Parlement en Wetenschap

Factsheet VOORGENOMEN WIJZIGINGEN IN DE WET OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN 2017

Deze factsheet is tot stand gekomen in het kader van de samenwerking van de Tweede Kamer met De Jonge Akademie, de Koninklijke Nederlandse Akademie van Wetenschappen (KNAW), de Nederlandse Federatie van Universitair Medische Centra (NFU), de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO), TNO en de Vereniging Universiteiten van Nederland (UNL).

6 september 2024 Prof. dr. Bart Jacobs, mr. drs. Rowin Jansen (beiden Radboud Universiteit)[1]

1. Inleiding

Waar de Wet op de inlichtingen- en veiligheidsdiensten uit 2017 (Wiv 2017) vooral in het teken stond van (kabel)interceptie, zal naar onze verwachting de nieuwe wetgeving voor de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) draaien om AI en dan in het bijzonder om geautomatiseerde data-analyse (GDA) van grootschalige (bulk)bestanden. De moderne inlichtingenprofessional speurt namelijk niet meer handmatig naar bedreigingen van de staatsveiligheid, bijvoorbeeld in openbare bronnen of toegespeelde notulen, maar laat gespecialiseerde software grote gegevensbestanden en communicatiestromen analyseren, op zoek naar patronen, afwijkingen (anomalieën) en nog onbekende bedreigingen van de nationale veiligheid en de democratische rechtsorde, om op basis van die aanwijzingen eventueel nader onderzoek te doen in specifieke gevallen.

Inlichtingen- en veiligheidsdiensten onderscheiden zich van bedrijven en andere overheidsorganen door het uiterst vertrouwelijke karakter van (een deel van) de gegevens die zij verwerven, doorzoeken en analyseren. Zij verkrijgen zulke gegevens uit interceptie, hacks of via klassieke methoden als bevraging en gegevensuitwisseling met partnerdiensten. Hun werkveld kenmerkt zich van oudsher door een hoge mate van dynamiek en onvoorspelbaarheid. In het digitale domein is die dynamiek nog verder toegenomen, via bijvoorbeeld nepnieuwscampagnes, digitale spionage en sabotage. De beoogde nieuwe wet zal niet alleen deze nieuwe datagedreven werkwijze mogelijk moeten maken, maar ook robuust toezicht daarop helder moeten reguleren. Dat vereist een (verdere) verschuiving naar *real-time* toezicht, waarbij het zwaartepunt komt te liggen op toezicht tijdens (*ex nunc*) en na afloop (*ex post*) van een operatie.

De nieuwe inlichtingenwet zal een veelheid aan complexe operaties beslaan. Deze notitie richt zich slechts op enkele relevante hoofdzaken, waarbij wij zoveel mogelijk aanknopen bij de Hoofdlijnennotitie,[2] en beoogt bij te dragen aan de bredere discussie over het nationale veiligheidsdomein.

---

[1] *Bart Jacobs is hoogleraar Computerbeveiliging en privacy aan de Radboud Universiteit, lid van de KNAW en Stevin-laureaat. Hij was lid van de Evaluatiecommissie Wiv 2017. Rowin Jansen is promovendus Algemene rechtswetenschap aan de Radboud Universiteit en rondt een proefschrift af over het toezicht op de AIVD en de MIVD.*

[2] *Kamerstukken II* 2022/23, 34 588, nr. 92.

2. Bevoegdheden en termijnen

De AIVD en de MIVD lijken op dit moment geen essentiële bevoegdheden te missen. Een verruiming van het bevoegdhedenarsenaal is nu dus niet aan de orde, zo constateerde ook de Evaluatiecommissie Wiv 2017. Wel is nadere uitleg, uniformering, versimpeling en verankering van bestaande regelingen nodig, met name op het gebied van interceptie, hacken, bulkdata en GDA. Wat ons betreft moet dat zoveel mogelijk plaatsvinden in lijn met de 'Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma' (de Cyberwet).

Een eerste voorstel, bedoeld om de diensten en ook toezichthouders efficiënter te kunnen laten werken, is het toestaan van variaties in de reguliere toestemmingstermijn van drie maanden. In bepaalde situaties is een (gemotiveerde) termijn van drie, zes of twaalf maanden namelijk gepast. Een dergelijke aanpassing is zinvol in 'standaardsituaties', bijvoorbeeld van telefoon- en internet-taps bij bepaalde functies, organisaties of systemen, of bij strategische operaties die een lange voorbereidingstijd kennen en waarvan de opbrengst doorgaans niet snel duidelijk is.

