AMNESTY INTERNATIONAL

Afdeling Nederland
Keizersgracht 177
Postbus 1968
1000 BZ Amsterdam

T 020 626 44 36
F 020 624 08 89
E amnesty@amnesty.nl
I www.amnesty.nl

Aan
de Minister-President, Minister van Algemene Zaken
de Minister van Binnenlandse Zaken en Koninkrijksrelaties
de Minister van Defensie
de Minister van Veiligheid en Justitie

Datum
31 augustus 2015

Onderwerp
Bijdrage Amnesty International consultatie Wet op de inlichtingen en veiligheidsdiensten 20XX

Ons kenmerk
Dir/en/2015/302

Uw kenmerk

Geachte heer Rutte, heer Plasterk, mevrouw Hennis-Plasschaert en heer Van der Steur,

Amnesty International maakt graag gebruik van de consultatie met betrekking tot de voorgestelde nieuwe wet inzake de bevoegdheden van de Nederlandse inlichtingen- en veiligheidsdiensten (hierna Wiv 20XX). Zij heeft kennis genomen van de intentie de inbreng van stakeholders binnen zes weken te verwerken.[1] Amnesty International hoopt dat haar inbreng en die van andere stakeholders in ogenschouw wordt genomen en op zorgvuldige wijze wordt verwerkt.

Amnesty International is zeer bezorgd over de impact van het wetsvoorstel Wiv 20XX op de samenleving, het recht op eerbiediging van de persoonlijke levenssfeer en andere mensenrechten van individuen en groepen mensen in binnen- en buitenland. Dat terwijl Amnesty International niet overtuigd is van het nut en de noodzaak van de voorgestelde nieuwe en ruimere bevoegdheden voor de Nederlandse inlichtingen- en veiligheidsdiensten. In een democratische rechtsstaat zoals Nederland kan het nooit noodzakelijk zijn om de gehele bevolking onder communicatie-surveillance te plaatsen. Het wetsvoorstel breekt met een wereldwijde trend om meer waarborgen op te nemen in de bevoegdheden van inlichtingen- en veiligheidsdiensten om niet-noodzakelijke en disproportionele inbreuken op mensenrechten te voorkomen of te compenseren. Ook is het maar de vraag of het stelsel van waarborgen zoals voorgesteld in de Wiv 20XX aan mensenrechtenstandaarden voldoet, zoals bijvoorbeeld in het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden is vastgelegd.

Uiteraard lichten wij onze bijdrage graag aan u toe.

Met vriendelijke groet,

Eduard Nazarski
Directeur Amnesty International, afdeling Nederland

[1] 'De verwachting is dat hiervoor een periode van zes weken moet worden genomen.' Brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer van 17 maart 2015, TK 2014-2015, 33 820, nr. 5.

Bijdrage Amnesty International consultatie Wet op de inlichtingen en veiligheidsdiensten 20XX

Amnesty International ziet steeds vaker dat in binnen- en buitenland mensenrechten onder druk staan als gevolg van communicatie-surveillance. Activisten zijn niet veilig, maar ook non-gouvernementele organisaties als Amnesty International zelf zijn de dupe. Recent bleek nog uit een rechtszaak in het Verenigd Koninkrijk, die onder andere door Amnesty International was aangespannen, dat Amnesty-communicatie onrechtmatig was opgeslagen.[2] De onthullingen van Edward Snowden tonen aan dat overheden wereldwijd, heimelijk en nagenoeg zonder toezicht, de privé-communicatie van miljoenen mensen aftappen, verzamelen, opslaan, analyseren en delen.

In de afgelopen twee jaar oordeelden nationale rechtbanken, parlementaire onderzoeken, juristen, technologiedeskundigen en maatschappelijke organisaties dat (massale) communicatie-surveillance door inlichtingen- en veiligheidsdiensten buitensporig is. Het is een schending van mensenrechten. Ook instanties als de Verenigde Naties (VN)[3], de VN Hoge Commissaris voor de Rechten van de Mens[4] en de Raad van Europa[5] tonen zich bezorgd over (massa-)surveillance- en interceptieprogramma's en waarschuwen voor de (neven)effecten voor mensenrechten. Momenteel lopen verschillende zaken over communicatie-surveillance bij het Europese Hof voor de Rechten van de Mens. Het is niet ondenkbaar dat het Hof scherpere en specifiekere voorwaarden aan de interceptie van communicatie, rechtstreekse toegang en onderzoek van geautomatiseerde werken door geheime diensten zal stellen.[6]

In een recent rapport wijzen Amnesty International en Privacy International erop dat, in weerwil van de publieke opinie, een trend zichtbaar is dat overheden massa-surveillance willen behouden en uitbreiden.[7] Verder blijkt uit een internationale opiniepeiling van Amnesty International uit 2015 dat een meerderheid van de Nederlandse respondenten (58 procent) van mening is dat de Nederlandse overheid zich niet moet inlaten met het onderscheppen, opslaan en analyseren van hun communicatie via internet en mobiele telefoons. Daarmee nemen de Nederlandse respondenten stelling tegen massa-surveillance.[8]

Nut en noodzaak van de Wet op de inlichtingen- en veiligheidsdiensten 20XX

Overheden kunnen legitieme redenen hebben voor communicatie-surveillance, bijvoorbeeld om de nationale veiligheid te beschermen. Amnesty International is dan ook niet tegen technologie-onafhankelijke interceptie van communicatie, onderzoeken van geautomatiseerde werken (*hacking*) of de 'verwerking van gegevens' zoals omschreven in artikel 1 Wiv 20XX[9] *an sich*. Dit wetsvoorstel voorziet

---

[2] Investigatory Powers Tribunal (IPT, Verenigd Koninkrijk), Determination, zaaknummers: IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH, 22 juni 2015, http://www.ipt-uk.com/section.aspx?pageid=8; IPT, Letter and email, zaaknummer: IPT/13/77/H, 2 juli 2015, http://www.ipt-uk.com/section.aspx?pageid=8.

[3] In december 2013 nam de Algemene Vergadering van de Verenigde Naties (VN) een resolutie over het recht op privacy in het digitale tijdperk aan, waarin zij aangaf zeer bezorgd te zijn over '*…the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights.*', VN Algemene Vergadering, resolutie 68/456/ADD.2, 10 december 2013.

[4] *Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age*, VN Mensenrechtenraad, A/HRC/27/37, 30 juni 2014.

[5] Raad van Europa, Europese Commissie voor Democratie door Recht (Commissie van Venetië), *Update of the 207 report on the democratic oversight of the security services and report on the democratic oversight of signals intelligence services*, CDL–AD(2015)006 (Straatsburg 2015).

[6] *10 Human Rights Organizations versus the United Kingdom: additional submissions on the facts of complaints, complaints to the ECHR,* https://privacyinternational.org/sites/default/files/HR%20Orgs%20v%20UK.pdf, zie ook https://www.amnesty.org/en/documents/ior60/1415/2015/en/; Europees Hof voor de Rechten van de Mens (EHRM) 7 januari 2014, nr. 58170/13, *Big Brother and Others/The United Kingdom*.

