AUTORITEIT
PERSOONSGEGEVENS

Reactie Autoriteit Persoonsgegevens op het wetsvoorstel "Wet op de inlichtingen- en veiligheidsdiensten 20.."

1. Achtergrond

De Autoriteit Persoonsgegevens (AP) is de Nederlandse toezichthouder op de naleving van de privacywetgeving. Uit dien hoofde houdt de AP toezicht op de verwerking van persoonsgegevens[1], door onder meer de overheid, bedrijven en de Nationale Politie[2]. Daarnaast is de AP - in samenwerking met Europese mede-toezichthouders - onder meer betrokken bij het toezicht op Europol[3] en Eurojust[4]. Ook adviseert de AP over wetsvoorstellen die "geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens".[5]

Krachtens de Wet bescherming persoonsgegevens (Wbp) strekken de bevoegdheden van de AP zich niet uit tot de verwerking van persoonsgegevens door de inlichtingen- en veiligheidsdiensten (de diensten).[6] De AP is dientengevolge niet verzocht een advies over het wetsvoorstel "Wet op de inlichtingen- en veiligheidsdiensten 20.."[7] uit te brengen.

Het is van groot belang dat de diensten ter bescherming van de nationale veiligheid gebruik kunnen maken van bevoegdheden die effectief en *up to date* zijn. Niettemin zijn de gevolgen van het wetsvoorstel verstrekkend. Het wetsvoorstel biedt de diensten immers de mogelijkheid om grote hoeveelheden persoonsgegevens van (alle) burgers in bulk te onderscheppen en analyseren. Ook biedt het wetsvoorstel de diensten expliciet de mogelijkheid om apparatuur van derden te hacken, om zich op die manier toegang te verschaffen tot apparatuur van concrete doelwitten.[8] In de praktijk betekent dit onder meer dat de diensten informatie afkomstig van apparatuur van burgers mogen gebruiken en *malware* op apparatuur van burgers mogen plaatsen, om op die manier hun eigenlijke doelwit te bereiken.

Naast de nieuwe bevoegdheden om gegevens te verzamelen, biedt het wetsvoorstel de diensten ruime mogelijkheden om eenmaal onderschepte gegevens uit te wisselen met andere partijen. Zo kunnen onder meer niet-geëvalueerde gegevens worden verstrekt aan buitenlandse inlichtingen- en veiligheidsdiensten, waarbij van tevoren niet duidelijk is welke informatie van Nederlandse burgers precies wordt verstrekt. Tevens kunnen de diensten gegevens verstrekken aan de Nationale Politie – bijvoorbeeld om handelingsperspectief te bieden[9] – en kan in de praktijk ondersteuning worden verleend aan de Nationale

[1] Krachtens de Wet bescherming persoonsgegevens (Wbp).
[2] Krachtens de Wet politiegegevens (Wpg).
[3] Besluit van de Raad van 6 april 2009 tot oprichting van de Europese politiedienst (2009/371/JBZ).
[4] Besluit van de Raad inzake het versterken van Eurojust en tot wijziging van Besluit 2002/187/JBZ betreffende de oprichting van Eurojust teneinde de strijd tegen ernstige vormen van criminaliteit te versterken (5347/3/09).
[5] Artikel 51, tweede lid, Wbp.
[6] Artikel 2, tweede lid, onder b, Wbp.
[7] Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 20..), Kamerstukken II, 2016-2017, 34588 nr. 2 (voorstel van wet).
[8] In de memorie van toelichting stelt de regering zich op het standpunt dat deze bevoegdheid tot het hacken "via derden" momenteel al impliciet bestaat, maar dat deze bevoegdheid in het nieuwe wettelijk kader voortaan expliciet wordt opgenomen. Zie o.a. Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 15.
[9] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 96.

Politie. Er bestaat op veel fronten dan ook een relatie tussen het werk van de diensten en de Nationale Politie, terwijl het toezicht op de Nationale Politie en de diensten verdeeld en onderscheidenlijk van aard is.

De nieuwe bevoegdheid om gegevens (die via de kabel worden verzonden) in bulk te onderscheppen, de bevoegdheid om toegang te krijgen tot geautomatiseerde werken via "derden", de ruime mogelijkheden om eenmaal onderschepte gegevens aan buitenlandse diensten te verstrekken en de relatie tussen het werk van de diensten en de Nationale Politie, leiden ertoe dat er een onmiskenbare verwevenheid bestaat tussen het wetsvoorstel en het algemene beschermingsniveau van de persoonlijke levenssfeer - en de bescherming van de persoonsgegevens in het bijzonder - in Nederland.

De verwevenheid tussen het wetsvoorstel en de bescherming van de persoonsgegevens van Nederlandse burgers, is voor de AP aanleiding een reactie op het wetsvoorstel te geven. In deze reactie wordt ingegaan op een aantal onderdelen van het wetsvoorstel dat belangrijke gevolgen heeft voor de bescherming van de persoonlijke levenssfeer. Hierbij benadrukt de AP dat, als de bevoegdheden van de diensten worden versterkt – zoals in het onderhavige wetsvoorstel het geval is – de waarborgen tegen willekeur en disproportionele inbreuken, alsmede het toezicht op de activiteiten van de diensten, navenant zouden moeten worden versterkt. Volgens de AP is dit in het wetsvoorstel nog niet afdoende het geval.

De AP baseert zich in deze reactie voornamelijk op het Europees Verdrag voor de Rechten van de Mens (EVRM)[10], de jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) en de Grondwet. Zowel het EVRM als de Grondwet zijn immers direct van toepassing op de activiteiten van de diensten.

Uit het EVRM vloeien vier voorwaarden voort, waaraan het wetsvoorstel zou moeten voldoen. Hierbij gaat het ten eerste om de voorwaarde dat de noodzaak van de voorgestelde bevoegdheden afdoende moet worden onderbouwd, ten tweede om de voorwaarde dat de voorgestelde bevoegdheden afdoende kenbaar en voorzienbaar moeten zijn voor burgers, ten derde om de voorwaarde dat de inzet van de voorgestelde bevoegdheden met afdoende waarborgen moet zijn omkleed ter bescherming van de rechten van burgers en ten vierde om de voorwaarde dat sprake moet zijn van effectief en onafhankelijk toezicht op de diensten.

Voor ieder van de vier bovengenoemde voorwaarden wordt in deze reactie beknopt weergegeven welke invulling hieraan wordt gegeven in het (Europees) recht, waarna de AP vervolgens haar reactie geeft op de wijze waarop deze voorwaarden in het wetsvoorstel zijn verwerkt.

2. Inhoud wetsvoorstel

Het wetsvoorstel "Wet op de inlichtingen- en veiligheidsdiensten 20.." strekt ter vervanging van de huidige Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002). Directe aanleiding daartoe vormt de in 2013 uitgevoerde evaluatie van de Wiv 2002 door de Evaluatiecommissie Wiv 2002 (commissie Dessens). Met het wetsvoorstel wordt, aldus de regering, beoogd een wettelijk kader voor de inlichtingen- en veiligheidsdiensten in brede zin te realiseren, dat toekomstvast is en in lijn met de eisen van de Grondwet alsmede het EVRM.[11]

[10] Zie met name artikel 8 en 13 EVRM.
[11] Zie onder meer Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 234.

