

I Een nieuwe wet

16 juni 1994 is een dag die geschiedenis maakte in de wereld van de Nederlandse inlichtingendiensten. Die dag werd een barstje geschoten in de dikke muren van het bolwerk van de Binnenlandse Veiligheidsdienst. Dankzij een uitspraak van de Raad van State werd het mogelijk om, onder voorwaarden, inzage te krijgen in gegevens die de BVD verzameld had. De uitspraak was gebaseerd op een uitspraak van het Europees Hof van de Rechten van de Mens uit 1993, die niet alleen zorgde voor de mogelijkheid tot inzage, maar ook eisen stelde aan de democratische controle op inlichtingendiensten en harde voorwaarden stelde aan het toepassen van speciale onderzoeksmethoden. Het was inlichtingendiensten hierdoor niet langer mogelijk om ongecontroleerd hun gang te gaan, zoals de praktijk tot op dat moment was.

Nadat de eerste paniek enigszins weggeëbd was, besloot de regering tot een korte periode van bezinning. Deze bezinning leidde uiteindelijk tot het besluit een nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten (WIV) op te stellen. De eerste versie is op 7 februari 1998 naar de Tweede Kamer gestuurd om, na twee gewijzigde versies, in 2001 behandeld te worden. In 2002 ging ook de Eerste Kamer akkoord. En op 29 mei 2002 trad de nieuwe wet in werking. De BVD werd die dag AIVD.

De Nederlandse burger komt er in de WIV beroerd af. De uitspraak van de Raad van State, die negatief was voor de inlichtingendiensten, wordt in hun voordeel aangewend. De bijzondere bevoegdheden van de AIVD en de Militaire Inlichtingendienst (MID) (affluisteren, inbreken, infiltreren en dergelijke) worden zo ruim mogelijk gedefinieerd, terwijl de controle op de praktijken van de diensten op een bedroevend laag niveau blijft hangen. Verder is de burger nauwelijks in staat om zijn recht te halen tegen onrechtmatig handelen.

Wat verandert er zo al?

Een eerste verandering is de naam: BVD en MID verdwenen en

werden omgedoopt in Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Deze naamswijziging is bedoeld om de vlag de lading te laten dekken, namelijk dat beide diensten zich wijden aan zowel veiligheids- als inlichtingenwerk.

De meest ingrijpende verandering is dat de uitstraling en beschrijving van bevoegdheden veel offensiever is dan voorheen. De AIVD moet een dienst zijn die midden in de maatschappij staat en daar ook een duidelijk sturende invloed op moet hebben. De BVD was – althans officieel – een inlichtingendienst die een goede informatiepositie moest hebben op het gebied van mogelijke bedreigingen van de Nederlandse status-quo. In zekere zin is deze verandering echter een formalisering van de huidige praktijk, aangezien de BVD al langer actief stuurde in het maatschappelijk en politiek leven.

Met de nieuwe wet is dit echter een stuk gemakkelijker geworden. Een aantal wettelijke beperkingen waar de BVD en met name de MID mee te maken hadden, is namelijk geschrapt. De taakstelling beperkt zich niet langer tot het in de gaten houden van groepen, personen en ontwikkelingen die een gevaar zijn voor de staat, er wordt nu bijvoorbeeld ook gesproken over daadwerkelijk ingrijpen door een inlichtingendienst om aan geconstateerde bedreigingen van de staat het hoofd te bieden.

Verder is ook de samenwerking met politie en justitie geregeld. De afgelopen jaren bleek dit altijd een bron van ruzie en ergernis: allerlei informatie die justitie wilde hebben om een zaak rond te kunnen maken, hield de BVD voor zichzelf, omdat anders mogelijk zijn eigen activiteiten schade oplepen. In de nieuwe wet is nu formeel geregeld dat de dienst een aanspreekpunt bij justitie krijgt om melding te maken van strafbare feiten die men tijdens het doen van onderzoek is tegengekomen. Bovendien regelt de wet wanneer de inlichtingendiensten tot melding van strafbare feiten moeten overgaan. Overigens bestaat er momenteel al een dergelijk aanspreekpunt in de persoon van de landelijke hoofdofficier van justitie voor de inlichtingendiensten, maar met de nieuwe wet krijgt dit aanspreekpunt een wettelijke basis.