[7] Amnesty International & Privacy International, *Two Years after Snowden. Protecting Human Rights in an age of mass surveillance* (Londen 2015).

[8] Q.A.M. Eijkman, *Nederlanders kritisch over ongerichte communicatie–surveillance*, 17 maart 2015, http://weblogs.amnesty.nl/mensenrechtenvandaag/2015/03/17/nederlanders-kritisch-over-ongerichte-communicatie-surveillance/.

[9] In deze bijdrage wordt met surveillance en interceptie van communicatie hetzelfde bedoeld als met de term verwerking van gegevens, zoals gedefinieerd in artikel 1 Wiv 20XX.

echter in het op zo'n ongekende schaal verwerven, voorbewerken en verwerken van willekeurig en ongericht geïntercepteerde communicatie dat het massa-surveillance door de Nederlandse inlichtingen- en veiligheidsdiensten legitimeert en legaliseert; 'het sleepnet' zoals voorgesteld in artikel 33 Wiv 20XX. Willekeurige, ongerichte interceptie is altijd in strijd met de fundamentele rechten van de mens. Het is een inbreuk op het recht op privacy van iedereen. Het is in strijd met artikel 8 Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) en artikelen 7 en 8 van het Handvest van de Grondrechten van de Europese Unie (EU). Onder andere het Hof van Justitie van de EU heeft in 2014 het massaal opslaan van telecomgegevens van burgers heeft verboden.[10] Hiermee werd de EU dataretentierichtlijn in 2014 ongeldig verklaard. De Nederlandse implementatie van die richtlijn, de Wet bewaarplicht telecommunicatiegegevens, werd op 11 maart 2015 door de rechter buiten werking gesteld, mede op grond van de bezwaren die grootschalige opslag van communicatiegegevens en omdat daarmee een ontoelaatbare inbreuk op het recht op privacy werd gemaakt.[11] Amnesty International is pertinent tegen het legaliseren van willekeurig, ongericht intercepteren van communicatie door de Nederlandse inlichtingen- en veiligheidsdiensten. Daarmee worden namelijk de mensenrechten van betrokken individuen die door deze activiteiten worden geraakt, veronachtzaamd.

In de inleiding van de memorie van toelichting op de Wiv 20XX wordt gesuggereerd dat er in Nederland mede dankzij nieuwe communicatietechnologieën en de manier waarop de inlichtingen- en veiligheidsdiensten en buitenlandse diensten die willen gebruiken, behoefte zou zijn aan een nieuw wettelijk kader voor interceptie van communicatie en het onderzoeken van geautomatiseerde werken. In de memorie van toelichting wordt het nut en de noodzaak van deze nieuwe ruimere bijzondere bevoegdheden voor de Nederlandse inlichtingen- en veiligheidsdiensten echter onvoldoende duidelijk gemaakt. Er wordt verwezen naar 'kwesties in de toepassingspraktijk' en de bevindingen en aanbevelingen uit het evaluatierapport van de commissie-Dessens over de Wiv 2002. De commissie-Dessens adviseert weliswaar een aanpassing van de bijzondere bevoegdheden ten aanzien van technologie-(on)afhankelijke interceptie, maar zij benadrukt ook het belang van balans: meer technologie-onafhankelijke bevoegdheden moeten worden gecompenseerd met sterke wettelijk geregelde waarborgen en transparantie. Die balans ontbreekt volgens Amnesty International in het huidige wetsvoorstel.

In tegenstelling tot de aanbeveling van de commissie-Dessens en die van de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD) om een (onmiddellijk) bindende rechtmatigheidstoets mogelijk te maken, blijft de regering volharden in een systeem van politiek en bestuurlijk toezicht.[12] Juist omdat de inlichtingen- en veiligheidsdiensten over het algemeen buiten het zicht van de maatschappij opereren, zijn waarborgen zoals transparantie en onafhankelijke rekenschap en toezicht des te belangrijker.

Het is dan ook niet helder waaruit blijkt dat de huidige bevoegdheden niet voldoen. De Wiv 20XX, noch de memorie van toelichting beantwoordt de vraag welk probleem met het creëren van technologie-onafhankelijke en andere verruimde bevoegdheden precies wordt ondervangen. Volgens Amnesty International worden het nut en de noodzaak voor nieuwe ruimere bijzondere bevoegdheden voor de technologie-onafhankelijke interceptie van communicatie en het binnendringen in geautomatiseerde werken door de Nederlandse inlichtingen- en veiligheidsdiensten dan ook niet aangetoond.
Bovendien zijn de voorgestelde mensenrechtelijke waarborgen voor internationale en interinstitutionele samenwerking en het toezicht op de inzet van de ruimere bevoegdheden in de Wiv 20XX niet toereikend. Onder meer het feit dat toestemming van de betrokken minister voor het verwerven van communicatie en de ministeriële toestemming voor het voorbewerken en verwerken van bewaarde metadata en soms ook inhoudelijke communicatiegegevens.

---

[10] Hof van Justitie van de Europese Unie 8 april 2014, nrs. C-293/12 en C294/12, *Digital Rights Ireland* en *Seitlinger*.
[11] Rechtbank Den Haag 11 maart 2015, ECLI:NL:RBDHA:2015:2498, *Privacy First c.s./De Staat.*
[12] Brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties aan de Tweede Kamer van 17 maart 2015, TK 2013-2014, 33 820, nr. 2; Brief van de Commissie van Toezicht op de Inlichtingen- en veiligheidsdiensten (CTIVD) aan de Vaste Commissie voor Binnenlandse Zaken van de Tweede Kamer 11 maart 2014, *Reactie van de CTIVD op het rapport commissie-Dessens*.

Hoofdpijnpunten

1. Toestemmingsvereisten inzet van bijzondere bevoegdheden
2. Toegang tot geautomatiseerde werken: rechtstreekse toegang en hacken
3. 'Doelgericht' interceptiestelsel
4. Medewerkingsplicht bij ontsleuteling
5. Bewaartermijnen en gebruik van bewaarde gegevens
6. Notificatieplicht
7. Gevoelige persoonsgegevens
8. Onafhankelijk en onpartijdig toezicht
9. Samenwerking tussen inlichtingen- en veiligheidsdiensten en andere instanties
10. Klachtbehandeling
11. Melding vermoedens van misstanden: de klokkenluidersregeling
12. Bescherming van mensenrechten van Nederlanders in het buitenland en van niet-Nederlanders

Hieronder wordt afzonderlijk ingegaan op de hoofdpijnpunten van de Wiv 20XX.

1. Toestemmingsvereisten inzet van bijzondere bevoegdheden

Amnesty International vindt dat toestemming voor het inzetten van bijzondere bevoegdheden niet een politieke of bestuurlijke, maar een onafhankelijke juridische - bij voorkeur een rechterlijke - beslissing zou moeten zijn. Daarom zou de voorafgaande toestemming daarvoor niet, zoals nu voorgesteld in de Wiv 20XX, door de desbetreffende minister of namens deze moeten worden gegeven, maar door een rechter of een vergelijkbare onafhankelijke juridische instantie. De toestemmingsvereisten zoals voorgesteld in artikel 24 Wiv 20XX zijn daarom vooralsnog niet toereikend.

