Wetsvoorstel van Wet op de inlichtingen- en veiligheidsdiensten 20xx

Bezwaren Amnesty International Nederland

Eind oktober 2016 diende het kabinet bij de Tweede Kamer een wetsvoorstel in om de Nederlandse geheime diensten meer bevoegdheden te geven (de Wet op de inlichtingen- en veiligheidsdiensten, of Wiv 20xx). Amnesty International is zeer bezorgd over de impact van de wet op de samenleving, het recht op eerbiediging van de persoonlijke levenssfeer en andere mensenrechten van individuen en groepen mensen in binnen- en buitenland indien deze wordt vastgesteld zoals nu is voorgesteld.

Het verwerven van communicatie maakt altijd inbreuk op verschillende mensenrechten, met name op het recht op privacy. Of het nu om het onderscheppen van e-mail, telefoongesprekken, sms'jes social mediaberichten gaat, het Europees Hof voor de Rechten van de Mens (EHRM) beschouwt het als een inmenging in het recht op privacy (artikel 8 lid 1 EVRM).[1] Dit geldt ook voor metadata.[2] Tevens is er volgens het Hof sprake van inmenging als deze geïntercepteerde data worden opgeslagen.[3] Overheden kunnen legitieme redenen hebben voor het verwerven van communicatiegegevens, bijvoorbeeld om de nationale veiligheid te beschermen (artikel 8 lid 2 EVRM). Amnesty International is dan ook niet tegen communicatie-surveillance *an sich*, zolang aan strikte en een aantal mensenrechtelijke voorwaarden is voldaan.

Zo moet een inbreuk op het recht op privacy in overeenstemming zijn met de wet[4], wat onder andere inhoudt dat de in te zetten surveillancebevoegdheden een in de wet vastgelegd doel moeten dienen. Daarnaast moeten de bevoegdheden uitsluitend ingezet kunnen worden als zij gericht op een specifiek persoon of specifieke organisatie. Bovendien moet daarbij sprake zijn van een redelijke verdenking dat iemand een gevaar vormt voor de nationale veiligheid of de democratische rechtsorde en moet uitoefening van de bevoegdheid voldoen aan de strikte eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. Dit betekent dat het doel van de inzet van de bevoegdheid niet op een andere wijze bereikt kan worden en dat de uitoefening van de bevoegdheid niet tot een onevenredig nadeel mag leiden voor het individu ten aanzien van wie de bevoegdheid wordt ingezet. Bovendien moet voor díe maatregel gekozen worden die het minste nadeel oplevert voor het betrokken individu. Waarborgen ter bescherming van rechten moeten voor iedereen gelijk gelden.

Via dit document deelt Amnesty International de grootste pijnpunten met betrekking tot het wetsvoorstel voor de Wet op de inlichtingen- en veiligheidsdiensten 20xx met betrekking tot enkele bevoegdheden, waarborgen en toezicht en internationale samenwerking.

1. Ongerichte verzameling van gegevens
2. 'Hacken van derden'
3. Medewerkingsplicht ontsleuteling
4. Geautomatiseerde gegevensverwerking
5. Onafhankelijk, bindend toezicht op alle fases
6. Notificatieplicht
7. Klachtbehandeling
8. Klokkenluidersregeling
9. Samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten
10. Bescherming van mensenrechten van Nederlanders in het buitenland en van niet-Nederlanders

---

[1] EHRM 6 september 1978, nr. 5029/71, *Klass e.a./Duitsland*, §41; EHRM 26 juni 2006, nr. 54934/00, *Weber en Savaria/Duitsland*, §77; EHRM 8 mei 2006, nr. 276839/05, *Kennedy/Verenigd Koninkrijk*, §118.
[2] EHRM 2 augustus 1984, nr. 8691/79, *Malone/Verenigd Koninkrijk*, §84.
[3] EHRM 29 juni 2006, nr. 27798/95, *Amann/Zwitserland*. In het bijzonder als het gaat om een database en de overdracht daarvan aan andere instanties, zie EHRM 26 juni 2006, nr. 54934/00, *Weber en Savaria/Duitsland*, §79.
[4] Zie onder meer EHRM 4 mei 2000, nr. 28341/95 *Rotaru/ Roemenië*, §52, EHRM 10 februari 2009, nr. 25198/02 *Iordachi e.a./Moldavië*, §37. Zie ook Weber en Savaria/Duitsland waarin nadere eisen zijn beschreven waaraan de nationale wettelijke regeling moet voldoen in EHRM 29 juni 20116, nr. 54934/00 *Weber en Savaria/Duitsland*, §95.

