Toezichtsrapport

Over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD

CTIVD nr. 55

28 december 2017

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 55

TOEZICHTSRAPPORT

Over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD

Inhoudsopgave

CTIVD nr. 55

SAMENVATTING

Over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD

Toezichtsrapport nr. 55 gaat over het door de AIVD en de MIVD verwerven van door derden op internet aangeboden bulkdatasets. Met het 'verwerven van bulkdatasets' wordt het verzamelen van bestanden met een grote hoeveelheid gegevens bedoeld. Deze gegevenssets worden door derden aangeboden, al dan niet tegen betaling, via een website, forum of online systeem voor het versturen van bestanden. De datasets zijn bijvoorbeeld beschikbaar gekomen als gevolg van datalekken of hacks bij bedrijven of instellingen.

De grondslag van de verwerving van deze bulkdatasets is de algemene bevoegdheid van de diensten voor het verzamelen van gegevens die noodzakelijk zijn voor hun taakuitvoering. Meer specifiek gaat het hierbij om het verzamelen van gegevens uit open bronnen of via het raadplegen van informanten. De wet sluit niet uit dat daarbij grote hoeveelheden gegevens (bulk) worden vergaard, waaronder gegevens van personen die niet in de aandacht van de diensten staan. Voor de inzet van de algemene bevoegdheid gelden minder waarborgen dan bij de inzet van een bijzondere bevoegdheid, zoals de toepassing van de hackbevoegdheid of de telefoontap.

In dat kader moet worden benadrukt dat het hier gaat om bulkdatasets die door een ieder kunnen worden vergaard. De gegevens in de datasets zijn reeds 'gestolen' of gelekt bij een organisatie en publiekelijk aan een ieder aangeboden. In deze zin heeft zich al een ernstige privacy-inmenging bij de betrokkenen voorgedaan, alleen niet door toedoen van de overheid. Bij de verwerving en verdere verwerking van deze bulkdatasets door de diensten, als onderdelen van de overheid, kan echter wederom een meer ernstige privacy-inmenging plaatsvinden. Onder omstandigheden zijn hier bepaalde aanvullende (bovenwettelijke) waarborgen omtrent toestemming voor de verwerving en de verwerking van gegevens op hun plaats. Beide diensten hebben daarom op eigen initiatief bovenwettelijke waarborgen in intern beleid opgenomen.

In dit toezichtsrapport wordt de verwerving en verdere verwerking van vier bulkdatasets beschreven. In twee gevallen ging het om bulkdatasets *zonder* persoonsgegevens. Deze datasets bevatten technische informatie. De datasets zijn in hun geheel aan de relevante organisatieonderdelen van beide diensten beschikbaar gesteld. De verdere verwerking van de gegevens in deze datasets, zoals het raadplegen en analyseren hiervan, houdt geen privacy-inmenging in. De verwerving van deze bulkdatasets en verdere verwerking van de gegevens was ten behoeve van de taakuitvoering van de diensten noodzakelijk en daarmee onder de huidige Wiv 2002 *rechtmatig*. Ook onder de Wiv 2017 zou de verwerving en verdere verwerking van de gegevens rechtmatig zijn geweest.

Daarnaast zijn twee bulkdatasets *met* persoonsgegevens verworven. Beide datasets bestonden telkens uit een beperkt aantal typen gegevens, zoals namen, e-mailadressen en wachtwoorden. De datasets bevatten elk de gegevens van meer dan honderd miljoen personen, die hoofdzakelijk geen onderwerp van onderzoek zijn en dat ook nooit zullen worden. De verwerving en verdere verwerking van de

gegevens uit deze datasets leveren een meer ernstige privacy-inmenging op. De gegevens voorzien echter in een duidelijke inlichtingenbehoefte en waren noodzakelijk om onder meer targets te kunnen identificeren. Ook kunnen de gegevens worden aangewend voor de inzet van de hackbevoegdheid. Zowel de Wiv 2002 en als de Wiv 2017 bieden tezamen met het aanvullende interne beleid van de diensten een adequate wettelijke basis voor het verwerven van door derden op internet aangeboden bulkdatasets met persoonsgegevens.

De toestemming voor de verwerving van de eerste dataset, die naar inschatting een zeer beperkt aantal persoonsgegevens van Nederlands ingezetenen bevat, is op het juiste niveau verleend (de minister van BZK). De tweede dataset bevat persoonsgegevens van relatief veel Nederlands ingezetenen en is zeer algemeen van aard. De toestemming voor de verwerving van de tweede dataset is op een te laag niveau gegeven (de directeur-generaal van de AIVD en de directeur van de MIVD). De verwerving van de eerste dataset is dus *rechtmatig* en de verwerving van de tweede dataset *onrechtmatig*. Deze conclusie blijft onder de Wiv 2017 ongewijzigd.

De diensten hanteren met betrekking tot de datasets met persoonsgegevens op grond van hun interne beleid een bovenwettelijke bewaartermijn van drie jaar. Tevens wordt in de verdere verwerking de zogenaamde *'buitenbak-binnenbakprocedure'* toegepast. De buitenbak-binnenbakprocedure houdt in dat de gehele dataset na verwerving in de buitenbak wordt gezet, waar de operationele teams niet bij kunnen. De buitenbak is alleen toegankelijk voor een klein aantal technische beheerders en data-analisten. Op deze wijze wordt uitvoering gegeven aan de vereisten van functie- en taakscheiding en het need-to-knowbeginsel.

Als een operationeel team van de gegevens in de buitenbak gebruik wil maken, moet eerst een toestemmingsprocedure worden doorlopen. De diensten motiveren daartoe schriftelijk waarom zij bepaalde kenmerken, zoals een naam of een e-mailadres, in de buitenbak willen laten naslaan. Als toestemming wordt verleend, worden de resultaten van de naslag van de buitenbak naar de binnenbak verplaatst. Daarmee zijn deze gegevens voor een groot aantal operationele medewerkers van beide diensten raadpleegbaar. Alle onderzochte verzoeken zijn voldoende gemotiveerd en noodzakelijk, proportioneel en subsidiair. Dit maakt dat de buitenbak-binnenbakprocedure en alle verzoeken tot toegang tot de gegevens als *rechtmatig* zijn beoordeeld. Deze conclusie blijft onder de Wiv 2017 gehandhaafd.

In het rapport doet de CTIVD enkele aanbevelingen. Deze aanbevelingen zien op het helder formuleren en op de medewerkers overbrengen van de toepasselijke juridische grondslagen bij de verwerving en verdere verwerking van de gegevens in de bulkdatasets. Ook wordt de diensten aanbevolen een algemeen beleidskader voor het in bulk verwerven en verder verwerken van persoonsgegevens op te stellen en dit te publiceren. Ten slotte doet de CTIVD twee aanbevelingen in het kader van dataminimalisatie. Dataminimalisatie betekent dat gegevens niet (langer) worden verwerkt dan strikt noodzakelijk voor de taakuitvoering van de diensten. De diensten dienen de verwerking van persoonsgegevens tot het noodzakelijke minimum te beperken en daarmee het recht op privacy van de betrokken te waarborgen.

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 55

TOEZICHTSRAPPORT

Over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD

1. Inleiding

Verwerven van door derden op internet aangeboden bulkdatasets

Steeds vaker worden bestanden met persoonsgegevens door derden op het internet aangeboden. Deze datasets zijn bijvoorbeeld beschikbaar gekomen als gevolg van een datalek en kunnen gegevens over miljoenen mensen bevatten. De gegevens kunnen door derden worden aangeboden voor bijvoorbeeld geldelijk gewin of om de ondermaatse beveiliging van bedrijven en instellingen aan te tonen. De op internet aangeboden datasets kunnen ook relevant zijn voor de taakuitvoering van de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst (hierna: AIVD en MIVD, tezamen: de diensten). Daarbij moet vooral gedacht worden aan het onderkennen en identificeren van targets.