In het wetsvoorstel wordt een aantal wijzigingen voorgesteld ten opzichte van de huidige Wiv 2002, waaronder de introductie van een aantal nieuwe bevoegdheden. Aan de hand van deze nieuwe bevoegdheden wordt, zo beargumenteert de regering in de memorie van toelichting, gewaarborgd dat de diensten ook in de huidige tijd - waarin steeds meer communicatie plaatsvindt via het internet - effectief kunnen opereren. Momenteel zijn de bevoegdheden van de diensten volgens de regering te beperkt om (grote hoeveelheden) gegevens te onderscheppen.[12] Ook wordt, in lijn met de jurisprudentie van het EHRM, een bindend klachtenmechanisme voor burgers ingevoerd.[13]

De meest in het oog springende nieuwe bevoegdheid voor de diensten, is - naast het expliciet maken van de hackbevoegdheid via "geautomatiseerde werken van derden" - de bevoegdheid tot "onderzoeksopdrachtgerichte interceptie" en de daarmee samenhangende bevoegdheden tot het (geautomatiseerd) analyseren van onderschepte gegevens.[14] Met deze bevoegdheid worden de diensten in staat gesteld grote hoeveelheden gegevens te onderscheppen. Het gaat, met andere woorden, om "bulkinterceptie". Doordat de bevoegdheid tot bulkinterceptie in het wetsvoorstel techniekonafhankelijk is geformuleerd, wordt het onder meer mogelijk om op grootschalige wijze kabelgebonden communicatie te onderscheppen. Op grond van de huidige Wiv 2002 is dit niet mogelijk en kunnen de diensten kabelgebonden communicatie alleen gericht onderscheppen. De diensten mogen daarentegen wel reeds ongericht dataverkeer onderscheppen dat via niet-kabelgebonden kanalen wordt gecommuniceerd, zoals radiofrequenties.[15]

Door de techniekonafhankelijke aard van de voorgestelde bevoegdheden, is de maatschappelijk impact van het wetsvoorstel groot: uit de memorie van toelichting blijkt dat ongeveer 90% van alle huidige telecommunicatie via kabelnetwerken verloopt.[16] In de praktijk gaat het dan vooral om internetverkeer via het kabelinternet, maar ook om communicatie via *smartphones*.[17] Een concreet maatschappelijk gevolg van het wetsvoorstel is dan ook dat vrijwel alle communicatie via *social media*, die immers veelal plaatsvindt via kabelinternet en/of *smartphones*, voortaan in aanmerking komt voor onderschepping in bulk. Daarnaast wordt het mogelijk om gegevens te onderscheppen die door zogeheten "slimme" apparaten worden verwerkt, als gevolg van de opkomst van het *Internet of Things*.[18] Door het onderscheppen van dergelijke gegevens, zoals gegevens afkomstig van auto's, thermostaten, koelkasten, horloges of andere (huishoudelijke) gecomputeriseerde apparatuur - maar ook met internet verbonden camera's of opnameapparatuur - wordt het voor de diensten in toenemende mate mogelijk om gedragspatronen van burgers in kaart te brengen. Voor de hackbevoegdheid geldt bovendien dat het niet ondenkbaar is dat deze in de praktijk een (toenemend) belangrijke rol zal spelen, aangezien het onderscheppen van communicatie door toenemende versleuteling minder effectief kan worden.

Het wetsvoorstel biedt voorts de mogelijkheid om eenmaal onderschepte bulkgegevens voor een periode van drie jaar te bewaren. Gedurende deze periode kunnen de bulkgegevens op relevantie worden

[12] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 8-13.
[13] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 178 e.v.
[14] Artikelen 48-50 van het wetsvoorstel.
[15] Artikelen 26 en 27, Wiv 2002.
[16] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 94.
[17] Communicatie op de smartphone gebeurt deels via niet-kabelgebonden kanalen en deels wel via de kabel. Dataverkeer afkomstig van smartphones wordt eerst naar een zendmast gezonden, vanwaar de data vervolgens ofwel via de telefoonkabel ofwel via kabelinternet verder kan worden gezonden. Momenteel is het niet mogelijk communicatie via smartphones *ongericht* te onderscheppen wanneer de data eenmaal via de kabel wordt verwerkt. Alleen op het niet-kabelgebonden traject is dergelijke ongerichte onderschepping op grond van de huidige Wiv immers mogelijk. Op grond van het wetsvoorstel zou deze mogelijkheid tot ongerichte onderschepping op het kabelgebonden traject daarentegen wel ontstaan.
[18] Zie in dit kader bijvoorbeeld Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 75.

onderzocht, waarbij geldt dat gegevens niet alleen relevant kunnen zijn voor de zoekopdracht waarvoor zij in beginsel zijn onderschept, maar mogelijk ook voor andere onderzoeken voor de diensten.[19] Tevens geeft de regering aan dat het voor de diensten van belang is om te beschikken over een database van grote hoeveelheden historische gegevens, zodat aan de hand daarvan beter inzicht kan worden verkregen in nog onbekende dreigingen.[20] Gedurende de bewaarperiode van drie jaar kunnen onderschepte gegevens tot slot worden uitgewisseld met buitenlandse diensten. Het wetsvoorstel biedt de diensten hierbij ook de mogelijkheid om gegevens waarvan de inhoud nog niet bekend is (niet-geëvalueerde gegevens) te verstrekken aan buitenlandse diensten.[21]

3. Reactie Autoriteit Persoonsgegevens

3.1 Noodzakelijk in een democratische samenleving

3.1.1 Juridisch kader

Een inbreuk op de bescherming van de persoonlijke levenssfeer is alleen onder voorwaarden geoorloofd. Uit artikel 8 EVRM en de jurisprudentie van het EHRM volgt dat een dergelijke inbreuk "noodzakelijk moet zijn in een democratische samenleving".[22]

Uit de jurisprudentie van het EHRM volgt dat verschillende aspecten meewegen bij het beoordelen of een inbreuk daadwerkelijk noodzakelijk is in een democratische samenleving. Zo moet worden gekeken naar het doel van een inbreuk. Dit doel moet kunnen worden aangemerkt als "legitiem" in een democratische samenleving.[23] Wanneer sprake is van een legitiem doel, dient vervolgens te worden gekeken naar de (maatschappelijke) noodzaak van de voorgenomen inbreuk in verhouding tot dit legitieme doel. Hierbij speelt een rol of de voorgestelde inbreuk geschikt is om dat doel te bereiken en daarbij niet verder gaat dan noodzakelijk is (proportionaliteit)[24], of minder ingrijpende middelen voorhanden zijn om hetzelfde resultaat te bereiken (subsidiariteit) en of afdoende waarborgen zijn ingesteld om disproportionele inbreuken en willekeur te voorkomen.[25]

Ten aanzien van de inlichtingen- en veiligheidsdiensten heeft het EHRM geoordeeld dat inbreuken op de persoonlijke levenssfeer ter bescherming van de nationale veiligheid kunnen gelden als een legitiem doel in een democratische samenleving.[26] Deze inbreuken moeten dan uiteraard daadwerkelijk noodzakelijk zijn ter bescherming van dit legitieme doel. Er zal dan ook steeds een afweging moeten worden gemaakt of activiteiten van de diensten daadwerkelijk noodzakelijk zijn.

[19] Zie artikel 48, vijfde lid, van het wetsvoorstel.
[20] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), o.a. p. 13, 93 en 100.
[21] Zie artikelen 64 en 89 van het wetsvoorstel.
[22] Zo volgt uit artikel 8 van het Europees Verdrag voor de Rechten van de Mens. Zie tevens: EHRM 6 september 1978, 5029/71, Klass e.a. t. Duitsland, par. 49. Zie voor een uitgebreide analyse van het juridisch kader ten aanzien van de inlichtingendiensten: Sarah Eskens, Ot van Daalen en Nico van Eijk, Ten standards for oversight and transparency of national intelligence services, Institute for Information Law (IViR, University of Amsterdam), 2015.
[23] Zie o.a. EHRM 4 december 2015, 47143/06, Roman Zakharov t. Rusland, par. 227.
[24] Zie onder meer EHRM 26 maart 1987, nr. 9248/81, Leander t. Zweden, par. 58.
[25] EHRM 4 december 2015, 47143/06, Roman Zakharov t. Rusland, par. 227-234; EHRM 6 september 1978, 5029/71, Klass e.a. t. Duitsland, par. 50.
[26] Zie o.a. EHRM 6 september 1978, 5029/71, Klass e.a. t. Duitsland, par. 48-50.

