Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Vastgesteld

Toezichtrapport

over verwerking van bulkdatasets door de AIVD en MIVD

CTIVD nr. 84
Vastgesteld op 11-06-2026

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

CTIVD nr. XX

TOEZICHTRAPPORT

Over de naleving van wettelijke regels bij de verwerking van bulkdata door de AIVD en de MIVD

Inhoudsopgave

Inhoudsopgave 1

1 Hoofdboodschap 3

2 Inleiding 5

2.1 De verwerking van bulkdatasets door de AIVD en de MIVD 5

2.2 Aanleiding voor het onderzoek van de CTIVD 7

2.3 Scope van het rapport 8

2.4 Beoordelingskader 9

2.5 Leeswijzer - De levenscyclus van bulkdatasets 10

2.6 Toelichting op de gebruikte onderzoeksmethodes 13

3 Het technisch voortraject 14

3.1 Inleiding en wettelijke criteria 14

3.2 Beoordeling van het technisch voortraject 16

3.2.1 Het bepalen of sprake is van een bulkdataset 16

3.2.2 Datareductie vooraf 18

3.2.3 Technische ontsluiting van de bulkdataset op de systemen 19

4 Bepalen van het toegangsregime 21

4.1 Inleiding en wettelijke criteria 21

4.2 Beoordeling van het proces omtrent de bepaling van het toegangsregime 23

4.2.1 Het beoordelen van de inbreuk op de privacy 23

4.2.2 Het vaststellen van toegangsregimes en melding daarvan aan de CTIVD 26

5 Toegangsmanagement bij bulkdatasets 26

5.1 Inleiding en wettelijke criteria 27

5.2 Beoordeling van toegangsmanagement bij bulkdatasets 29

5.2.1 Toegangsmanagement bij bulkdatasets met een standaard toegangsregime 29

5.2.2 Toegangsmanagement bij bulkdatasets met een beperkt en strikt beperkt toegangsregime 30

5.2.3 Logging van toegang en gebruik van gegevens 31

6 Gebruik van bulkdatasets 33

6.1 Inleiding en wettelijke criteria 33
6.2 Beoordeling van het gebruiken van bulkdatasets 35
6.2.1 Gebruik van bulkdatasets bij de uitvoering van wettelijke taken 35
6.2.2 Gebruik van bulkdatasets ter ondersteuning van de uitvoering van wettelijke taken 37
7 Beoordeling noodzaak tot verwijdering en nieuwe gebruikstermijnen 39
7.1 Inleiding en wettelijke criteria 39
7.1.1 Wettelijk regels bij A-bulkdatasets 40
7.1.2 Wettelijk regels bij B-bulkdatasets 40
7.2 Beoordeling van de processen omtrent periodieke beoordelingen en nieuwe gebruikstermijnen 42
7.2.1 Periodieke beoordeling van de noodzaak tot verwijdering (bij A-bulkdatasets) 42
7.2.2 Nieuwe gebruikstermijnen (bij B-bulkdatasets) 43
7.2.3 Procesverloop bij dynamische bulkdatasets (A en B) 44
7.2.4 Overkoepelende bevindingen 44
8 Verwijdering en vernietiging van gegevens 46
8.1 Inleiding en wettelijke criteria 46
8.2 Beoordeling van de verwijdering en vernietiging van gegevens uit bulkdatasets 47
9 Conclusie en overzicht van bevindingen 50
9.1 Conclusie 50
9.2 Overzicht bevindingen en aanbevelingen 52

1 Hoofdboodschap

Hoofdstuk 1 – Hoofdboodschap

In dit rapport concludeert de CTIVD dat een aantal belangrijke waarborgen voor het gebruik van bulkdatasets door de AIVD en de MIVD niet op orde is. Daardoor bestaan verhoogde risico's op onrechtmatigheden en onzorgvuldigheden, die zich in sommige gevallen hebben verwezenlijkt.

Het gebruik van bulkdatasets is belangrijk voor de uitvoering van de wettelijke taken van de diensten. Tegelijkertijd behelst het een aanzienlijke privacyinbreuk voor de personen over wie gegevens voorkomen in deze bulkdatasets. Een bulkdataset is een omvangrijke gegevensverzameling waarbij het merendeel van de gegevens betrekking heeft op organisaties en/of personen die geen onderwerp van onderzoek van een dienst zijn en dat ook niet worden. De AIVD en de MIVD maken op grote schaal en op verschillende plekken in de organisatie gebruik van bulkdatasets.

