommissie Inzet Bevoegdheden (TIB), die bestaat uit drie leden. Ten minste twee commissieleden moeten minimaal zes jaar ervaring als rechter hebben, maar hoeven dat niet noodzakelijkerwijs te zijn. Leden van de toetsingscommissie worden benoemd via een nogal ingewikkelde procedure met elementen van medezeggenschap voor het parlement en de rechterlijke macht. Uiteindelijk heeft de regering echter de beslissende stem.[25] De TIB doet geen uitspraak in een procedure op tegenspraak: hoewel het alle relevante informatie en overige medewerking mag vragen aan de minister (art. 36 lid 1 Wiv 2017), worden geen 'public advocates' of technisch experts benoemd.[26] Een ministeriële toestemming die onrechtmatig wordt geacht vervalt van rechtswege, zodat de betreffende bevoegdheid niet kan worden uitgeoefend (art. 36 lid 2 jo. art. 37 Wiv 2017). Zittingen van de TIB zijn niet openbaar en het is onduidelijk of uitspraken in enige vorm zullen worden gepubliceerd.

De Wiv 2017 handhaaft daarnaast het bestaande *ex post* toezicht door de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) en breidt dat toezicht verder uit. De CTIVD bestaat uit ten minste vier leden, die geen specifieke juridische of technische expertise hoeven hebben (art. 98, 99 Wiv 2017). Zij worden via dezelfde complexe procedure benoemd als leden van de TIB, dat wil zeggen met beslissende stem van de regering. De CTIVD vervult haar toezichthoudende taak op drie manieren: door publicatie van toezichtrapporten; door klachten van klokkenluiders te onderzoeken; en in een klachtprocedure. Die laatste procedure staat open voor eenieder jegens wie optreden door de diensten heeft plaatsgevonden (art. 114 jo. 121(d) Wiv 2017). Onduidelijk is of daar-

22 Voor het begrip 'geautomatiseerd werk' in art. 45 Wiv 2017 verwijst de wetgever naar de definitie van art. 80 sexies Wetboek van Strafrecht, dat – kort gezegd – zowel individuele computers en computernetwerken omvat. Het aanhangige wetsvoorstel Computercriminaliteit III (*Kamerstukken* 34 372) breidt die definitie uit naar ieder 'apparaat, of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken'.

23 MvT, p. 241.

24 Ibid.

25 Leden van de TIB worden bij Koninklijk Besluit benoemd, op voordracht van de betrokken ministers gezamenlijk, die kunnen kiezen uit een lijst met drie kandidaten aangeboden door de Tweede Kamer, op basis van een niet-bindende aanbevelingslijst van ten minste drie kandidaten opgesteld door de vicepresident van de Raad van State, de president van de Hoge Raad en de Ombudsman gezamenlijk (art. 33 lid 4 jo. 99 Wiv 2017).

26 Een probleem dat in de Verenigde Staten voor het beruchte FISA-court wel werd aangepakt met de Freedom Act, zie voor een overzicht: https://www.washingtonpost.com/graphics/politics/usa-freedom-act/.

onder ook de tot medewerking verplichte aanbieders van communicatiediensten vallen. Het normatieve kader voor klachten is troebel: de CTIVD moet onderzoeken of door de diensten 'behoorlijk is gehandeld' (art. 124 lid 1 Wiv 2017). Onduidelijk is in hoeverre dat een toets behelst van de geschiktheid en noodzakelijkheid van een bepaalde maatregel en of daarbij alleen wordt gekeken naar de impact op het algemeen belang, of ook naar de rechten van individuele partijen, zoals eventueel betrokken communicatieaanbieders. In (alleen) een klachtprocedure kan de CTIVD de minister bevelen om een lopend onderzoek of de uitoefening van een bevoegdheid te staken, en om verzamelde gegevens te verwijderen en vernietigen (art. 123 lid 4 Wiv 2017). Een oordeel wordt schriftelijk aan de klager meegedeeld en gemotiveerd voor zover de staatsveiligheid dat toelaat (art. 124 lid 3 Wiv 2017).

Kritische noten

Tijdens de behandeling van de nieuwe wet stonden tegenstanders prominent op de barricaden. Bits of Freedom voerde samen met Free Press Unlimited en de Internet Society Nederland een uitvoerige campagne onder de noemer 'geen sleepnet' en Privacy First vormde nog voor de wet was aangenomen alvast een coalitie voor een rechtszaak over de burgerrechtelijke bestaanbaarheid ervan. Ook nu het jarenlange wetgevingsproces voltooid is, verstomt de kritiek nog niet. Een groepje Amsterdamse studenten bewees dat actievoeren niet voorbehouden is aan hun ouders of de jaren zeventig en verzamelde, geholpen door satiricus Arjen Lubach, in korte tijd voldoende handtekeningen voor een raadgevend referendum, dat nu op 21 maart 2018 zal plaatsvinden.[27] Kortom, de Wiv 2017 houdt de gemoederen nog wel even bezig, mogelijk zelfs tot in Straatsburg.