1. Ongerichte verzameling van gegevens

Online en rechtstreekse toegang tot gegevens van andere partijen
Het wetsvoorstel regelt in artikel 39 de algemene bevoegdheid dat de diensten aan iedereen mag vragen gegevens te verstrekken die de diensten nodig menen te hebben voor het uitvoeren van hun wettelijke taken. Hierbij maakt de wet (via artikel 39 lid 3 Wiv 20xx) rechtstreeks geautomatiseerde toegang tot de data van die andere partijen mogelijk. Deze bevoegdheid zou een basis kunnen worden voor massa-surveillance-praktijken, zoals die door Edward Snowden aan de kaak zijn gesteld. Immers, het mogelijk maken van het intercepteren van grote hoeveelheden ruwe data lijkt een vergelijkbare praktijk mogelijk te makel als die met de interceptieprogramma's die door de Amerikaanse *National Security Agency* (NSA) en de Britse *Government Communications Headquarters* (GCHQ) zijn gebruikt. Het op soortgelijke wijze verzamelen van gegevens geeft de Nederlandse inlichtingen- en veiligheidsdiensten ongekend ruime interceptiemogelijkheden.

In de Memorie van Toelichting wordt uitgelegd dat 'met rechtstreeks geautomatiseerde toegang' een online en real time verbinding tussen de dienst en de verstrekkende partij wordt bedoeld, waarbij zonder menselijke tussenkomst aan de kant van de verstrekkende partij, de desbetreffende dienst de gegevens die deze nodig heeft kan opvragen en verstrekt krijgt. De Memorie benadrukt vervolgens dat het bestaan van rechtstreeks geautomatiseerde toegang de verstrekker er niet toe verplicht gegevens te delen met de diensten.[5] Hoe dat in de praktijk werkt wordt niet duidelijk uitgelegd in de Memorie van Toelichting. Bovendien is niet duidelijk wie precies bedoeld wordt met 'een ieder die geacht wordt de benodigde gegevens te kunnen verstrekken' (artikel 39 lid 1 Wiv 20xx). Het lijkt te kunnen betekenen dat elke Nederlander, buitenlander, organisatie, bedrijf of overheidsinstantie verzocht kan worden mee te werken. Want de Memorie van Toelichting stelt: 'Kort gezegd kan de dienst zich tot een ieder wenden met een verzoek om gegevens.'[6]

Als deze bevoegdheid als algemene bevoegdheid wordt opgenomen in de Wiv 20xx dan is de potentiële inbreuk op mensenrechten groot, terwijl de waarborgen voor bescherming van mensenrechten geminimaliseerd zijn. Met name het ontbreken van verplichte toestemming (door een rechter) vooraf voor inzet van de bevoegdheid, het voldoen aan een aantal vereisten daarvoor, dat de inzet gericht moet zijn op een specifiek persoon of specifieke organisatie en de in artikel 27 Wiv 20x vastgelegde plicht de verkregen gegevens zo spoedig mogelijk te onderzoeken op relevantie voor het onderzoek waarvoor ze verworven zijn. Bovendien lijkt geen termijn te worden gesteld aan de duur waarvoor de gegevens bewaard mogen worden.

Ongerichte interceptie
De artikelen 48, 49 en 50 van het wetsvoorstel bevatten een regeling opgenomen voor onderzoeksopdrachtgericht onderzoek van communicatie. Hierbij worden drie verschillende fasen onderscheiden: het verwerven, de voorbewerking en de (verdere) verwerking van de verworven communicatiegegevens. In de eerste fase hoeft geen sprake te zijn van specifieke personen of organisaties van wie een redelijke verdenking bestaat dat ze een gevaar vormen voor de nationale veiligheid en daardoor in het vizier van de diensten zijn gekomen. Daardoor kunnen grote hoeveelheden gegevens worden geïntercepteerd van in principe iedereen.

Naast de hierboven genoemde bevoegdheid van de diensten om andere partijen om automatische, directe toegang tot gegevens te vragen, wordt voorgesteld hiermee de Nederlandse diensten ook de mogelijkheid te geven om zelf op ongekende schaal communicatiegegevens te verwerven van een niet-gespecificeerde persoon, organisatie, computer of telefoon.

Beide bevoegdheden kunnen leiden tot massa-surveillance. Bij beide bevoegdheden is bij voorbaat geen sprake van een onderzoek dat gericht is op een specifiek persoon of een specifieke organisatie ten aanzien van wie een ernstig vermoeden bestaat dat hij of zij een gevaar vormt voor de democratische rechtsorde of nationale veiligheid. Amnesty International meent dat bij het willekeurig en ongericht verwerven van communicatie nooit sprake kan zijn van proportionaliteit, waardoor een ongeoorloofde inbreuk op het recht op privacy wordt gemaakt.