De aanleiding van het onderzoek

Doordat zich in de datasets zeer grote hoeveelheden persoonsgegevens kunnen bevinden, vindt er met de verwerving en ontsluiting van de gegevens een potentieel ernstige privacy-inmenging plaats. De datasets worden vergaard op basis van de algemene bevoegdheid (het verzamelen van gegevens uit open bron of de informantenregeling). Daarbij zijn minder (strenge) waarborgen van toepassing dan bij de inzet van bijzondere bevoegdheden. Onder omstandigheden is hier echter additioneel (bovenwettelijk) beleid met waarborgen omtrent toestemming en verwerking van gegevens op zijn plaats. De diensten hebben dat in dit geval onderkend en interne beleidsnotities over het verwerven van door derden op internet aangeboden bulkdatasets vastgesteld. Een en ander vormde de aanleiding tot het starten van dit onderzoek. De CTIVD gaat in dit rapport na in hoeverre het handelen van de AIVD en de MIVD aangaande de verwerving en verdere verwerking van de door derden op internet aangeboden bulkdatasets rechtmatig is.

De reikwijdte van het onderzoek

Op 11 juli 2017 heeft de CTIVD aangekondigd een kortlopend onderzoek te verrichten naar de verwerving van op internet aangeboden bestanden met grote hoeveelheden gegevens (bulkdatasets).[1] Het onderzoek beslaat de periode 1 januari 2016 tot en met 11 juli 2017 en heeft betrekking op de in die periode op internet verworven bulkdatasets. De beoordeling van de rechtmatigheid is gebaseerd op de huidige wet, de Wet op de inlichtingen- en veiligheidsdiensten 2002 (hierna: Wiv 2002). In het rapport wordt ook de Wet op de inlichtingen- en veiligheidsdiensten 2017 (hierna: Wiv 2017) betrokken. Deze wet, die waarschijnlijk in 2018 in werking treedt, kent een uitbreiding van de bevoegdheden van de

[1] De aanbiedingsbrief is beschikbaar op ctivd.nl.

diensten en een versterking van de waarborgen tegen misbruik.[2] In het rapport wordt aangestipt waar de nieuwe wet afwijkt van de oude wet. Waar relevant wordt de nieuwe wet ook in de aanbevelingen meegenomen.

Onderzoeksmethodiek

De CTIVD heeft een toetsingskader ontwikkeld om het beleid en de praktijk van de verwerving en ontsluiting van op internet aangeboden bulkdasets te kunnen toetsen. Het kader is gebaseerd op de wet, jurisprudentie, eerdere toezichtsrapporten en door de ministers van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) en van Defensie in dat verband overgenomen aanbevelingen. Ook het interne beleid van beide diensten is bij het ontwikkelen van het kader in aanmerking genomen.

Tijdens het onderzoek zijn interviews met juristen, beleidsmedewerkers en operationele medewerkers van de diensten gehouden. Deze gesprekken zijn gevoerd om een beter beeld te krijgen van het handelen van de diensten en ter verificatie van de gevonden onderzoeksresultaten. Voor de bestudering van de ontsluiting en verdere verwerking van de gegevens zijn gesprekken gevoerd met technische experts van beide diensten. Daarnaast is door medewerkers van de diensten een aantal demonstraties gegeven. Daarmee is een beeld verkregen van de technische en organisatorische maatregelen met betrekking tot de logging van de gegevens en autorisaties in de systemen van de diensten.

Ten slotte zijn alle in de onderzoeksperiode uitgevoerde operaties waarbij door derden op internet aangeboden bulkdatasets zijn verworven of waarin gegevens uit deze datasets in het operationeel proces zijn gebruikt op rechtmatigheid onderzocht. Daarvoor zijn de gemotiveerde toestemmingen voor de operaties in de systemen opgezocht en geanalyseerd. Aan de hand van het toetsingskader is allereerst beoordeeld of de motiveringen in de verzoeken tot toestemming telkens de inzet konden dragen, dat wil zeggen of deze alle redengevende feiten en omstandigheden bevatten. Bovendien is beoordeeld of de afwegingen die zijn gemaakt in het kader van de noodzaak, proportionaliteit en de subsidiariteit ook daadwerkelijk tot een rechtmatige inzet hebben geleid. Daarbij is ook getoetst of de toestemming voor de verwerving op het juiste niveau is gegeven.

De beoordeling van praktijk en werkwijze

In Bijlage 1 wordt het toetsingskader omtrent de verwerving en ontsluiting van op internet aangeboden bulkdatasets uiteengezet. Op grond van dit kader is beoordeeld of een werkwijze of praktijk rechtmatig is geweest. Bij het oordeel onrechtmatig is sprake van strijdigheid met wet- of regelgeving. Deze wet- en regelgeving bestaat uit de Wet op de inlichtingen- en veiligheidsdiensten, jurisprudentie, door de ministers naar aanleiding van eerdere toezichtsrapporten overgenomen aanbevelingen en het vastgestelde interne beleid. Indien de werkwijze van een dienst in wenselijkheid tekortschiet, maar niet onrechtmatig is, wordt hiervan in het rapport melding gemaakt.

Het openbare toezichtsrapport en de geheime bijlage

Alle geconstateerde onrechtmatigheden en tekortkomingen in de werkwijze zijn in het openbare toezichtsrapport opgenomen. Vanwege de bescherming van de nationale veiligheid is een aantal nadere details van de beoordeelde operaties in de geheime bijlage beschreven. Deze geheime bijlage is beperkt in omvang (vier pagina's) en kent geen vermeldingen van onrechtmatigheden die niet in het openbare toezichtsrapport zijn opgenomen.

Het verloop van het onderzoek

Het onderzoek is met het opstellen van dit rapport afgerond op 10 november 2017. De ministers van BZK en van Defensie zijn in de gelegenheid gesteld te reageren op de in het toezichtsrapport opgenomen bevindingen. De reacties van de ministers van BZK en Defensie zijn op 22 december 2017

---

[2] *Stb*. 2017, 317. Inwerkingtreding op een bij koninklijk besluit te bepalen tijdstip.

ontvangen. Deze reacties hebben geleid tot enkele wijzigingen, waarna het toezichtsrapport op 28 december 2017 is vastgesteld.

De leeswijzer

Het rapport is als volgt opgebouwd. In hoofdstuk 2 staan de feitelijke bevindingen van het onderzoek met betrekking tot de verwerving en verdere verwerking van door derden op internet aangeboden bulkdatasets. In hoofdstuk 3 vindt de juridische toets op rechtmatigheid plaats met betrekking tot de verwerving van de bulkdatasets. In hoofdstuk 4 wordt nagegaan in hoeverre de verdere verwerking van gegevens uit de datasets op rechtmatige wijze plaatsvindt. In hoofdstuk 5 worden de conclusies beschreven. Ten slotte worden in hoofdstuk 6 acht aanbevelingen gedaan.

2. De bevindingen

In dit hoofdstuk wordt het via internet verwerven en ontsluiten van bestanden met grote hoeveelheden gegevens (bulkdatasets) door de AIVD en MIVD beschreven. Deze uiteenzetting vormt de feitelijke basis waaraan de rechtmatigheid van de handelingen wordt getoetst.

2.1 De verwerving van de datasets

Met het 'verwerven van bulkdatasets' wordt het verzamelen van bestanden met een grote hoeveelheid gegevens bedoeld. Deze bestanden kunnen tezamen informatie over miljoenen personen bevatten. In de context van dit onderzoek vindt het verwerven van deze datasets op internet plaats. Deze gegevenssets worden, al dan niet tegen betaling, via een website, forum of online systeem voor het versturen van bestanden door derden aangeboden.

De datasets kunnen voor de diensten relevante informatie inhouden. Zo is het mogelijk dat daarin (technische) informatie voorkomt die bij het uitvoeren van operaties van belang kan zijn. Als datasets persoonsgegevens bevatten, zoals namen en e-mailadressen, dan kunnen deze al dan niet in combinatie met andere databronnen bijdragen aan het identificeren van targets.

De diensten hebben de uitvoering van het verwerven en verder verwerken van de bulkdatasets belegd bij de *'Joint Sigint Cyber Unit'* (hierna: JSCU). De JSCU is een gezamenlijke uitvoeringseenheid van de AIVD en de MIVD op het gebied van 'sigint' en 'cyber'. Sigint staat voor 'signals intelligence'. Het gaat hierbij onder andere om het onderscheppen van communicatieverkeer in de ether, zoals satelliet- en radioverkeer. 'Cyber' wordt gebruikt als verzamelnaam voor verschillende activiteiten die te maken hebben met computernetwerken en datastromen. Deze omvatten bijvoorbeeld de inzet van de hackbevoegdheid.