Belangrijk is dat de noodzakelijkheidseis niet alleen ziet op de *inzet* van bevoegdheden van de diensten, maar dat de introductie van nieuwe bevoegdheden *an sich* noodzakelijk moet zijn in een democratische samenleving. Uit de jurisprudentie van het EHRM volgt namelijk dat reeds het enkele bestaan van wetgeving op grond waarvan persoonsgegevens kunnen worden onderschept, geldt als een inbreuk op de bescherming van de persoonlijke levenssfeer.[27]

Er moet, met andere woorden, eerst worden gekeken of er in een democratische samenleving wel plaats is voor bepaalde bevoegdheden van de diensten, alvorens wordt gekeken naar de manier waarop deze bevoegdheden zouden mogen worden ingezet.

3.1.2 Reactie Autoriteit Persoonsgegevens

Het wetsvoorstel leidt ertoe dat de aard en omvang van de bevoegdheden van de diensten fundamenteel zullen veranderen. Zoals uiteengezet, voorziet het wetsvoorstel immers in de mogelijkheid om gegevens in bulk te onderscheppen, waarbij geldt dat deze gegevens geautomatiseerd mogen worden verwerkt, gedurende geruime tijd mogen worden bewaard - onder meer voor het onderzoeken van nog onbekende dreigingen - en bovendien mogen worden uitgewisseld met buitenlandse diensten.

De (nieuwe) bevoegdheden van de diensten zullen onmiskenbaar gevolgen hebben voor Nederlandse burgers, en in het bijzonder voor het recht op bescherming van de persoonlijke levenssfeer. Er bestaat een reële kans dat de introductie van deze bevoegdheden fundamentele vrijheden die ten grondslag liggen aan de Nederlandse rechtsstaat, negatief beïnvloedt. In dit kader kan onder meer worden gewezen op het *"chilling effect"*, waarvan wordt gesproken in het rapport van de Wetenschappelijke Raad voor het Regeringsbeleid getiteld "Big Data in een vrije en veilige samenleving".[28] De grootschalige verzameling, opslag en analyse van gegevens door de inlichtingen- en veiligheidsdiensten, kan ertoe leiden dat burgers hun gedrag hierop aanpassen.[29] Hierdoor kan de grootschalige verwerking van gegevens - naast een inbreuk op de persoonlijke levenssfeer - bijvoorbeeld ook gevolgen hebben voor de vrijheid van meningsuiting, doordat burgers of maatschappelijke organisaties zich op voorhand geremd kunnen voelen in hun uitingsvrijheid. Het EHRM waarschuwt er dan ook voor dat *"a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it".*[30]

Hoewel in de memorie van toelichting wordt ingegaan op de (operationele) noodzaak van nieuwe bevoegdheden voor de diensten, wordt onvoldoende aandacht besteed aan de mogelijke negatieve effecten van het wetsvoorstel. Met name wordt onvoldoende ingegaan op de gevolgen die de nieuwe bevoegdheden van de diensten *in onderlinge samenhang* zullen hebben voor de fundamentele rechten van Nederlandse burgers in het algemeen, en de bescherming van persoonsgegevens in het bijzonder.

Uit het juridisch kader blijkt bovendien dat bij de onderbouwing van de noodzaak van nieuwe bevoegdheden aandacht moet worden besteed aan de vraag of de voorgestelde inbreuken op de persoonlijke levenssfeer geschikt zijn om het legitieme doel te bereiken en niet verder gaan dan nodig is,

[27] EHRM 4 december 2015, 47143/06, Roman Zakharov t. Rusland, par. 168-171; EHRM 6 september 1978, 5029/71, Klass e.a. t. Duitsland, par. 41. Zie tevens: Sarah Eskens, Ot van Daalen en Nico van Eijk, Ten standards for oversight and transparency of national intelligence services, Institute for Information Law (IViR, University of Amsterdam), 2015, p. 14.
[28] "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." Zie: Wetenschappelijke Raad voor het Regeringsbeleid, Big Data in een vrije en veilige samenleving (2016), p. 92 e.v.
[29] Kamerstukken II, 2016-2017, 34588 nr. 4 (Advies afdeling advisering Raad van State en Nader rapport), p. 27.
[30] EHRM 29 juni 2006, 54934/00, Weber en Saravia t. Duitsland, par. 106.

alsmede aan de vraag of er geen minder ingrijpende middelen voorhanden zijn om dat doel te bereiken. In de memorie van toelichting wordt echter niet afdoende ingegaan op de internationale discussies omtrent de effectiviteit van grootschalige data-interceptie, bijvoorbeeld in relatie tot de toenemende versleuteling van communicatie. Hoewel argumenten worden gegeven waarom het voor de diensten noodzakelijk is om gegevens in bulk te kunnen onderscheppen, wordt niet inhoudelijk ingegaan op onderzoeken waaruit blijkt dat de effectiviteit van grootschalige data-interceptie niet zonder meer vaststaat.[31] Evenmin wordt in de memorie van toelichting duidelijk gemaakt welke alternatieven zijn overwogen.

Samenvattend zou de noodzaak van het wetsvoorstel beter moeten worden onderbouwd, door aandacht te besteden aan de mogelijke negatieve effecten van de voorgestelde nieuwe bevoegdheden *in onderlinge samenhang*, de effectiviteit van de bevoegdheid tot bulkinterceptie en tot slot de overwogen alternatieven. Een dergelijke fundamentele beschouwing is volgens de AP nodig om de noodzaak van het wetsvoorstel daadwerkelijk afdoende te kunnen onderbouwen: alleen op die manier kan immers worden beoordeeld of er in een democratische samenleving als Nederland plaats is voor de bevoegdheden van de diensten, zoals voorgesteld in het wetsvoorstel.

3.2 Kenbaarheid en voorzienbaarheid

3.2.1 Juridisch kader

Uit het EVRM en de jurisprudentie van het EHRM vloeit voort dat inbreuken op de persoonlijke levenssfeer bij wet moeten zijn voorzien. Dit betekent niet alleen dat er een concrete wettelijke basis moet zijn op grond waarvan een inbreuk kan worden gemaakt, ook heeft het EHRM herhaaldelijk benadrukt dat deze wettelijke basis aan bepaalde kwaliteitseisen moet voldoen.[32] Volgens het Hof moet te allen tijde worden voorzien in regels die kenbaar en voorzienbaar zijn voor burgers. In de praktijk betekent dit onder meer dat het voor burgers - eventueel na het inwinnen van deskundig advies - mogelijk moet zijn om in te schatten wat de gevolgen van bepaalde handelingen zullen zijn.[33]

Ten aanzien van de diensten oordeelt het EHRM dat het voorzienbaarheidsvereiste niet zover gaat dat een burger in specifieke gevallen zou moeten weten wanneer de diensten communicatie onderscheppen.[34] Wanneer burgers dit weten, zouden zij hierop immers hun gedrag kunnen aanpassen, waardoor het effectief functioneren van de diensten onmogelijk zou worden gemaakt. Wel moet de wet de reikwijdte van de bevoegdheden van de diensten en de toepassing daarvan met voldoende helderheid aangeven om het individu adequate bescherming te bieden tegen arbitraire inbreuken op zijn persoonlijke levenssfeer.[35] Hierdoor worden immers kaders aangegeven waarbinnen de bevoegdheden mogen worden uitgeoefend.[36]

Binnen de context van geheime interceptiebevoegdheden is het volgens het EHRM dan ook nodig dat burgers onder meer kennis kunnen nemen van de doelen waarvoor interceptiebevoegdheden kunnen

[31] Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Programme Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court, 23 January 2014, p. 11. Het College voor de Rechten van de Mens verwijst in haar advies over het wetsvoorstel tevens naar dit onderzoek. Zie: College voor de Rechten van de Mens, Advies "conceptwetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20..", 31 augustus 2015, p. 7-8.
[32] EHRM 24 april 1990, 11801/85, Kruslin t. Frankrijk, par. 30-36.
[33] EHRM, 2 augustus 1984, 8691/79, Malone t. Verenigd Koninkrijk, par. 67.
[34] EHRM, 2 augustus 1984, 8691/79, Malone t. Verenigd Koninkrijk, par. 67-68.
[35] EHRM 26 maart 1987, nr. 9248/81, Leander t. Zweden, par. 51. Zie tevens Kamerstukken II, 2016-2017, 34588 nr. 4 (Advies afdeling advisering Raad van State en Nader rapport), p. 8-9.
[36] EHRM 29 juni 2006, 54934/00, Weber en Saravia t. Duitsland, par. 93.

worden ingezet, de categorieën van personen jegens wie deze bevoegdheden mogen worden ingezet, de periode waarbinnen deze bevoegdheden mogen worden ingezet en de procedure die moet worden gevolgd voor het onderzoeken, gebruiken en bewaren van onderschepte gegevens.[37] De ratio achter deze voorwaarden is dat willekeur hiermee wordt voorkomen. Juist omdat de diensten in de praktijk heimelijk opereren, moet in de wet duidelijk worden aangegeven wanneer bepaalde bevoegdheden mogen worden ingezet tegen burgers.

