Bits of Freedom
Prinseneiland 97hs
1013 LN Amsterdam

Lotte Houwing
+31 6 8320 7546
lotte@bitsoffreedom.nl

bitsoffreedom.nl
IBAN: NL73 TRIO 0391 1073 80
KVK: 34 12 12 86, Amsterdam

Geachte Evaluatiecommissie,

Allereerst bedankt voor uw uitnodiging tot het inzenden van een reactie aan uw commissie. Bits of Freedom en Vrijschrift waarderen deze open benadering van uw taakopvatting en wij delen graag onze observaties met u.

Zoals u weet staan Bits of Freedom en Vrijschrift zeer kritisch ten opzichte van de Wet op de Inlichtingen- en Veiligheidsdiensten 2017 en zijn wij van mening dat de wet beter kan. Voor onze kritiekpunten op de wet in zijn algemeniteit verwijzen wij u naar de website van Bits of Freedom.[1] In deze reactie zullen wij ons zoveel mogelijk beperken tot onze observaties vanaf de implementatie van de wet in mei 2018, zoals u in uw brief vraagt.

Helaas is het zo dat het inherent is aan het werk van de geheime diensten dat er weinig informatie beschikbaar is over hoe het werk er in de praktijk uitziet. Dat betekent dat wij voor onze observaties helaas ook beperkt zijn tot de u welbekende bronnen zoals de rapportages van de TIB en de CTIVD.

Hieronder zullen wij ingaan op een aantal van onze zorgen die gebaseerd zijn op observaties van de praktijk sinds mei 2018 en die vallen binnen uw taakomschrijving zoals die is weergegeven in het Instellingsbesluit.

Uiteraard zijn wij gaarne bereid tot een eventuele toelichting indien gewenst.

Met vriendelijke groet,
namens Stichting Bits of Freedom en Stichting Vrijschrift

Lotte Houwing en Walter van Holst

1 https://www.bitsoffreedom.nl/dossiers/geheime-diensten/

Reactie Bits of Freedom en Vrijschrift evaluatie Wiv 2017

Een ongelijke verhouding tussen waarborgen en bevoegdheden van de diensten

De verhouding tussen de bevoegdheden en de waarborgen van de geheime diensten is in de Wiv 2017 niet in balans. Ook in het Wijzigingsvoorstel is onvoldoende tegemoet gekomen aan de fundamentele bezwaren die in de maatschappelijke discussie die aan het referendum vooraf ging naar voren zijn gebracht, en ten grondslag lagen aan de uitslag. Deze disbalans komt met name voort uit de introductie van de zogenaamde bulkbevoegdheden; Onderzoeksopdrachtgerichte(OOG-)interceptie, de informantenbevoegdheid, de hackbevoegdheid en het uitwisselen van (ongeëvalueerde) gegevens met buitenlandse diensten. Deze bevoegdheden zorgen ervoor dat meer burgers vaker en voorkoombaar onterecht in het vizier van de geheime diensten komen. Wij vinden dit onacceptabel, en zijn van mening dat de wijzigingen die worden voorgesteld in het huidige Wijzigingsvoorstel onvoldoende aan deze fundamentele bezwaren tegemoet komen, en daardoor niet in staat zijn deze disbalans te herstellen.[2]

Maak van de informantenbevoegdheid een bijzondere bevoegdheid

Er gelden verschillende waarborgen ten aanzien van bulkbevoegdheden in de Wiv 2017. Zo kan er bijvoorbeeld met de informantenbevoegdheid real-time toegang worden verkregen tot gehele databanken of de gehele databank worden overgenomen, terwijl deze bevoegdheid niet als een bijzondere bevoegdheid is geclassificeerd. Hiermee valt de inzet van deze bevoegdheid buiten het toezichtsregime van ministeriële toestemming met toetsing door de TIB. Deze inconsistentie in het toekennen van waarborgen bij ingrijpende bevoegdheden waarmee gegevens in bulk kunnen worden verzameld leidt tot een lacune in het totale waarborgenstelsel.