De JSCU heeft het initiatief genomen met betrekking tot het verwerven van door derden op internet aangeboden bulkdatasets beleid te formuleren, omdat de gegevens in de bulkdatasets gevoelig van aard zijn. De gegevens zijn bovendien niet door de betrokken personen zelf, maar door een derde geopenbaard. De leiding van beide diensten heeft de beleidsnotities vastgesteld.

2.2 De ontsluiting van de gegevens

De op internet verworven bulkdatasets kunnen door de diensten op twee manieren worden ontsloten. Datasets die geen persoonsgegevens bevatten worden direct aan de relevante organisatieonderdelen (bijvoorbeeld operationele teams) van de AIVD en de MIVD beschikbaar gesteld. De datasets die wel persoonsgegevens bevatten, worden ontsloten via de zogenaamde *'buitenbak-binnenbakprocedure'.*

De buitenbak-binnenbakprocedure houdt in dat de gehele dataset eerst in de buitenbak wordt gezet, waardoor de operationele teams daar niet zomaar bij kunnen. De buitenbak is alleen direct toegankelijk voor een klein aantal technische beheerders en een deel van de data-analisten van de AIVD. Ook een select aantal medewerkers van de MIVD heeft toegang tot de buitenbak. Deze medewerkers zijn allen werkzaam bij de JSCU, maar kunnen wel verbonden zijn aan een operationeel team. Op deze wijze wordt uitvoering gegeven aan het vereiste dat bij het werken met bulkgegevens functie- en taakscheiding wordt toegepast. Deze verplichting is een uitwerking van het need-to-knowbeginsel. Dit houdt in dat informatie alleen aan die medewerkers wordt verstrekt voor zover dat noodzakelijk is voor de aan hen opgedragen taken.

Daarnaast is een groot deel van de bewerkers van de operationele teams van de AIVD en de data-analisten van de MIVD geautoriseerd voor applicaties (computerprogramma's) die het mogelijk maken de buitenbak uitsluitend te doorzoeken op basis van een hit/no hit-systeem. Dit houdt in dat zij gericht naar kenmerken, zoals een telefoonnummer of een e-mailadres, kunnen zoeken. Als blijkt dat een kenmerk in de dataset voorkomt, krijgt de medewerker te zien dat sprake is van een 'hit'. Als het kenmerk niet in de dataset voorkomt, levert dit een 'no-hit' op. De aanwezigheid van een hit kan reden zijn deze kenmerken 'na te slaan', dat wil zeggen dat medewerkers nagaan of er informatie beschikbaar is die aan een bepaald kenmerk kan worden gerelateerd. Te denken valt aan het naslaan van een e-mailadres om te kijken in welke informatiebronnen deze nog meer voorkomt en welke additionele informatie over het e-mailadres beschikbaar is.

Als een medewerker van een operationeel team een kenmerk wil naslaan, moet eerst een aparte procedure worden doorlopen. Allereerst moet een schriftelijke aanvraag worden opgesteld. In deze aanvraag tot naslag wordt aangegeven voor welk doel bepaalde kenmerken worden nageslagen. Tevens dient de aanvraag een motivering te bevatten waarom de naslag noodzakelijk, proportioneel en subsidiair is. Ook de betrouwbaarheid van de kenmerken of de bron waaruit deze afkomstig zijn, dient te worden vermeld. Deze aanvraag moet bij de AIVD door het desbetreffende teamhoofd worden goedgekeurd. Bij de MIVD is daarvoor – na goedkeuring van onder andere de Stafafdeling Juridische Zaken – toestemming van de directeur noodzakelijk.

Na de toestemming maakt de JSCU de resultaten van de naslag voor het operationele team beschikbaar. Deze handeling kan worden voorgesteld als het verplaatsen van gegevens van de buitenbak naar de binnenbak. Als de gegevens eenmaal in de binnenbak zitten, zijn ze voor een groot aantal operationele medewerkers, ook van andere dan van het verzoekende team, van beide diensten raadpleegbaar.

3 Beoordeling van verwerving van de bulkdatasets

In dit hoofdstuk wordt de rechtmatigheid van de verwerving van de bulkdatasets beoordeeld. Het toetsingskader is uitvoerig uiteengezet in hoofdstuk 2 van bijlage 1 bij dit rapport. In paragraaf 3.1 wordt het toetsingskader samengevat. In paragraaf 3.2 vindt de beoordeling plaats met betrekking tot de verwerving van datasets zonder persoonsgegevens. In paragraaf 3.3 vindt de beoordeling plaats met betrekking tot de verwerving van datasets met persoonsgegevens. In de geheime bijlage wordt nader ingegaan op de aard van de verworven datasets en de omstandigheden waaronder ze zijn verworven. De beoordeling op rechtmatigheid vindt in dit hoofdstuk uitsluitend plaats op basis van de relevante bepalingen uit de Wiv 2002.

3.1 Toetsingskader

De verwerving van op internet aangeboden bulkdatasets kan een ernstige inmenging met het recht op privacy van de betrokkene(n) met zich meebrengen. Of dat is het geval is, is afhankelijk van de aard van de dataset. De verwerving van datasets *zonder* persoonsgegevens vormt geen inmenging met het recht op privacy. Wel kan sprake zijn van een inmenging met andere rechten en vrijheden, zoals auteursrechten. De verwerving van dataset *met* persoonsgegevens kan een ernstige privacy-inmenging met zich meebrengen, vanwege de grote hoeveelheid en de aard van gegevens in de dataset.

De drie juridische grondslagen in de Wiv 2002 en Wiv 2017 voor de verwerving van de door derden op internet aangeboden bulkdatasets zijn als volgt:

1. **Het verzamelen van gegevens uit een voor ieder toegankelijke informatiebron (open bron)**
   In dit geval kunnen de gegevens zonder meer door een ieder worden geraadpleegd. Daarbij kan gedacht worden aan openbare websites, maar ook gesloten websites, waarvoor registratie en/of betaling noodzakelijk is. Als vuistregel geldt dat de grondslag voor openbronnenonderzoek zijn begrenzing kent daar waar de diensten overgaan tot het interacteren met de aanbieder van de bulkdataset.

   Wettelijke grondslag: artikel 6, 7, 12 en 31 Wiv 2002 en artikel 25 lid 1 sub a Wiv 2017.

2. **Het verzamelen van gegevens via raadpleging van informanten (informantenregeling)**

   Als de bulkdataset op internet aan een ieder wordt aangeboden, kunnen de diensten deze basis van de informantenregeling verwerven. Medewerkers van de diensten mogen daartoe (onder een valse naam) met de aanbieder interacteren, voor zover daarbij niet sturend wordt opgetreden.

   Wettelijke grondslag: artikel 17 lid 1 sub a Wiv 2002 en artikel 39 lid 1 Wiv 2017.

3. **Het verzamelen van gegevens door de inzet van een agent (agentregeling)**
   Als een medewerker, die zich van een valse identiteit bedient, of een derde onder aansturing en instructie van de dienst een bulkdataset verwerft, is de agentregeling van toepasing.

   Wettelijke grondslag: artikel 21 Wiv 2002 en artikel 41 Wiv 2017.

In hoofdstuk 2 van het toetsingskader bij dit rapport (bijlage 1) worden de grondslagen voor de verwerving van door derden op internet aangeboden bulkdatasets uitgebreid besproken. Daarbij wordt opgemerkt dat de wet niet uitsluit dat met de inzet van deze bevoegdheden grote hoeveelheden gegevens (bulk) worden vergaard, waaronder gegevens van personen die niet in de aandacht van de

diensten staan. Wel zijn als gevolg hiervan (en de potentieel ernstige privacy-inmenging) additionele waarborgen op hun plaats, die in bovenwettelijk beleid kunnen worden geformuleerd.