Bijzondere bevoegdheden

Met de nieuwe wiv is er het een en ander veranderd in de bevoegdheden van de inlichtingendiensten. Met name de mivd heeft er een flink aantal bijzondere bevoegdheden bijgekregen en is wat dit betreft gelijk getrokken met de aivd. Opvallend aan dit deel van de wet is dat het zozeer lijkt op het ideale verlanglijstje van een inlichtingendienst dat het bijna niet anders kan dan dat het door de inlichtingendiensten is ingefluisterd. Zo is het mogelijk om zonder rechterlijke toestemming het briefgeheim te schenden. Hiervoor moet zelfs de grondwet worden gewijzigd. Argument voor deze radicale verandering is dat de bvd geen brieven mag openen, maar wel e-mail mag lezen. Was er voor een telefoontap altijd toestemming nodig van drie ministers, nu volstaat de toestemming van de voor de dienst verantwoordelijke minister, waarmee de minimale controle nog minimaler wordt. Voor de aivd is de minister van Binnenlandse Zaken, voor de mivd de minister van Defensie verantwoordelijk.

Het lijkt dat, gevolg gevend aan de uitspraak van het Europees Hof, de bevoegdheden duidelijk zijn geregeld. Dat is helaas niet waar. Ondanks de uitdrukkelijke Europese verplichting, is in de nieuwe wet niet duidelijk te lezen wanneer een burger te maken kan krijgen met welke bijzondere bevoegdheid. Het blijft dus onduidelijk hoe je je moet gedragen om niet het slachtoffer te worden van schendingen van mensenrechten door de inlichtingendiensten.

De bijzondere bevoegdheden worden in de nieuwe wiv uitputtend opgesomd. Het gaat hierbij grotendeels om een legalisatie van de bestaande praktijk. Aanvankelijk bevatte het wetsvoorstel nog een restartikel dat de aivd de bevoegdheid gaf nieuwe bijzondere bevoegdheden te introduceren en die pas na een jaar aan de Tweede Kamer bekend te maken. Dit artikel is in een nota van wijziging van 19 maart 2001 vervallen omdat het de regering duidelijk was geworden dat dit onderdeel in tegenspraak was met het Europees Verdrag voor de Rechten van de Mens en zou sneuvelen bij een eventuele rechtszaak.

De inlichtingendiensten mogen *observeren en volgen*. Ze mogen personen en goederen observeren, al dan niet met behulp van observatie- en registratiemiddelen. Verder mag er gevolgd worden, al dan niet met behulp van volgmiddelen, plaatsbepalingsapparatuur en registratiemiddelen. Observatie- en volgacties mogen met toestemming van het hoofd van de dienst plaatsvinden. Wanneer echter geobserveerd wordt door apparatuur te plaatsen in een woning, hebben de diensten toestemming van de minister nodig. Het betreft video- en fotoapparatuur, (elektronische) kijkers, beeldversterkers en allerhande plaatsbepalingsinstrumenten, waaronder peilbakens en GSM-telefoons. Ook kunnen combinaties van GPS (Global Positioning System, een computer die met behulp van satellietsignalen zeer precies de plaats op aarde kan bepalen) en GSM worden ingezet, waarbij de lokatie van een object bepaald wordt door GPS en vervolgens aan de observant wordt doorgegeven door een daaraan gekoppelde GSM-telefoon.

Om goed te kunnen *infiltreren* mogen agenten van inlichtingendiensten zonder verdere controle valse identiteiten aannemen en met valse papieren door het leven gaan. Deze infiltranten mogen strafbare feiten plegen en zullen hiervoor niet gestraft worden. Er wordt in de wet geen beperking gesteld aan de te plegen misdaden. In principe mag de agent dus alles. Als excuus wordt aangevoerd dat een infiltrant anders te testen zou zijn: wanneer hij erop uit wordt gestuurd om een moord te plegen en dit weigert, zou hij kunnen worden ontmaskerd. Dit is op zijn zachtst gezegd wel een zeer eenzijdig scenario.