De geheime diensten overspoelen zichzelf met data

Deze disbalans heeft naast het principiële probleem dat wij er mee hebben, zijn weerslag op de praktijk. De diensten overspoelen zichzelf met gegevens. Dit heeft niet alleen nadelige effecten op de rechten en vrijheden van burgers, maar evengoed

2 https://www.trouw.nl/opinie/laat-onze-stem-niet-verloren-gaan-ga-niet-akkoord-met-cosmetische-aanpassingen-van-de-sleepwet~bbba84f2/

op de uitvoeringspraktijk en slagkracht van de diensten zelf[3], en daarmee op onze nationale veiligheid. Uit de derde voortgangsrapportage van de CTIVD blijkt dat al voordat de OOG-interceptiebevoegdheid in werking was gesteld de geheime diensten meer gegevens verzamelden dan zij kon verwerken[4], wat grote vragen oproept over de proportionaliteit van de inzet van dit data-intensieve middel.

Dit probleem leidde ertoe dat gegevens een half jaar langer werden bewaard dan de wettelijke termijnen toestaan en dat niet langer de gegevens zelf, maar een grote verzameling gegevens in één keer op relevante werd beoordeeld. Deze praktijk is op beide punten onrechtmatig, het langer dan de wettelijke termijnen toestaan bewaren van gegevens van burgers is een onrechtmatige inbreuk op hun privacy en het beoordelen van de gegevens in bulk is zelfs schadelijk voor de uitvoeringspraktijk van de diensten. Immers, als een dataset overwegend gegevens bevat die als niet-relevant worden beoordeeld, wordt dan de hele verzameling, inclusief wel relevante gegevens verwijderd? Dan gaat er wellicht waardevolle informatie verloren. Wordt een hele verzameling als relevant beoordeeld omdat er waardevolle informatie inzit? Dan worden de niet-relevante gegevens in die verzameling onrechtmatig lang bewaard, met alle gevolgen voor de rechten van de personen wiens data het betreft van dien. Om met de woorden van de toezichthouder te spreken: “Hier is geen sprake meer van een risico, maar van een onrechtmatigheid.”[5]

Het gerichtheidsvereiste bij OOG-interceptie.

In de aanloop naar het referendum werd ons door de geheime diensten en de wetgever verzekerd dat er een belangrijk verschil zou zijn tussen ongericht en ‘onderzoeksopdrachtgericht’. Dit verschil zou vorm krijgen in de toepassing van het criterium ‘zo gericht mogelijk’.

In de eerste voortgangsrapportage van de CTIVD wordt vervolgens vastgesteld dat er geen sprake is van implementatie van deze waarborg. De toezichthouder schrijft:

> “Aan het criterium ‘zo gericht mogelijk’ is geen herkenbare invulling gegeven in het beleid en de werkprocessen van de beide diensten. Het beleid, de werkinstructies en de feitelijke werkprocessen van de beide diensten maken niet duidelijk hoe ‘zo gericht mogelijk’ in de praktijk uitwerking krijgt. De toepassing van het criterium ten aanzien van de verschillende stadia van het interceptieproces lijkt vanaf 1 mei 2018 dus vrijwel achterwege te zijn gebleven, terwijl het juist daar ook een richtinggevende werking kan en moet hebben.”[6]

3 Zie ook https://www.bitsoffreedom.nl/2019/12/04/geheime-diensten-overspoelen-zichzelf-met-gegevens/

4 CTIVD Voortgangsrapportage 3, nr. 66, p. 9-11.

5 CTIVD Voortgangsrapportage 3, nr. 66, p. 9.

6 CTIVD Voortgangsrapportage 1, nr. 59, p. 10.

De toezichthouder geeft opvolging aan dit rapport door een onderzoek in te stellen naar de toepassing van filters bij OOG-interceptie door de geheime diensten. Waar zij in de voortgangsrapportage sprak van een hoog risico op onrechtmatigheden gaat zij in deze rapportage in op de vraag hoe de filters die het gerichtheidsvereiste in de praktijk moeten brengen, worden toegepast en of deze toepassing voldoet aan de vereisten van rechtmatigheid en de Wiv 2017.