Voor de inzet van bijzondere bevoegdheden om communicatie te intercepteren - zowel metadata als inhoudelijke data - dient op transparante wijze toestemming te zijn verleend in overeenstemming met de wet, die toegankelijk én begrijpelijk moet zijn voor het publiek (artikel 8 EVRM en artikelen 7 en 8 EU Handvest van de Grondrechten). Deze toestemming zou geautoriseerd moeten worden door een rechter of een vergelijkbare onafhankelijke instantie en dus niet door de verantwoordelijke minister, of een namens de minister gemandateerde functionaris. Amnesty International vindt dat de toestemmingsvereisten zoals nu opgenomen in artikel 24 Wiv 20XX duidelijker en specifieker moeten worden geformuleerd. Zo moet in het verzoek om toestemming ook een duidelijke afbakening van het beoogde onderzoek worden aangegeven, zowel inhoudelijk, als in tijd. De Wiv 20XX lijkt de mogelijkheid te geven dat onderzoeken oneindig voortduren, aangezien verlengingen keer op keer kunnen worden verzocht. Daarnaast vindt Amnesty International de omschrijving van ‘een beoogd doel’ van de inzet van de bevoegdheid in artikel 24 lid 6 Wiv 20XX niet specifiek genoeg.

2. Toegang tot geautomatiseerde werken: rechtstreekse toegang en hacken

<u>Rechtstreekse toegang</u>
Met de algemene bevoegdheid om een verzoek om rechtstreekse geautomatiseerde toegang tot gegevens in te dienen bij ‘een ieder die geacht wordt de benodigde gegevens te kunnen verstrekken’, krijgen de Nederlandse inlichtingen- en veiligheidsdiensten een ongekend verregaande algemene bevoegdheid voor de verzameling van (geautomatiseerde) gegevens (artikel 22 Wiv 20XX). Deze bevoegdheid zou een basis kunnen worden voor massa-surveillance-praktijken, zoals die door Edward Snowden aan de kaak zijn gesteld. Amnesty International vindt dat bij een dergelijke bevoegdheid bij voorbaat geen sprake is van een gericht onderzoek. Daarom kan de Wiv 20XX in zo’n geval de toets van een legitiem doel en noodzakelijkheid in een democratische samenleving zoals vereist in artikel 8 lid 2 EVRM niet doorstaan.

Het is verontrustend dat een dergelijke ingrijpende bevoegdheid als *algemene* bevoegdheid wordt opgenomen in de Wiv 20XX. Hierdoor worden de waarborgen voor bescherming van mensenrechten geminimaliseerd: met name het verlenen van toestemming voor inzet van de bevoegdheid en het voldoen aan een aantal vereisten daarvoor. Ook is de bevoegdheid te ruim geformuleerd. Het is niet duidelijk wie precies bedoeld wordt met ‘een ieder die geacht wordt de benodigde gegevens te kunnen verstrekken’ (artikel 22 lid 1 Wiv 20XX). Betekent dit dat elke Nederlander of in het buitenland verblijvende persoon verzocht kan worden hieraan mee te werken?

Amnesty International vindt het ook onduidelijk in hoeverre het meewerken door communicatiediensten daadwerkelijk louter op vrijwillige basis zal zijn. Zowel in het wetsvoorstel als in de Telecommunicatiewet is opgenomen hoe en in welke omstandigheden bepaalde communicatiediensten en/of -netwerken verplicht zijn om mee te werken. Of dergelijke verplichtingen ook van toepassing kunnen zijn op de algemene bevoegdheid om gegevens te verzamelen via rechtstreekse toegang tot geautomatiseerde werken in artikel 22 Wiv 20XX blijkt niet duidelijk uit het wetvoorstel en de memorie van toelichting. Zo staat bijvoorbeeld in artikel 11.2a lid 2 sub d Telecommunicatiewet dat aanbieders van bepaalde communicatiediensten en/of -netwerken zich moeten onthouden van aftappen, afluisteren en het anderszins onderscheppen van de communicatie tenzij deze handelingen noodzakelijk zijn ter uitvoering van een wettelijk voorschrift. Amnesty International vindt dat indien de regering besluit de bevoegdheid

uit artikel 22 Wiv 20XX toch op te nemen in de wet, ondubbelzinnig duidelijk moet zijn dat voor iedereen geldt dat meewerken aan het uitoefenen van deze bevoegdheid ook daadwerkelijk vrijwillig is. Dit laat onverlet dat Amnesty International vindt dat artikel 22 Wiv 20XX de basis legt voor massa-surveillance partkijken (zie hiervoor).

Overigens wordt in de memorie van toelichting op de Wiv 20XX aangegeven dat alleen de niet-controversiële voorgestelde wijzigingen uit het ingetrokken post-Madridwetsvoorstel uit 2007 zijn overgenomen. Dit terwijl onder andere de Vaste Kamercommissie van Binnenlandse Zaken en Koninkrijksrelaties van de Eerste Kamer ook zeer kritisch heeft gereageerd op een soortgelijk voorstel over rechtstreekse toegang in artikel 17a van het ingetrokken post-Madridwetsvoorstel. [13] Er was daarover zowel maatschappelijke als politieke controverse. Dat meewerken in het huidige voorstel in artikel 20 Wiv 20XX niet verplicht wordt gesteld, neemt de controverse geenszins weg. Immers, het mogelijk maken van intercepteren van grote hoeveelheden ruwe data is vergelijkbaar 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.[14]

Overigens verwacht Amnesty International dat het College bescherming persoonsgegevens onder andere over de bevoegdheid verwoordt in artikel 22 Wiv 20XX wordt geraadpleegd.

<u>Hacking</u>
Amnesty International constateert dat *hacking* wereldwijd beschouwd als een extreme verregaande vorm van surveillance. Nederland is één van de weinige landen ter wereld die het binnendringen in geautomatiseerde werken door de inlichtingen- en veiligheidsdiensten legitimeert door wetgeving zoals de Wiv 20XX. De meeste andere staten vinden deze vorm van inmenging te ingrijpend. De Nederlandse regering moet zeer ernstig afwegen of hacken überhaupt op een veilige en proportionele manier ingezet kan worden. Zoals de VN-rapporteur over de vrijheid van meningsuiting heeft verklaard "vanuit een mensenrechtenperspectief is het gebruik van zulke technologie zeer zorgwekkend."[15]

Ten aanzien van de Wiv 20XX is Amnesty International van mening dat de bijzondere bevoegdheid om direct dan wel indirect geautomatiseerde werken van het onderzoekssubject, of *target*, te verkennen en binnen te dringen veel te ruim is geformuleerd in artikel 30 Wiv 20XX. Er wordt onder andere voorgesteld om in het kader van het hacken gebruik mogelijk te maken van valse signalen en valse sleutels, en in een valse hoedanigheid binnen te dringen in een geautomatiseerd werk, eventueel zelfs via het geautomatiseerde werk van een derde. Ook mogen daarbij technische voorzieningen aangebracht worden (artikel 30 lid 1 sub b en lid 2 Wiv 20XX). Aangezien het in de Wiv 20XX onduidelijk is hoe omgegaan wordt met het al dan niet moeten herstellen van aangebrachte veranderingen in gehackte geautomatiseerde werken, lopen *targets* het risico dat hun werkelijk bedreigende activiteiten niet meer te onderscheiden zijn van fictie.