De infiltrant is bovendien niet alleen een informatieverzamelaar. Hij kan ook maatregelen nemen ter bescherming van door de betrokken dienst te behartigen belangen, zoals het kapotmaken van een organisatie door onderlinge ruzies te creëren of te bevorderen.

Inlichtingendiensten mogen *inbreken in woningen*, maar moeten hier schriftelijke toestemming van de betrokken minister voor hebben. Hier geldt echter een aantal uitzonderingen op:

wanneer er ingebroken moet worden om af luister- of video-apparatuur aan te brengen, om peilzenders aan te brengen, om de woning te doorzoeken, om een computer te doorzoeken of om communicatieapparatuur te onderzoeken, dan mogen zij dit doen zonder verdere toestemming. In feite zijn hiermee nagenoeg alle redenen om een woning binnen te dringen opgesomd, en is er in de praktijk dus nauwelijks verdere toestemming voor inbraak nodig.

Het *briefgeheim* is in de wiv niet langer heilig. Tot nu toe mochten de inlichtingendiensten, zonder gerechtelijke toestemming, alles met een brief, behalve hem openmaken. Met toestemming van de rechter mag een brief wel worden geopend. Ook deze controle zal, als het aan de minister ligt, uit de wet verdwijnen, waarmee alleen nog formele toestemming van een minister nodig zal zijn om een brief te openen. Daarvoor moet een Grondwetswijziging komen, die momenteel al in behandeling is.

De diensten mogen *computers hacken* om toegang te krijgen tot opgeslagen informatie of om het versleutelen van gegevens tegen te gaan. Te denken valt aan het installeren van 'geheime' programma's, die een gebruiker niet ziet, maar die ondertussen allerlei gegevens, zoals wachtwoorden, doorgeven aan de dienst.

De diensten mogen *communicatie aftappen en opnemen*, inclusief telefoongesprekken en conversaties in de kroeg en andere openbare plaatsen. Hiervoor is toestemming nodig van een minister. De diensten mogen alle communicatie die door de ether loopt opnemen. Volgens de nieuwe wiv moest een nummer vermeld worden in de tap-aanvraag. Als het aan de diensten gelegen had, was het mogelijk hier alle mogelijke nummers op te geven (naast telefoonnummers, ook typenummers van GSM-toestellen of identificatienummers van Pentium III-processoren). Dit plan is echter gesneuveld: nummer betekent in dit geval telefoonnummer.

Om iets aan deze enorme baal aan gegevens te hebben, moeten de bruikbare gegevens eruit gefilterd worden. Voor *selectie* van deze gegevens (op verzender of ontvanger, op inhoud of op bijvoorbeeld telefoonnummer) is toestemming nodig van een minister. De AIVD kan bovendien iemand verplichten mee te werken aan het ontsleutelen van een gecodeerd bericht.

De AIVD mag draadloos verzonden berichtenverkeer dat oorsprong of bestemming in het buitenland heeft, (elektronisch) *doorzoeken* op inhoud. Dat wil zeggen dat al deze communicatie mag worden opgevangen en met behulp van computers gefilterd kan worden. De filters die worden toegepast, kunnen communicatie selecteren op basis van persoons- of technische kenmerken (bijvoorbeeld stemherkenning of GSM-nummer), op basis van trefwoorden en dergelijke. Hiervoor is geen ministeriële toestemming nodig. Volgens de Raad van State zou deze bevoegdheid strijdig kunnen zijn met de grondwet. De minister van Binnenlandse Zaken Bram Peper ontkende dit. Door te searchen zouden de diensten namelijk geen kennis nemen van de volledige communicatie. Daarom zou deze speciale bevoegdheid te vergelijken zijn met het doen van technische controles door de telecommunicatieleverancier, waarbij ook niet uitgesloten kan worden dat (delen van) gesprekken worden opgevangen. Bovendien zou er niet van tevoren om toestemming kunnen worden gevraagd, aangezien de diensten niet van tevoren weten waarnaar ze op zoek zijn: er wordt immers in het wilde weg gezocht naar interessante informatie of interessante personen, zonder dat vooraf vaststaat óf dergelijke informatie wel aanwezig is. Wanneer de diensten op basis van gesearchte informatie besluiten communicatie van een specifieke persoon verder op te vangen, is hiervoor wel toestemming nodig. Zo kunnen berichten met een bepaalde inhoud of van een bepaalde persoon opgespoord worden zonder dat van tevoren vaststaat dat dit bericht bestaat.