Daarnaast wordt in het toetsingskader (paragraaf 3.4, bijlage 1) uitgewerkt dat bij iedere verwerving van bulkdatasets gemotiveerd moet worden aangegeven wat het doel is van de verwerving en waarom deze noodzakelijk is. De motivering moet tevens een afweging bevatten tussen het belang voor de nationale veiligheid en de privacybelangen van de betrokkenen (proportionaliteit) en aangeven waarom de diensten de informatie niet met een lichter middel kunnen verwerven (subsidiariteit).

De diensten hebben op eigen initiatief additioneel intern beleid opgesteld omtrent het verwerven van op internet aangeboden datasets. In de beleidsnotities maken de diensten terecht onderscheid tussen op internet aangeboden datasets *zonder persoonsgegevens* en datasets *met persoonsgegevens*. Voor de verwerving van datasets met persoonsgegevens gelden strengere voorwaarden en waarborgen, vanwege de meer ernstige privacy-inmenging die daarbij kan plaatsvinden.

Op grond van de beleidsnotities moet voor het verwerven van datasets *zonder persoonsgegevens* het (plaatsvervangend) unithoofd van de JSCU toestemming geven. Voor het verwerven van een dataset *met persoonsgegevens* is toestemming van de directeur-generaal van de AIVD of de directeur van de MIVD of hun plaatsvervangers noodzakelijk. In het geval de aard van de gegevens of de mate van inbreuk op de privacy een toestemming op hoger niveau noodzakelijk maakt, wordt de aanvraag ook nog aan de minister voorgelegd.

3.2 Beoordeling verwerving datasets zonder persoonsgegevens

De diensten hebben in de onderzoeksperiode twee bulkdatasets zonder persoonsgegevens verworven. Deze datasets bevatten slechts technische informatie. De toestemming voor het verwerven van deze datasets is gegeven door het plaatsvervangend unithoofd van de JSCU.

Voor de verwerving zijn twee afzonderlijke verzoeken om toestemming opgesteld die grote overeenkomsten vertonen. Beide datasets werden op een openbare website aangeboden en waren eenvoudig te downloaden. Deze datasets zijn daarmee terecht als publiek beschikbare gegevens uit open bron beschouwd.

De verzoeken om toestemming bevatten een korte motivering. De diensten schetsen daarin kort de achtergrond van de gegevens, het doel waarvoor zij worden verworven en voor welke afdelingen binnen de diensten de informatie (mogelijk) relevant is. Ook wordt in de motivering een belangenafweging met betrekking tot de proportionaliteit en de subsidiariteit gemaakt. Deze motivering was toereikend. De verwerving van deze twee bulkdatasets wordt dan ook *rechtmatig* beoordeeld.

3.3 Boordeling verwerving datasets met persoonsgegevens

Tijdens de onderzoeksperiode hebben de AIVD en MIVD twee door derden op internet aangeboden datasets met persoonsgegevens verworven. Deze datasets bevatten beide gegevens van meer dan honderd miljoen personen. De overgrote meerderheid van deze personen hebben geen aanleiding gegeven in de aandacht van de diensten te staan en zullen dat ook nooit staan. De datasets bevatten daarmee hoofdzakelijk informatie die niet relevant is voor de goede taakuitvoering van de diensten. Daarbij zijn de gegevens niet door de betrokkenen zelf publiekelijk geopenbaard en zullen zij dat, gegeven de vertrouwelijkheid van deze gegevens, ook niet snel doen. Deze omstandigheden leiden tot

de conclusie dat de verwerving van deze bulkdatasets een meer ernstige privacy-inmenging oplevert.[3] De privacy-inmenging is door de diensten onderkend en de aanleiding geweest in de beleidsnoties een aanvullend toestemmingsvereiste op te nemen. Ten tijde van de verwerving van de datasets was dit beleid nog niet vastgesteld.

De twee datasets zijn op dezelfde manier verworven. In beide gevallen lazen medewerkers van de JSCU op een nieuwssite dat de datasets werden aangeboden. Omdat het voor mogelijk werd gehouden dat de gegevens slechts voor beperkte tijd op internet beschikbaar zouden blijven, is direct gehandeld. De medewerkers hebben de datasets bij een aanbieder op een illegale internetmarktplaats op het dark web aangekocht. Daarbij was het noodzakelijk onder een valse naam via een berichtensysteem met de aanbieder van de dataset te communiceren over onder meer de wijze van betaling en ontvangst van de gegevens. De gegevens zijn daarmee niet meer te kwalificeren als afkomstig uit een open bron, omdat sprake is geweest van meer dan alleen registratie of betaling, namelijk interactie met de aanbieder.

De interactie met de aanbieder was kortstondig en paste binnen de gebruikelijke werkzaamheden van de desbetreffende medewerkers van de diensten. De communicatie was beperkt tot hetgeen strikt noodzakelijk was om de datasets te kunnen afnemen. Aangezien de aanbieder al in het bezit was van de dataset en vanuit de diensten geen sturing gericht op het verzamelen van de gegevens heeft plaatsgevonden, kon de aanbieder als informant worden aangemerkt.

De diensten hebben de twee datasets aangemerkt als 'publiek toegankelijke gegevens' (open bron). De aanbieders van de dataset hadden op basis van artikel 17 van de Wiv 2002 echter als informant moeten worden aangemerkt. Dit betekent dat een onjuiste grondslag is toegepast. Dit leidt op zichzelf nog niet tot een onrechtmatigheid, omdat de wettelijke vereisten voor beide grondslagen in dit geval gelijk zijn. De CTIVD stelt wel vast dat bij de medewerkers van de JSCU onduidelijkheid bestaat over de grenzen van het verzamelen van gegevens uit open bron en de toepassing van de informanten- en agentregeling. Aanbevolen wordt daartoe personele en organisatorische maatregelen te treffen. Dergelijke maatregelen zijn onderdeel van een proces van zorgvuldige gegevensverwerking en passen ook binnen de in de Wiv 2017 opgenomen zorgplicht voor de kwaliteit van de gegevensverwerking.

De rechtmatigheid van het verwerven van de afzonderlijke bulkdatasets wordt in de twee hiernavolgende subparagrafen beoordeeld.

3.3.1 De eerste dataset met persoonsgegevens

Vanwege de aard en zeer grote hoeveelheid van de gegevens is voor de eerste dataset aan de minister van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) telefonisch toestemming gevraagd en verkregen voordat tot verwerving is overgegaan. Daarbij is de voorwaarde gesteld dat de dataset pas mocht worden gebruikt wanneer daarvoor schriftelijk toestemming van de directeur-generaal van de AIVD was verkregen. Later is dit mondeling akkoord van de minister met een schriftelijke toestemming van de directeur-generaal geformaliseerd. In de motivering is niet expliciet gemaakt op welke grondslag de verwerving van de datasets heeft plaatsgevonden. De MIVD is niet in dit proces betrokken.

Het verzoek om toestemming aan de directeur-generaal van de AIVD beschrijft duidelijk de doelen waarvoor de gegevens zijn verworven. Zo wordt voldoende duidelijk gemaakt dat de informatie onder meer kan bijdragen aan het identificeren van targets gerelateerd aan een specifieke, voor de dienst belangrijke onderzoeksopdracht. De dataset bevat ook wachtwoorden. Om deze reden kunnen de gegevens ook worden aangewend bij de inzet van de hackbevoegdheid.

---

[3] Zie ook hoofdstuk 1 van het toetsingskader (Bijlage 1).

De schriftelijke motivering maakt duidelijk dat de dataset persoonsgegevens bevat van een zeer groot aantal personen dat geen onderwerp van onderzoek is. Van deze personen is naar inschatting slechts een zeer beperkt aantal Nederlands ingezetenen. De AIVD heeft overtuigend gemotiveerd dat het verwerven van de eerste dataset noodzakelijk was. In de motivering wordt aangegeven in welke inlichtingenbehoefte de verwerving voorziet en waarom het belang voor de nationale veiligheid zwaarder dient te wegen dan de privacybelangen van de betrokkenen.