Opkomende technologische ontwikkelingen op het gebied van *artificial intelligence* en andere vormen van geautomatiseerde data-analyse kunnen niet alleen de effectiviteit van het gebruik van gegevens uit bulkdatasets verder vergroten, maar óók de daarmee gepaard gaande privacyinbreuk. De maatschappij en de politiek moeten erop kunnen vertrouwen dat er goede waarborgen zijn voor het werken met bulkdatasets en de diensten zich aan de geldende regelgeving houden.

De belangrijkste bevindingen uit dit rapport komen enerzijds voort uit technische tekortkomingen in de systemen van de diensten, en anderzijds uit procedurele tekortkomingen in de naleving van beleid en geldende wet- en regelgeving:

- Het gebruik van bulkdatasets is in de loop der jaren behoorlijk toegenomen. De diensten verwerven bulkdatasets via de inzet van meerdere bevoegdheden, waarvoor verschillende regels gelden. Ook wordt op steeds meer plekken binnen de diensten met bulkdatasets gewerkt. Als gevolg daarvan is voor bulkdatasets een versnipperd datalandschap ontstaan, waarop geen centrale regie wordt gevoerd. Hierdoor bestaan verhoogde risico's op onrechtmatigheden en onzorgvuldigheden, die zich in sommige gevallen ook hebben verwezenlijkt.
- Gegevensverzamelingen zijn soms onterecht niet in beeld als bulkdatasets.
- Verschillende afdelingen binnen de diensten hanteren verschillende werkwijzen, die soms ook nog onrechtmatig zijn. Hierdoor is er onvoldoende zicht op het verstrijken van beoordelingstermijnen voor individuele bulkdatasets.

- Naast het ontbreken van centrale regie zijn er ook ernstige procedurele en technische tekortkomingen in het toegangsmanagement voor bulkdatasets. Dit heeft geleid tot verschillende onrechtmatigheden en onzorgvuldigheden op dit gebied. Zo zijn in dit onderzoek meerdere gevallen aan het licht gekomen waarin dienstmedewerkers toegang hadden tot gegevens uit bulkdatasets met een (strikt) beperkt toegangsregime, terwijl zij daartoe niet (langer) bevoegd waren. Deze voorvallen zijn onrechtmatig.

De wet biedt waarborgen bij de verwerking van bulkdatasets. Met de inwerkingtreding van de Tijdelijke regeling is voorzien in passende waarborgen bij de verwerking van bulkdatasets waarbij onder meer de nodige aandacht is voor de beoordeling van de privacyinbreuk van de verdere verwerking van een bulkdataset. Daarnaast voorziet de Tijdelijke wet in waarborgen waarmee wordt voorkomen dat bepaalde bulkdatasets langer worden gebruikt dan noodzakelijk. Tijdens dit onderzoek heeft de CTIVD vastgesteld dat deze waarborgen toereikend zijn, maar de voornaamste risico's doen zich voor in de uitvoering ervan door de diensten. De (verdere) verbetering van de uitvoering staat bij de diensten hoog op de agenda. Ook zijn al tijdens de onderzoeksperiode verbeteringen doorgevoerd. De CTIVD doet in dit rapport aanbevelingen om hiertoe bij te dragen.