Ook mag de AIVD alle niet-kabelgebonden telecommunicatie (waaronder GSM-verkeer) doorzoeken aan de hand van identiteiten, nummers en trefwoorden. De opgevangen

gegevens mogen een jaar bewaard worden. Wanneer het om versleutelde berichten gaat, mag de communicatie bewaard worden tot een jaar nadat de dienst deze heeft ontsleuteld. Voor het gebruik van deze trefwoorden is geen toestemming nodig. Een keer per jaar krijgt de minister achteraf een lijst onder ogen.

De Inlichtingendiensten kunnen *gegevens opvragen* over wie er met wie heeft gebeld (*log-files*) of op wiens naam een telefoonnummer staat. *Log-files* bevatten alle data van een bepaald telecommunicatienummer: welke nummers er vanaf dit nummer gebeld zijn, welke nummers dit nummer hebben gebeld en hoe lang de gesprekken hebben geduurd. Opmerkelijk is dat ook gegevens moeten worden verstrekt van oproepen die niet tot een verbinding hebben geleid (in gesprek, afgesloten nummer, niet thuis). *Log-files* kunnen zowel voor een periode in de toekomst als met terugwerkende kracht door de diensten worden opgevraagd.

Ten slotte mag de AIVD zich wenden tot eenieder die over gegevens beschikt die voor de diensten van belang kunnen zijn. De Bevolkingsadministratie, Postbank, Albert Heijnbonuscardadministratie, de videobanden van cameratoezicht in een station, dit alles en nog veel meer kan probleemloos worden opgevraagd.

Cryptografie

Cryptografie – de techniek van het versleutelen en ontsleutelen van gegevens – neemt een bijzondere plaats in de wet in. Dit heeft te maken met de grote bedreiging die de inlichtingendiensten in het gebruik van encryptie – het versleutelen – zien. Wanneer men zich op grote schaal bedient van sterke versleutelingstechnieken, wordt het werk voor de diensten een stuk moeilijker. Om die bedreiging het hoofd te bieden is in de wiv een aantal kunstgrepen toegepast.

Ten eerste hebben de diensten op een aantal plaatsen toestemming gekregen om encryptie ongedaan te maken. Wanneer zij telecommunicatie aftappen, hebben zij ook de

bevoegdheid om versleuteling ongedaan te maken en zijn telecommunicatieleveranciers verplicht om versleuteling die de leveranciers hebben aangebracht, ongedaan te maken. Ook bij het scannen (het ongericht ontvangen en opnemen van niet-kabelgebonden telecommunicatie) hebben de diensten de bevoegdheid gekregen om versleuteling ongedaan te maken. Dit gaat om algemeen gebruikte encryptie (zoals het GSM-protocol voor de mobiele telefonie), maar ook om door personen of organisaties zelf aangebrachte versleuteling. Of de diensten van deze bevoegdheid gebruik kunnen maken, is in dat geval afhankelijk van de technische mogelijkheden, de kracht van het gebruikte encryptie-algoritme (de reken-techniek die gebruikt is om te versleutelen) en het kennisniveau van de betreffende dienst. Wanneer een sterk encryptie-algoritme is gebruikt, zal het niet eenvoudig zijn een verkregen bericht te ontcijferen. Dit is slechts mogelijk wanneer daar voldoende rekenkracht of kennis tegenover staat. Deze kennis kan bijvoorbeeld bestaan uit technische details over hoe dergelijke encryptie gekraakt moet worden, maar kan ook betrekking hebben op kennis van het wachtwoord.