3. Interceptie en bulk

Voor interceptie van communicatie(gegevens) van een specifiek target gelden al heldere procedures: voor de aanvraag, de toekenning en de toepassing. Die lijken in de praktijk goed te functioneren. In de Wiv 2017 is ook de zogenoemde onderzoeksopdrachtgerichte (OOG) interceptie verankerd. Deze bredere, niet-targetgerichte vorm van interceptie is nu – zo'n zes jaar na invoering – nauwelijks ingezet. De destijds verwachte operationele winst van dit nieuwe inlichtingenmiddel is dus nog niet verzilverd. Afgezien van de technische moeilijkheden is het uitblijven van OOG-interceptie te wijten aan de gebrekkige codificatie in de Wiv 2017 (deels gerepareerd in de Cyberwet) en aan interpretatiegeschillen tussen diensten en toezichthouders (een voortdurend probleem). Het zogeheten 'snapshotten', dat wil zeggen het verrichten van een proefinterceptie om informatiestromen in kaart te brengen en vervolgens gerichter te kunnen intercepteren, behoeft in lijn met de aanbevelingen van de CTIVD een permanente wettelijke grondslag.[3]

In navolging van de motie-Recourt is in de Wiv 2017 de eis gecodificeerd dat een bevoegdhedeninzet altijd zo gericht mogelijk moet zijn.[4] Dit gerichtheidsvereiste heeft een belangrijke normatieve waarde, maar leidt in de praktijk tot veel discussie tussen de diensten en de toezichthouders. Dat resulteert in vertragingen en ook in blokkades. De gerichtheidseis kan namelijk slechts in de loop van de interceptieactiviteiten betekenisvol worden ingevuld: kabelinterceptie zal in de beginfase per definitie ongericht zijn, om vervolgens, wanneer inzicht ontstaat in de verkregen gegevensstromen, door een systeem van filtering en continue datareductie, pas in latere verwerkingsstadia steeds gerichter te worden. Het gerichtheidscriterium dient onzes inziens daarom niet slechts statisch (vooraf) te worden getoetst, maar vooral dynamisch (*real-time*) te worden ingevuld.

---

3 CTIVD-Toezichtsrapport nr. 75 over de inzet van kabelinterceptie door de AIVD en de MIVD. De snapshotfase (2022).
4 *Kamerstukken II* 2016/17, 34 588, nr. 66.

Via OOG-interceptie kunnen grote hoeveelheden gegevens worden verkregen. Zoals de Evaluatiecommissie Wiv 2017 heeft bepleit, dient er een uniforme regeling voor zulke bulkdata te komen, onafhankelijk van of de gegevens via bijvoorbeeld interceptie of hacken verkregen zijn.

4. Hackoperaties

De AIVD en de MIVD beschikken al geruime tijd over de bevoegdheid om geautomatiseerde werken binnen te dringen.[5] 'Hacken' heeft grote operationele waarde, zeker in een tijdperk waarin communicatie steeds beter is versleuteld, zodat relevante informatie slechts op de eindpunten in onversleutelde vorm kan worden verzameld.[6] De inzet van dit instrument ligt gevoelig, vanwege de mogelijk zware inbreuk op de privacy en potentiële nevenschade.[7] Onze taxatie is dat de wetgever te zeer schone handen wil houden op een gebied dat per definitie rommelig is.[8] In de Wiv 2017 is geprobeerd hackoperaties juridisch dicht te spijkeren, vooral door strikte toetsing vooraf. Maar dat werkt niet: computersystemen kennen doorgaans verschillende lagen van beveiliging, waarbij op voorhand alleen de buitenste laag (enigszins) zichtbaar is. Hacken is daarmee een dynamische activiteit, met een hoge mate van onvoorspelbaarheid. Daarbij geldt *high-risk-high-gain*.