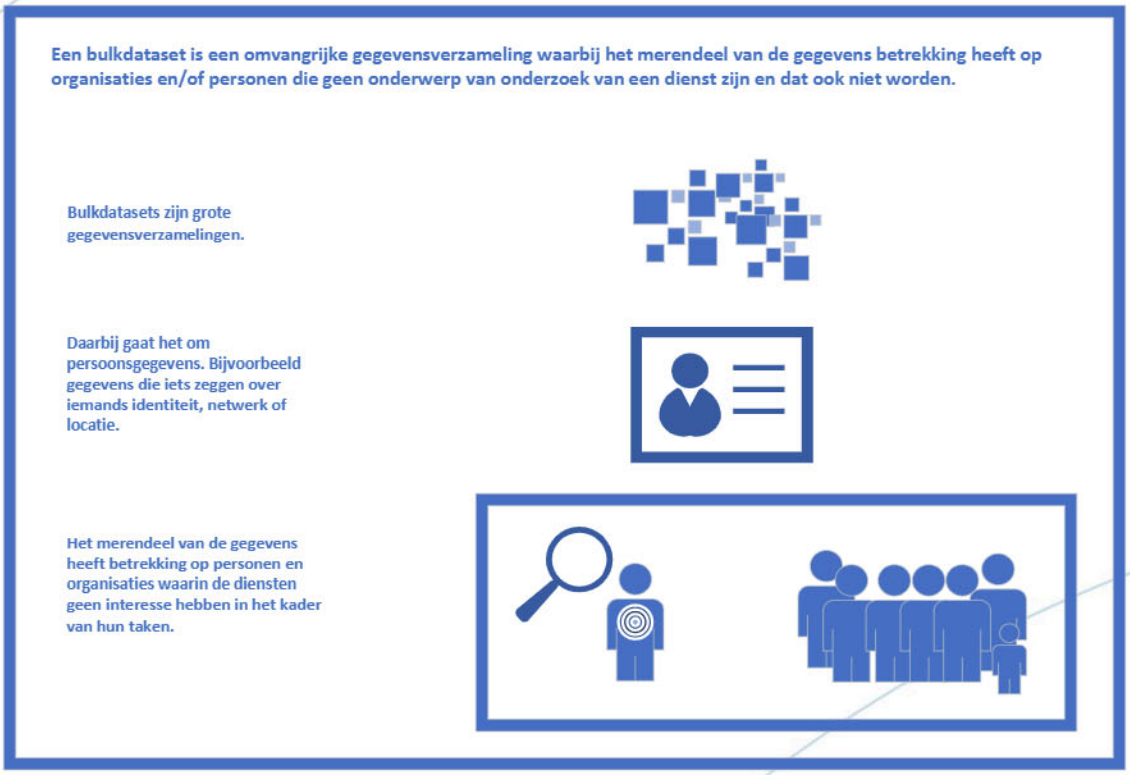
Van dit rapport is géén staatsgeheime versie. Ook is er géén staatsgeheime bijlage.

2 Inleiding

Hoofdstuk 2 – Inleiding

2.1 De verwerking van bulkdatasets door de AIVD en de MIVD

De Algemene Inlichtingen- en Veiligheidsdienst (‘**AIVD**’) en de Militaire Inlichtingen- en Veiligheidsdienst (‘**MIVD**’) (hierna samen: ‘**de diensten**’) verwerven en verwerken grote hoeveelheden persoonsgegevens. De wet geeft de diensten deze bevoegdheid, zodat zij hun wettelijke taken goed kunnen uitvoeren. Een van deze taken is bijvoorbeeld het onderzoek naar terrorisme en spionage in Nederland door andere landen. De diensten zijn daartoe bevoegd om gegevens te verwerken uit zogenaamde *bulkdatasets*. De CTIVD legt in dit rapport uit of de wijze waarop de diensten werken met de gegevens uit bulkdatasets voldoet aan de wettelijke eisen.



Een bulkdataset is een omvangrijke gegevensverzameling met persoonsgegevens. Met *omvangrijk* wordt bedoeld dat de gegevensverzameling dusdanig groot is dat het voor de diensten niet werkbaar is om alle informatie in de gegevensverzameling gericht te bekijken. De praktijk leert dat het kan gaan om databestanden die oplopen tot miljoenen regels persoonsgegevens.

Persoonsgegevens

Het begrip 'persoonsgegevens' wordt gedefinieerd als *"gegevens die betrekking hebben op een identificeerbare of geïdentificeerde, individuele natuurlijke persoon"*.

(Artikel 1 lid 3, sub e van de Wiv 2017)

Bij persoonsgegevens denkt men vaak aan identificerende gegevens zoals namen en (e-mail)adresgegevens, maar het kan bijvoorbeeld ook gaan om informatie over uiterlijke kenmerken van mensen, telefoonnummers, chatberichten, sociale mediagegevens, locatiegegevens, technische kenmerken zoals IP-adressen of elke andere vorm van gegevens, mits deze gekoppeld of te koppelen zijn aan een bepaald persoon.