2. 'Hacken van derden'

Amnesty International beschouwt het hacken van computers als een extreem verregaande vorm van surveillance. Computers spelen een grote rol in het privéleven van mensen. Via het hacken van een computer kan inzicht worden verkregen in het gehele leven van een individu. Niet alleen

[5] Memorie van Toelichting bij Wiv 20xx, p. 76
[6] Memorie van Toelichting bij Wiv 20xx, p. 74

communicatie die op dat moment plaatsvindt kan worden onderschept, ook het communicatieverleden wordt inzichtelijk. Bovendien geeft hacken toegang tot zaken, zoals foto's of documenten, die nooit eerder met anderen zijn gedeeld, kan met terugwerkende kracht de locatie worden getraceerd, en is er bijvoorbeeld de mogelijkheid om heimelijk de bezitter van de computer te filmen en op te nemen. De Nederlandse regering moet zeer ernstig afwegen of hacken überhaupt op een veilige en proportionele manier kan worden ingezet. Zoals de VN-rapporteur over vrijheid van meningsuiting verklaarde: 'Vanuit een mensenrechtenperspectief is het gebruik van zulke technologie zeer zorgwekkend.'[7]

Op dit moment beschikken de Nederlandse inlichtingen- en veiligheidsdiensten al over een bevoegdheid om binnen te dringen in 'geautomatiseerde werken', oftewel een hackbevoegdheid (artikel 24 Wiv 2002). Het wetsvoorstel stelt voor om deze bevoegdheid uit te breiden naar het 'hacken van derden'. Individuele burgers worden niet van dit begrip uitgesloten.[8] Wat de technische relatie tussen de derde partij en het doelwit van de diensten precies inhoudt wordt niet duidelijk gemaakt. Daarnaast maakt artikel 45 lid 8 Wiv 20xx mogelijk dat ook andere geautomatiseerde werken van de derde partij gehackt mogen worden dan waarvoor toestemming is gegeven. Dit kan dus betekenen dat een onbeperkt aantal apparaten van een derde gehackt mogen worden, nádat toestemming is gegeven voor het binnendringen van één daarvan.

De voorgestelde uitbreiding van de hackbevoegdheid leidt tot een grote inbreuk op mensenrechten van derden, zonder dat zij aanleiding hebben gegeven om in het vizier van de inlichtingen- en veiligheidsdiensten terecht te komen. Het is voor derden amper te voorzien dat ze gehackt kunnen worden door de geheime diensten. Bovendien lijkt de mogelijkheid te bestaan dat gegevens van deze derde niet hoeven te worden vernietigd als deze relevant zijn voor een ander lopend onderzoek. Daarmee wordt de gehackte computer een zelfstandige bron van informatie, zonder dat de daarvoor gestelde waarborgen in acht zijn genomen. Daarnaast zijn de diensten ingevolge artikel 59 Wiv 20xx niet verplicht om een derde te notificeren dat diens computer gehackt is geweest. Dit terwijl er een risico bestaat dat de technische hulpmiddelen, zoals malware, die zijn gebruikt om het hacken mogelijk te maken niet altijd verwijderd kunnen worden (artikel 45, lid 7 Wiv 20xx). De gehackte derde partij beschikt dan vervolgens over een onveiligere computer zonder daarvan af te weten en is daarmee kwetsbaarder geworden voor digitale dreigingen. De verregaande inbreuk die hiermee gemaakt wordt op onder andere het recht op privacy van derden is naar de mening van Amnesty International niet proportioneel in relatie tot het te bereiken doel.

3. Medewerkingsplicht ontsleuteling

Amnesty International onderschrijft het belang van mogelijkheden om anoniem en vertrouwelijk te kunnen communiceren op internet, zoals dat in mei 2015 ook is uiteengezet door de speciale VN-rapporteur over vrijheid van meningsuiting.[9] Versleuteling van gegevens, of encryptie, is één van de voorwaarden voor het genieten van het recht op privacy.[10] Dit is van belang voor binnenlandse en buitenlandse activisten, dissidenten en klokkenluiders, maar ook voor anderen die zich (terecht) zorgen maken over het vastleggen van online gedrag omdat die gegevens in de toekomst tegen hun wensen en belangen kunnen opduiken in andere contexten. Versleuteling is vooralsnog de enige manier om digitale communicatie te beschermen tegen inbreuken als cybercriminaliteit, identiteitsdiefstal of onrechtmatige interceptie door overheden. Amnesty International is dan ook van mening dat overheden technologie waarmee gegevens versleuteld kunnen worden, en het gebruik daarvan, niet mag verbieden.

De voorgestelde wet verbiedt encryptie niet, maar stelt wel een medewerkingsplicht in voor ontsleuteling via artikel 57 en artikel 45 lid 9. Niet meewerken is een strafbaar feit waarop twee jaar gevangenisstraf staat volgens artikel 143.