In dit kader moet worden benadrukt dat het hier gaat om bulkdatasets die door een ieder – al dan niet na communicatie met de aanbieder – kunnen worden vergaard. De gegevens in de datasets zijn reeds 'gestolen' of gelekt bij een organisatie en publiekelijk aan een ieder aangeboden. In deze zin heeft zich al een privacy-inmenging bij de betrokkenen voorgedaan. Bovendien ging het hier om een dataset die door middel van een aankoop kon worden vergaard. Dit moet minder vergaand worden geacht dan het zelf verwerven van de gegevens door middel van een eigen inbreuk op de systemen, zoals een hack. Al met al is de verwerving van deze bulkdataset proportioneel en subsidiair.

De conclusie is dan ook dat de (schriftelijke) motivering voor de verwerving van deze dataset voldoet. Bovendien is voorafgaand aan de verwerving op het hoogst mogelijke niveau toestemming gevraagd en gegeven. Daarmee hebben de diensten laten zien dat zij – geconfronteerd met een nieuwe situatie waarin zij snel moesten handelen – zich bewust waren van de gevoelige aard van de informatie en de meer ernstige privacy-inmenging die met de verwerving gepaard ging. De verwerving van de eerste dataset wordt dan ook als *rechtmatig* beoordeeld.

3.3.2 De tweede dataset met persoonsgegevens

Voor de verwerving van de tweede dataset heeft de verwervende JSCU medewerker overleg gehad met zijn leidinggevende en een aantal medewerkers van een ander intern bureau. Ten tijde van de verwerving is niet formeel om toestemming gevraagd. Met het een aantal maanden later vaststellen van de beleidsnotitie zijn de directeur-generaal van de AIVD en de directeur van de MIVD achteraf alsnog akkoord gegaan met de verwerving en het gebruik van de dataset. In het opgestelde beleid zelf werd de verwerving en verdere verwerking van deze dataset expliciet gemotiveerd. Het beleid vormt in dit geval aldus tegelijkertijd de toestemming voor de verwerving en het gebruik van de tweede dataset.

De verwerving van de tweede dataset wordt als *onrechtmatig* beoordeeld. De reden daarvoor is dat de minister(s), bij het vaststellen van de interne beleidsnotities, niet alsnog om toestemming is gevraagd. Dit had wel gemoeten, omdat de gegevens in de bulkdataset zeer algemeen van aard zijn. De dataset bevat gegevens van meer dan honderd miljoen personen, van wie relatief veel Nederlands ingezetenen. De verwerving van een zodanige hoeveelheid persoonsgegevens brengt een ernstige privacy-inmenging met zich mee. Het door de diensten (later) zelf opgestelde beleid schrijft voor dat in dit soort bijzondere gevallen toestemming aan de minister(s) had moeten worden gevraagd.

De schriftelijke motivering omtrent de verwerving van de dataset bevat tekortkomingen, omdat niet expliciet wordt gemaakt op welke grondslag de verwerving van de dataset heeft plaatsgevonden. Evenmin wordt aangegeven op basis van welke inlichtingenbehoefte de verwerving van de dataset noodzakelijk is. Daarnaast blijkt onvoldoende dat de dataset zeer grote hoeveelheden persoonsgegevens bevat van personen die geen onderwerp van onderzoek zijn. De motivering geeft wel aan dat de gegevens onder meer zullen worden gebruikt ter (nadere) identificatie van targets. In aanvullende gesprekken met medewerkers in het kader van het onderzoek is de CTIVD overtuigd geraakt van de

noodzaak, proportionaliteit en subsidiariteit van de verwerving van de dataset ten behoeve van de door de diensten schriftelijk geformuleerde doeleinden.[4]

3.4 Tussenconclusie

De op internet verworven bulkdatasets zonder persoonsgegevens zijn op *rechtmatige* wijze op basis van de algemene bevoegdheid voor het verzamelen van gegevens uit open bron verworven.

Bij de verwerving van de twee op internet verworven bulkdatasets met persoonsgegevens zijn de aanbieders ten onrechte niet als informant aangemerkt. In één geval had op een hoger niveau toestemming moeten worden gevraagd. De CTIVD beoordeelt de verwerving van deze dataset als *onrechtmatig*.

De bevindingen in dit hoofdstuk brengen met zich dat het beleid van de diensten omtrent de verwerving van door derden op internet aangeboden bulkdatasets moet worden aangepast. De Wiv 2017 vormt hier eveneens aanleiding voor. De CTIVD beveelt aan in het interne beleid op te nemen dat per individuele dataset een expliciete keuze voor een wettelijk grondslag dient te worden gemaakt. Daarnaast moet de verwerving van een bulkdataset voldoende worden gemotiveerd. In paragraaf 3.4 van Bijlage 1 worden daartoe handreikingen gedaan.

[4] Hierbij gelden dezelfde overwegingen omtrent de subsidiariteit als bij de eerste dataset.

4 Beoordeling verdere verwerking van de datasets

In dit hoofdstuk beoordeelt de CTIVD de verdere verwerking van door derden de op internet aangeboden bulkdatasets. Het toetsingskader is uitvoerig uiteengezet in hoofdstuk van 2 van bijlage 1 bij dit rapport. In paragraaf 4.1 wordt het toetsingskader samengevat. Daarna worden de ontsluiting van de datasets zonder persoonsgegevens (paragraaf 4.2) en de datasets met persoonsgegevens beoordeeld (paragraaf 4.3). In paragraaf 4.4 wordt ingegaan op de naslagenprocedure en in paragraaf 4.5 wordt beoordeeld of de naslagen rechtmatig zijn. De beoordeling op rechtmatigheid vindt in dit hoofdstuk uitsluitend plaats op basis van de relevante bepalingen uit de Wiv 2002.

4.1 Toetsingskader

Een privacy-inmenging dient een voor het publiek toegankelijke (kenbare en beschikbare) wettelijke basis te hebben. Bovendien moet de kwaliteit van deze wet zodanig zijn dat deze waarborgen tegen misbruik biedt. Hoe ernstiger de privacy-inmenging is, hoe meer gedetailleerde wetgeving met procedurele waarborgen is vereist.

De wet stelt enkele belangrijke voorwaarden aan de verwerking van gegevens. De verwerking van gegevens mag slechts plaatsvinden voor een bepaald doel en slechts voor zover dat noodzakelijk is voor de goede taakuitvoering van de diensten. De verwerking van gegevens moet bovendien op een behoorlijke en zorgvuldige wijze plaatsvinden met een verwijzing naar de betrouwbaarheid van de gegevens of de bron waaraan de gegevens zijn ontleend.

Tevens moeten voorzieningen worden getroffen ter bevordering van de juistheid en volledigheid van de gegevens die worden verwerkt. Medewerkers van de diensten mogen slechts toegang krijgen tot de gegevens voor zover dat noodzakelijk is voor de hun opgedragen taken (need-to-know). Indien een gegevensset hoofdzakelijk persoonsgegevens bevat van personen die niet in de aandacht van de dienst staan, dienen daaraan tevens de nadere voorwaarden van functie- en/of taakscheiding te worden verbonden. Daarnaast dient in dat geval een bewaartermijn te worden vastgesteld, bij afloop waarvan de bulkdataset moet worden vernietigd.

Met de invoering van de Wiv 2017 wordt tevens de *zorgplicht* voor de kwaliteit van de gegevensverwerking van kracht. Deze zorgplicht houdt in dat de hoofden van de diensten zorg moeten dragen voor de technische, personele en organisatorische maatregelen ter bevordering van de kwaliteit van de gegevensverwerking. Daaronder worden ook de daarbij gehanteerde algoritmen en modellen begrepen.

Ten slotte stelt de wet verplichtingen omtrent de verwijdering en vernietiging van gegevens. Gegevens die hun betekenis hebben verloren moeten worden verwijderd en vernietigd, tenzij wettelijke regels omtrent bewaring daaraan aan de weg staan. Onder de Wiv 2017 is in aanvullende zin nieuw dat bij gegevens die op basis van een bijzondere bevoegdheid worden verworven, zoals de agentregeling, een relevantietoets moet worden uitgevoerd. Deze toets houdt in dat zo spoedig mogelijk, en in ieder geval binnen een jaar, moet worden onderzocht of de gegevens relevant zijn voor enig onderzoek van de diensten. Gegevens die niet-relevant worden bevonden of gegevens die niet binnen de bewaartermijn worden beoordeeld, moeten terstond worden vernietigd.[5]

[5] Zie artikel 27 Wiv 2017. De bewaartermijn kan eenmalig met een half jaar worden verlengd. Deze bepaling is niet van toepassing op de onderzoeksopdrachtgerichte interceptie van artikel 48 van de Wiv 2017.