Geaccepteerd zal moeten worden dat deze bevoegdheid improvisatie door de diensten vergt, toegesneden op de individuele casus, en dat daar dus ook juridische ruimte voor moet zijn. Wat ons betreft vraagt de operationele praktijk om niet al te rigide wetgeving voor hackoperaties, een meer flexibele (in juristenjargon: 'teleologische') interpretatie van regels als de technologische realiteit dat vergt, meer dynamische vormen – maar geen reductie – van toezicht, rolvast handelen door toezichthouders en gepast vertrouwen in de professionaliteit van betrokken hackers. Om het verder toe te spitsen: het toestemmingsniveau voor voorbereidende activiteiten (het zogeheten 'verkennen') zou intern bij de diensten moeten worden belegd en het abstractieniveau van de TIB-toets zou moeten worden verhoogd[9] door de omschrijving van de technische risico's te beperken tot enkel de direct voorzienbare. De TIB zou daarbij (meer) mogen vertrouwen op het vervolgtoezicht van de CTIVD.

5. Geautomatiseerde data-analyse (GDA)

Waar een inlichtingen- en veiligheidsdienst zich honderd jaar geleden kon beperken tot het in de gaten houden van het brief-, telegraaf- en telefoonverkeer van bepaalde targets, dient een moderne dienst zo nodig toegang te hebben tot het gehele digitale domein, met een grote variëteit aan communicatiemiddelen en bestanden, met bijbehorende beveiligingsmechanismen (zoals versleuteling en authenticatie).

---

5 Artikel 45 Wiv 2017.
6 Zie ook Adviesbrief inzake reële alternatieven voor rechtmatige toegang tot end-to-end versleutelde communicatie, anders dan inperking van encryptie van de Cyber Security Raad, d.d. 23 augustus 2022.
7 B.J. Koops e.a., *Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdiensten 20XX*, Tilburg 2016, p. 103.
8 Zie ook B.P.F. Jacobs & R.H.T. Jansen, 'Hoe hackers vastlopen. Over uitvoeringsproblemen bij hackoperaties van de politie en van de inlichtingen- en veiligheidsdiensten', *Computerrecht* 2024, afl. 1, p. 10-21.
9 Vergelijk ook B.P.F. Jacobs, 'Proportionaliteit en abstractie van gegevensverwerking', *Ars Aequi* 2023, afl. 4, p. 246-248.

Tegenwoordig is de hoeveelheid gegevens menselijkerwijs niet te omvatten en zijn geautomatiseerde mechanismen vereist om relevante informatie en gebeurtenissen te herkennen en te analyseren. Daarvoor is niet alleen informatie van targets nodig, maar ook van non-targets, juist om software goed te kunnen trainen, zodat een precies onderscheid kan worden gemaakt en foutieve classificatie en 'bias' worden voorkomen.

De Wiv 2017 kenmerkt sommige gegevensverwerkingen als 'GDA'. Het oorspronkelijke doel daarbij was om het gebruik van AI-technieken apart te reguleren. Zulk onderscheid tussen verschillende vormen van verwerkingen (zoals GDA en niet-GDA) is echter niet langer houdbaar en kan beter vervallen. In het algemeen zijn verschillende juridische benaderingen die zijn gebaseerd op technische verschillen niet goed werkbaar en ook snel achterhaald. Wij stellen een benadering voor die aansluit bij de AVG-systematiek: neem doelbinding en data-minimalisatie als uitgangspunt, waarbij de doelen heel concrete onderzoeksopdrachten van de dienst zijn, zoals een rapport over *dit* onderwerp of aanvalsbescherming van *die* infrastructuur. Op basis daarvan kan over het algemeen goed vastgesteld worden, zeker in de loop van de uitvoering, welke gegevens noodzakelijk zijn voor het gestelde doel. Die (minimale) noodzakelijkheid moet de rechtsgrond voor verwerking vormen.

De AIVD en de MIVD slaan de door hen verzamelde (bulk)gegevens op in een beschermde 'bak'. Omwille van de privacybescherming is toegang van dienstmedewerkers tot die bak beperkt via functiescheidingen. In de nieuwe wet zal geregeld moeten worden dat de medewerkers met toegang tot die bak daar ook software moeten kunnen trainen, ook met gegevens van non-targets, juist om goede classificaties (zoals targets en niet-targets) te kunnen maken. Vervolgens zullen de aanwijzingen van software die gegevens uit de bak analyseert een wettelijke grond moeten kunnen vormen voor selectie van gegevens uit die bak voor gebruik in het inlichtingenproces. Al deze verwerkingen vereisen *real-time* toezicht.