In de memorie van toelichting wordt aangegeven dat zelfs personen die geen *target* zijn, non-*targets*, kunnen worden gehackt omdat het *target* mogelijk te veiligheidsbewust zou zijn. Amnesty International vindt dit veiligheidsbewustzijn geen afdoende reden om *non-targets* te hacken. Daardoor lopen zij het risico in de sleepnetten van inlichtingen- en veiligheidsdiensten te komen zonder dat een inbreuk op hun mensenrechten gerechtvaardigd is. Het kan strikt noodzakelijk zijn om het *target* te oberveren, maar het bewerken van geautomatiseerde bestanden van een *non-target* daartoe, maakt de kans op misbruik van bevoegdheden groter, zonder dat daarvoor toereikende waarborgen zijn geformuleerd. Er is een groot

[13] Voorlopig verslag van de Vaste Commissie voor Binnenlandse Zaken en de Hoge Colleges van Staat / Algemene Zaken en Huis de Koningin van 23 september 2008, EK 2008-2009, 30 553, nr. E.
[14] Amnesty International & Privacy International, *Two Years after Snowden. Protecting Human Rights in an age of mass surveillance* (Londen 2015) p. 5.
[15] *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.

risico dat de uitoefening van deze bijzondere bevoegdheid leidt tot een onevenredig nadeel voor een individu die niet eens een *target* is. Overigens zet Nederland haar internationale positie als voorvechter van internetvrijheden op het spel als zij zou binnendringen op buitenlandse geautomatiseerde werken zonder toestemming van het gastland.[16]

Niet alleen is de te ruime formulering van de bijzondere bevoegdheid tot direct of indirect verkennen en binnendringen onwenselijk, maar ook de daarbij behorende waarborgen en het toezicht zijn onvoldoende. De voorgestelde waarborgen hiervoor, zoals de schriftelijke toestemming van de verantwoordelijke minister aan het hoofd van de dienst, zijn geen onafhankelijke toets vooraf of het inzetten van deze bijzondere bevoegdheid noodzakelijk en proportioneel is (onder andere geformuleerd in de artikelen 25 lid 1, 30 en 32 lid 1 Wiv 20XX). (Zie ook punt 1 over toestemmingsvereisten en punt 9 over toezicht.)

3. 'Doelgericht' interceptiestelsel

De interceptie van communicatie maakt een inbreuk mensenrechten. Of het nu om e-mail, telefoongesprekken, sms-en of het verspreiden van berichten via social media gaat, het Europees Hof voor de Rechten van de Mens (EHRM) beschouwd het als een inmenging van het recht op privacy (artikel 8 lid 1 EVRM).[17] Dit geldt ook voor metadata.[18] Tevens is er volgens het Hof sprake van inmenging als deze geïntercepteerde data wordt opgeslagen.[19] Echter overheden kunnen legitieme redenen kunnen hebben voor communicatie-interceptie, bijvoorbeeld om de nationale veiligheid te beschermen (artikel 8 lid 2 EVRM). Amnesty International is dan ook niet tegen interceptie van communicatie en het 'verwerken van gegevens', zoals de wet het noemt en omschrijft in artikel 1 Wiv 20XX, *an sich*, zolang zware en specifieke wettelijke waarborgen zijn opgenomen (artikel 17 lid 2 Internationaal Verdrag inzake burger en politieke rechten). Zo moeten de in te zetten interceptiebevoegdheden een doel dienen dat in de wet is vastgelegd. Ook moeten de bevoegdheden uitsluitend gericht worden ingezet (doelbinding). Dit betekent dat personen, organisaties, locaties en/of technische kenmerken geëxpliciteerd moeten worden. Daarnaast moet 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 noodzakelijk, 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 de individu ten aanzien van wie de bevoegdheid wordt ingezet. Bovendien moet voor die maatregel gekozen worden die het minste nadeel oplevert voor het betrokken individu. Waarborgen ter bescherming van rechten moeten voor iedereen gelijke gelding hebben. Indien onderscheid wordt gemaakt op basis van bijvoorbeeld nationaliteit of locatie, moet dit objectief zijn en gegrond zijn in de wet. Voor de inzet van een dergelijke bevoegdheid moet toestemming worden gegeven door een rechter of vergelijkbare onafhankelijke en onpartijdige instantie.

Dat de inzet van interceptiebevoegdheden gericht is op een doel (onderzoeksgebonden), is vanzelfsprekend. Dat het voorgestelde geheel vernieuwde interceptiestelsel vereist dat interceptie doelgericht is, is dan ook geen noviteit. Amnesty International vindt echter dat wanneer interceptie moet voldoen aan die hiervoor beschreven voorwaarden, waarbij de inzet van de bevoegdheid gericht moet zijn, waarbij de persoon, organisatie, locatie en/of technisch kenmerk expliciet moet zijn gemaakt.

Het 'onderzoek van communicatie in andere gevallen' of het zogenoemde doelgerichte interceptiestel zoals dat nu is voorgesteld in de Wiv 20XX in de artikelen 33, 34 en 35 legaliseert het op ongekende schaal verwerven, voorbewerken en verder verwerken van communicatiegegevens. Het legitimeert daarmee in feite willekeurige en ongerichte inzet van technologische interceptiebevoegdheden, oftewel

[16] Adviesraad Internationale Vraagstukken (AIV), *Het Internet: De Wereldwijde Vrije Ruimte met Begrensde Staatsmacht* , No. 91 (Den Haag, 2014), p. 61.
[17] 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.
[18] EHRM 2 augustus 1984, nr. 8691/79, *Malone/Verenigd Koninkrijk*, § 84.
[19] 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.

massa-surveillance. Uit de memorie van toelichting blijkt ook dat de overheid deze intentie heeft. Amnesty International vindt dat hiermee per definitie sprake is van een bevoegdheid die de eisen van een legitiem doel en noodzakelijkheid in een democratische samenleving niet doorstaat. Daardoor komt de Nederlandse overheid haar mensenrechtenverplichtingen niet na.

Indien de wetgever besluit om middels het nieuwe interceptiestelsel in de Wiv 20XX massa-surveillance bij wet te voorzien, dan biedt het wetsvoorstel ontoereikende waarborgen tegen misbruik van bevoegdheden. De fasering van het interceptiestelsel zou een belangrijke waarborg moeten zijn, maar het verlenen van zogenoemde combinatielasten, waarbij gelijktijdig toestemming wordt verleend voor de inzet van bevoegdheden voor verschillende fasen, doet het effect van deze waarborg teniet. Waarborgen bij zowel internationale als interinstitutionele samenwerking moeten stevig versterkt worden. Transparantie, onafhankelijk en onpartijdig toezicht is onontbeerlijk.