Via deze ontsleutelplicht kunnen de diensten iemand die vermoedelijk kennis heeft van de wijze van versleuteling verplichten mee te werken, door die kennis te delen of de versleuteling ongedaan te maken. Het is echter niet duidelijk wie precies verplicht kan worden mee te werken aan ontsleuteling. Betreft dit bijvoorbeeld de aanbieders van (besloten) communicatiediensten, de makers of aanbieders van producten zoals smartphones en laptops? Organisaties als Amnesty International zullen vanwege

[7] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank la Rue, VN Algemene Vergadering, 17 april 2013, A/HRC/23/40, §62.
[8] Memorie van Toelichting, pp. 102-103.
[9] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, David Kaye, VN Mensenrechtenraad, A/HRC/29/32, 22 mei 2015.
[10] Amnesty International, *Encryption. A matter of human rights*, Londen, maart 2016.

de aard van hun missie en daaruit volgende werkzaamheden soms contact onderhouden met personen die zich ook in het vizier van de diensten bevinden. Is de reikwijdte van de wet zodanig dat medewerkers van deze organisaties verplicht worden mee te werken aan ontsleuteling? Of kan ook elke Nederlander of buitenlander met enige kennis van zaken verplicht worden hieraan mee te werken? Amnesty meent dat bij een dergelijke verplichting voor het algemene publiek, waar een gevangenisstraf van twee jaar op staat indien men niet meewerkt, geen sprake is van proportionaliteit.

In de Memorie van Toelichting wordt opgemerkt dat de diensten geen achterdeuren mogen (laten) inbouwen in systemen om op die manier toegang tot de ontsleutelde gegevens te krijgen. Ook is er geen enkele verplichting voor bijvoorbeeld aanbieders van communicatiediensten om de encryptie die in hun systemen is toegepast te verzwakken. Dit juicht Amnesty toe. Andere methoden om toegang te krijgen tot ontsleutelde gegevens lijken echter niet uitgesloten, zoals de ontwikkeling van een gecompromitteerde versie van een door het doelwit gebruikte chat app die als download aangeboden wordt aan alleen dit doelwit.

4. Geautomatiseerde gegevensverwerking

Artikel 60 Wiv 20xx geeft de diensten de bevoegdheid tot geautomatiseerde data-analyse. Zo mogen gegevensbestanden op geautomatiseerde wijze onderling met elkaar vergeleken worden, mogen bestanden onderzocht worden aan de hand van profielen, kunnen de bestanden worden vergeleken om zo patronen op te sporen en om te komen tot voorspellende analyses. Deze gegevensbestanden kunnen inhoudelijke gegevens bevatten, maar ook gegevens over de communicatie (metadata).

Uitkomsten van de geautomatiseerde gegevensanalyse kunnen verregaande gevolgen hebben voor een individu of organisatie, bijvoorbeeld doordat op basis van die uitkomsten een van de diensten een onderzoek start naar die persoon of organisatie. Ook kunnen dergelijke analyses, zonder correctie, leiden tot discriminatie van bepaalde groepen in de samenleving. De Wetenschappelijke Raad voor het Regeringsbeleid publiceerde in april 2016 het rapport *Big data in een vrije en veilige samenleving*, en noemde discriminatie daarin als één van de risico's van geautomatiseerde data-analyse. Ook beschrijft het rapport het risico op *chilling effects*: 'De grootschalige verzameling en opslag van data door private partijen en overheden, niet in de laatste plaats door inlichtingen- en veiligheidsdiensten, hebben bredere maatschappelijke effecten. […] dat er een negatief sociaal effect uitgaat van het constante (elektronische) toezicht door publieke en private partijen in het digitale tijdperk. Wanneer overheidsorganisaties ook private data voor veiligheidsdoeleinden gaan gebruiken, zal dit effect naar alle waarschijnlijkheid sterk worden uitvergroot. Met name in de (machts)relatie tussen burgers en de overheid geeft dit een aanzet tot wat bekend staat als chilling effects op het genieten en uitoefenen van bepaalde rechten. Mensen kunnen het gevoel krijgen dat hun recht op privacy en vrijheid van meningsuiting in gevaar is. Als deze effecten optreden bij journalisten, schrijvers, klokkenluiders, ngo's en advocaten, komt ook het functioneren van de bredere democratie in het geding'.[11]

Het wetsvoorstel staat niet toe dat uitsluitend op basis van de uitkomsten van de diverse vormen van geautomatiseerde gegevensverwerking maatregelen getroffen worden ten aanzien van een persoon. Dit is een belangrijke waarborg voor de bescherming van mensenrechten is, maar dit is niet toereikend, omdat verdere waarborgen voor deze bevoegdheid ontbreken. De Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD) schrijft hierover: 'Gelet op de risico's die geautomatiseerde gegevensverwerking met zich meebrengt en de belangrijke waarborgfunctie die in geautomatiseerde processen besloten kan liggen, is het essentieel dat de kwaliteit van geautomatiseerde gegevensverwerking geborgd wordt en dat erop kan worden toegezien dat geautomatiseerde processen werken zoals ze behoren te werken.' De toezichthouder stelt voor dat hiertoe een zorgplicht voor de diensten in de wet wordt vastgelegd.[12] Amnesty International deelt deze opvatting van het CTIVD.