Uit dit rapport blijkt dat procesbeschrijvingen en werkinstructies om de filters bij OOG-interceptie toe te passen ontbraken, en dat het beleid dat hier wel voor was te weinig houvast bood om te kunnen dienen als kader voor het toepassen van filters en daarmee het rechtmatig uitoefenen van de OOG-interceptie bevoegdheid.[7] In de praktijk bleek er bij etherinterceptie wel gefilterd te worden, en er ten aanzien van de bevoegdheid tot OOG-interceptie op de kabel wel een voornemen te bestaan om te filteren. Echter, deze filtering was voornamelijk ingegeven door capaciteitsoverwegingen en technische beperkingen, en voldeed daarom intrinsiek niet aan de strengere eisen die de wetgeving vanuit de bescherming van het recht op privacy worden gesteld.[8]

Daarnaast werd door de minister in april 2018 de toezegging gedaan dat, omdat inzet van OOG-interceptie voor onderzoek in Nederland vrijwel nooit subsidiair zou zijn, het vrijwel uitgesloten zou zijn dat deze bevoegdheid de komende jaren zou worden ingezet voor onderzoek naar communicatie met oorsprong en bestemming in Nederland (met uitzondering van onderzoek voor cyber-defence). De CTIVD werd verzocht om hierop verscherpt toezicht te houden.[9] Idealiter zouden dus als het verzoek niet op Nederland betrekking heeft deze gegevens al in de eerste negatieve filtering worden weggefilterd. Uit berichtgeving van de TIB[10] komt naar voren dat deze toezegging van de minister nu door zowel de geheime diensten, als de minister zelf in het verlenen van toestemming, niet wordt nagekomen.[11]

Het wettelijk gerichtheidsvereiste is dus niet, of niet voldoende, vertaald naar zowel beleid als uitvoeringspraktijk van de geheime diensten. Hierdoor bestaan er onvoldoende waarborgen om ervoor te zorgen dat de interceptie daadwerkelijk ‘onderzoeksopdracht gericht’ is en niet ongericht.[12] Het wel implementeren van de bevoegdheid, maar het achterwege laten van de implementatie van de waarborgen die daarbij horen vormen een groot risico voor de rechten en vrijheden van burgers en maken dat de huidige uitvoering onwettig is, en dus niet langer zou moeten worden doorgezet.

7 CTIVD Toezichtsrapport nr. 63 over de toepassing van filters bij OOG-interceptie door de AIVD en de MIVD, p. 7.

8 CTIVD Toezichtsrapport nr. 63 over de toepassing van filters bij OOG-interceptie door de AIVD en de MIVD, p. 8.

9 Kamerbrief van 6 april 2018 <https://www.rijksoverheid.nl/documenten/kamerstukken/2018/04/06/kamerbrief-met-reactie-op-raadgevend-referendum-wet-op-de-inlichtingen-en-veiligheidsdiensten>

10 https://twitter.com/TIB_IVD/status/1277935114001973249

11 Zie voor uitgebreidere berichtgeving over dit punt: https://www.netkwesties.nl/1447/hoe-staat-het-nu-precies-met-het-sleepnet.htm

12 https://www.bitsoffreedom.nl/2019/09/04/rapport-vol-onvoldoendes-voor-geheime-diensten/

Geautomatiseerde data-analyse en bevoegdheids(on)afhankelijke waarborgen

Bits of Freedom en Vrijschrift pleiten ervoor om de waarborgen voor geautomatiseerde data-analyse die nu uitsluitend gelden wanneer de gegevens zijn verzameld via OOG-interceptie, van toepassing te verklaren ongeacht de bevoegdheid op grond waarvan de gegevens verkregen zijn. De waarborgen voor geautomatiseerde data-analyse worden daarmee bevoegdheidsneutraal. Hiermee onderschrijven wij wat de TIB hierover zegt in haar reactie op het wijzigingsvoorstel.[13]

In de Wiv 2017 wordt de bevoegdheid tot geautomatiseerde data-analyse beschreven in artikel 60. Daarnaast kent de wet ook een specifieker artikel 50. Dit artikel beschrijft geautomatiseerde data-analyse van meta-data die zijn verzameld met de inzet van OOG-interceptie en waarbij de analyse is gericht op de identificatie van personen of organisaties.