4. Medewerkingsplicht bij ontsleuteling

Amnesty International vindt dat overheden (het gebruik van) technologie waarmee data gecodeerd en geanonimiseerd kan worden niet mag verbieden. Amnesty International onderschrijft het belang van het bestaan van mogelijkheden om anoniem en vertrouwelijk te kunnen communiceren op internet, zoals dat in mei 2015 is uiteengezet door de speciale VN-rapporteur voor vrijheid van meningsuiting.[20] Voor binnenlandse en buitenlandse activisten dissidenten en klokkenluiders, maar ook voor anderen die zich (terecht) zorgen maken over het vastleggen van online gedrag vanwege de mogelijkheid dat de vastgelegde gegevens in de toekomst tegen hun wensen en belangen opduiken in andere contexten. Versleuteling, of encryptie, is de enige manier waarop digitale communicatie beschermd kan worden tegen inbreuken als cybercriminaliteit, identiteitsdiefstal, of onrechtmatige interceptie door overheden. De voorgestelde Wiv 20XX verbiedt encryptie niet specifiek, maar stelt wel een medewerkingsplicht in voor ontsleuteling. Hierdoor wordt via een omweg hetzelfde resultaat bereikt: namelijk dat inlichtingen- en veiligheidsdiensten te allen tijde toegang kunnen hebben tot versleutelde gegevens en dat mensen hun communicatie niet effectief mogen beschermen. De geheime diensten mogen zich volgens artikel 41 lid 1 Wiv 20XX wenden tot 'degene van wie redelijkerwijs vermoed wordt dat hij kennis draagt van de wijze van versleuteling van desbetreffende gesprekken […].'

Amnesty International vindt dat niet duidelijk is wie precies verplicht kan worden mee te werken aan ontsleuteling. Betreft dit bijvoorbeeld de aanbieders van (besloten) internetdiensten, de makers of aanbieders van producten zoals smartwatches, thermostaten en auto's? Of kan elke Nederlander of in het buitenland verblijvende persoon met enige kennis van zaken verplicht worden hieraan mee te werken? Het is belangrijk om in dit verband ook op te merken dat het strafbaar stellen van het niet meewerken onwenselijk is (artikel 132 Wiv 20XX). Een verdachte mag nooit worden gedwongen aan zijn eigen veroordeling mee te werken. Dit is vastgelegd in artikel 6 van het EVRM. Volgens artikel 41 lid 4 Wiv 20XX zouden de Nederlandse inlichtingen- en veiligheidsdiensten dit straks toch kunnen eisen, omdat een persoon aan wie het verzoek tot ontsleuteling is gericht daaraan verplicht dient mee te werken.

Uit een opiniepeiling van Amnesty International uit 2015 blijkt dat 56 procent van de ondervraagde Nederlanders van mening is dat technologiebedrijven internetcommunicatie moeten beveiligen, zodat de inhoud van de gegevens (zoals e-mails, app-berichten of sociale media-activiteiten) niet zonder toestemming van de gebruikers toegankelijk is. In andere woorden: de opiniepeiling geeft aan dat Nederlanders de versleuteling van onze communicatiegegevens door het bedrijfsleven toejuichen.

Amnesty International is van mening dat de bij wet voorziene medewerkingsplicht bij ontsleuteling per definitie sprake is van een bevoegdheid die de eisen van een legitiem doel en noodzakelijkheid in een democratische samenleving niet doorstaat. Daardoor komt de Nederlandse overheid met deze voorgestelde bijzondere bevoegdheid haar mensenrechtenverplichtingen niet na. Het verplicht

[20] *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.

meewerken aan ontsleuteling en het strafbaar stellen van het niet meewerken daaraan is dus onwenselijk.

5. Bewaartermijnen en gebruik van bewaarde gegevens

Amnesty International vindt dat aan de vereisten van strikte noodzakelijkheid, proportionaliteit en subsidiariteit voor de inzet van interceptie en aftapbevoegdheden alleen kan worden voldaan als er, in de praktijk effectieve, waarborgen zijn. Zo moet de bewaarperiode van gegevens beperkt worden. Er moeten duidelijke instructies zijn voor het vernietigen van dergelijke gegevens. Ook zou in de wet vastgelegd moeten worden dat de bewaarde data zodra dit mogelijk is verwijderd moeten worden en op z'n laatst nadat zij niet meer strikt noodzakelijk zijn om het doel van het onderzoek waarvoor de gegevens verworven waren te bereiken. De gegevens zouden in de periode dat ze bewaard worden alleen gebruikt mogen worden voor het onderzoek waarvoor ze verworven zijn en niet voor andere onderzoeken. Alleen in uitzonderlijke situaties kan hiervan worden afgeweken en alleen indien er een duidelijke wettelijke basis voor vervolggebruik is. Bovendien moeten waarborgen in de wet worden opgenomen met betrekking tot de procedures voor secundair gebruik van gegevens en de omstandigheden waarin daarvoor toestemming verleent mag worden.

Het wetsvoorstel legt in verschillende artikelen vast welke gegevens op welke manier verworven mogen worden, hoe lang deze verworven gegevens bewaard mogen worden en in sommige gevallen ook waarvoor ze in die periode gebruikt mogen worden, voordat ze verwijderd en/of vernietigd moeten worden. Amnesty International vindt dat in de Wiv 20XX en memorie van toelichting niet duidelijk is aangegeven dat verdere verwerking van bewaarde gegevens alleen is toegestaan in het kader van een onderzoek waarvoor de gegevens oorspronkelijk verworven zijn. Het wetsvoorstel lijkt het daarmee mogelijk te maken om de bewaarde gegeven voor andere doeleinden te gebruiken. Zo stelt artikel 47 Wiv 20XX dat eigen gegevensbestanden van de diensten gebruikt mogen worden voor geautomatiseerde verwerking. In het verzoek voor toestemming daarvoor hoeft niet gemotiveerd te worden met betrekking tot welk (wettelijk vastgelegd) doel de verwerking plaatsvindt. Om misbruik van bevoegdheden te voorkomen, moet nadrukkelijk in de wet worden opgenomen dat verworven gegevens uitsluitend gebruikt mogen worden voor (het doel van) dat onderzoek waarvoor ze oorspronkelijk verworven zijn.

In enkele artikelen wordt aangegeven dat indien verworven gegevens niet relevant blijken voor het onderzoek, ze na ten hoogste 12 maanden vernietigd moeten worden (artikelen 30 lid 9 sub c, 32 lid 10 en 38 lid 7 Wiv 20XX). Op basis van artikel 57 lid 1 Wiv 20XX zouden ze al wel vast verwijderd moeten worden. In de memorie van toelichting wordt uitgelegd dat verwijderde gegevens opnieuw gebruikt mogen worden, indien het doel waarvoor ze verworven waren weer actueel is, of voor een eventueel ander doel. Hergebruik - en voorwaarden daarvoor - van bewaarde, dan wel verwijderde gegevens is niet met zoveel woorden geregeld in de wet. Amnesty International vindt dat onwenselijk. De juridische basis hiervoor moet ondubbelzinnig geregeld zijn in de wet, inclusief toereikende waarborgen. Overigens lijkt de formulering in de wet te suggereren dat indien relevantie wel gebleken is, de gegevens langer dan drie jaar bewaard zouden mogen worden.