5. Onafhankelijk, bindend toezicht op alle fases

Goed toezicht door een onafhankelijke, juridische instantie op het handelen van de inlichtingen- en veiligheidsdiensten is een cruciaal onderdeel van een democratische rechtsstaat. Dat garandeert dat er wordt getoetst dat geen machtsmisbruik plaatsvindt. De diensten moeten zich immers

[11] Wetenschappelijke Raad voor het Regeringsbeleid, *Big data in een vrije en veilige samenleving*, Amsterdam University Press, Amsterdam 2016, p. 92
[12] Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD), *Bijlage 1 bij de Zienswijze van de CTIVD op het wetsvoorstel Wiv 20..*, 9 november 2016, pp. 20-27.

verantwoorden aan de maatschappij. Hiervoor is volwaardig, onafhankelijk, bindend toezicht in alle fases van het handelen van de diensten van cruciaal belang.

Toetsing vooraf
In toenemende mate is er consensus onder Europese rechters dat onafhankelijk, bindend juridisch toezicht de sterkste waarborg is tegen niet-noodzakelijke en disproportionele surveillance van communicatie.[13] Het is een stap vooruit dat de regering het toezicht voorafgaand aan de inzet van bepaalde bevoegdheden wil versterken door de invoering van een aparte Toetsingscommissie Inzet Bevoegdheden (TIB). Maar de toetsing door de TIB is met minder waarborgen omkleed dan een gang naar de rechter. Die wordt immers voor het leven benoemt én maakt geen onderdeel uit van de uitvoerende macht. De onafhankelijkheid van de rechter wordt doorgaans ook niet betwist. Daarnaast is de rechter het beste in staat om juridische concepten als proportionaliteit, subsidiariteit en noodzakelijkheid te beoordelen en eigenstandig tot een oordeel te komen over het verzoek van de diensten om bepaalde bevoegdheden in te zetten, waarbij toegang mogelijk moet zijn tot alle relevante informatie bij de diensten. De TIB daarentegen toetst enkel de toestemming van de minister. De rechter kan externe deskundigen raadplegen waar nodig. In elk geval zou het beginsel van hoor en wederhoor toegepast moeten worden. Er is geen reden om voorafgaande toetsing door een onafhankelijke rechter te beperken tot uitsluitend die gevallen waarin brieven worden geopend (artikel 44 Wiv 20xx), de communicatie tussen advocaten (artikel 30, lid 3 Wiv 20xx) en hun cliënten wordt afgeluisterd of om de bronnen van journalisten te achterhalen (artikel 30, lid 2 Wiv 20xx).

Toetsing tijdens en na inzet bevoegdheid
Naast toezicht vóóraf, blijft onafhankelijk, bindend toezicht tijdens de inzet van bevoegdheden om gegevens te verzamelen en vervolgens te verwerken én achteraf onontbeerlijk. Noodzaak en proportionaliteit kunnen immers tijdens de uitvoering van een operatie wegvallen. Hiervoor zijn adequate en toetsbare waarborgen nodig.

De toezichthouder op de inlichtingen- en veiligheidsdiensten (CTIVD) is bevoegd tot het houden van toezicht tijdens en na de inzet van bevoegdheden door de geheime diensten, maar de verantwoordelijke minister kan de aanbevelingen van de CTIVD naast zich neerleggen. Dit is problematisch omdat toezicht eigenlijk in de plaats komt van het rechtsmiddel dat iemand die onderworpen is aan surveillance kan inroepen, omdat deze persoon niet afweet van de inbreuk op diens recht op privacy. De CTIVD zou het gebruik van een bevoegdheid onrechtmatig moeten kunnen verklaren én herstelmaatregelen moeten kunnen bevelen, zoals het vernietigen van reeds verzamelde gegevens.[14] In het huidige wetsvoorstel heeft zij deze bevoegdheid echter niet.

6. Notificatieplicht

Een van de waarborgen tegen misbruik van bevoegdheden door de diensten is als degene die onderworpen is aan surveillance genoegdoening kan krijgen. Om misbruik aan de orde te kunnen stellen, moet een individu ervan op de hoogte zijn dat hij of zij het doelwit was van een surveillanceoperatie. Het Europees Hof heeft meerdere malen gesteld dat de notificatieplicht de mogelijkheid waarborgt om de rechtmatigheid van de inzet van bevoegdheden achteraf te betwisten en daarmee beschermt tegen misbruik van bevoegdheden.[15]