Wij zijn van mening dat de waarborgen die gelden voor de bevoegdheid tot geautomatiseerde data-analyse betrekking hebben op de analyse die plaatsvindt, en dus niet afhankelijk zouden moeten zijn van de wijze waarop de betreffende gegevens zijn verzameld. Immers, de waarborgen voor de verzameling van gegevens horen thuis bij de bevoegdheden op basis waarvan de gegevens worden verzameld. Waar het aankomt op de bevoegdheid tot analyse van de gegevens gelden de waarborgen die toegesneden zijn op de analyse en is de wijze van verzamelen niet langer relevant. Dit onderscheid in waarborgen heeft derhalve geen grond.

Bulkhacks

De Wiv 2017 maakt onderscheid in de geldende waarborgen tussen OOG-interceptie en zogenaamde bulkhacks. Dit terwijl er in beide gevallen op grootschalige wijze gegevens kunnen worden verkregen, waaronder van personen die geen onderwerp van onderzoek van de diensten zijn. Deze inconsistentie is opmerkelijk, gezien de hackbevoegdheid zelfs mogelijkheden biedt die OOG-interceptie niet biedt, zoals het verzamelen van historische gegevens, of het opnieuw verzamelen van gegevens die eerder als niet-relevant zijn beoordeeld. Bits of Freedom en Vrijschrift zien, evenals de TIB[14], voor dit onderscheid geen grond, en willen zelfs stellen dat gezien de verdergaande mogelijkheden van de hackbevoegdheid er hier sprake is van een lacune.

Bits of Freedom en Vrijschrift maken zich grote zorgen over de praktijk van de hackbevoegdheid. In het laatste jaarverslag van de TIB wordt het volgende beeld geschetst:

13 Zie hiervoor ook de reactie op het wijzigingsvoorstel Wiv 2017 van de TIB, 23 augustus 2018, p. 3-4.

14 Jaarverslag TIB 2018/2019, p. 13.

> “Bij de beoordeling van hackverzoeken heeft de TIB geconstateerd dat bulkhacks, waarbij soms gegevens over miljoenen personen kunnen worden verkregen, om meer zicht te krijgen op relatief weinig targets, op gespannen voet staan met de vereisten van proportionaliteit en gerichtheid. Dit geldt vooral als de gerichtheid niet direct na de verwerving wordt hersteld en de bulkgegevens langer beschikbaar blijven voor de dienst. Als ongerichte verwerving een doel op zich is, bijvoorbeeld om ongekende dreigingen te ontdekken, is er eigenlijk sprake van onderzoeksopdrachtgerichte hacks. De Wiv 2017 biedt wel waarborgen bij bulkgegevens die verzameld zijn door onderzoeksopdrachtgerichte interceptie van de kabel of via de satelliet, maar niet als het gaat om bulkgegevens die verworven zijn door een hackoperatie.”

Hieruit komt duidelijk de lacune aan waarborgen bij de hackbevoegdheid naar voren. Bovendien wordt er gesproken over een inzet van de hackbevoegdheid als bulkbevoegdheid om ongekende dreigingen te ontdekken. Wij constateren hier een praktijk die erg ver is afgedwaald van de originele inzet bij de introductie van de hackbevoegdheid. In de memorie van toelichting wordt deze bevoegdheid namelijk als volgt omschreven:

> “De bevoegdheid tot het binnendringen van een geautomatiseerd werk is gericht van aard, dat wil zeggen dat de inzet van de bijzondere bevoegdheid zich doorgaans zal richten op een geautomatiseerd werk dat bij een onderzoeksubject (target) van de AIVD of MIVD in gebruik is. […] De technische realiteit leert dat targets over het algemeen veiligheidsbewust zijn, maar dat zich operationele kansen tot het benutten van zwakheden kunnen voordoen bij technische randgebruikers, zoals medehuurders van een bepaalde server, welke kunnen leiden tot het succesvol binnendringen van het geautomatiseerde werk van het target. Het wordt in het belang van de bescherming van de nationale veiligheid noodzakelijk geacht de diensten ook in dergelijke situaties in staat te stellen om via geautomatiseerde werken van derden binnen te dringen in geautomatiseerde werken die bij targets in gebruik zijn. Het geautomatiseerde werk is hier de corridor naar het geautomatiseerd werk van het target.”