Het verkrijgen en het gebruik van bulkdatasets door de diensten kan een vergaande inbreuk maken op de privacy van de personen over wie gegevens in de bulkdataset voorkomen. Met behulp van gegevens uit bulkdatasets kan soms een relatief volledig beeld ontstaan over bepaalde aspecten van iemands privéleven. Daarnaast staat vast dat het merendeel van de personen over wie gegevens in de dataset voorkomen, geen onderwerp van onderzoek van een dienst is en dat ook niet wordt. Dit betekent dat het grootste deel van de gegevens in een bulkdataset gaat over mensen waarin de diensten geen interesse hebben, omdat deze mensen niks te maken hebben met zaken waar de diensten onderzoek naar doen (zoals terrorisme en spionage). Zij vormen geen bedreiging voor de nationale veiligheid. Het is daarom van belang dat er passende waarborgen zijn voor het verwerken van gegevens uit bulkdatasets, die ervoor zorgen dat de privacyinbreuk bij deze gegevensverwerking niet onnodig groot is en in verhouding staat tot het beoogde doel.

Tegelijkertijd zijn bulkdatasets voor de diensten een belangrijk middel. Bulkdatasets kunnen bijvoorbeeld worden gebruikt om kenmerken van personen of organisaties na te slaan. Zo kan nieuwe informatie, die waardevol is voor een onderzoek van de diensten, worden ontdekt. Een voorbeeld betreft het opzoeken van een telefoonnummer om deze te koppelen aan de naam van een persoon. Naast het opzoeken van kenmerken kunnen bulkdatasets door middel van data-analyse ook worden gebruikt om (ongekende) dreigingen te identificeren en te onderkennen.

Gegevensverwerking

Het begrip 'gegevensverwerking' wordt gedefinieerd als *"elke handeling of elk geheel aan handelingen met betrekking tot gegevens, waaronder in elk geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens"*.

(Artikel 1 lid 3 sub f van de Wiv 2017)

2.2 Aanleiding voor het onderzoek van de CTIVD

De CTIVD erkent het belang en de actualiteit van het onderwerp bulkdatasets. Zowel de AIVD als de MIVD maken op grote schaal en op verschillende plekken in de organisatie gebruik van bulkdatasets. Dit is belangrijk voor de taakuitvoering van de diensten, maar behelst ook een aanzienlijke privacyinbreuk voor de personen over wie gegevens voorkomen in deze bulkdatasets. Het verwerven en verwerken van bulkgegevens heeft daarom eerder tot maatschappelijke onrust geleid. Opkomende technologische ontwikkelingen op het gebied van *artificial intelligence* en andere vormen van geautomatiseerde data-analyse kunnen de effectiviteit maar ook de privacyinbreuk bij het gebruik van gegevens uit bulkdatasets nog verder vergroten. De maatschappij en de politiek moeten erop kunnen vertrouwen dat er goede waarborgen zijn voor het werken met bulkdatasets en dat de diensten zich aan de geldende regelgeving houden.

De CTIVD heeft in haar toezicht altijd aandacht gehad voor de verwerving en verwerking van bulkdatasets door de diensten en het daarbij geldende wettelijke kader. De CTIVD heeft eerder kritische kanttekeningen geplaatst bij (het werken met) bulkdatasets in onder meer toezichtrapporten nrs. 70, 71 en 79. Ook heeft de CTIVD al langer aandacht voor de datahuishouding van de AIVD en de MIVD. In haar voortgangsrapportages over de implementatie van de Wiv 2017 (toezichtrapporten nrs. 59, 62, 66 en 69) heeft zij kritische kanttekeningen geplaatst bij de wijze waarop de diensten hun datahuishouding hebben vormgegeven, hetgeen ook relevant is voor het werken met bulkdatasets. Daarnaast is het wettelijk kader ten aanzien van bulkdatasets sinds de inwerkingtreding van de Wiv 2017 herhaaldelijk aangepast en aangevuld, omdat hierin mede door de CTIVD geconstateerde knelpunten bestonden. Zo zijn er met de Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017 (hierna: Tijdelijke regeling) nadere regels gekomen voor de toegang van dienstmedewerkers tot gegevens uit bulkdatasets (zie hoofdstuk 4 en 5). Ook is de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkdatasets en overige voorzieningen (hierna: de Tijdelijke wet) ingevoerd. Hiermee is het voor de diensten mogelijk geworden nieuwe eindtermijnen voor het gebruik van bepaalde bulkdatasets aan te vragen bij de betrokken minister, met daarop bindend toezicht van de CTIVD (zie hoofdstuk 7). Inmiddels hebben de diensten voldoende de tijd gehad

om ervaring op te doen met het aangepaste wettelijke kader. Daarmee acht de CTIVD dit een goed moment om de uitvoering te toetsen.