Artikel 59 Wiv 20xx regelt een notificatieplicht. Vijf jaar nadat een surveillanceonderzoek beëindigd is, moeten de diensten onderzoeken of de betreffende persoon daarover geïnformeerd kan worden. Maar deze plicht geldt slechts voor enkele bijzondere bevoegdheden, namelijk voor het doorbreken van het briefgeheim, het gericht afluisteren van personen of organisaties en in gevallen waarin is binnengetreden in een woning zonder toestemming van de bewoner. Amnesty International meent dat de notificatieplicht een sterkere waarborg tegen misbruik van bevoegdheden biedt als deze geldt voor de inzet van *alle* bijzondere bevoegdheden, dus ook voor bijvoorbeeld het binnendringen in geautomatiseerde werken (hacken). Daarbij meent Amnesty dat in het verslag dat wordt uitgebracht aan de onderzochte persoon moet staan op basis van welke juridische grond de bevoegdheid is uitgevoerd, welke gegevens zijn verzameld en op welke rechtsmiddelen de onderzochte persoon een beroep kan doen.

---

[13] EHRM 6 september 1978, nr. 5029/71, *Klass e.a./Duitsland*, §56; EHRM 18 mei 2010, nr. 26839/05, *Kennedy/Verenigd Koninkrijk*, §167; EHRM 22 februari 2013, nr. 39315/06, *Telegraaf e.a./Nederland*, §98.
[14] Zie ook: Loof J.P. e.a., *Het Mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten*, Universiteit Leiden, augustus 2015; Instituut voor Informatierecht, Universiteit van Amsterdam, *Ten standards for oversight and transparency of national intelligence services* (Amsterdam 2015).
[15] EHRM 6 september 1978, nr. 5029/71, *Klass e.a./Duitsland*, §39, 56-57, EHRM 28 juni 2007, nr. 62540/00, *Association for European Integration and Human rights en Ekimdzhiev v. Bulgarije*, § 101.

Volgens artikel 59 Wiv 20xx mag de notificatieplicht worden uitgesteld of vervallen als het legitieme doel van een surveillanceoperatie door notificatie in gevaar komt. Amnesty benadrukt hierbij het belang dat de inlichtingen- en veiligheidsdiensten hier geen te ruime invulling aan geven. In het verleden constateerde de CTIVD dat zij dat wel deden.[16]

7. Klachtbehandeling

Amnesty International is van oordeel dat de klachtbehandeling onder de Wiv 20xx ook van toepassing zou moeten zijn op anderen dan degene jegens wie het optreden heeft plaatsgevonden. Ook andere maatschappelijke actoren, waaronder ngo's en journalisten, moeten het recht hebben om een klacht in te dienen namens en groep mensen of in het algemeen belang. Het Europese Hof heeft diverse malen benadrukt dat de klager niet hoeft aan te tonen dat hij daadwerkelijk onderworpen is geweest aan een surveillanceoperatie door een van de diensten.[17] Of het wetsvoorstel middels de klachtenregeling in §7.2.3 deze mogelijkheid ook daadwerkelijk biedt is onduidelijk, aangezien de afdeling klachtbehandeling van de CTIVD volgens artikel 121 sub c niet verplicht is een onderzoek in te stellen als het belang van de klager kennelijk onvoldoende is.

8. Klokkenluidersregeling

In de artikelen 125-131 van het wetsvoorstel is een klokkenluidersregeling opgenomen. Het is goed dat ambtenaren van de inlichtingen- en veiligheidsdiensten en anderen, zoals medewerkers van telecombedrijven, die betrokken zijn geweest bij de uitvoering van de Wiv, een melding van (een vermoeden van) een misstand kunnen indienen bij de afdeling klachtbehandeling van de CTIVD. Het oordeel dat de afdeling klachtbehandeling van de CTIVD over de melding velt is niet bindend. Het betekent dat de desbetreffende minister niet verplicht is om ervoor te zorgen dat de situatie verandert. En de minister is niet verplicht om (al dan niet deels) gehoor te geven aan eventuele aanbevelingen van de afdeling klachtbehandeling. Dit is onwenselijk.

9. Samenwerking met buitenlandse inlichtingen- en veiligheidsdiensten

Amnesty International is van mening dat het samenwerken, inclusief het delen van gegevens, met buitenlandse inlichtingen- en veiligheidsdiensten alleen mag plaatsvinden binnen een wettelijk kader dat voldoet aan mensenrechtenverplichtingen. Amnesty is in eerste instantie dan ook verheugd dat in het wetsvoorstel is vastgelegd dat voorafgaand aan eventuele samenwerking met een buitenlandse dienst eerbiediging van de mensenrechten, de democratische inbedding, en de professionaliteit en betrouwbaarheid van die dienst moeten worden afgewogen. Toch sluit dit niet uit dat informatie kan worden gedeeld met repressieve regimes. Het uitgangspunt blijft namelijk dat geen enkele samenwerking op voorhand wordt uitgesloten. Er bestaat hierdoor een reëel risico dat internationale samenwerking met buitenlandse geheime diensten leidt tot schending van mensenrechten. Het werk en leven van onder andere individuele activisten, journalisten en oppositieleden kan zodoende door het handelen van Nederland in gevaar komen. Onduidelijkheden hierover in de wet moeten worden opgehelderd.