De tegenstanders moet onmiddellijk worden toegegeven dat zij strijden voor belangrijke idealen. De privacy en informatievrijheid van burgers staat in de eenentwintigste eeuw op allerlei manieren onder druk en het 'gevaar' is zeker ook afkomstig van een datahongerige overheid. Tegenstanders van de wet worden in hun kritische houding ook gesteund door het Europese Hof van Justitie en het EHRM.[28] Beide colleges zijn in opeenvolgende uitspraken kritisch over grootschalige gegevensverzameling over burgers door overheden.[29] Over de vraag hoe inlichtingen- en veiligheidsdiensten in het huidige maatschappelijke en technische landschap hun werk dan wel moeten doen, blijft het in deze hoek echter oorverdovend stil. Felle kritiek op het 'sleepnet' of het verzwakken van encryptie lijkt op zijn plaats, maar beantwoordt nog niet de vraag hoe inlichtingendiensten dan wel moeten omgaan met terroristen die aanslagen voorbereiden via een Playstation 4. Het blijft vooralsnog wachten op een moraalridder met zijn voet in de klei.

Andersom is goed invoelbaar dat bij de overheid behoefte bestaat aan een modernisering van inlichtingenbevoegdheden, om in een technisch en maatschappelijk complexe maatschappij dreigingen tijdig te kunnen onderkennen en bestrijden. De wetgever verspeelt die goodwill vervolgens echter onmiddellijk door op allerlei punten zorgvuldigheid te suggereren, zonder die te vertalen in concrete en harde waarborgen. Welke wetgevingsjurist durft in populaire taal te benadrukken dat bulkinterceptie niet lichtvaardig zal worden toegepast (met als hoogtepunt de paragraaf 'wat gaan wij nu wel en niet doen'),[30] als de wettekst slechts de summiere beperking bevat dat er een koppeling 'een onderzoeksopdracht' zal zijn? Hoe bestaat het dat de meest concrete voorbeelden van de nieuwe bevoegdheden vervolgens uitlekken in een gelekte ministeriële brief, maar niet genoemd staan in de honderden pagina's memorie van toelichting.[31] Dat AIVD-directeur Bertholee intussen in een interview liet weten dat hij de privacydiscussie 'beu' is komt de beeldvorming niet ten goede.[32]

Een voor de hand liggende reactie is dat dergelijke voorbeelden inzicht zouden (kunnen) geven in de werkwijze van de diensten en staatsgeheim zou kunnen of moeten zijn. Over de (on)mogelijkheid en (on)wenselijkheid van een dergelijke geheimhouding valt in het huidige tijdsgewricht echter nog wel wat meer te zeggen.[33] Dat dat niet is gebeurd is (ook) een gemiste kans. Een dergelijke geheimhoudingsdiscussie speelt bovendien niet waar het gaat over het systeem van toezicht op de geheime diensten. De Commissie Dessens, die de oude Wiv 2002 evalueerde en wier advies de opmaat vormde voor de herziening van de wet, maakte in 2013 al het overtuigende kernargument dat er ruimere bevoegdheden én verdergaande waarborgen nodig waren.[34] De CTIVD zou intensiever toezicht moeten houden en (a) steeds, (b) onmiddellijk en (c) juridisch bindend moeten kunnen oordelen over de uitoefening van

27 Voor een bespreking zie: H. Modderkolk, 'Een referendum over privacy dient zich aan; moeten we dat wel willen?', *de Volkskrant* 21 september 2017; N. van Eijk & E.J. Dommering, 'Het referendum verstoort de toetsing van de sleepwet', *Het Parool* 10 oktober 2017; A. Arnbak, 'Referendum "Sleepwet" voorbode digitale perikelen Rutte III', *Het Financieele Dagblad* 2 november 2017.

28 Zie voor een bespreking bijv. O. van Daalen, 'Over waterfilters en bioscoopschermen: het WIV-voorstel en Tele2/Watson', *Mediaforum* 2017-2.