Ten slotte wordt momenteel gewerkt aan de herziening van de Wiv 2017. Hiermee beoogt het kabinet onder meer het wettelijk kader voor bulkdatasets opnieuw aan te passen. De CTIVD wenst met de beoordeling van de verwerking van bulkdatasets op basis van het huidige wettelijke kader in dit rapport een bijdrage te leveren aan de wetsherziening en het maatschappelijke debat.

2.3 Scope van het rapport

De CTIVD heeft onderzoek gedaan naar de rechtmatigheid van de verdere verwerking van bulkdatasets door de diensten. Met de *verdere verwerking* wordt bedoeld: elke vorm van gebruik van de gegevens, anders dan de verwerving van die gegevens. Voor het verder verwerken van gegevens uit bulkdatasets geldt een afgebakende set regels. Dit zorgt voor een natuurlijke afbakening van het toetsingskader voor dit rapport.

Het onderzoek van de CTIVD beslaat de gehele verdere verwerkingsketen van bulkdatasets. Om het onderzoek behaphaar te houden, heeft zij ervoor gekozen om drie onderwerpen buiten scope te laten. Ten eerste valt de verwerving van bulkdatasets door de diensten buiten de scope van dit rapport. De CTIVD heeft hier in eerdere rapporten wel al aandacht aan besteed. Zie bijvoorbeeld toezichtrapport nr. 70 (2020) over het verzamelen van bulkdatasets met de hackbevoegdheid door de AIVD en de MIVD en toezichtrapport nr. 79 (2024) over de inzet van virtuele agenten door de AIVD en de MIVD.

Ten tweede valt de verwerving en verwerking van zogenaamde *onderzoeksopdrachtgerichte gegevens* buiten de scope van dit rapport. De diensten kunnen bulkdatasets verwerven met inzet van de bevoegdheid tot *onderzoeksopdrachtgerichte interceptie* (bijvoorbeeld kabelinterceptie). Daarbij gaat het ook om bulkgegevens. Voor de inzet van deze bevoegdheid, en voor de verdere verwerking van de gegevens die met deze bevoegdheid zijn verzameld, geldt echter een specifiek, strikter wettelijk regime (zie de artikelen 48 tot en met 50 van de Wiv 2017). De CTIVD heeft eerder aandacht gehad voor onderzoeksopdrachtgerichte interceptie door de AIVD en de MIVD in haar toezichtrapporten nr. 63 (2019) en nr. 75 (2022).

Ten derde valt het delen van gegevens uit bulkdatasets met buitenlandse partnerdiensten buiten de scope van dit rapport. Op verschillende momenten in de levenscyclus kunnen gegevens uit bulkdatasets door de diensten worden gedeeld met buitenlandse inlichtingendiensten. Voor dit specifieke doel bestaan specifieke wettelijke bevoegdheden met aanvullende waarborgen. De CTIVD heeft in eerdere rapporten al aandacht gehad voor het delen van gegevens met buitenlandse diensten. Zo heeft toezichtrapport nr. 65 betrekking op de verstrekking van ongeëvalueerde gegevens aan buitenlandse diensten door de AIVD en de MIVD (2019).