Ten tweede is toestemming gegeven om (tijdens een hack-actie door de diensten) in een computer aangebrachte of nog aan te brengen cryptografie-programmatuur te corrumperen, of om sleutels te achterhalen waarmee door de diensten zelf ontsleuteld kan worden.

Ten derde spreekt de wet op verschillende plaatsen over de medewerkingsplicht om te ontsleutelen. Opmerkelijk is de luchtigheid waarmee dit gebeurt. Er wordt alleen gerept over de verplichting mee te werken aan ontsleuteling van versleutelde berichten of bestanden. Wanneer iemand medewerking weigert, kan dit de weigeraar een gevangenisstraf opleveren, zelfs wanneer de weigering niet opzettelijk is. Het gebrek aan uitleg in de Memorie van Toelichting is vreemd, aangezien medewerkingsplicht aan ontsleuteling van (eigen) berichten in de praktijk moeilijk uitvoerbaar is. Hoe kan immers iemand meewerken die zijn eigen wachtwoord vergeten is of zijn codesleutel is kwijtgeraakt? En hoe verhoudt deze verplichting zich met het grondrecht om niet mee te hoeven

werken aan zijn eigen veroordeling? Wanneer iemand gedwongen wordt om een bericht te ontsleutelen en het blijkt dat daarin sprake is van strafbare feiten, is er een probleem. In dat geval blijkt men achteraf een verdachte gedwongen te hebben om mee te werken aan zijn eigen veroordeling.

Notificatie

Wanneer de dienst gebruikt maakt van het schenden van het briefgeheim, aftappen van telecommunicatie of inbraak, zal na vijf jaar bekeken worden of het slachtoffer van deze activiteiten hiervan in kennis kan worden gesteld (notificatieplicht). Overigens is de plicht in de wet ver te zoeken. Mocht de dienst tot de conclusie komen dat dit niet kan worden medegedeeld, dan moet een jaar later bekeken worden of er nu wel genotificeerd kan worden. De diensten kunnen echter afzien van notificatie indien het melden van gebruik van een bevoegdheid ertoe zou kunnen leiden dat bronnen van de dienst, toepassingen van gebruikte methoden of de identiteit van personen die de dienst geholpen hebben, onthuld kunnen worden, dan wel dat betrekkingen met andere landen geschaad kunnen worden.

Buitenland

De relatie met de buitenlandse zusterdiensten wordt als een belangrijk argument gebruikt voor alle geheimzinnigheid rond de BVD ('wij zouden nog wel willen, maar als we iets moeten blootgeven, krijgen we nooit meer informatie'). De buitenlandse diensten kunnen zich echter beter zorgen maken over de nieuwe taken van de AIVD dan over een deugdelijk democratisch toezicht in Nederland. De dienst is na aanvaarding van de nieuwe wet op diverse manieren actief geworden in het buitenland.

In 1994 werd de Inlichtingendienst Buitenland (IDB) na een reeks van schandalen opgeheven. De buitenlandse inlichtingentaak (spionage) kwam daarmee in een vacuüm terecht. Het militaire deel bleef een taak van de MID en de BVD, die altijd al een concurrerende taak ten opzichte van de IDB voor zichzelf zag, sprong ook voor een deel in dat gat. Met de

nieuwe wet in aantocht wordt deze spionagetaak geformaliseerd. De dienst krijgt daarvoor honderd medewerkers (ongeveer het dubbele van de IDB) en een aparte ruimte in een kantoorgebouw buiten het AIVD-complex.