3.2.2 Reactie Autoriteit Persoonsgegevens

Het wetsvoorstel heeft, zoals eerder uiteengezet, belangrijke gevolgen voor het beschermingsniveau van de persoonlijke levenssfeer in Nederland. Niet alleen biedt het wetsvoorstel de mogelijkheid om gegevens in bulk te onderscheppen, ook mogen eenmaal onderschepte gegevens worden verstrekt aan buitenlandse diensten en is het mogelijk om apparaten van derden te hacken, om zo toegang te krijgen tot apparatuur van doelwitten. Juist omdat het wetsvoorstel een grondslag biedt om de persoonlijke levenssfeer van burgers op heimelijke wijze aan te tasten, zou het wetsvoorstel burgers - in overeenstemming met artikel 8 EVRM en de jurisprudentie van het EHRM - voldoende duidelijk moeten maken wanneer en op welke wijze deze bevoegdheden mogen worden ingezet. Op dit moment is dit echter nog onvoldoende het geval. Hieronder wordt dit nader uitgewerkt ten aanzien van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie en de bevoegdheid tot hacken via “derden”.

3.2.2.1 Onderzoeksopdrachtgerichte interceptie

De inzet van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie is op dit moment nog niet afdoende kenbaar en voorzienbaar voor burgers. Dit komt door de gebruikte terminologie en het gebrek aan uitgewerkte voorbeelden, het gekozen driefasenmodel en door de onduidelijkheid over de precieze doelen en bewaartermijnen van de bulkinterceptie.

Ten eerste zorgt de terminologie van het wetsvoorstel ervoor dat onvoldoende duidelijk is wat de bevoegdheid tot “onderzoeksopdrachtgerichte interceptie” in de praktijk zal inhouden.[38] Doordat de woorden “onderzoeksopdracht” en “gericht” worden gebruikt, kan het beeld ontstaan dat deze bevoegdheid gerichter is, dan zij in werkelijkheid zal zijn. Uit de memorie van toelichting blijkt namelijk dat het hier onder meer kan gaan om het onderscheppen van gegevens in het kader van bepaalde thema’s, waarbij onder meer communicatie van en naar een bepaald geografisch gebied kan worden onderschept.[39] Aan de hand van voorbeelden zou dan ook duidelijker moeten worden gemaakt wat onderzoeksopdrachten in de praktijk kunnen inhouden en in hoeverre sprake is van op die onderzoeksopdrachten “gerichte” interceptie.

Ten tweede is de procedure voor het inzetten van de bevoegdheid tot bulkinterceptie weinig inzichtelijk. De regering heeft er namelijk voor gekozen de procedure voor bulkinterceptie te verdelen over drie fasen, die zijn opgenomen in drie afzonderlijke wetsartikelen. Zo wordt een onderscheid gemaakt tussen

[37] Zie in dit kader onder meer het document van de Artikel 29 Werkgroep, waarin wordt ingegaan op de voorwaarden die gelden voor de inlichtingen- en veiligheidsdiensten: Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), p. 7. Zie tevens: EHRM 29 juni 2006, 54934/00, Weber en Saravia t. Duitsland, par. 95.

[38] In dit kader merkt de AP op dat in de Privacy Impact Assessment (PIA) die is uitgevoerd ten aanzien van een eerdere conceptversie van het wetsvoorstel, kritische uitspraken werden gedaan over het soms ”verhullende” taalgebruik in het wetsvoorstel en de daarbij behorende toelichting. Zie: Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdiensten 20XX, 12 februari 2016, p. 24.

[39] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 92.

"onderschepping"[40], "voorbewerking van onderschepte gegevens"[41] en het "(verder) verwerken van onderschepte gegevens"[42]. In de praktijk zijn deze drie fasen echter sterk verweven, zoals ook is opgemerkt door de Commissie van Toezicht op de Inlichtingen en Veiligheidsdiensten (CTIVD)[43] en de Afdeling Advisering van de Raad van State (de Afdeling).[44] Kort gezegd zal sprake zijn van een continu proces van verwerving, selectie, analyse en onderzoek, waarbij deze fasen steeds opnieuw doorlopen kunnen worden en de resultaten van de verschillende fasen elkaar beïnvloeden.[45] Hierdoor zullen de verschillende werkzaamheden gelijktijdig plaatsvinden en zal - in tegenstelling tot de wettekst - niet voor iedere fase afzonderlijk om toestemming worden gevraagd. Zo kan er blijkens de memorie van toelichting om een "combi-last" worden verzocht, die relatief algemeen en abstract zal zijn geformuleerd.[46] Wanneer in de praktijk gebruik zal worden gemaakt van een combi-last, zou deze mogelijkheid echter expliciet in het wetsvoorstel moeten worden uitgewerkt, zodat voor burgers duidelijk is welke waarborgen van toepassing zijn op de verschillende, al dan niet samenvallende fasen van de bulkinterceptie.[47] Tevens zou de precieze werking van de drie verschillende fasen meer inzichtelijk moeten worden gemaakt, door het uitwerken van diverse voorbeelden. Op die manier wordt het voor burgers - in lijn met artikel 8 EVRM - beter voorzienbaar over welke bevoegdheden de diensten precies beschikken, wanneer deze bevoegdheden mogen worden ingezet en welke waarborgen tegen willekeur en disproportioneel gebruik in iedere afzonderlijke fase, dan wel in overlappende fasen, van het proces gelden.

Tot slot dient meer duidelijkheid te worden geboden over de doelen waarvoor gegevens mogen worden verwerkt en, daarmee in samenhang, over de vernietiging van niet-relevante gegevens. Het wetsvoorstel en de memorie van toelichting lijken op dit punt tegenstrijdig te zijn. In de memorie van toelichting bij het wetsvoorstel wordt benadrukt dat de diensten de bevoegdheid tot onderzoeksopdrachtgerichte interceptie zo gericht mogelijk zullen inzetten.[48] Dit betekent onder meer dat de diensten onderschepte gegevens die niet relevant zijn voor het onderzoek, zullen vernietigen. In de praktijk zou volgens de regering dan ook het overgrote deel van de onderschepte gegevens na een eerste filtering worden vernietigd *("select while you collect").*[49] In aanvulling daarop zou er - binnen het driefasen model - voortdurend worden gekeken of gegevens relevant zijn, waarbij irrelevante gegevens doorlopend worden vernietigd.[50] In de memorie van toelichting wordt echter tegelijkertijd benadrukt dat het voor de diensten van belang is te beschikken over grote (historische) datasets, om op die manier inzicht te verkrijgen in nog onbekende dreigingen.[51] Het wetsvoorstel biedt hiervoor ook de ruimte, gezien de ruime bewaartermijn voor onderschepte gegevens en de mogelijkheid om gegevens die weliswaar niet relevant zijn voor het onderzoek waarvoor zij in eerste instantie zijn onderschept, te gebruiken in het kader van andere onderzoeken.