Het voorgestelde interceptiestelsel legitimeert in feite willekeurige en ongerichte inzet van interceptiebevoegdheden. Amnesty International vindt dat hiermee per definitie sprake is van een bevoegdheid die de eisen van een legitiem doel en noodzakelijkheid in een democratische samenleving niet doorstaat. Daardoor komt de Nederlandse overheid met het wettelijk vastleggen van deze bevoegdheid haar mensenrechtenverplichtingen onder artikel 8 EVRM niet na. Ook het bewaren en anderszins verwerken van gegevens die op basis van deze artikelen verworven, voorbewerkt en verder bewerkt zijn daarmee in strijd.

6. Notificatieplicht

Amnesty International vindt dat alle personen ten aanzien van wie bijzondere bevoegdheden zijn ingezet daarover geïnformeerd moeten worden, tenzij dat overduidelijk onmogelijk is omdat iemand bijvoorbeeld overleden is. In artikel 46 Wiv 20XX wordt voorgesteld dat de notificatieplicht mag worden uitgesteld of vervalt als het legitieme doel van communicatie-interceptie daardoor in gevaar komt. Amnesty International benadrukt hierbij het belang dat de inlichtingen- en veiligheidsdiensten hier geen te ruime invulling aangeven, een praktijk die in het verleden door het CTIVD geconstateerd is.[21]

In artikel 46 Wiv 20XX wordt een notificatieplicht slechts voor enkele bijzondere bevoegdheden geregeld. Amnesty International is van mening dat de notificatieplicht zou moeten gelden voor de inzet van *alle* bijzondere bevoegdheden. Bovendien is Amnesty International van mening dat in het verslag dat wordt uitgebracht aan de onderzochte persoon ook moet worden aangegeven op basis van welke juridische grond de bevoegdheid is uitgevoerd, welke gegevens zijn verzameld en op welke rechtsmiddelen een beroep gedaan kan worden.

Het voorgestelde interceptiestelsel legitimeert in feite willekeurige en ongerichte inzet van interceptiebevoegdheden van communicatie, oftewel massa-surveillance. Amnesty International vindt dat hiermee per definitie sprake is van een bevoegdheid die de eisen van een legitiem doel en noodzakelijkheid in een democratische samenleving niet doorstaat. Daardoor komt de Nederlandse overheid met het wettelijk vastleggen van deze bevoegdheid haar mensenrechtenverplichtingen niet na. Indien de overheid besluit over te gaan tot het uitvoeren van bevoegdheden in lijn met het voorgestelde interceptiestelsel, dient duidelijk gesteld te worden dat alle *non-targets* wiens gegevens verworven en eventueel verder bewerkt zijn ook als zodanig worden aangemerkt. De overheid moet beter uitwerken hoe *non-targets* genotificeerd zullen worden.

7. Gevoelige persoonsgegevens

Amnesty International vindt dat de Wiv 20XX te beperkt aangeeft welke gevoelige persoonsgegevens niet verwerkt mogen worden door de inlichtingen- en veiligheidsdiensten. Zo is in artikel 18 lid 3 Wiv 20XX politieke gezindheid niet opgenomen. In de memorie van toelichting wordt aangegeven dat politieke gezindheid beschouwd wordt als een gevoelig gegeven, maar artikel 18 lid 3 en 4 Wiv 20XX wordt hierop niet van toepassing geacht om 'evidente redenen'. Mede met het oog op hoe het wetsvoorstel het delen van gegevens met buitenlandse diensten mogelijk maakt, is dit voor Amnesty International helemaal niet evident. Amnesty International vindt dan ook dat politieke gezindheid opgenomen moet worden in artikel 18 lid 3 Wiv 20XX.

8. Onafhankelijk en onpartijdig toezicht

In de Wiv 20XX is de betrokken minister verantwoordelijk voor een goede uitvoering van de wet (door de respectievelijke inlichtingen- en veiligheidsdiensten en eventuele andere betrokkenen), moet de betrokken minister zelf toestemming geven voor de inzet van een bijzondere bevoegdheid, en bepaalt dezelfde betrokken minister of hij/zij de bevindingen en aanbevelingen van de CTIVD onderschrijft en overneemt, of naast zich neerlegt. De betrokken minister keurt in feite zijn/haar eigen vlees. Amnesty International vindt dat een onwenselijke praktijk. Onafhankelijk, onpartijdig, bindend toezicht, vóóraf is de sterkste waarborg tegen misbruik van (bijzondere) bevoegdheden.[22]

In toenemende mate is er consensus onder Europese rechters dat onafhankelijk, onpartijdig, bindend juridisch toezicht de sterkste waarborg tegen niet-noodzakelijke en disproportionele surveillance en

[21] CTIVD, *Toezichtsrapport Inzake de rechtmatigheid van de uitvoering van de notificatieplicht door de AIVD,* nr. 24 (2010).
[22] Instituut voor Informatierecht, Universiteit van Amsterdam, *Ten standards for oversight and transparency of national intelligence services* (Amsterdam 2015).

interceptie van communicatie is. Het Europees Hof van de Rechten van de Mens is dit al sinds lange tijd van oordeel.[23] De meeste recente uitspraak hierover is van het Hof van Justitie van de Europese Unie in Digital Rights tegen Ierland over de retentie van communicatiedata onder de Europese dataretentierichtlijn (2006/24/EC) en de verenigbaarheid daarvan met artikel 8 EVRM en de artikelen 7 en 8 van het Handvest van de Grondrechten van de Europese Unie. [24]

Voor de inzet van bijzondere bevoegdheden ten aanzien van journalisten en met betrekking tot het briefgeheim zoals geformuleerd in artikel 13 van de Grondwet is rechterlijke toestemming nodig. Amnesty International vindt dat de inhoudelijke argumentatie waarom rechterlijke toestemming niet nodig zou zijn voor de inzet van overige bijzondere bevoegdheden, of de inzet van die bevoegdheden ten aanzien van andere personen ontbreekt. Het voldoet nu niet aan de eisen die de jurisprudentie van het Europese Hof voor de Rechten van de Mens stelt.

Amnesty International vindt dat toestemming voor het inzetten van bijzondere bevoegdheden, zoals het binnendringen van geautomatiseerde werken en internationale samenwerking, door een rechter of vergelijkbare onafhankelijke juridische instantie moet worden gegeven.

Als het voorstel om de minister - of een door de minister gemandateerde functionaris - toestemming te laten geven voor de inzet van bijzondere bevoegdheden desondanks wordt doorgezet, is een onmiddellijke preventieve bindende toets door een onafhankelijke en onpartijdige juridische instantie zoals een rechter vereist. Een minder gewenst alternatief is dat dit door de afdeling toezicht van de CTIVD gedaan zou kunnen worden, zoals genoemd in artikel 85 Wiv 20XX. Een toets door deze afdeling moet dan wel een juridisch bindend oordeel omvatten, wat in het wetsvoorstel niet het geval is. Het belang hiervan is benadrukt in onder andere EHRM-jurisprudentie[25], het evaluatierapport van de commissie-Dessens[26], de reactie van het CTIVD op dit evaluatierapport[27], en de jaarrapportage 2015 van het College voor de Rechten van de Mens[28]. Als vervolgens blijkt dat de toestemming voor de inzet van een bijzondere bevoegdheid onrechtmatig is, zou de betrokken inlichtingen- en veiligheidsdienst de uitvoering daarvan niet mogen aanvangen of moet zij deze direct staken of opschorten en eventueel reeds verzamelde gegevens terstond vernietigen, zodat (verdere) inbreuken op mensenrechten, waaronder het recht op privacy, voorkomen wordt.