In een nota van wijziging van 19 maart 2001 is economische spionage, na een stroom van kritiek van de parlement fracties van GroenLinks, D66, CDA en PVDA, weer uit de wiv gehaald. Verder is kritiek van de Europese Commissie op deze bevoegdheid een reden om het te schrappen. Of dit de AIVD daadwerkelijk van het economisch spioneren af kan houden, is nog maar de vraag. Minister van Binnenlandse Zaken Klaas de Vries licht het besluit namelijk als volgt toe: 'Bij de introductie van het overkoepelende begrip "nationale veiligheid" in de taakstelling van de AIVD heeft de regering zich op het standpunt gesteld dat het begrip "nationale veiligheid" ruim mag worden uitgelegd en dat de genoemde activiteiten onder het begrip "nationale veiligheid" zijn te vatten. Voor zover er niettemin enige twijfel zou kunnen bestaan of het verrichten van onderzoeken die gerelateerd zijn aan vitale economische belangen van Nederland wel onder het begrip "nationale veiligheid" vallen, is besloten die twijfel weg te nemen door te komen tot een explicitering van de vitale economische belangen in de omschrijving van de inlichtingentaak buitenland van de AIVD. Inmiddels is, vanwege de misverstanden die dit onderdeel van de taakomschrijving bleek op te roepen, besloten de vitale economische belangen als afzonderlijk bestanddeel van de taakomschrijving te schrappen, met de aantekening dat onderzoek naar dit soort onderwerpen wel mogelijk is als het belang van de nationale veiligheid in het geding is.'

Inzage

Een van de aanleidingen om de nieuwe wiv te schrijven was, zoals gezegd, de uitspraak van de Raad van State in 1994 waardoor het in beperkte mate mogelijk werd je eigen BVD-dossier in te zien. De nieuwe wet volgt in grote lijnen de praktijk zoals die er nu na een aantal gerechtelijke uitspraken ligt. Er moet aan een aantal voorwaarden zijn voldaan wil je inzage krijgen in je eigen dossier. Ten eerste moeten de te verstrekken

gegevens meer dan vijf jaar oud zijn. Ten tweede mag over de aanvrager de afgelopen vijf jaar geen nieuwe informatie zijn geregistreerd over het onderwerp waarin inzage wordt gevraagd. Ten derde mogen de gegevens niet relevant meer zijn voor enig ander lopend onderzoek. Ten vierde moeten de bronnen en de werkwijze van de dienst geheim blijven. Daarnaast kan inzage worden geweigerd als zich een van de vele weigergronden van de Wet Openbaarheid van Bestuur (wob) voordoet.

Aanvankelijk wilde de minister ook een juridisch unicum creëren. Bij eventuele inzage mochten geen aantekeningen of kopieën worden gemaakt, noch mocht men een raadsman meenemen. Dit is echter in een nota van wijziging uit de wet gehaald toen ook dit niet haalbaar in Europa bleek te zijn.

Vanaf 1994 konden journalisten en historici inzage krijgen in in historisch opzicht belangrijke persoons-dossiers. In 1995 sloot de Raad van State deze inzagemogelijkheid echter weer af: eerst moest er een deugdelijke regeling komen. De nieuwe wet handhaaft de blokkade van 1995 en maakt daarmee inzage door journalisten en historici onmogelijk. In de nota van wijziging van 19 maart 2001 is nog een kleine geste gemaakt ten aanzien van inzage door derden. Familieleden in de eerste lijn kunnen inzage krijgen in het dossier van een overleden familielid als is voldaan aan de eerder opgesomde voorwaarden.

Klachtrecht

Een ander punt dat uiteindelijk waarschijnlijk af zal ketsen bij toetsing door de rechter is de manier waarop het klachtrecht is geregeld. Het Europees Hof heeft vastgesteld dat een instantie die klachten over geheime diensten onderzoekt, een sanctiebevoegdheid moet hebben. Met andere woorden, de beklagde inlichtingendienst moet door de onderzoeker van de klacht gedwongen kunnen worden om te luisteren. Daarnaast moet er een hoger beroep mogelijk zijn voor een klager. In de nieuwe wiv is de Nationale Ombudsman aangewezen als instantie die de klachten over de inlichtingendiensten moet onderzoeken. De Ombudsman kan wettelijk

gezien echter niets anders doen dan een klacht onderzoeken en zijn mening over het gebeurde geven. De beklagde instantie kan deze uitslag vervolgens volledig naast zich neerleggen. Wanneer een klager het niet eens is met de beslissing van de Ombudsman, kan hij geen hoger beroep aantekenen.