De commissie Jones-Bos raadt aan[10] dat de minister toestemming geeft voor de ontwikkeling van nieuwe technische functionaliteiten ten behoeve van GDA, en de CTIVD daarover informeert. Het is dan aan de CTIVD om mee te kijken bij het ontwerp, de ontwikkeling en de inzet van deze nieuwe functionaliteiten, gericht op zorgvuldige en afgewogen toepassing. Dit lijkt ons een adequate benadering, verbreed tot alle vormen van gegevensverwerkingen (en dus niet alleen GDA). Verdere regulering van verwerking zal generiek en doelgericht moeten zijn, los van de manier waarop de gegevens die geanalyseerd worden verkregen zijn.

6. Strategische operaties

Bij de totstandkoming van de Cyberwet is enige aandacht besteed aan het fenomeen 'strategische operaties'. Zulke operaties komen in verschillende werkvelden van de diensten voor. Het gaat dan niet zozeer om het verwerven van gegevens voor het beantwoorden van een concrete onderzoeksvraag of op basis van een acute dreiging, maar vooral om het opbouwen van een strategische positie zodat de diensten zich op toekomstige ontwikkelingen kunnen voorbereiden.[11] Strategische operaties zijn daarmee krachtige, maar gevoelige operaties met een lange looptijd. Wij achten het verkieslijk om

10 Aanbeveling 18 op p. 76.
11 Evaluatierapport, p. 96-97.

een expliciet wettelijk kader te ontwikkelen voor strategische operaties. Zo krijgen de diensten en de toezichthouders betere handvatten om te bepalen welke middelen en risico's – op eventuele nevenschade en op geopolitieke repercussies – toelaatbaar zijn.

7. Stelsel van toetsing, toezicht en klachtbehandeling

Het stelsel van toezicht op de AIVD en de MIVD is omvangrijk, maar ook gefragmenteerd.[12] Allereerst beoordelen de eigen ministers de voorstellen ('lasten') van de AIVD en MIVD om bijzondere bevoegdheden in te zetten. De TIB is gepositioneerd in de autorisatiefase en beoordeelt een last van de minister tot het inzetten van een bevoegdheid rechtmatig is. Dat is een *go/no go*-beslissing: als de TIB een reeds verleende ministeriële toestemming afkeurt, gaat de bevoegdhedeninzet niet door. Iets soortgelijks geldt voor de rechtbank Den Haag. Die rechtbank komt in beeld als het gaat om het openen van poststukken of om een voorgenomen bevoegdhedeninzet jegens een journalist of advocaat. Het toezicht op de taakuitvoering door de diensten is belegd bij de CTIVD. Sinds de inwerkingtreding van de Wiv 2017 bestaat deze instantie uit twee gescheiden afdelingen: de afdeling toezicht en de afdeling klachtbehandeling. Waar de afdeling klachtbehandeling bindende klachtbeslissingen kan nemen, kon de afdeling toezicht tot voor kort enkel rapporteren, signaleren en adviseren, maar niet interveniëren. De Algemene Rekenkamer ziet toe op de rechtmatigheid en de doelmatigheid van financiële huishouding van de diensten. De Commissie voor de Inlichtingen- en Veiligheidsdiensten van de Tweede Kamer buigt zich over operationele (dus staatsgeheime) aspecten van het inlichtingen- en veiligheidswerk, terwijl de Commissies voor Binnenlandse Zaken en voor Defensie toezien op alle andere aspecten. Nederlandse rechters buigen zich, ten slotte, incidenteel over bepaalde aspecten van de taakuitvoering door de diensten, en internationale rechters[13] schetsen in hun uitspraken soms kaders die ook voor Nederland relevant zijn.

De Cyberwet heeft het toezichtstelsel fundamenteel gewijzigd.[14] Kort en goed: de *ex ante*-toets door de TIB is op enkele punten geschrapt of ingeperkt, terwijl het *ex nunc*- en *ex post* toezicht is uitgebouwd met een bindende oordeelsbevoegdheid voor de CTIVD. Wat de TIB heeft verloren, heeft de CTIVD dus gewonnen. Vanwege de (potentieel) grote operationele impact van de toezichtbeslissingen kunnen de diensten voortaan procederen tegen zulke oordelen bij de Afdeling bestuursrechtspraak van de Raad van State. Deze wijzigingen beogen dynamisch toezicht mogelijk te maken. Op dit moment is dit nieuwe stelsel van toetsing en toezicht nog uitsluitend van toepassing op een bepaalde categorie cyberoperaties, maar het ligt in de lijn der verwachting dat dit breder wordt uitgerold in