[40] Artikel 48 van het wetsvoorstel.
[41] Artikel 49 van het wetvoorstel.
[42] Artikel 50 van het wetsvoorstel.
[43] CTIVD, Reactie CTIVD op het concept-wetsvoorstel Wet op de inlichtingen- en veiligheidsdiensten 20XX, consultatieversie juni 2015, p. 3 en 26 e.v.
[44] Kamerstukken II, 2016-2017, 34588 nr. 4 (Advies afdeling advisering Raad van State en Nader rapport), p. 31.
[45] Zie artikelen 48-50 van het wetsvoorstel en tevens: CTVID, Zienswijze CTIVD op wetsvoorstel Wiv 20.., Bijlage I Essentiële waarborgen (november 2016), p. 13. Zie tevens: Kamerstukken II, 2016-2017, 34588 nr. 4 (Advies afdeling advisering Raad van State en Nader rapport), p.31.
[46] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 104. Zie tevens: Kamerstukken II, 2016-2017, 34588 nr. 4 (Advies afdeling advisering Raad van State en Nader rapport), p. 32 en 40.
[47] Zie in dit kader Kamerstukken II, 2016-2017, 34588 nr. 4 (Advies afdeling advisering Raad van State en Nader rapport), p. 31.
[48] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), o.a. p. 6-8.
[49] Aan dit principe wordt, blijkens de memorie van toelichting, op hoofdlijnen recht gedaan. Zie: Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 255.
[50] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 102.
[51] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 13 en 100-101.

Door deze tegengestelde doelen - enerzijds zo gericht mogelijk werken, en anderzijds willen beschikken over een grote hoeveelheid historische gegevens - maken het wetsvoorstel en de memorie van toelichting onvoldoende duidelijk in welke mate gegevens die niet relevant zijn voor het onderzoek waarvoor zij zijn vergaard, in de praktijk daadwerkelijk worden vernietigd dan wel worden gebruikt voor een ander doel dan de oorspronkelijke onderzoeksopdracht. Deze onduidelijkheid staat haaks op de voorzienbaarheidseis van artikel 8 EVRM. In het wetsvoorstel en de toelichting zou concreet moeten worden uitgewerkt *welke* gegevens *wanneer* moeten worden vernietigd (zie in dit kader tevens paragraaf 3.3.2.1).

3.2.2.2 Toegang tot technische voorzieningen van "derden"

In artikel 45 van het wetsvoorstel is de bevoegdheid opgenomen om "door tussenkomst van het geautomatiseerde werk van een derde" binnen te dringen in een geautomatiseerd werk van een doelwit van de diensten. In de praktijk gaat het om een hackbevoegdheid, op grond waarvan de diensten zich met tussenkomst van apparatuur van derden toegang tot apparatuur van doelwitten mogen verschaffen. Hierbij kunnen de diensten niet alleen gebruik maken van zwakheden in de software van derden - hetgeen tevens gevolgen kan hebben voor anderen die van die software gebruik maken - maar kunnen zij bijvoorbeeld ook zelf *malware* aanbrengen op computers van derden. Wanneer de diensten zich toegang verschaffen tot een geautomatiseerd werk van een derde, kunnen zij bovendien gegevens overnemen.[52]

De derden waarvan in het wetsvoorstel wordt gesproken, zullen in de praktijk veelal "technisch gerelateerde" partijen zijn, zoals providers, tussenleveranciers of dienstverleners.[53] In de praktijk kan het hierdoor gaan om bedrijven die beschikken over persoonsgegevens van grote hoeveelheden burgers. Het kan echter ook gebeuren dat de diensten zich toegang zullen verschaffen tot geautomatiseerde werken van individuele burgers, die verder geen doelwit van de diensten zijn.[54] Het wetsvoorstel en de bijbehorende memorie van toelichting maken echter onvoldoende duidelijk wat de precieze reikwijdte van deze hackbevoegdheid is en wanneer deze bevoegdheid precies jegens "derden" kan worden ingezet. In het wetsvoorstel en de toelichting wordt namelijk geen duidelijke afbakening gegeven van het begrip "derden" en wordt evenmin nader uiteengezet hoe ruim of nauw de "technische relatie" tussen een derde en het eigenlijke doelwit van de diensten in de praktijk kan zijn.[55] Mogen de diensten zich bijvoorbeeld toegang verschaffen tot het geautomatiseerde werk van hun doelwit door middel van meerdere derden, die via elkaar in verband staan met het doelwit?[56]

Juist bij ingrijpende middelen als de hackbevoegdheid, waardoor "derden" kunnen worden geraakt, bijvoorbeeld doordat *malware* wordt aangebracht op apparatuur of doordat gebruik wordt gemaakt van zwakke plekken in de beveiliging van algemeen gebruikte software, zou inzicht moeten worden geboden in de reikwijdte van de bevoegdheden van de diensten. Het is niet ondenkbaar dat de hackbevoegdheid in de praktijk een (toenemend) belangrijke rol zal spelen in de taakuitoefening van de diensten, aangezien het onderscheppen van communicatie door toenemende versleuteling minder effectief kan worden. Het moet voor burgers - in overeenstemming met artikel 8 EVRM - dan ook afdoende kenbaar en voorzienbaar zijn wanneer en hoe de diensten deze bevoegdheid kunnen inzetten.

[52] Artikel 45, tweede lid, onder d, van het wetsvoorstel.
[53] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 78.
[54] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 78.
[55] Zie in dit kader CTVID, Zienswijze CTIVD op wetsvoorstel Wiv 20.., Bijlage I Essentiële waarborgen (november 2016), p. 28-30.
[56] Zie in dit kader CTVID, Zienswijze CTIVD op wetsvoorstel Wiv 20.., Bijlage I Essentiële waarborgen (november 2016), p. 28-29.

3.3 De inzet van bevoegdheden: waarborgen tegen willekeur en disproportionele inbreuken

3.3.1 Juridisch kader

Uit artikel 8 EVRM en de jurisprudentie van het EHRM vloeit voort dat de inzet van bevoegdheden die een inbreuk maken op de persoonlijke levenssfeer, onderworpen moet zijn aan effectieve waarborgen om willekeur en disproportionele inbreuken te voorkomen.[57] Bevoegdheden die een inbreuk maken op de persoonlijke levenssfeer mogen immers alleen worden ingezet wanneer dit noodzakelijk en proportioneel is en wanneer er geen minder ingrijpende middelen voorhanden zijn.

Bij de beoordeling of sprake is van afdoende waarborgen[58], kijkt het EHRM naar het gehele systeem waarbinnen de inlichtingen- en veiligheidsdiensten opereren. In de praktijk betekent dit dat er geen eenduidig overzicht bestaat waaraan alle inlichtingen- en veiligheidsdiensten moeten voldoen.[59] Per systeem moet worden gekeken of de inzet van bevoegdheden niet verder gaat dan noodzakelijk en proportioneel is en of er afdoende waarborgen zijn om willekeur en disproportionele inbreuken te voorkomen.[60] Uit de jurisprudentie van het Hof kan worden afgeleid dat hierbij onder meer de aard, omvang en duur van de inbreuk op de persoonlijke levenssfeer een rol spelen.[61] In de praktijk kan in dit kader bijvoorbeeld worden gedacht aan het bestaan van proportionele bewaartermijnen en duidelijke regels voor het vernietigen van gegevens.

3.3.2 Reactie Autoriteit Persoonsgegevens

De AP benadrukt dat, wanneer de bevoegdheden van de inlichtingen- en veiligheidsdiensten worden versterkt, de waarborgen tegen willekeur en disproportionele inbreuken navenant zouden moeten worden versterkt. In het wetsvoorstel is dit nog niet voldoende het geval. Hierop wordt in de onderstaande paragrafen nader ingegaan.