Door de uitvoering van bevoegdheden door inlichtingen- en veiligheidsdiensten wordt inbreuk gemaakt op mensenrechten. Daarom vindt Amnesty International het noodzakelijk dat via toezicht achteraf, zoals dat nu geregeld is voor de CTIVD, een juridisch bindend oordeel geveld kan worden, zodat effectief toezicht plaats kan vinden. De Wiv 20XX zou dan ook op dit onderdeel moeten worden aangepast.

9. Samenwerking tussen inlichtingen- en veiligheidsdiensten en andere instanties

<u>Internationale samenwerking</u>
Amnesty International vindt dat het delen van gegevens met buitenlandse inlichtingen- en veiligheidsdiensten alleen mag plaatsvinden binnen een wettelijk kader dat voldoet aan mensenrechtenverplichtingen. Amnesty International is in eerste instantie dan ook verheugd dat onder andere het mensenrechtenbeleid van een land wordt getoetst voordat gegevens met buitenlandse

[23] 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.
[24] Hof van Justitie van de Europese Unie 8 april 2014, nrs. zaken C-293/12 en C294/12, *Digital Rights Ireland* en *Seitlinger,* § 62.
[25] EHRM 6 september 1978, nr. 5029/71, *Klass e.a./Duitsland*, § 50; EHRM 29 juni 2006, nr. 54934/00, *Weber en Saravia/Duitsland*, § 106; EHRM 18 mei 2010, nr. 26839/05 *Kennedy/Verenigd Koninkrijk*, § 153; EHRM 24 november 2005, nr. 53886/00, *Tourancheau en July/Frankrijk*.
[26] Commissie-Dessens, *Evaluatie van de Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen* (2013), p. 102.
[27] Brief van de CTIVD aan de Vaste Commissie voor Binnenlandse Zaken van de Tweede Kamer 11 maart 2014, *Reactie van de CTIVD op het rapport commissie-Dessens*, p. 6-7.
[28] College voor de Rechten van de Mens, *Mensenrechten in Nederland. Jaarlijkse rapportage 2014* (Utrecht 2015) p. 86.

diensten van dat land worden uitgewisseld. De toelichting op hoe in de praktijk invulling gegeven kan worden aan het naleven van deze eis is echter dusdanig ruim geformuleerd, dat samenwerking met alle diensten mogelijk is ongeacht de staat van de mensenrechten in het land waarmee wordt samengewerkt. Dat in de praktijk inderdaad wordt samengewerkt met alle diensten blijkt uit toezichtsrapporten van het CTIVD.[29] Hoe het criterium 'respecteren van mensenrechten' begrepen moet worden, moet duidelijker en veel specifieker worden uitgewerkt. Overigens dienen ook de overige criteria, zoals democratische inbedding, professionaliteit en betrouwbaarheid ingevuld te worden.

Ook voor met buitenlandse diensten te delen communicatie-gegevens moet volgens Amnesty International gelden dat ze in principe niet voor een ander doel dan waarvoor ze verworven zijn verwerkt mogen worden én dat er waarborgen moeten zijn voor het verlenen van toestemming voor secundair gebruik. In het wetsvoorstel wordt via artikel 49 Wiv 20XX echter het delen van niet geëvalueerde, oftewel ruwe, nog niet voor onderzoek verwerkte, data met buitenlandse diensten een mogelijkheid. Daarnaast wordt via artikel 18 lid 1 sub d Wiv 20XX mogelijk gemaakt dat met buitenlandse diensten gegevens gedeeld kunnen worden over een persoon 'over wie door een andere inlichtingen- of veiligheidsdienst gegevens zijn ingewonnen.' Voor deze personen hoeft dus niet beargumenteerd te worden waarom het noodzakelijk is om ten aanzien van hen bevoegdheden in te zetten. Amnesty International maakt zich hier grote zorgen om.

Amnesty International vindt ook dat onvoldoende is uitgelegd welke belangen van buitenlandse inlichtingen- en veiligheidsdiensten behartigd mogen worden door de Nederlandse diensten. Het wetsvoorstel Wiv 20XX maakt niet duidelijk of voor buitenlandse inlichtingen- en veiligheids-diensten andere belangen behartigt mogen worden dan voor de Nederlandse diensten is toegestaan.

Het voorgestelde interceptiestelsel legitimeert in feite willekeurige en ongerichte inzet van interceptiebevoegdheden, oftewel massa-surveillance. Amnesty International vindt dat hiermee per definitie sprake is van een bevoegdheid die de eisen van een legitiem doel en noodzakelijkheid in een democratische samenleving niet doorstaat. Amnesty International vindt het verwerven en verder verwerken van bulkgegevens, zoals gedefinieerd in de wet, niet in lijn met de mensenrechtenverplichtingen van de Nederlandse overheid. Het delen van informatie die in bulk verzameld zijn met buitenlandse diensten is net zo ongewenst. Alleen gericht verzamelde inlichtingen zouden gedeeld moeten kunnen worden, en alleen voor zover aan strikte waarborgen is voldaan.

De mogelijkheden die de Wiv 20XX biedt voor internationale samenwerking, mede ook in combinatie met het in feite legaliseren van massa-surveillance, vindt Amnesty International zeer zorgelijk. Amnesty International benadrukt dat de Nederlandse mensenrechtenverplichtingen ook extraterritoriaal gelden. (Meer hierover in punt 12). Als gevolg daarvan vindt Amnesty International dat de waarborgen voor bescherming van mensenrechten, waaronder het recht op eerbiediging van de persoonlijke levenssfeer, in het wetsvoorstel ontoereikend zijn. Ook de waarborg van ministeriële toestemming is onvoldoende. (Zie ook punt 1 over toestemmingsvereisten en punt 9 over toezicht).

<u>Interinstitutionele samenwerking</u>
Amnesty International vindt dat het samenwerken tussen de Nederlandse inlichtingen- en veiligheidsdiensten met andere overheidsdiensten alleen mag plaatsvinden binnen een wettelijk kader en als het nut en de noodzaak voor een specifiek onderzoek worden aangetoond. Het is zeer opmerkelijk dat deze samenwerking veel ruimer wordt in de Wiv 20XX in vergelijking met de huidige wet. Zo wordt de kring van functionarissen die werkzaamheden verrichten voor de Nederlandse inlichtingen- en veiligheidsdiensten verrichten uitgebreid (artikel 79 Wiv 20XX). Amnesty International vraagt zich af waarom de Hoofddirecteur van de Immigratie- en Naturalisatie dienst of de inspecteur-generaal van de inspectie SWZ van het Ministerie van de Sociale Zaken bijvoorbeeld werkzaamheden voor de AIVD

[29] CTIVD, *Toezichtsrapport Over de samenwerking van de AIVD met buitenlandse inlichtingen– en/of veiligheidsdiensten*, nr. 22a (2009); CTIVD, *Toezichtsrapport Over de samenwerking van de MIVD met buitenlandse inlichtingen– en/of veiligheidsdiensten*, nr. 22b (2015).

zouden moeten verrichten. Ook is het de vraag waarom de inlichtingen- en veiligheidsdiensten meer ondersteuning moeten gaan bieden aan de opsporing en vervolging van strafbare feiten. In de memorie van toelichting wordt nauwelijks beargumenteerd waarom dit nodig is. Bij deze voorgestelde uitbreiding wordt het samenwerkingsverband CT Infobox genoemd, dat gericht is op terrorismebestrijding. Of het nuttig, noodzakelijk en/of wenselijk is in relatie tot bescherming van mensenrechten dat functionarissen een extra taak krijgen is een vraag die niet wordt beantwoord.