12 Zie ook M. Hagens, 'Toezicht op de inlichtingen- en veiligheidsdiensten: een blik op het heden, het verleden en de toekomst', in E. Bakker e.a. (red.), *Terrorisme. Studies over terrorisme en terrorismebestrijding*, Deventer: Wolters Kluwer 2017, p. 555-594; M. Hagens, 'Toezicht in de Wiv 2017. Kansen en uitdagingen voor een effectief en sterk toezichtstelsel', *Justitiële Verkenningen* 2018, afl. 3, p. 85-98; R.H.T. Jansen, 'Toezicht onder de Wet op de inlichtingen- en veiligheidsdiensten 2017: een tour de force', *Nederlands Tijdschrift voor de Mensenrechten/NJCM-Bulletin* 2021, afl. 4, p. 419-443.

13 Met name het Europees Hof voor de Rechten van de Mens (EHRM) en in mindere mate ook het Hof van Justitie van de Europese Unie (HvJEU).

14 Zie over de spanningen in het toezichtstelsel Evaluatiecommissie Wiv 2017, hoofdstuk 9, en over de cyberwetwijzigingen R.H.T. Jansen, 'Van accentverschuiving naar stelselwijziging. Toezicht in het conceptvoorstel Tijdelijke cyberwet voor de AIVD en de MIVD, *Nederlands Juristenblad* 2022, afl. 30, p. 2406-2416 ; S.A.M. Harleman, 'Een tijdelijke Cyberwet maakt nog geen sleepwet', *Nederlands Juristenblad* 2022, afl. 38, p. 3120-3127.

de nieuwe Wiv. Feitelijk is de Cyberwet een tijdelijke experimenteerwet.[15] Alvorens het toezicht over de gehele linie te hervormen, is het daarom verstandig om na te gaan hoe de maatregelen uitpakken in de praktijk. Een dergelijk evaluatieonderzoek zal nog moeten plaatsvinden, maar wij verwachten dat dit een zinnige verschuiving van het toezicht is die beter aansluit bij de (dynamische) operationele praktijk. Wij achten deze verschuiving ook EVRM-*proof.*

Meer in algemene zin menen wij dat de huidige institutionele knip tussen de TIB enerzijds en de CTIVD anderzijds ongelukkig uitpakt. Tussen deze twee instanties bestaat een onhandige asymmetrie. De TIB kan operaties aan de poort stoppen, maar is geheel afhankelijk van de informatie die de diensten zelf aanleveren bij een lastaanvraag. De CTIVD heeft daarentegen toegang tot alles en iedereen, maar kan bij geconstateerde onrechtmatigheden (meestal) niet zelf interveniëren. De semi-rechterlijke status van de TIB schept daarnaast nodeloze onduidelijkheden: de TIB is geen rechterlijk college, dat in individuele gevallen beslist, maar evenmin een toezichthouder, die met de ondertoezichtgestelden meedenkt. De onderlinge verhouding tussen deze instanties is bovendien niet goed doordacht.[16] Wij menen dat het beter past om de toetsingstaken van de TIB te beleggen bij een afzonderlijke afdeling van de CTIVD. Het nieuwe artikel 13 Grondwet over het communicatiegeheim maakt het mogelijk om de toetsingstaak van de rechtbank Den Haag eveneens over te hevelen naar die nieuw op te richten afdeling.[17] Het zoveel mogelijk concentreren van de toetsing en het toezicht bij één instantie komt de rechtseenheid en daarmee de rechtszekerheid en de rechtsgelijkheid ten goede. Ook zou het samenvoegen van de TIB en de CTIVD de stabiliteit, afstemming en samenwerking op het personele vlak kunnen vergroten.

Ter bescherming van grondrechten zou de samengevoegde toezichtinstantie, in het voetspoor van de Cyberwet, de bevoegdheid moeten krijgen om operaties (tijdelijk) stil te leggen en eventueel het wissen van bepaalde gegevens af te dwingen. Met de Evaluatiecommissie Wiv 2017 zijn wij evenwel van mening dat het niet alleen praktisch onwenselijk, maar ook principieel niet juist zou zijn dat de toezichthouder het laatste woord krijgt over de uitleg van wettelijke normen, de toetsingsintensiteit én de toepassing van die normen in concrete situaties.[18] Wij ondersteunen daarom het idee van een beroepsprocedure bij de Afdeling bestuursrechtspraak van de Raad van State of bij een ander rechterlijk college, zoals aanvankelijk voorgesteld door de Evaluatiecommissie Wiv 2017 en inmiddels voor bepaalde operaties verankerd in de Cyberwet.