Twee regelingen voor gegevensuitwisseling
Op twee verschillende plekken is in de wet geregeld onder welke voorwaarden de diensten gegevens uit mogen wisselen met buitenlandse diensten. Artikelen 88-90 Wiv 20xx regelt de samenwerking met buitenlandse diensten, waaronder ook het delen van informatie. Daaruit volgt dat na beoordeling van de buitenlandse dienst moet worden besloten of er kan worden samengewerkt, en wat de aard en intensiteit van die samenwerking kan zijn. Deze beoordeling is een belangrijke waarborg voor het beschermen van de persoonlijke levenssfeer en mensenrechten in bredere zin. Daarnaast is in §3.4.2 een regeling opgenomen over het extern verstrekken van gegevens 'in het kader van een goede taakuitvoering van die diensten' aan onder andere buitenlandse diensten. Hierbij wordt niet de voorwaarde gesteld dat uitwisseling van gegevens met een buitenlandse dienst moet plaatsvinden binnen de kaders van een samenwerkingsrelatie met de betreffende dienst. Het bestaan van deze twee regelingen naast elkaar creëert onduidelijkheid. Het uitgangspunt zou moeten zijn dat het delen van informatie met buitenlandse diensten altijd in het kader van een samenwerkingsrelatie moet gebeuren. Dat verkleint het risico op onrechtmatige inbreuken op mensenrechten.

[16] CTIVD, *Toezichtsrapport Inzake de rechtmatigheid van de uitvoering van de notificatieplicht door de AIVD,* nr. 24 (2010).
[17] EHRM 6 september 1978, no. 5029/71 (*Klass e.a. t. Duitsland*), §36, EHRM 2 augustus 1984, no. 8691/79 (*Malone t. VK*), §64.

Delen van ongeëvalueerde gegevens
De samenwerking met buitenlandse diensten is extra problematisch bij de uitwisseling van grote hoeveelheden ongeëvalueerde gegevens. Dit zijn gegevens waarvan nog niet onderzocht is of ze relevant zijn voor het onderzoek waarvoor ze verzameld zijn. Daardoor is niet bekend welke gegevens precies worden verstrekt en wat hiervan de consequenties kunnen zijn. Hierdoor kunnen zeer gevoelige gegevens in handen komen van regimes die hier zelf mee aan de haal gaan zonder dat Nederland hierop enige controle kan uitoefenen. Het is dan ook van belang dat uitsluitend gericht verzamelde en geëvalueerde gegevens kunnen worden gedeeld met buitenlandse diensten. Van dergelijke gegevens kan veel duidelijker de wenselijkheid en noodzakelijkheid van de uitwisseling en het gebruik van die gegevens worden getoetst. In geen geval mogen er gegevens worden uitgewisseld als er een ernstig vermoeden bestaat dat dit de rechten van de betreffende persoon of organisatie schendt.

Gegevensgebruik door buitenlandse diensten
Bovendien zouden veel betere waarborgen in de wet moeten worden ingebouwd rondom het gebruik, de opslag en de vernietiging van gegevens door de ontvangende buitenlandse diensten. Zonder deze waarborgen kan niet worden uitgesloten dat de verstrekte gegevens worden misbruikt om de rechten en vrijheden van individuen in het buitenland in te perken. Het wetsvoorstel regelt in artikel 65 dat bij het verstrekken van gegevens aan buitenlandse diensten de voorwaarde moet worden gesteld dat deze gegevens niet aan andere partijen worden verstrekt. Maar van deze regel kan worden afgeweken.[18] Mensenrechten worden beter beschermd als voorwaarden die toezien op het gebruik van de gegevens door de buitenlandse dienst altijd schriftelijk moeten worden vastgelegd. Het gaat dan bijvoorbeeld om het doel waarvoor de gegevens gebruikt mogen worden en voorwaarden rondom opslag en vernietiging van de gegevens. Dit vastleggen maakt de voorwaarden toetsbaar en maakt een beter toezicht op de rechtmatigheid van de uitvoering van samenwerking met buitenlandse diensten mogelijk. Hoe de buitenlandse diensten de gegevens gebruiken, onttrekt zich immers aan het zicht van de Nederlandse toezichthouder.