Tevens zijn er onvoldoende waarborgen voor interinstitutionele samenwerking. Volgens het wetsvoorstel zouden bijvoorbeeld werkzaamheden die de Hoofddirecteur van de Immigratie- en Naturalisatiedienst voor de AIVD verricht onder de verantwoordelijkheid van de minister van Binnenlandse Zaken en Koninkrijksrelaties komen te vallen. Het is echter onduidelijk of de rekenschap en het toezicht zoals voorgesteld in de Wiv 20XX dan ook op deze minister van toepassing is. Verder is een pijnpunt dat een verzoek om ondersteuning van het bevoegd gezag aan de geheime diensten deels wordt gewaarborgd door tussenkomst van het Openbaar Ministerie (artikel 83 Wiv 20XX). Volgens Amnesty International zou een dergelijk verzoek getoetst moeten worden door een onafhankelijk juridische entiteit. (Zie hierover punt 1.) Ook is het niet wenselijk dat de verantwoordelijkheid voor de feitelijke uitvoering onder het bevoegd gezag valt.

Amnesty International vindt dat in de Wiv 20XX en wetten waarin de kaders voor gegevensverwerking door andere instanties geregeld zijn, vastgelegd zou moeten worden dat voor het verwerken van gegevens dan wel de inzet van bevoegden via of door Nederlandse instanties minimaal dezelfde waarborgen moeten gelden als voor de AIVD en MIVD. Zolang dat niet het geval is, creëert de overheid een situatie waarin de afweging van belangen van de staat tegenover de rechten van individuele burgers en organisaties niet plaats hoeft te vinden. De Nederlandse overheid komt hiermee haar mensenrechtenverplichtingen niet na.

10. Klachtbehandeling

Amnesty International vindt dat de klachtbehandeling onder de Wiv 20XX ook van toepassing zou moeten zijn op anderen dan degene jegens wie het optreden heeft plaatsgevonden. Ook familieleden van de betrokkenen en andere maatschappelijke actoren, waaronder non-gouvernementele organisaties of journalisten zouden het recht moeten hebben om een klacht in te dienen (artikel 110 Wiv 20XX). Sinds de onthullingen van Edward Snowden hebben Amnesty International en andere maatschappelijke organisaties[30] gezamenlijk de interceptie en het aftappen van hun communicatie aangekaart bij het Britse *Investigatory Powers Tribunal* en het Europese Hof voor de Rechten van de Mens.[31] Eén van hun argumenten was dat het werk van non-gouvernementele organisaties en mensenrechtenactivisten gehinderd wordt door het intercepteren en internationaal delen van informatie.

11. Melding vermoedens van misstanden: de klokkenluiderregeling

Amnesty International vindt dat klokkenluiders sterkere juridische bescherming moeten krijgen dan nu wordt voorgesteld in de Wiv 20XX. Het is verheugend dat ambtenaren van de inlichtingen- en veiligheidsdiensten en anderen, zoals medewerkers van telecombedrijven, die betrokken zijn geweest bij de uitvoering van de Wet op de inlichtingen en veiligheidsdiensten, een melding van (een vermoeden van) een misstand kunnen indienen bij de afdeling klachtbehandeling van de CTIVD. Het is echter de vraag of de melder als klokkenluider voldoende beschermt wordt. De professionele en persoonlijke gevolgen voor de melder lijken weinig tot geen aandacht te krijgen in het wetsvoorstel Wiv 20XX.

[30] De andere betrokken organisaties zijn Liberty (The National Council of Liberties), Privacy International, the American Civil Liberties Union & others (ACLU), Amnesty International Limited and Bytes For All.
[31] IPT, Judgement, zaaknummers: IPT/13/77/H, IPT/13/92/CH, IPT/13/168-173/H, IPT/13/194/CH, IPT/13/204/CH, § 3–6, 5 december 2014, http://www.ipt-uk.com/section.aspx? pageid=8; *10 Human Rights Organizations versus the United Kingdom: additional submissions on the facts of complaints, complaints to the ECHR,* https://privacyinternational.org/sites/default/files/HR%20Orgs%20v%20UK.pdf, zie ook https://www.amnesty.org/en/documents/ior60/1415/2015/en/; EHRM 7 januari 2014, nr. 58170/13, *Big Brother e.a./Verenigd Koninkrijk.*

Volgens de Ambtenarenwet mogen ambtenaren geen nadelige gevolgen ondervinden voor hun rechtspositie tijdens en na het volgen van de procedure (artikel 125 quinquies lid 3). Deze regel is echter niet van toepassing op melders die geen ambtenaar zijn. In de wet zou vastgelegd moeten worden dat zij minimaal dezelfde bescherming genieten. Indien via toekomstige wetgeving, anders dan in de Wiv 20XX, betere bescherming voor klokkenluiders wordt geregeld, dient de bescherming die via de Wiv 20XX wordt gegeven daaraan gelijkgesteld te worden.

De CTIVD neemt de melding van een vermoeden van een misstand niet in behandeling als het gaat om een gedraging waarvan een procedure bij de strafrechter aanhangig is (artikel 117 lid 2). Er zijn onvoldoende waarborgen opgenomen om misbruik te voorkomen waarbij er een strafrechtelijke procedure wordt gestart om te voorkomen dat een melding in behandeling wordt genomen.

Het oordeel dat de afdeling klachtbehandeling van de CTIVD over de melding velt is niet bindend. Dit is onwenselijk. Indien het vermoeden van een misstand (deels) waar blijkt te zijn, is de desbetreffende minister vervolgens niet verplicht om ervoor te zorgen dat de situatie verandert. Ook is hij niet verplicht om gehoor te geven aan eventuele aanbevelingen van de afdeling klachtbehandeling.

Amnesty International vindt dat er betere waarborgen opgenomen moeten worden om ervoor te zorgen dat bijvoorbeeld een (gemelde) onrechtmatige uitoefening van een bevoegdheid wordt gestaakt en om de kwetsbare positie waarin de melder zich kan bevinden beter te beschermen.

12. 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 het recht van de individu waar inbreuk op wordt gemaakt. Amnesty International vindt in de context van interceptie van communicatie en hacken dit het geval is en onder andere het recht op eerbiediging van een individu’s persoonlijke levenssfeer en vrije meningsuiting in het geding zijn.

Amnesty International 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 (wiens 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.