De voornoemde wijzigingen nopen wat ons betreft tot het verplaatsen van de klachtbehandelingstaak. Het behandelen van klachten over (vermeend) optreden van de AIVD en de MIVD zou volgens ons moeten worden weggehaald bij de CTIVD, om een

---

15 B.P.F. Jacobs & R.H.T. Jansen, Position paper t.b.v. rondetafelgesprek over de Tijdelijke wet cyberoperaties, d.d. 23 maart 2023.
16 Zie ook E.R. Muller & W.J.M. Voermans, 'Nieuwe wet op de Inlichtingen- en Veiligheidsdiensten. Een nieuw evenwicht tussen veiligheid en waarborgen', *Nederlands Juristenblad* afl. 2, p. 102-109 aldaar m.n. p. 107-108; *Kamerstukken II* 2022/23, 34 588, nr. 92, p. 24.
17 Zie ook R.H.T. Jansen, 'De modernisering van artikel 13 Grondwet. Een techniekonafhankelijke bescherming van het communicatiegeheim', in: J.H. Gerards, J. Goossens & E.Y. van Vugt (red.), *Constitutionele verandering in Nederland?*, Den Haag: Boom juridisch 2023, p. 175-202 aldaar m.n. p. 193-196. Met daarbij overigens de uitzondering voor de taak met betrekking tot journalisten, die overeenkomstig Europese jurisprudentie bij een rechter moet liggen.
18 Vergelijk ook Evaluatiecommissie Wiv 2017, *Evaluatie 2020*, Den Haag 2021, p. 134-137.

stapeling en mogelijk vermenging van uiteenlopende toezichttaken (de 'dubbele-petten-problematiek') te voorkomen. Het ligt in de rede om de klachtbehandeling te beleggen bij het Hoge College van Staat dat speciaal is opgericht om op te komen voor de belangen van burgers en dat daartoe ook goed geoutilleerd is: de Nationale ombudsman. In het verleden is van regeringszijde wel aangevoerd dat zoiets lastig zou zijn, omdat de ombudsman geen toegang heeft tot staatsgeheime informatie. Dat argument overtuigt niet. Men kan zoiets immers ondervangen door een of meerdere medewerkers van de ombudsman conform de Wet veiligheidsonderzoeken te screenen en een eenzelfde toegang (op locatie) tot de diensten te geven als de CTIVD. De onafhankelijkheid van de klachtbehandelaar staat dan buiten kijf, waardoor deze procedure zonder twijfel de toets aan het EVRM kan doorstaan.[19]

8. Naar een Wet op de nationale veiligheid

Het nationale veiligheidsdomein is breder dan alleen het werkveld van de AIVD en de MIVD. Een andere invloedrijke speler is de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De gebrekkige rechtsgrondslagen van zijn activiteiten hebben de afgelopen jaren meermaals tot publieke en politieke discussie geleid. Inmiddels is de Wet coördinatie terrorismebestrijding en nationale veiligheid van kracht. Deze wet regelt de verwerking van (persoons)gegevens door de NCTV, maar bevat ook een eigenstandige verwervingsbevoegdheid: het verrichten van openbronnenonderzoek voor trend- en fenomeenanalyses. De komst van die wet is in die zin een stap vooruit, dat er voorheen geen duidelijke grondslag was en nu wel. Tegelijkertijd is voor de NCTV een gefragmenteerde toezichtconstellatie met een belangrijke rol voor de Autoriteit Persoonsgegevens opgetuigd, die afwijkt van de Wiv 2017 en waarin de CTIVD geen enkele rol speelt. Dat bestendigt het juridische en departementale silodenken, waarin de diensten en de NCTV los van elkaar opereren.