29 HvJ EU 8 april 2014, zaaknrs. C-293/12, C-594/12 (*Digital Rights Ireland*), *Mediaforum* 2015-3, p. 112 e.v., m.nt. K. Irion, M-P Granger en S.J. Eskens; HvJ EU 6 oktober 2015, zaak C-362/14 (*Facebook/Schrems*), ECLI:EU:C:2015:650; HvJ EU 21 december 2016, C-203/15 en C-698/15 (*Tele2/Watson*); EHRM 1 juli 2008, appl. nr. 58243/00 (*Liberty e.a./Verenigd Koninkrijk*); EHRM 4 december 2015, appl. nr. 47143/06 (*Zhakarov/Rusland*), *NJ* 2017/185, m.nt. E.J. Dommering; EHRM 12 juni 2016, appl. 37138/14 (*Szabó & Vissy/Hongarije*); zie voor een inhoudelijke bespreking: S. Eskens, O. van Daalen & N. van Eijk, *Ten standards for oversight and transparency of national intelligence services*, Amsterdam: Instituut voor Informatierecht 2015.

30 MvT, par. 1.7, zie hiervoor voetnoot 10.

31 Terwijl de vrees voor een (te) ruime inzet van de bevoegdheid, ook afgezien van de Snowden-onthullingen, reëel lijkt. In Duitsland publiceerde de hoogste federale privacytoezichthouder een vernietigend rapport waaruit bleek dat de Duitse inlichtingendienst op tal van punten de wet had geschonden en bovendien het onderzoek ernstig had gehinderd. Kort daarna werd bekend dat 's werelds grootste internetknooppunt De-CIX de Duitse regering aanklaagt voor het onrechtmatig aftappen van haar systemen. Zie: A. Meister, 'Secret Report: German Federal Intelligence Service BND Violates Laws And Constitution By The Dozen', www.netzpolitik.org 2 september 2016; K. McCarthy, 'World's largest internet exchange sues Germany over mass surveillance', theregister.co.uk 16 september 2016.

32 H. Modderkolk, 'Dreiging is in jaren niet zo groot geweest, Rob Bertholee, hoofd van veiligheidsdienst AIVD', *de Volkskrant* 17 september 2016. Bertholee noemde de AIVD in een vakblad voor leerlingen en docenten maatschappijleer ook 'de best gecontroleerde dienst van Europa', een uitlating die 'NRC checkt' als 'niet te checken' kwalificeerde; K. Versteegh, 'NRC checkt: De AIVD is de best gecontroleerde dienst van Europa', *NRC Handelsblad* 10 juli 2017.

33 Getuige bijvoorbeeld de rechtszaak van Bits of Freedom voor openbaarmaking van de tapstatistieken van de AIVD, zie: R. Zenger, 'Hoger beroep om AIVD tapstatistieken', Bof.nl 20 september 2017; Lezenswaardig is ook het interview van CIA-directeur James Clapper in *Wired*, over onder meer de 'unkind reality [that] the workforce has to get out in front of a new era in which the government can hide far less'. Zie: https://www.wired.com/2016/11/james-clapper-us-intelligence/.

34 C.W.M. Dessens e.a., 'Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen', 2 december 2013. Zie: https://www.rijksoverheid.nl/actueel/nieuws/2013/12/02/commissie-dessens-wet-op-de-inlichtingen-en-veiligheidsdiensten-moet-worden-aangepast, met verwijzing naar het (eveneens online gepubliceerde) evaluatierapport.

ingrijpende onderzoeksbevoegdheden.[35] Een vergelijkbare oproep deed ook de CTIVD zelf en een groep wetenschappers in een open brief tijdens het wetgevingstraject, terwijl ook de Raad van State in zijn advies bij het wetsontwerp ernstige twijfel uitte of het systeem van toezicht in overeenstemming is met de criteria ontwikkeld door het EHRM.[36] Dat de wetgever weliswaar een voorafgaande toets door de TIB heeft ingevoerd, maar overigens heeft gemeend te kunnen volstaan met het huidige intransparante, gefragmenteerde en niet écht onafhankelijke toezicht op de (ver) verruimde bevoegdheden, is onbegrijpelijk.

35 Ibid.

36 Open brief aan Tweede Kamer: 'Onvoldoende waarborgen in nieuwe nationale veiligheidswet', 13 december 2016, zie: https://www.ivir.nl/nl/open-brief-aan-tweede-kamer-onvoldoende-waarborgen-nieuwe-nationale-veiligheidswet/; Zie ook de noot van E.J. Dommering onder het EHRM-arrest *Zakharov*, die er rekening mee houdt dat de rechter nadat de wet is aangenomen een oordeel over de verenigbaarheid van de wet met Straatsburgse normen zal moeten geven. EHRM 4 december 2015 (*Rusland/Zhakarov*), *NJ* 2017/185, m.nt. E.J. Dommering.