3.3.2.1 Vernietiging niet-relevante gegevens bij onderzoeksopdrachtgerichte interceptie en bewaartermijn

Zoals uiteengezet in paragraaf 3.2.2.1, maken het wetsvoorstel en de memorie van toelichting niet voldoende voorzienbaar in welke mate gegevens die niet relevant zijn voor het onderzoek waarvoor zij zijn vergaard, in de praktijk daadwerkelijk worden vernietigd. Deze onduidelijkheid staat niet alleen haaks op de voorzienbaarheidseis van artikel 8 EVRM, maar betekent ook dat een belangrijke waarborg in het wetsvoorstel onvoldoende is uitgewerkt. Uit de jurisprudentie van het EHRM volgt namelijk dat data die niet relevant zijn voor het doel waarvoor ze zijn verkregen, onmiddellijk moeten worden vernietigd.[62]

[57] EHRM 6 september 1978, 5029/71, Klass e.a. t. Duitsland, par. 50. Zie in dit kader tevens: Sarah Eskens, Ot van Daalen en Nico van Eijk, Ten standards for oversight and transparency of national intelligence services, Institute for Information Law (IViR, University of Amsterdam), 2015, p. 14-15.
[58] Het bestaan van effectief en onafhankelijk toezicht op de inlichtingen- en veiligheidsdiensten speelt een belangrijke rol bij het beantwoorden van de vraag of sprake is van afdoende waarborgen. Vanwege het belang van effectief en onafhankelijk toezicht, wordt hieraan specifiek aandacht besteed in de volgende paragraaf.
[59] EHRM 6 september 1978, 5029/71, Klass e.a. t. Duitsland, par. 50.
[60] EHRM 26 maart 1987, nr. 9248/81, Leander t. Zweden, par. 60; EHRM 29 juni 2006, 54934/00, Weber en Saravia t. Duitsland, par. 106.
[61] EHRM 6 september 1978, 5029/71, Klass e.a. t. Duitsland, par. 50; EHRM 29 juni 2006, 54934/00, Weber en Saravia t. Duitsland, par. 106.
[62] EHRM 4 december 2015, 47143/06, Roman Zakharov t. Rusland, par. 255. Zie tevens Kamerstukken II, 2016-2017, 34588 nr. 4 (Advies afdeling advisering Raad van State en Nader rapport), p. 32.

Het wetsvoorstel biedt strikt genomen de ruimte om grote hoeveelheden data die niet relevant zijn voor het onderzoek waarvoor zij zijn verzameld, te bewaren. Tevens biedt het wetsvoorstel de ruimte om grote hoeveelheden gegevens die niet op relevantie zijn onderzocht, te bewaren. Door het ontbreken van strikte regels omtrent de vernietiging van niet-relevante en niet-onderzochte gegevens, bestaat het risico dat de vernietiging van deze gegevens in de praktijk eerder uitzondering dan regel zal zijn.[63] Om te voldoen aan de eisen van artikel 8 EVRM, zou het principe van *"select while you collect"*[64] dan ook expliciet in de wettekst moeten worden vastgelegd. Gegevens die niet relevant zijn voor het doel waarvoor zij zijn verzameld, zouden terstond moeten worden vernietigd, terwijl gegevens waarvan de relatie met de onderzoeksopdracht niet is onderzocht binnen een kortere termijn dan drie jaar zouden moeten worden vernietigd.

Hiermee in samenhang geldt dat de bewaartermijn van drie jaar dient te worden beperkt, aangezien deze termijn (als zodanig) niet proportioneel lijkt te zijn en op gespannen voet staat met artikel 8 EVRM.[65] In de memorie van toelichting stelt de regering weliswaar dat een bewaartermijn van drie jaar noodzakelijk is om beter inzicht te verkrijgen in nog onbekende dreigingen, maar - zoals de Raad voor de Rechtspraak opmerkt - geldt dat bewaartermijnen niet kunnen worden gebaseerd op het criterium "mogelijk nuttig".[66] Bij de constatering dat de bewaartermijn verder lijkt te gaan dan noodzakelijk en proportioneel is, speelt mee dat het gedurende de bewaartermijn van drie jaar mogelijk is om de (bulk)gegevens te verstrekken aan buitenlandse diensten, waaronder ook niet-geëvalueerde gegevens. Juist gezien de omvang en (mogelijk) ingrijpende aard van de inbreuk op de persoonlijke levenssfeer van individuen, zou de bewaartermijn ten aanzien van de bevoegdheid tot onderzoeksopdrachtgerichte interceptie beperkt moeten zijn.

3.3.2.2 Verstrekking (niet-geëvalueerde) gegevens aan het buitenland

Het wetsvoorstel biedt de diensten de mogelijkheid om gegevens - waaronder niet-geëvalueerde gegevens - te verstrekken aan buitenlandse inlichtingen- en veiligheidsdiensten. Dergelijke verstrekkingen kunnen zowel plaatsvinden binnen een samenwerkingsverband (artikel 89, tweede lid) als aan diensten met wie geen samenwerkingsverband is gesloten (artikel 64, eerste lid). Het kan hierbij in de praktijk gaan om grote hoeveelheden niet-geëvalueerde gegevens.[67]

Het verstrekken van gegevens - en dan met name niet-geëvalueerde gegevens - brengt in de praktijk bijzondere risico's met zich mee voor individuele burgers en bedrijven.[68] Zo kan het gebeuren dat bijzondere persoonsgegevens, zoals gegevens over de seksuele geaardheid of gegevens over politieke of religieuze overtuigingen, worden verstrekt aan autoriteiten in landen waar mensenrechten niet (ten volle) worden gerespecteerd.[69] Dit kan negatieve gevolgen hebben voor Nederlandse burgers wanneer zij deze

[63] Zie in dit kader bijvoorbeeld Kamerstukken II, 2016-2017, 34588 nr. 4 (Advies afdeling advisering Raad van State en Nader rapport), p. 32.
[64] Bart Jacobs, 'Select while you collect. Een bespreking van interceptie door inlichtingen- en veiligheidsdiensten', NJB 2016, blz. 256-261.
[65] Raad voor de Rechtspraak, "Advies Wet op de inlichtingen- en veiligheidsdiensten 20..", 15 november 2016, p. 6. Zie tevens: Kamerstukken II, 2016-2017, 34588 nr. 4 (Advies afdeling advisering Raad van State en Nader rapport), p. 33-34.
[66] Raad voor de Rechtspraak, "Advies Wet op de inlichtingen- en veiligheidsdiensten 20..", 15 november 2016, p. 6.
[67] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 163.
[68] Zie in dit kader tevens Kamerstukken II, 2016-2017, 34588 nr. 4 (Advies afdeling advisering Raad van State en Nader rapport), p. 35, waar o.a. wordt gewezen op het feit dat bewaartermijnen in andere landen sterk kunnen afwijken van de Nederlandse bewaartermijnen.
[69] Zie in dit kader tevens: Bits of Freedom, Reactie op consultatie Wet op de inlichtingen- en veiligheidsdiensten 20XX, 1 september 2015, p. 23.

landen bezoeken. Omdat met bulkinterceptie ook gegevens van niet-Nederlanders worden onderschept, kan het verstrekken van gegevens bovendien ingrijpende gevolgen hebben voor burgers die wonen in de landen waaraan deze gegevens worden verstrekt. Deze risico's zijn bij de verstrekking van niet-geëvalueerde gegevens nog groter; op voorhand staat immers niet vast welke informatie besloten ligt in de verstrekte gegevens.

In de memorie van toelichting wordt beargumenteerd dat de mogelijkheid tot het verstrekken van (niet-geëvalueerde) gegevens onder meer noodzakelijk is voor de goede samenwerking met buitenlandse diensten, de informatiepositie van de Nederlandse diensten en om effectief te kunnen inspelen op dreigingen.[70] Tegelijkertijd zijn de in het wetsvoorstel opgenomen waarborgen ten aanzien van de verstrekking van gegevens aan het buitenland, beperkt. Zo is voor een dergelijke verstrekking een voorafgaande rechtmatigheidstoets, al dan niet door de Toetsingscommissie Inzet Bevoegdheden (TIB), niet vereist.

Gezien de ruime mogelijkheden die het wetsvoorstel biedt om gegevens te verstrekken aan buitenlandse diensten en de bijzondere risico's die daaraan verbonden zijn, zou deze bevoegdheid met aanvullende waarborgen moeten worden omkleed om disproportionele inbreuken te voorkomen. Denkbaar is dat juíst de CTIVD hierbij in het uitvoeringsstadium een rol speelt. Ten aanzien van de bevoegdheid om niet-geëvalueerde gegevens te verstrekken, zou te meer moeten worden overwogen of de inzet van deze bevoegdheid, ook met aanvullende waarborgen, daadwerkelijk proportioneel kán zijn ten opzichte van de mogelijk ingrijpende consequenties voor individuen.