Wat ons betreft is deze situatie op de lange termijn niet houdbaar.[20] De activiteiten van de NCTV zijn in belangrijke mate verknoopt geraakt met die van de AIVD en de MIVD. Gelet op de verdere doorontwikkeling van informatietechnologie en toenemende datadelingsmogelijkheden is doorlopend toezicht op informatiestromen in het nationale veiligheidsdomein wat ons betreft noodzakelijk om de grondrechten van burgers effectief te kunnen beschermen. Wij raden dan ook aan om de AIVD, de MIVD en de NCTV onder te brengen in één wettelijk kader. Dat kan worden bewerkstelligd door de Wiv 2017 om te dopen tot een 'Wet op de nationale veiligheid' of door een separate Kaderwet nationale veiligheid tot stand te brengen, waarin de overkoepelende uitgangspunten voor het verwerven, verwerken en verspreiden van (persoons)gegevens binnen dit domein worden uitgewerkt. Ook een deel van het politiewerk, met name daar waar het hacken en strategische operaties betreft, zou hier onder kunnen vallen of zou op vergelijkbare wijze gereguleerd kunnen worden. Activiteiten die min of meer hetzelfde behelzen, zoals verschillende vormen van digitale surveillance en internetmonitoring, zullen dan ook op dezelfde wijze zijn genormeerd en dus met dezelfde waarborgen zijn omkleed. Bovendien

19 Zie ook R.H.T. Jansen, 'Big Brother Watch e.a., Centrum för Rättvisa en het toezicht op de inlichtingen- en veiligheidsdiensten', *Computerrecht* 2022, afl. 2, p. 97-109 aldaar m.n. p. 108.
20 Zie ook M.F.H. Hirsch Ballin, 'Als een spin in het web voor de bestrijding van terrorisme en zware criminaliteit', *Tijdschrift voor Constitutioneel Recht* 2022, afl. 2, p. 1-26; R.H.T. Jansen, 'Less is more? Over het grondslagenvraagstuk van de Nationaal Coördinator Terrorismebestrijding en Veiligheid', *Nederlands Juristenblad* 2024, afl. 9, p. 588-599.

wordt zo doorlopend toezicht op het gehele systeem van nationale veiligheid mogelijk. Met haar diepgaande domeinkennis en royale onderzoeksmogelijkheden is de CTIVD daartoe het best geëquipeerd, in elk geval beter dan de reeds overbelaste Autoriteit Persoonsgegevens.

9. Regelcomplexiteit en overgangsrecht

De Wiv 2017 is een complexe wet voor een nog veel complexere praktijk. De Cyberwet heeft de juridische complexiteit verder vergroot. Enige complexiteit is in dit domein, uit de aard der zaak, onvermijdelijk.[21] De wetgever zou de invoering van een Wet op de nationale veiligheid kunnen aangrijpen om een frisse start te maken met heldere, technologieneutrale kaders. Het 'dichtmetselen' van juridische begrippen in de toelichtende parlementaire stukken, zoals bij de Cyberwet is gebeurd, verdient dan ook geen navolging. Open normen en teleologische interpretatie zijn nodig om wetgeving bij de tijd te kunnen houden, zeker omdat het hier gaat om het reguleren van overheidshandelen in een zeer veranderlijke technologische context.[22] Wij roepen de wetgever op om de bestaande reflex van 'eng, dus méér regels en méér toezicht' te overstijgen en om te zetten in een benadering gericht op gecontroleerde daadkracht.

Tot slot. Bij de invoering van Wiv 2017 ontbrak overgangsrecht. Vanaf dag één moesten de diensten dus handelen naar de nieuwe wet, inclusief de nieuwe privacywaarborgen, terwijl 'de winkel open moest blijven'. Dat heeft geleid tot allerhande praktische problemen en een soepele overgang naar het nieuwe wettelijke regime in de weg gestaan.[23] Voor de invoering van de beoogde nieuwe wet achten wij uitvoeringstoetsen en overgangsrecht dan ook noodzakelijk. Wat ons betreft is het aanbevelenswaardig om ook ditmaal de wetsimplementatie te laten monitoren door de CTIVD.[24]

21 Zie ook J.J. Oerlemans & M. Hagens, 'De Wet op de inlichtingen- en veiligheidsdiensten 2017: een technologisch gedreven wet', *Computerrecht* 2018, afl. 3, p. 130-141; J.J. Oerlemens & M. Hagens, 'Privacy en bulkinterceptie in de Wiv 2017', *Ars Aequi* 2019, afl. 7/8, p. 560-568.
22 Zie ook Raad van State, *Regelcomplexiteit. Een verkenning aan de hand van twee casestudy's*, Den Haag 2023.
23 Algemene Rekenkamer, *Slagkracht AIVD en MIVD*, Den Haag 2021, p. 57-60. Vgl. Evaluatiecommissie Wiv 2017, p. 149.
24 Zie de CTIVD-Voortgangsrapportages I (2018) tot en met IV (2020).