Delen van onjuiste en verouderde persoonsgegevens
Het wetsvoorstel regelt in artikel 69 dat persoonsgegevens niet verstrekt mogen worden als de juistheid daarvan niet redelijkerwijs kan worden vastgesteld of als die persoonsgegevens meer dan tien jaar geleden zijn verwerkt en ten aanzien van de desbetreffende persoon geen nieuwe gegevens zijn verwerkt. Hierop is vervolgens een uitzondering gemaakt voor, onder andere, buitenlandse diensten. Deze uitzondering zou volgens de Memorie van Toelichting mogelijk moeten zijn omdat 'Het feit dat een persoon niet meer in de aandachtsfeer van de AIVD of MIVD bevindt', nog niet wil zeggen 'dat hij zich niet in de aandachtsfeer van een buitenlandse collegadienst kan bevinden.' Dit is een veel beperktere uitzondering op de regel dan de uitzondering geformuleerd in artikel 69 lid 2 Wiv 20xx. Dit brengt grote risico's met zich mee voor het recht op privacy van de personen om wier gegevens het gaat. Zoals de Privacy Impact Assessment benadrukt gaat het immers om gegevens die hoogstwaarschijnlijk niet relevant zijn of waarvan de relevantie (vanwege de onbetrouwbaarheid) niet kan worden vastgesteld, en waarvan niet kan worden gecontroleerd op welke manier de buitenlandse dienst er gebruik van zal maken. De Nederlandse waarborgen zijn daarop niet van toepassing.[19]

Toestemming
In het wetsvoorstel is geregeld dat toestemming gegeven moet worden voor de inzet van bijzondere bevoegdheden door Minister, waarbij de Toetsingscommissie Inzet Bevoegdheden een bindende rechtsmatigheidstoets uitvoert, of door de Rechtbank. Voor het delen van de gegevens die hiermee verkregen zijn met, of voor het inzetten van deze bevoegdheden ten behoeve van een buitenlandse dienst is geen voorafgaande toestemming op dit zelfde niveau nodig. Ook voor het ontvangen van gegevens en ondersteuning van buitenlandse diensten met het inzetten van bijzondere bevoegdheden geldt dit niet. Amnesty International meent dat ook deze besluiten onderworpen moeten worden aan voorafgaande toetsing. Dat verkleint het risico op onrechtmatige inbreuken op mensenrechten.

Leemte in rechtsbescherming
In artikel 166 Wiv 20xx is een overgangsbepaling opgenomen die regelt dat een aantal artikelen over samenwerking met buitenlandse diensten gedurende twee jaar nadat de wet in werking is getreden buiten toepassing blijven.[20] Dit betekent dat de diensten in die periode mogen samenwerken met buitenlandse diensten die niet beoordeeld zijn op in ieder geval de criteria eerbiediging van de

[18] MvT pagina 183 – 'Zo kan wanneer een buitenlandse collegadienst onderkent dat er in het belang van een tijdige en efficiënte reactie op een dreiging nog een collegadienst moet worden ingelicht, toestemming worden verleend om gegevens verder te verstrekken. Wel kunnen aan die toestemming voorwaarden worden verbonden, zoals over de aard en het doel van het gebruik.'
[19] PI-Lab Privacy Impact Assessment Wiv20xx, blz. 70-71.
[20] Het betreft artikel 88 lid 2-5, 89 lid 6 en 90 lid 4.

mensenrechten, democratische inbedding en professionaliteit en betrouwbaarheid door of van die buitenlandse dienst. Deze beoordeling, of weging, is een belangrijke waarborg voor het beschermen van de persoonlijke levenssfeer. Door deze regeling twee jaar buiten toepassing te laten ontstaat een leemte in de rechtsbescherming. De CTIVD heeft in Toezichtsrapport 48 aandacht besteed aan de beperkte prioriteit die de diensten hebben gegeven aan het vaststellen van wegingsnotities door de diensten.[21] De gevolgen hiervan - gebrek aan rechtsbescherming - mogen niet op het conto van de burger komen.

10. Bescherming van mensenrechten van Nederlanders in het buitenland en van niet-Nederlanders

De internationale mensenrechtenverplichtingen van de Nederlandse overheid zijn ook extraterritoriaal van toepassing voor zover de staat effectieve controle heeft over de rechten van het individu waarop inbreuk wordt gemaakt. Amnesty International meent dat de overheid deze verantwoordelijkheid ook heeft bij interceptie van communicatie en hacken. Onder andere het recht op eerbiediging van een individu's persoonlijke levenssfeer en vrije meningsuiting zijn hier in het geding.

Amnesty vindt ook dat in het wetsvoorstel en in de memorie van toelichting duidelijker moet blijken dat ook de gegevens van buitenlanders in Nederland, en de communicatie van Nederlanders en niet-Nederlanders die in het buitenland verblijven, verwerkt mogen worden. Als gevolg van deze verwerking van gegevens heeft de Nederlandse overheid effectieve controle over de inbreuk op de rechten van individuen van wie gegevens verwerkt zijn. Het moet ondubbelzinnig duidelijk zijn dat alle rechten en plichten, waaronder waarborgen voor bescherming van mensenrechten, op dezelfde manier van toepassing zijn op al deze individuen.

[21] CTIVD, *Toezichtsrapport over de invulling van samenwerkingscriteria door de AIVD en MIVD*, nr. 48 (2016).