3.3.2.3 Aanvullende maatregelen Big data en geautomatiseerde gegevensverwerkingen

Zoals uit het wetsvoorstel en de toelichting blijkt, zullen geautomatiseerde data-analyse en de verwerking van Big Data in de praktijk een belangrijke rol spelen in de taakuitoefening van de diensten.[71] Aan dergelijke verwerkingen kleven echter bijzondere risico's. Zo bestaat het gevaar dat structureel teveel gegevens worden verwerkt, dat het doelbindingsprincipe geheel teniet wordt gedaan en dat bepaalde groepen in de samenleving disproportioneel worden geraakt door geautomatiseerde analyses. Daarnaast zijn de profielen, algoritmen en methoden die door de diensten zullen worden gebruikt in de praktijk niet transparant voor burgers en toezichthouders, hetgeen ertoe kan leiden dat het maatschappelijk vertrouwen in de diensten afneemt.[72] Aan de geautomatiseerde analyse van grote, gecombineerde gegevensbestanden zouden dan ook aanvullende waarborgen moeten worden verbonden. In het wetsvoorstel wordt hierin nog onvoldoende voorzien.

Zowel door de CTIVD[73], als door de Afdeling[74] en in de PIA[75], wordt in dit kader gewezen op de Algemene Verordening Gegevensbescherming[76], waarin expliciet is opgenomen dat passende technische en organisatorische maatregelen moeten worden genomen die erop zijn gericht de beginselen van gegevensbescherming bij het ontwerpen van systemen te incorporeren. Zo kan worden gedacht aan het implementeren van de beginselen van *privacy by design* en *privacy by default* bij het ontwerpen van systemen.

[70] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), o.a. p. 158.
[71] Zie in dit kader met name artikel 60 van het wetsvoorstel.
[72] Wetenschappelijke Raad voor het Regeringsbeleid, Big Data in een vrije en veilige samenleving (2016), p. 10.
[73] CTVID, Zienswijze CTIVD op wetsvoorstel Wiv 20.., Bijlage I Essentiële waarborgen (november 2016), p. 25.
[74] Kamerstukken II, 2016-2017, 34588 nr. 4 (Advies afdeling advisering Raad van State en Nader rapport), p. 37.
[75] Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdiensten 20XX, 12 februari 2016, p. 148.
[76] Deze verordening is weliswaar niet van toepassing op de diensten, maar kan niettemin ter inspiratie dienen voor de omgang met persoonsgegevens door de diensten.

Aan de hand van deze beginselen kan worden bewerkstelligd dat systemen vanaf het begin af aan zo worden ingericht, dat zij een zo min mogelijke inbreuk op de privacy met zich brengen. De regering volgt deze adviezen echter niet en volstaat met een algemene zorgplicht voor de diensthoofden[77], omdat "in het wetsvoorstel al een specifiek kader voor diverse aspecten van gegevensverwerking is opgenomen, waarbij in de afweging de privacyrisico's - uitgewerkt in diverse waarborgen - reeds zijn meegewogen".[78]

De AP volgt deze redenering niet en merkt op dat het opnemen van algemene zorgplichten in het wetsvoorstel niet afdoende is; deze plichten moeten nader worden ingevuld om in de praktijk te bewerkstelligen dat willekeur en disproportionele inbreuken worden voorkomen. Ook wordt het aan de hand van meer concrete (zorg)plichten beter mogelijk om effectief toezicht uit te oefenen op de diensten. Zoals de CTIVD opmerkt, zou het wetsvoorstel kunnen worden aangevuld met een expliciete zorgplicht ten aanzien van de kwaliteit van geautomatiseerde gegevensverwerkingen.[79] Ter nadere invulling van deze zorgplicht zou een gegevensbeschermingsbeleid[80] moeten worden gevoerd en zou- voorafgaand aan de toepassing of aanbesteding van nieuwe, geautomatiseerde gegevensverwerkingsprojecten - een gegevenseffectbeoordeling[81] moeten worden uitgevoerd.

3.4 Effectief en onafhankelijk toezicht

3.4.1 Juridisch kader

Effectief en onafhankelijk toezicht op de diensten is van bijzonder belang. Omdat de inlichtingen- en veiligheidsdiensten heimelijk opereren, hebben burgers doorgaans immers geen kennis van het feit dat hun persoonsgegevens zijn onderschept. Dit betekent dat burgers, wanneer sprake is van een onrechtmatige inbreuk op de persoonlijke levenssfeer, veelal niet zelf aanspraak kunnen maken op een effectief rechtsmiddel tegen deze onrechtmatige inbreuk. Effectief en onafhankelijk toezicht dient in het geval van de diensten dan ook als een belangrijke aanvulling op het recht op een *effective remedy,* zoals neergelegd in artikel 13 EVRM. Wanneer de burger vanwege de heimelijke aard van de operaties van de diensten zelf niet in staat is te controleren of zijn persoonlijke levenssfeer op onrechtmatige wijze wordt aangetast, moet dit gebrek worden gecompenseerd door het bestaan van een effectief en onafhankelijk systeem van toezicht. Effectief en onafhankelijk toezicht is, kort gezegd, *"an essential component of the protection of individuals with regard to the protection of personal data"*.[82]

Uit de jurisprudentie blijkt dat het EHRM bij het beoordelen van het toezicht op de inlichtingen- en veiligheidsdiensten kijkt naar het gehele systeem.[83] Het is, met andere woorden, niet doorslaggevend of onafhankelijke controle vooraf of achteraf plaatsvindt, zolang maar effectief toezicht op het toepassen van bevoegdheden mogelijk is.[84] Niettemin heeft het EHRM een voorkeur uitgesproken voor een

[77] Zie artikel 24 van het wetsvoorstel.
[78] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 249.
[79] CTVID, Zienswijze CTIVD op wetsvoorstel Wiv 20.., Bijlage I Essentiële waarborgen (november 2016), p. 23-25.
[80] Zie artikel 24 van de Algemene Verordening Gegevensbescherming.
[81] Zie artikel 35 van de Algemene Verordening Gegevensbescherming.
[82] Artikel 29 Werkgroep, Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees), p. 9. Zie: Hof van Justitie van de Europese Unie, 9 maart 2010, Commissie t. Duitsland, C-518/07.
[83] Zie voor een uitgebreide analyse onder meer: Sarah Eskens, Ot van Daalen en Nico van Eijk, Ten standards for oversight and transparency of national intelligence services, Institute for Information Law (IViR, University of Amsterdam), 2015.
[84] Zie onder meer EHRM 6 september 1978, 5029/71, Klass e.a. t. Duitsland 49-60; EHRM 18 mei 2010, 26839/05 Kennedy t. Verenigd Koninkrijk, par. 166-170.

onafhankelijke (rechterlijke) toets voorafgaand aan het inzetten van bijzondere bevoegdheden.[85] Ook moet het toezicht zien op de gehele uitoefening van bevoegdheden van de diensten. Alleen voorafgaande autorisatie door een onafhankelijke instantie is niet genoeg, er moet ook *ex post* rechtmatigheidstoezicht zijn op de uitvoering van de operatie. Door middel van *ex post* toezicht kan immers worden gecontroleerd of de operatie binnen de grenzen van de verleende toestemming is uitgevoerd en of de (uitvoering van de) operatie de grenzen van het EVRM, met name wat betreft de noodzaak, proportionaliteit en subsidiariteit, niet heeft overschreden.[86]

3.4.2 Reactie Autoriteit Persoonsgegevens

De AP benadrukt dat, wanneer de bevoegdheden van de diensten worden versterkt, het toezicht op de diensten navenant zou moeten worden versterkt. Juist omdat de activiteiten van de diensten zich afspelen buiten het zicht van het publiek, moet worden voorzien in een systeem van daadwerkelijk onafhankelijk en effectief toezicht op de activiteiten van de diensten. In de huidige vorm voorziet het wetsvoorstel daarin nog niet.