We zien hier een ontwikkeling in de praktijk van deze bevoegdheid waar van te voren voor gewaarschuwd is: De wet biedt onvoldoende waarborgen om van de bevoegdheid die intentioneel gericht van aard is geen ongerichte bulkbevoegdheid te maken.

De verstrekking van ongeëvalueerde gegevens met buitenlandse diensten

Al voor het ingaan van de wet maakten wij ons grote zorgen over deze bevoegdheid. Ons principiële punt dat de diensten geen gegevens moeten uitwisselen die zij niet eerst zelf hebben bekeken blijft staan. De praktijk sinds mei 2018 heeft onze zorgen helaas niet weggenomen, maar versterkt. De uitwisseling van ongeëvalueerde gegevens met buitenlandse diensten is een ingrijpende bevoegdheid, terwijl het beleid van de diensten rommelig doet voorkomen.[15]

1. Een inconsistente invulling van het begrip (on)geëvalueerd leidt tot het ontbreken van de toestemmingswaarborg bij het delen van deze gegevens met buitenlandse diensten..
In het toestemmingsregime voor de verstrekking van gegevens aan buitenlandse diensten wordt onderscheid gemaakt tussen geevalueerde en ongeëvalueerde gegevens, waarbij ten aanzien van de laatste toestemming vereist is. Deze waarborg staat of valt dus met de invulling van wanneer gegevens als geëvalueerd mogen worden beschouwd. Er zou van geëvalueerde gegevens gesproken mogen worden als de gegevens dermate zijn bekeken dat een dienst weet wat zij geeft. De praktijk wijst uit dat het beleid en de praktijk van de diensten daarin tekortschieten. Gegevens worden onterecht als geëvalueerd geclassificeerd, waardoor de vereiste toestemming van de minister als waarborg vervalt, en de gegevens toch aan buitenlandse diensten worden verstrekt.[16] Het is van groot belang dat er een helder en consistent begrip wordt geformuleerd (of gehanteerd) van wanneer gegevens als geëvalueerd mogen worden beschouwd. Hierbij moet de functie, een beoordeling van de gegevens die de diensten in staat stelt te weten wat zij geeft, voorop staan.

2. Er is in het beleid onvoldoende aandacht voor de vraag of datasets communicatie van advocaten of journalisten bevat. Dat is wel verplicht, omdat het hier om zeer gevoelige, beschermde gegevens gaat die niet zomaar aan buitenlandse diensten verstrekt mag worden. In het beleid van beide diensten wordt niet gerept over de afweging of een dergelijke filtering nodig is, en ook in de praktijk blijft deze filtering achterwege.[17]

3. In artikel 65 lid 2 schrijft de Wiv 2017 voor dat er bij een gegevensverstrekking moet worden vastgelegd dat de ontvangende buitenlandse dienst de gegevens niet doorgeeft. Deze derde-partij regel komt niet terug in het beleid van de diensten en wordt in de praktijk niet structureel nageleefd.[18]

15 https://www.bitsoffreedom.nl/2019/10/15/de-geheime-diensten-houden-zich-alweer-niet-aan-de-wet/ en https://www.bitsoffreedom.nl/2019/10/21/slordige-diensten-sluizen-teveel-informatie-weg/

16 CTIVD Toezichtsrapport nr. 65 over het verstrekken van ongeëvalueerde gegevens aan buitenlandse diensten door de AIVD en de MIVD, p. 11-13.

17 CTIVD Toezichtsrapport nr. 65 over het verstrekken van ongeëvalueerde gegevens aan buitenlandse diensten door de AIVD en de MIVD, p. 17-18.

18 CTIVD Toezichtsrapport nr. 65 over het verstrekken van ongeëvalueerde gegevens aan buitenlandse diensten door de AIVD en de MIVD, p 17.