4.2 Beoordeling ontsluiting datasets zonder persoonsgegevens

De datasets *zonder* persoonsgegevens zijn in hun geheel – dus zonder toepassing van een buitenbak-binnenbakprocedure – aan de relevante organisatieonderdelen van beide diensten beschikbaar gesteld. De diensten zijn verplicht deze gegevens te vernietigen als deze hun betekenis hebben verloren.

De verdere verwerking van de gegevens in deze datasets, zoals het raadplegen en analyseren van de gegevens, houdt geen privacy-inmenging in. De CTIVD heeft vastgesteld dat deze gegevens noodzakelijk zijn voor het doel waarvoor de desbetreffende teams de gegevens gebruiken. De gegevens hebben hun betekenis nog niet verloren. Het geheel toegankelijk maken van deze datasets zonder persoonsgegevens is daarom *rechtmatig*.

4.3 Beoordeling ontsluiting datasets met persoonsgegevens

In hun beleidsnotities schrijven de AIVD en de MIVD voor dat bij de verdere verwerking van de bulkdatasets met persoonsgegevens de buitenbak-binnenbakprocedure moet worden toegepast (zie paragraaf 2.2). Dit is bij de onderzochte bulkdatasets met persoonsgegevens ook gebeurd.

De noodzakelijkheidstoets brengt met zich dat niet meer gegevens worden verwerkt dan noodzakelijk. Dit vereiste wordt ook wel dataminimalisatie genoemd en is ook van toepassing op gegevens in de buitenbak. In het geval van de datasets betekent dit dat kritisch moet worden gekeken of alle typen gegevens noodzakelijk zijn om de in de motivering aangegeven doelen te bereiken. Is het doel identificatie dan is het begrijpelijk dat bijvoorbeeld namen en telefoonnummers in de buitenbak worden bewaard. Voor bijzondere persoonsgegevens als seksuele oriëntatie of gegevens over persoonlijke interesses ligt dit dan niet voor de hand. Gegevens die niet onder de doelomschrijving vallen moeten worden vernietigd. De in dit onderzoek betrokken bulkdatasets met persoonsgegevens bevatten geen gegevens die in dit kader niet hadden mogen worden bewaard. De CTIVD beveelt wel aan dit vereiste als toets in de beleidsnotities op te nemen.

In de beleidsnotities is aangegeven dat voor de bulkdatasets met persoonsgegevens een bovenwettelijke bewaartermijn van drie jaar geldt. Dit betekent dat de persoonsgegevens in de buitenbak na uiterlijk drie jaar na de verwerving worden vernietigd. Gelet op de relatief beperkte risico's die aan het opslaan van deze gegevens zijn verbonden en het doel dat met de verwerking wordt beoogd, te weten (toekomstige) identificatie, zijn er geen redenen voor een kortere bewaartermijn.[6]

Wel strekt het tot de aanbeveling binnen de bewaartermijn periodiek na te gaan of de bulkdatasets nog steeds noodzakelijk zijn voor het doel waarvoor zij zijn verworven. Als dit niet het geval is, moeten deze worden vernietigd. Te denken valt aan het jaarlijks evalueren van de hits en resultaten die de bulkdataset in operationele onderzoeken opleveren. De diensten zouden bijvoorbeeld op basis van loggegevens geautomatiseerd kunnen nagaan of een informatiebron, zoals een dataset, nog van betekenis is voor het inlichtingenproces. Een dergelijke technische maatregel is onderdeel van een proces van zorgvuldige gegevensverwerking en past binnen de in de Wiv 2017 de opgenomen zorgplicht voor de kwaliteit van de gegevensverwerking.

Met het plaatsen van de gegevens in de buitenbak en het hanteren van een bewaartermijn, wordt privacybescherming geboden. De gegevens zijn immers niet direct voor de operationele teams beschikbaar en worden na een bepaalde termijn vernietigd. Op deze manier zorgen de diensten

[6] Zie daarvoor ook Bijlage 1, paragraaf 3.4.

ervoor dat de gegevens slechts worden verwerkt voor zover dat noodzakelijk is. Dit maakt dat het op deze wijze verwerken van de gegevens in de buitenbak *rechtmatig* is.

Een kanttekening daarbij is wel dat een deel van de procedurele waarborgen niet publiekelijk toegankelijk is, omdat zij niet in de wet, maar in intern beleid staan beschreven. Om aan de vereisten van kenbaarheid en beschikbaarheid tegemoet te komen, zou (een gerubriceerde versie van) dit interne beleid gepubliceerd moeten worden. De algemene bevoegdheid is echter niet de enige bevoegdheid waarmee gegevens in bulk worden vergaard, terwijl daarvoor in de wet geen nadere waarborgen, zoals functie- en taakscheiding, zijn opgenomen.[7] Voorbeelden daarvan zijn het ongericht overnemen van gegevens door middel van een hack of het vergaren van grote hoeveelheden gegevens via de inzet van een agent.[8]

De CTIVD beveelt daarom aan een algemeen beleidskader voor het in bulk verwerven en verder verwerken van (persoons)gegevens op te stellen en dit te publiceren. Dit beleid zou dan van toepassing moeten zijn op alle bevoegdheden en (toekomstige) situaties waaronder bulkgegevens worden verworven, met uitzondering van de bevoegdheid tot bulkinterceptie. Deze laatste bevoegdheid kent immers wel in de wet opgenomen waarborgen. De vorm en de inhoud van het te publiceren beleid is in beginsel aan de diensten. Wel moet het voldoende gedetailleerd zijn om aan het kenbaarheidsvereiste te voldoen. Uit de publicatie moet dan ook in ieder geval kunnen worden afgeleid dat de buitenbak-binnenbakprocedure wordt toegepast en hoe de procedure voor het verplaatsen van gegevens van de buitenbak naar de binnenbak eruit ziet.

4.4 Beoordeling naslagprocedure

Operationele teams kunnen informatie krijgen waaruit blijkt dat een persoon achter een bepaald kenmerk, zoals een naam of telefoonnummer, betrokken is bij activiteiten waarnaar de diensten onderzoek doen. Ook kan het zijn dat zij meer over een bepaald target te weten willen komen. Op dat moment kijken de operationele medewerkers eerst of een kenmerk al in de binnenbak voorkomt. In de binnenbak staan de eerder relevant beoordeelde gegevens en informatie uit bijvoorbeeld open bronnen, zoals kranten en tijdschriften. Als dat niet het geval is, kan het team besluiten het kenmerk in de buitenbak te laten naslaan. Met een hit/no hit-zoekslag wordt dan achterhaald of informatie aan een bepaald kenmerk kan worden gekoppeld. Na het doorlopen van een toestemmingsprocedure waarin gemotiveerd om toestemming wordt verzocht, worden deze gegevens als het ware van de buitenbak naar de binnenbak verplaatst en beschikbaar gemaakt voor de geautoriseerde medewerkers van alle operationele teams.[9]

De naar de binnenbak verplaatste gegevens worden uiteindelijk door het operationele team dat de naslag heeft aangevraagd op relevantie beoordeeld. Uiteraard zijn niet alle gegevens als resultaat van de naslagprocedure relevant voor het onderzoek. Het kan zijn dat (delen van) kenmerken, zoals een naam of telefoonnummer, ook door andere personen worden gebruikt.

---

7 Bulkverwerving kent alleen voor de ongerichte interceptie (Wiv 2002) en de onderzoeksopdrachtgerichte interceptie (Wiv 2017) in de wet verankerde waarborgen.

8 Zie daarvoor: Toezichtsrapport nr. 53 over de inzet van de hackbevoegdheid door de AIVD en de MIVD, p. 28.

9 Zie ook paragraaf 2.2.

De AIVD en de MIVD hebben, als onderdeel van een zorgvuldige gegevensverwerking, de plicht de als niet-relevant beoordeelde gegevens uit de binnenbak te verwijderen. De gegevens worden daarbij als het ware weer terug in de buitenbak geplaatst. Dit dient naar het oordeel van de CTIVD, als aanbeveling, eveneens te gelden voor naar de binnenbak verplaatste gegevens, die na een bovenwettelijke termijn van drie maanden niet zijn beoordeeld. Het gevolg hiervan is dat gegevens niet meer voor de geautoriseerde medewerkers van alle operationele teams toegankelijk zijn.