Het wetsvoorstel voorziet in een stelsel van toezicht dat is verdeeld over de nieuw op te richten TIB, de CTIVD en het parlement.

De TIB oefent voorafgaand aan de inzet van bijzondere bevoegdheden bindend toezicht uit. Voordat een bijzondere bevoegdheid - zoals onderzoeksopdrachtgerichte interceptie - mag worden ingezet, moet de TIB hiervoor toestemming verlenen. In de praktijk betekent dit dat de diensten voorafgaand aan de inzet van bijzondere bevoegdheden toestemming moeten vragen aan de minister, waarna de minister vervolgens zijn instemming ter toetsing dient voor te leggen aan de TIB voor een bindende rechtmatigheidstoets. De TIB zal bestaan uit drie leden, waarvan ten minste twee juristen, en heeft geen zelfstandige toegang tot de systemen van de diensten.[87] In plaats daarvan regelt het wetsvoorstel dat de minister zijn besluit en het daaraan ten grondslag liggende verzoek van de diensten aan de TIB zal verstrekken, zodat de TIB dit besluit op rechtmatigheid kan controleren.

Naast de TIB oefent de CTIVD - zoals nu ook het geval is - toezicht uit op de diensten. De CTIVD beschikt in dit kader over zelfstandige onderzoeksbevoegdheden en is bevoegd rechtmatigheidsoordelen te geven over het concrete optreden van de diensten. De oordelen van de CTIVD zijn echter niet bindend[88] en het wetsvoorstel brengt hierin geen verandering. Nu de toets op de rechtmatigheid van het door de minister genomen besluit voorafgaand aan de inzet van een bijzondere bevoegdheid exclusief bij de TIB is belegd, brengt dat met zich mee dat de CTIVD de rechtmatigheid van dat besluit in beginsel dient te respecteren, zo wordt in de memorie van toelichting uiteengezet.[89] Alleen wanneer de CTIVD in het kader van haar toezicht op de uitvoering van een dergelijk besluit constateert dat het door de minister genomen besluit en het ter toetsing aan de TIB voorgelegde besluit is gebaseerd op onvolledige of onjuiste informatie, kan zij

[85] EHRM 6 september 1978, 5029/71, Klass e.a. t. Duitsland, par. 56; EHRM 18 mei 2010, 26839/05, Kennedy t. Verenigd Koninkrijk, par. 167.
[86] J.P. Loof e.a., "Het mensenrechtenkader voor het Nederlandse stelsel van toezicht op de inlichtingen- en veiligheidsdiensten", (Onderzoek in opdracht van het CTIVD, Universiteit Leiden, augustus 2015) p. 15.
[87] Zie artikelen 33 en 36 van het wetsvoorstel.
[88] Met uitzondering van de klachtenprocedure.
[89] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 52.

dit als bevinding aan de minister rapporteren.[90] Het is dan aan de minister om te overwegen of er aanleiding is een nieuw besluit te nemen en dat (opnieuw) aan de TIB voor te leggen.[91]

Tot slot is sprake van parlementaire controle, doordat de betrokken ministers politiek verantwoordelijk zijn voor het optreden van de diensten en hierover verantwoording afleggen aan het parlement, zowel in het openbaar als in beslotenheid aan de Commissie voor de Inlichtingen- en Veiligheidsdiensten[92] van de Tweede Kamer.

Zoals de Afdeling[93] en de Raad voor de Rechtspraak[94] eveneens opmerken, zal de toetsing van de TIB in de praktijk waarschijnlijk beperkt zijn, aangezien de TIB beperkt van omvang is en geen eigen onderzoeksbevoegdheden heeft. Daarmee in samenhang valt te vrezen dat de TIB - gezien haar beperkte omvang en bevoegdheden – niet afdoende kennis en inzicht kan vergaren om een inschatting te kunnen maken van de effectiviteit en effecten van het optreden van de diensten. Het beschikken over deze kennis en inzichten is echter onmisbaar om een weloverwogen oordeel over de noodzaak, proportionaliteit en subsidiariteit van de inzet van bijzondere bevoegdheden te vellen. Zoals de Afdeling waarschuwt, moet worden voorkomen dat de toets door de TIB in de praktijk nagenoeg altijd positief zal uitvallen, omdat de TIB enerzijds niet afdoende inzicht heeft in de noodzaak van de inzet van deze bevoegdheden maar anderzijds wel rekening dient te houden met de ingrijpende gevolgen die het weigeren van toestemming met zich kunnen brengen.[95] Er moet, met andere woorden, worden voorkomen dat de TIB niet meer dan een “stempelmachine” zal zijn.

Niet alleen kunnen vraagtekens worden gezet bij de effectiviteit van de TIB en de waarde van de voorafgaande rechtmatigheidstoets, maar ook is niet duidelijk hoe de oordelen van de TIB zich zullen verhouden tot de oordelen van de CTIVD, die – aan de hand van eigen onderzoeksbevoegdheden – wel toezicht kan uitoefenen op de *inzet* van bevoegdheden door de diensten. Hoewel in de memorie van toelichting wordt vermeld dat de CTIVD de rechtmatigheid van de besluiten van de TIB in beginsel moet respecteren, kan dit in de praktijk wringen indien de TIB niet beschikt over voldoende bevoegdheden en middelen om een daadwerkelijk effectieve rechtmatigheidstoets uit te voeren. Evenmin is duidelijk welke gevolgen de introductie van de TIB zal hebben voor de mate waarin de betrokken ministers eigenstandig verantwoording kunnen afleggen aan het parlement; ook de ministers zijn immers gebonden aan de oordelen van de TIB.

Samenvattend wordt in het wetsvoorstel een marginale rechtmatigheidstoets *ex ante* voorgesteld - waarbij geldt dat de TIB hoogstwaarschijnlijk niet beschikt over afdoende middelen en bevoegdheden om deze toets effectief uit te voeren - terwijl de introductie van de TIB niettemin gevolgen zal hebben voor zowel het parlementair toezicht op de minister, als het toezicht van de CTIVD op de diensten. Hierdoor is het ten zeerste de vraag of het wetsvoorstel voorziet in een stelsel van toezicht dat - in totaliteit bezien - daadwerkelijk effectief is en alle facetten van de activiteiten van de diensten omvat, zoals bedoeld in artikel 8 EVRM.[96] De AP benadrukt dat de verhouding tussen enerzijds toezicht *ex ante* en anderzijds toezicht *ex*

[90] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 52.
[91] Kamerstukken II, 2016-2017, 34588 nr. 3 (memorie van toelichting), p. 52.
[92] In de praktijk veelal aangeduid als de ”Commissie Stiekem”.
[93] De Afdeling spreekt zelfs van ”een zeer marginale en abstracte rechtmatigheidsbeoordeling ex ante”. Kamerstukken II, 2016-2017, 34588 nr. 4 (Advies afdeling advisering Raad van State en Nader rapport), p. 16.
[94] Raad voor de Rechtspraak, ”Advies Wet op de inlichtingen- en veiligheidsdiensten 20..”, 15 november 2016, p. 4-5.
[95] Kamerstukken II, 2016-2017, 34588 nr. 4 (Advies afdeling advisering Raad van State en Nader rapport), p. 16.
[96] Zie in dit kader tevens Kamerstukken II, 2016-2017, 34588 nr. 4 (Advies afdeling advisering Raad van State en Nader rapport), p. 2 en Raad voor de Rechtspraak, ”Advies Wet op de inlichtingen- en veiligheidsdiensten 20..”, 15 november 2016, p. 5.

post nadrukkelijk (wederom) onder de loep zou moeten worden genomen. Voorkomen moet worden dat *inhoudelijk* toezicht achteraf wordt vervangen door een (te) beperkte juridische toets voorafgaand aan de inzet van bevoegdheden. Waar de bevoegdheden van de diensten in het wetsvoorstel worden versterkt, zou het stelsel van toezicht ook moeten worden aangepast en – bovenal – versterkt.