4. Naast dat de toestemmingswaarborg kan worden omzeild door instrumenteel om te gaan met de term (on)geëvalueerd, wordt het vragen van toestemming ook wel eens simpelweg nagelaten. Tot slot wordt het beoordelen van een verzoek soms bemoeilijkt door niet de risico's op basis van de wegingsnotities voldoende in kaart te brengen in het verzoek waardoor het voor de minister wordt bemoeilijkt om een adequate inschatting te maken.[19]

5. Registreren en melden. Telkens bij een verstrekking van ongeëvalueerde gegevens aan een buitenlandse dienst moet van deze verstrekking een notitie worden gemaakt en deze worden gemeld bij de CTIVD. Uit het toezichtsrapport blijkt dat dit niet altijd gebeurt. Het niet structureel bijhouden van de verstrekkingen en naleven van de meldingsplicht bemoeilijkt het extern toezicht door de CTIVD.

Toezicht en internationalisering

Er is sprake van een toezichtshiaat. Waar de diensten steeds meer internationaal samenwerken is het toezicht gebonden aan nationale grenzen. Dit betekent dat een deel van het totale inlichtingenwerk en de gegevens die gedeeld worden zich onttrekt aan het toezicht. De wetgeving geeft geen wettelijke grondslag voor toezichthouders om internationaal samen te werken. Dit beperkt het toezicht op internationale gegevensuitwisselingen tot het nationale mandaat, en dus maar tot één zijde van een gegevensuitwisseling.[20] De noodzaak voor een sterkere internationalisering van het toezicht wordt ook door de CTIVD erkend in het Jaarverslag 2019. Daarin stelt zij dat de geheimhouding waar toezichthouders zich aan moeten houden een belangrijke drempel vormt voor de effectiviteit van het toezicht op internationale gegevensuitwisseling tussen inlichtingen- en veiligheidsdiensten wat leidt tot een mogelijk toezichtshiaat.[21] Toezichthouders uit vijf Europese landen hebben hierop een gezamenlijke verklaring geschreven om nationale wetgevers op te roepen de bestaande wettelijke geheimhoudingsverplichting tussen toezichthouders te herzien.[22] De verdergaande internationale samenwerking krijgt ook vorm in meer efficiënte vormen van gegevensdeling, bijvoorbeeld in gedeelde databanken, platforms, nieuwe technologieën en de uitwisseling van bulkdatasets. Het is lastig voor toezichthouders om deze ontwikkelingen bij te houden in het controleren van de uitwisselingen.[23]

Wij maken ons zorgen over de toename in de internationale gegevensuitwisseling en het achterblijven van de internationalisering aan de kant van het toezicht.

19 CTIVD Toezichtsrapport, nr. 65 over het verstrekken van ongeëvalueerde gegevens aan buitenlandse diensten door de AIVD en de MIVD, p. 14-15.

20 Speech dr. Mireille Hagens, International Intelligence Oversight Forum 2018, p. 3. <https://www.ctivd.nl/documenten/publicaties/2019/01/16/index>

21 CTIVD Jaarverslag 2019, p. 31. <https://www.ctivd.nl/documenten/jaarverslagen/2019/04/30/index>

22 https://www.ctivd.nl/documenten/persberichten/2018/11/14/index

23 Speech dr. Mireille Hagens, International Intelligence Oversight Forum 2018, p. 3. <https://www.ctivd.nl/documenten/publicaties/2019/01/16/index>

Hierdoor onttrekt een deel van het werk van de diensten en de gegevensuitwisselingen en -verwerkingen zich aan het toezicht.

Bindend advies van de CTIVD

Écht toezicht moet niet zomaar aan de kant te schuiven zijn. Daarom moeten de oordelen van de CTIVD bindend worden. Als de toezichthouder onrechtmatigheden constateert moet zij in staat zijn om de diensten bij de uitvoering van de betreffende bevoegdheid een halt toe te roepen. Dat kan nu niet. Hierdoor blijft het oordeel van de toezichthouder, en daarmee de borging van onze rechten en vrijheden, te vrijblijvend.