De regering interesseert zich niet echt voor dit probleem. Op kritiek van het GroenLinks-kamerlid Tara Oedayraj Sing Varma antwoordde minister Klaas de Vries op 19 maart 2001: 'Naar onze mening doet de fractie van GroenLinks de Nationale Ombudsman te kort, als zij stelt dat deze geen zinvolle rol kan spelen, alleen omdat hij niet bevoegd is tot bindende uitspraken en geen daadwerkelijke rechtsmiddelen kent. Op geen enkel terrein bezit de Nationale Ombudsman deze bevoegdheden en toch heeft hij zijn waarde sinds zijn instelling naar de mening van de regering meer dan bewezen. Bestuursorganen die door de Nationale Ombudsman op de vingers getikt worden, nemen over het algemeen de door de Ombudsman voorgestelde maatregelen over om te voorkomen dat hen dat een tweede maal overkomt. Wij zien vooralsnog geen enkele reden dat dat in het geval van de inlichtingen- en veiligheidsdiensten anders zal zijn.'

Naast allerlei nieuwe bevoegdheden is er ook heel wat veranderd in het ambtelijk apparaat. Door het invoeren van een aantal nieuwe functies moeten de inlichtingendiensten de toets van het Europees Hof van de Rechten van de Mens doorstaan.

Allereerst komt er een Commissie van Toezicht, die moet controleren of de diensten en hun medewerkers zich aan de wet houden en of zij hun werk goed doen. De commissie kan echter uitsluitend achteraf controleren en doet dit onder strikte geheimhouding. Ze moet bestaan uit drie leden die door de regering voor een periode van zes jaar worden benoemd. Zij krijgt een eigen secretariaat. De commissie moet de rechtmatigheid van de activiteiten van de inlichtingendiensten onderzoeken. Daartoe krijgt ze toegang tot alle informatie, gebouwen en personen die van belang zijn voor dat onderzoek. Medewerkers van de diensten kunnen zich niet op hun zwijgrecht beroepen en kunnen onder ede worden gehoord.

Een andere vernieuwing is het aanstellen van een coördinator van de inlichtingen- en veiligheidsdiensten. Deze functie wordt momenteel bekleed door de secretaris-generaal van het ministerie van Algemene Zaken, maar krijgt hiermee een wettelijke status. De rol van deze coördinator is die van een spin in het web. Hij bereidt de ministeriële vergaderingen over de inlichtingendiensten voor, coördineert de taken van de diensten en is de voorzitter van het Comité Verenigde Inlichtingendiensten Nederland (CVIN). Het CVIN is de ambtelijke laag tussen de inlichtingendiensten en de regering.

De regering en de AIVD presenteren de nieuwe wet als een grote stap voorwaarts. Er wordt duidelijkheid gegeven wat de AIVD op welk moment tegen wie mag doen. Er wordt vastgelegd hoe informatiestromen naar binnen en naar buiten lopen. De controle, de inzage en het klachtrecht zijn goed geregeld.

Als deze wet evenwel één ding duidelijk maakt, dan is het niet wát de AIVD en de MIVD mogen, maar dat de AIVD en MIVD álles mogen.

Op het gebied van controle, inzage en klachtrecht is er alleen stagnatie of achteruitgang. De parlementaire controle blijft liggen bij de overwerkte en ondeskundige fractievoorzitters, klagen kan nog steeds alleen bij de Nationale Ombudsman, die alleen advies mag uitbrengen, en inzage in dossiers wordt weggehaald bij de Wet Openbaarheid van Bestuur en binnen de strenge normen van de nieuwe wet gebracht. Er komt weliswaar een Commissie van Toezicht met verregaande bevoegdheden, maar die rapporteert wederom in het geheim.

Ten aanzien van de notificatieplicht is sprake van een vooruitgang. Aanvankelijk zou het gaan om een absolute vooruitgang, dat wil zeggen de inlichtingendiensten moesten te allen tijde notificeren en konden eventueel uitstel, maar zeker geen afstel krijgen. Inmiddels is dit onder druk van de BVD ook aangepast en behoort afstel tot de wettelijke mogelijkheden. Voor de bescherming van de inwoners van Nederland tegen de alwetende snuffelstaat zou het een goede zaak zijn als de voorgestelde Wet op de Inlichtingen- en Veiligheidsdiensten gesneuveld zou zijn.