De gedachte achter deze verplichtingen is dat voorkomen moet worden dat gegevens van personen die niet in de aandacht van de diensten staan voor een lange duur – ook na vernietiging van de bulkdatasets vanwege het verlopen van de bewaartermijn in de buitenbak – in de binnenbak beschikbaar blijven. Aanbevolen wordt deze verplichtingen in de beleidsnotities op te nemen en daaraan geautomatiseerd uitvoering te geven.

In het kader van een zorgvuldige gegevensverwerking past ook dat het verplaatsen, verwijderen en vernietigen van gegevens moet worden vastgelegd. Dit moet gebeuren op een manier waarbij herleidbaar is op grond van welke verzoeken en handelingen deze gegevensverwerkingen hebben plaatsgevonden. Tevens moet deze vastlegging interne controle, bijvoorbeeld in het kader van de zorgplicht voor de kwaliteit van de gegevensverwerking onder de Wiv 2017, en extern toezicht door de CTIVD mogelijk maken. De CTIVD beveelt aan dit door middel van logging en het aan de hand daarvan geautomatiseerd opstellen van rapportages uit te voeren.

4.5 Beoordeling naslagen

In het onderzoek zijn alle aanvragen tot naslag beoordeeld die in de twee bulkdatasets met persoonsgegevens een resultaat opleverden. Daarmee zijn dus alle gevallen onderzocht, waarin persoonsgegevens uit de bulkdatasets van de buitenbak naar de binnenbak zijn verplaatst. Uit het onderzoek is gebleken dat alle aanvragen tot een naslag noodzakelijk, proportioneel en subsidiair zijn geweest en dat de toestemming daarvoor op het juiste niveau is gegeven. Alle onderzochte aanvragen tot naslag zijn daarmee *rechtmatig*.

In vier gevallen was bij de AIVD sprake van een aanvraag met een groot aantal (honderden) kenmerken, behorend bij een groot aantal targets. Het doel van de aanvraag was om de targets te identificeren en netwerken rond deze targets inzichtelijk te maken. Daarbij was het niet direct duidelijk welke kenmerken bij welke targets behoorden en uit welke bronnen deze kenmerken afkomstig waren. Dit heeft de CTIVD met nader onderzoek alsnog kunnen vaststellen. De diensten dienen in het vervolg per groep kenmerken de bron of betrouwbaarheid aan te geven en uit te leggen op welke kenmerken welk deel van de motivering ziet.[10]

Ondanks de uitzonderlijk hoge aantallen kenmerken is de Afdeling Juridische Zaken (hierna: AJZ) niet in alle gevallen geconsulteerd. De CTIVD is van oordeel dat voor aanvragen met een grote hoeveelheid kenmerken advies van AJZ moet worden ingewonnen. Bij een negatief advies dient de toestemming op het niveau van een directeur te worden gegeven.

Daarnaast is uit het onderzoek gebleken dat het naslaan van grote hoeveelheden kenmerken ertoe leidt dat een veelvoud aan gegevens van de buitenbak naar de binnenbak worden verplaatst. Daarvan is een groot deel (naar verwachting) niet relevant voor het onderzoek. Deze bevinding onderstreept het belang van de verplichtingen tot het verwijderen van niet-relevant beoordeelde en na een termijn van drie maanden niet-beoordeelde gegevens uit de binnenbak, zoals in de vorige paragraaf

[10] Zie ter vergelijking ook: Toezichtsrapport nr. 46 inzake de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van sigint door de AIVD, p. 20-21.

is opgemerkt. Het verwijderen en vernietigen van gegevens vormt immers het sluitstuk van een zorgvuldige gegevensverwerking.[11]

4.6 Tussenconclusie

De CTIVD is van oordeel dat de werkwijze met betrekking tot de ontsluiting van de datasets zonder persoonsgegevens *rechtmatig* is. Met het toepassen van de buitenbak-binnenbakprocedure is ook het opslaan en gebruiken van de datasets met persoonsgegevens rechtmatig. Een kanttekening daarbij is wel dat een deel van de procedurele waarborgen niet publiekelijk toegankelijk is. De diensten worden aanbevolen een algemeen beleidskader voor het in bulk verwerven en verder verwerken van (persoons)gegevens op te stellen en dit te publiceren. Dit beleid biedt ook houvast voor toekomstige situaties waarbij, al dan niet op basis van andere bevoegdheden, bulkpersoonsgegevens worden verworven en verwerkt.

Tevens wordt op grond van het vereiste van dataminimalisatie aanbevolen in de beleidsnotities op te nemen dat gegevens die niet noodzakelijk zijn voor het beoogde doel direct na de verwerving uit de buitenbak worden vernietigd. Ook moet in dat kader periodiek worden getoetst of het binnen de gestelde bewaartermijn noodzakelijk is de bulkdatasets langer in de buitenbak te bewaren. Daarnaast moeten niet-relevant beoordeelde en na drie maanden niet-beoordeelde gegevens uit de binnenbak worden verwijderd door deze terug te plaatsen in de buitenbak.

Alle onderzochte aanvragen tot naslag waren voldoende gemotiveerd en noodzakelijk, proportioneel en subsidiair. Dit maakt de gevolgde naslagprocedure *rechtmatig*. De CTIVD beveelt aan aanvragen tot naslagen met een grote hoeveelheid kenmerken per groep kenmerken te motiveren en ter advies aan de Afdeling Juridische Zaken voor te leggen. Bij een negatief advies dient de toestemming op het niveau van een directeur te worden belegd.

[11] Zie artikel 12, 16 en 18 Wiv 2002. Zie ook de zorgplicht in artikel 24 Wiv 2017. De zorgplicht houdt in dat de hoofden van de diensten zorg moeten dragen voor de technische, personele en organisatorische maatregelen ter bevordering van de kwaliteit van de gegevensverwerking.

5 Conclusies

In dit rapport is nagegaan in hoeverre het handelen van de AIVD en de MIVD aangaande de verwerving (hoofdstukken 2 en 3) en verdere verwerking (hoofdstukken 2 en 4) van door derden op internet aangeboden bulkdatasets rechtmatig is geweest. In dit hoofdstuk worden de bevindingen kort weergegeven. De conclusies die in dit hoofdstuk op basis van de Wiv 2002 worden getrokken, blijven onder toepassing van de Wiv 2017 gehandhaafd.

5.1 Conclusies met betrekking tot het verwerven van de bulkdatasets

De twee door derden op internet aangeboden bulkdatasets *zonder* persoonsgegevens zijn op rechtmatige wijze verworven op basis van de algemene bevoegdheid voor het verzamelen van gegevens uit een ieder toegankelijk informatiebron (open bron). De verwerving van deze gegevens brengt geen inmenging met het recht op privacy met zich mee en is telkens voldoende gemotiveerd. Ook is op het juiste niveau toestemming verkregen.

De twee door derden op internet aangeboden bulkdatasets, die elk meer de persoonsgegevens bevatten van meer dan honderd miljoen personen, zijn ten onrechte als afkomstig uit open bron aangemerkt. De aanbieders van de dataset hadden als informant moeten worden aangemerkt. Dit betekent dat een onjuiste juridische grondslag is toegepast. Dit leidt niet tot een onrechtmatigheid, omdat de wettelijke vereisten en waarborgen voor beide grondslagen in dit geval gelijk zijn.

De verwerving van de eerste bulkdataset met persoonsgegevens is als *rechtmatig* beoordeeld. De AIVD heeft op het niveau van de minister van BZK toestemming verkregen voor de verwerving van deze dataset. Van de gegevens heeft naar inschatting slechts een zeer beperkt deel betrekking op Nederlands ingezetenen. Het verzoek om toestemming is goed gemotiveerd en de verwerving voldoet aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit.

De verwerving van de tweede bulkdataset met persoonsgegevens is als *onrechtmatig* beoordeeld. Op grond van het interne beleid, dat is vastgesteld na de verwerving van de datasets, was voor deze dataset toestemming op het niveau van minister op zijn plaats. De dataset bevat de persoonsgegevens van meer dan honderd miljoen personen, waarvan relatief veel van Nederlands ingezetenen, die niet in de aandacht van de diensten staan. De directeur-generaal van de AIVD en de directeur van de MIVD hebben in dit geval (achteraf, dat wil zeggen: met de vaststelling van het interne beleid) toestemming gegeven voor de verwerving van de dataset. Het verzoek om toestemming was daarbij niet voldoende gemotiveerd. Op basis van eigen onderzoek is de CTIVD overigens tot de conclusie gekomen dat de verwerving van de bulkdataset wel aan de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit voldeed.

5.2 Conclusies met betrekking tot het verder verwerken van de bulkdatasets

De gegevens in de op internet aangeboden bulkdatasets *zonder* persoonsgegevens zijn in hun geheel aan de relevante organisatieonderdelen binnen de AIVD en de MIVD ter beschikking gesteld. Deze verdere verwerking van de gegevens in de bulkdatasets, houdt geen privacy-inmenging in en heeft op een zorgvuldige wijze plaatsgevonden. Deze werkwijze wordt daarom als *rechtmatig* beoordeeld.

De gegevens in de door derden op internet aangeboden bulkdatasets *met* persoonsgegevens zijn niet aan relevante operationele teams binnen de AIVD en de MIVD ter beschikking gesteld, maar zijn eerst in de zogenoemde buitenbak gezet. Daardoor kunnen de operationele teams daar niet zonder meer bij. De buitenbak is alleen toegankelijk voor een klein aantal technische beheerders en een deel van de data-analisten. De bulkdatasets met persoonsgegevens in de buitenbak worden drie jaar bewaard, waarna zij op basis van bovenwettelijk beleid moeten worden vernietigd.

Als een medewerker van een operationeel team kennis wil nemen van de gegevens in de buitenbak, moet een zogenoemde naslagprocedure worden doorlopen. In een aanvraag moet het operationeel team gemotiveerd aangeven waarom zij bepaalde kenmerken, zoals een naam of een e-mailadres, willen laten naslaan in de buitenbak. Deze aanvraag moet bij de AIVD door het desbetreffende teamhoofd worden goedgekeurd. Bij de MIVD is daarvoor – na goedkeuring van onder andere de Stafafdeling Juridische Zaken – toestemming van de directeur noodzakelijk. Daarna maakt de JSCU de resultaten van de naslag voor het operationele team beschikbaar. Dit kan worden gezien als het verplaatsen van de gegevens van de buitenbak naar de binnenbak. Het verplaatsen van gegevens naar de binnenbak maakt dat deze voor een groot aantal operationele medewerkers, ook van andere dan het verzoekende team, rechtstreeks raadpleegbaar worden.

Het toepassen van de buitenbak-binnenbakprocedure met zijn functie- en taakscheiding gericht op het need-to-knowbeginsel en het hanteren van een (bovenwettelijke) bewaartermijn vormen tezamen een toepassing van een zorgvuldige gegevensverwerking. De CTIVD beoordeelt het verder verwerken van de bulkdatasets met persoonsgegevens daarom als *rechtmatig*.

5.3 Vervolgonderzoek

Dit onderzoek toont aan dat door de beide diensten op basis van de algemene bevoegdheid zeer grote hoeveelheden gegevens *kunnen* en *worden* vergaard. Dit vormt dan ook aanleiding in de nabije toekomst verder onderzoek te doen naar de activiteiten van de diensten op dit gebied. De inzet van de algemene bevoegdheid is immers doorgaans met minder waarborgen omkleed dan de inzet van bijzondere bevoegdheden.

Daarnaast is in dit onderzoek een aantal technische processen beoordeeld. Eerst bij navraag bleek dat de voor dit onderzoek noodzakelijke logging beschikbaar was. De logging wordt nog niet met het oogmerk van interne controle en extern toezicht gebruikt. In het kader van de Wiv 2017 zal de CTIVD haar toezicht meer op deze technische processen richten en daarin nagaan of de zorgplicht met betrekking tot de kwaliteit van de gegevensverwerking voldoende wordt nagekomen.

6 Aanbevelingen

In dit rapport is nagegaan in hoeverre het handelen van de AIVD en de MIVD aangaande de verwerving (hoofdstuk 3) en verdere verwerking (hoofdstuk 4) van door derden op internet aangeboden bulkdatasets rechtmatig is geweest. De resultaten van de bevindingen in deze hoofdstukken leiden tot de hiernavolgende aanbevelingen.

De wettelijke grondslag (Hoofdstuk 3)

1. Pas het interne beleid op een zodanige manier aan dat duidelijk wordt wanneer welke juridische grondslag (open bron, informant of agent) bij de verwerving van door derden op internet aangeboden bulkdatasets van toepassing is (paragraaf 3.4).

2. Vul de vereisten die aan de motivering voor de individuele verwerving van een bulkdataset moeten worden gesteld in het interne beleid aan. De noodzakelijke elementen die de motivering moet bevatten, zijn (1) een schriftelijke motivering, (2) het doel, (3) de noodzaak en (4) de belangafweging. In paragraaf 3.4 van het toetsingskader (Bijlage 1) worden deze elementen verder uitgewerkt (paragraaf 3.3).

3. Stel de medewerkers van de JSCU beter van voornoemde juridische grondslagen en de inhoud van het intern beleid in kennis (paragraaf 3.4).

De buitenbak-binnenbakprocedure (Hoofdstuk 4)

4. Stel een algemeen beleidskader op voor het in bulk verwerven en verder verwerken van persoonsgegevens en publiceer dit (paragraaf 4.3).

5. Verwijder, als onderdeel van een bovenwettelijk beleid, gegevens die als niet-relevant of na drie maanden nog niet zijn beoordeeld uit de binnenbak. Verplaats deze gegevens als het ware weer terug naar de buitenbak. Aanbevolen wordt deze verplichtingen in de beleidsnotities op te nemen en daaraan (geautomatiseerd) uitvoering te geven (paragraaf 4.4).

6. Motiveer aanvragen tot naslagen met een grote hoeveelheid kenmerken per groep kenmerken en leg deze aanvraag ter advies aan de Afdeling Juridische Zaken. Bij een negatief advies dient de toestemming op het niveau van een directeur te worden belegd (paragraaf 4.5).

7. Leg het verplaatsen, verwijderen en vernietigen van gegevens vast. De herleidbaarheid van de gegevensverwerkingen en het aan de hand van logging geautomatiseerd opstellen van interne rapportages (compliance) maken daar onderdeel van uit.

Dataminimalisatie (Hoofdstuk 4)

8. Beoordeel in het kader van dataminimalisatie direct na verwerving of alle (typen) gegevens in de bulkdataset daadwerkelijk noodzakelijk zijn om de in de motivering aangegeven doelen te bereiken, en neem dit als vereiste in het interne beleid op. Gegevens die niet noodzakelijk zijn voor het doel waarvoor zij worden verwerkt, moeten terstond uit de buitenbak worden vernietigd (paragraaf 4.3).

9. Neem in het kader van dataminimalisatie in het interne beleid op dat binnen de bewaartermijn van drie jaar periodiek wordt nagegaan of een bulkdataset nog steeds noodzakelijk is voor het doel waarvoor deze is verworven. Als dit niet het geval is, moet deze tussentijds worden vernietigd. Een mogelijkheid hiervoor zou zijn de hits *en* resultaten die de bulkdataset in operationele onderzoeken opleveren jaarlijks te evalueren. De diensten zouden bijvoorbeeld ook op basis van loggegevens geautomatiseerd kunnen nagaan of een informatiebron, zoals een dataset, nog van betekenis is voor het inlichtingenproces (paragraaf 4.3).

Tijdelijk adres:
Frederikkazerne, gebouw 35
Van Alkemadelaan 786 | 2597 Den Haag
Postbus 90701 | 2509 LS Den Haag

T 070 315 58 20 | **F** 070 381 71 68
E info@ctivd.nl | www.ctivd.nl