2.4 Beoordelingskader

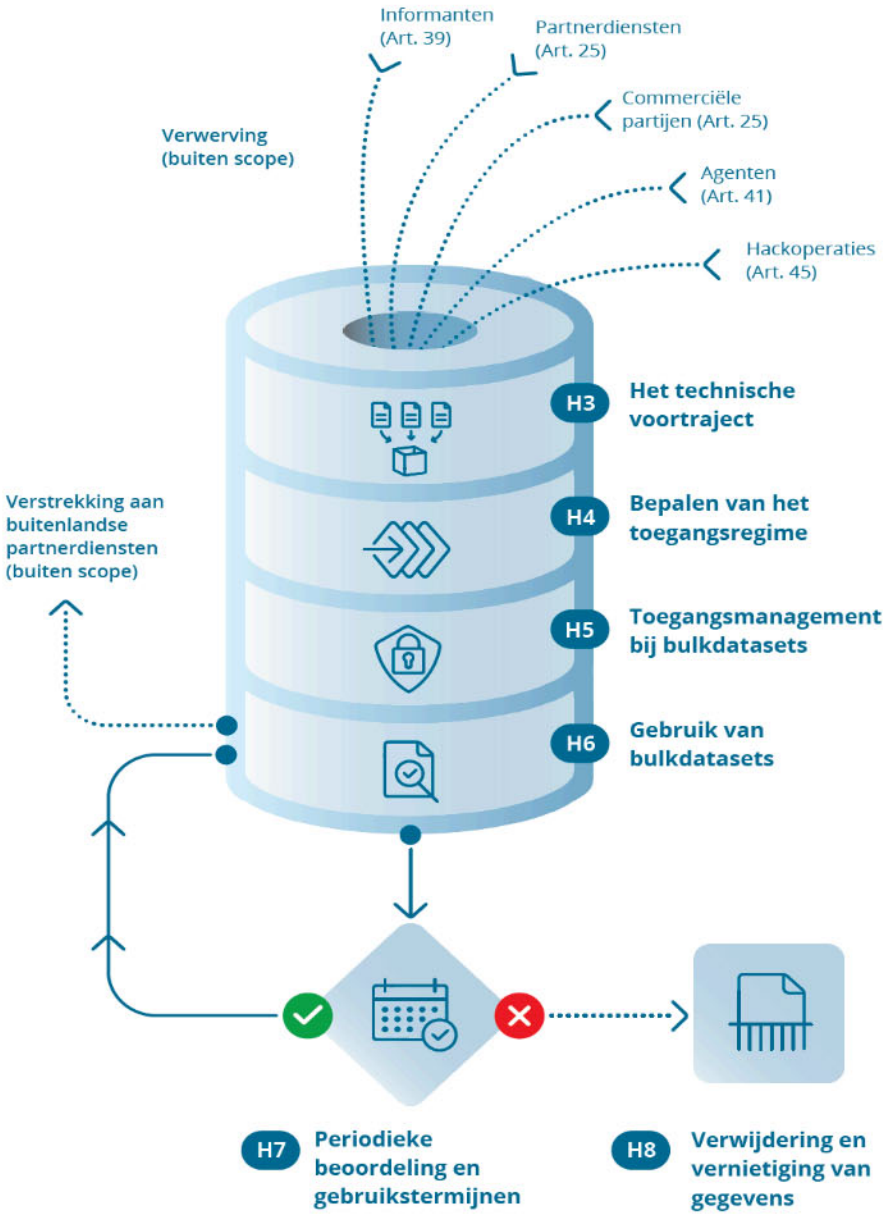
De CTIVD doet onderzoek naar de rechtmatigheid van het handelen van de diensten. In de wet staat beschreven dat de diensten persoonsgegevens mogen gebruiken. Daar staat ook beschreven hoe en in welke situaties de diensten dit mogen doen. Daarnaast zijn er in wet- en regelgeving specifieke eisen die betrekking hebben op het gebruik van gegevens uit bulkdatasets door de diensten. Het gaat om bepalingen uit de Wiv 2017, de Tw en de Tijdelijke regeling. Hieronder volgen de belangrijkste wettelijke criteria die relevant zijn voor de toetsing door de CTIVD in dit rapport:

1. Het bewaren en gebruiken van bulkdatasets vindt slechts plaats voor een bepaald doel en slechts voor zover dat noodzakelijk is voor de goede uitvoering van de Wiv 2017 of de Wet Veiligheidsonderzoeken (Wvo).
2. De diensten dienen gegevens behoorlijk en zorgvuldig te verwerken. Behoorlijke gegevensverwerking betekent onder meer dat de privacyinbreuk die de gegevensverwerking behelst in een redelijke verhouding moet staan tot het beoogde doel. Daarnaast toetst de CTIVD in het kader van zorgvuldige gegevensverwerking onder meer de wijze waarop de diensten hun datahuishouding ten aanzien van het gebruik van gegevens uit bulkdatasets hebben vormgegeven.
3. De diensten moeten datareductie toepassen, zodat niet meer gegevens worden verwerkt dan nodig is.
4. De diensten mogen géén medische persoonsgegevens verwerken, noch gegevens die betrekking hebben op iemands godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid of iemands seksuele leven. De verwerking van voornoemde persoonsgegevens is slechts toegestaan in aanvulling op de verwerking van andere gegevens en slechts voor zover dat voor het doel van de gegevensverwerking onvermijdelijk is.
5. Gegevens die betrekking hebben op vertrouwelijke communicatie tussen advocaat en diens cliënt mogen alleen met voorafgaande toestemming van de rechtbank Den Haag door de diensten worden verwerkt.
6. De diensten moeten intern schriftelijk vastleggen welke medewerkers toegang hebben tot welke gegevens. Deze toegang (of uitsluiting) moet vervolgens op een goede manier (technisch) worden afgedwongen.
7. Gegevens van de diensten moeten goed beschermd zijn tegen verlies of aantasting. Hiertoe moeten technische, organisatorische en personele maatregelen worden getroffen.
8. Gegevens mogen door de diensten niet langer worden bewaard dan wettelijk is toegestaan. Voor gegevens uit bulkdatasets gelden hieromtrent specifieke regels, maar die regels zijn niet in alle gevallen hetzelfde. Voor bepaalde bulkdatasets kunnen door de betrokken minister nieuwe eindtermijnen voor het gebruik worden vastgesteld. Dit is dan wel gekoppeld aan eisen omtrent noodzakelijkheid, proportionaliteit en subsidiariteit.

2.5 Leeswijzer - De levenscyclus van bulkdatasets

Er is een aantal stappen te onderscheiden in de levenscyclus van bulkdatasets die door de diensten worden gebruikt. De structuur van dit rapport volgt deze levenscyclus (zie figuur 1 hieronder). Elk hoofdstuk beschrijft een stap in de levenscyclus van een bulkdataset. Ook wordt telkens de werkwijze van de diensten aan de geldende wet- en regelgeving getoetst.

Levenscyclus van een bulkdataset



Figuur 1

- De levenscyclus van bulkdatasets begint bij de **verwerving** ervan door een dienst (stap 1 in figuur 1). De diensten kunnen bulkdatasets bijvoorbeeld verkrijgen van informanten, andere overheidsorganisaties, buitenlandse inlichtingendiensten, of tegen betaling van commerciële partijen. De diensten kunnen ook bijzondere bevoegdheden inzetten om bulkdatasets te verwerven. Dan gaat het bijvoorbeeld om de inzet van een hackoperatie of de aansturing van een (virtueel) agent om een bulkdataset te verwerven. De verwerving van bulkdatasets valt buiten de scope van dit rapport.

- Hoofdstuk 3 behandelt **het technische voortraject** waarbij bulkdatasets op de ICT-systemen van de diensten beschikbaar worden gemaakt (stap 2 in figuur 1). Hierbij is het in eerste instantie van belang dat de diensten scherp hebben welke gegevensverzamelingen kwalificeren als een bulkdataset. Dit is van belang omdat voor bulkdatasets speciale waarborgen moeten worden geïmplementeerd. Ook moeten de diensten er in deze fase al voor waken dat zij niet méér data beschikbaar maken op hun systemen dan nodig is voor de uitvoering van hun taken.

- Hoofdstuk 4 heeft betrekking op de beoordeling door de diensten van de mate waarin het gebruiken van de bulkdataset een inbreuk maakt op de persoonlijke levenssfeer van de personen van wie gegevens voorkomen in de set. Op basis daarvan wordt onder meer bepaald welke (groepen) functionarissen binnen de diensten toegang mogen krijgen tot de data. Concreet gaat het om **de bepaling of er een standaard, beperkt of strikt beperkt toegangsregime zal worden gehanteerd** (stap 3 in figuur 1).

- Hoofdstuk 5 gaat in op het treffen van de technische en procedurele maatregelen omtrent de toegang tot de data voor de medewerkers voor wie dat noodzakelijk is voor hun werkzaamheden. Dit wordt **toegangsmanagement** genoemd (stap 4 in figuur 1).

- Hoofdstuk 6 gaat over **het gebruik van bulkdatasets** door de diensten voor de uitvoering van hun taken, waaronder de uitvoering van de inlichtingenonderzoeken naar bijvoorbeeld terrorisme en spionage in Nederland door andere landen maar ook voor de uitvoering van daaraan ondersteunende taken (stap 5 in figuur 1).

- Hoofdstuk 7 behandelt de **beoordeling van de noodzaak tot verwijdering en het eventueel vaststellen van nieuwe gebruikstermijnen** van bulkdatasets (stap 6 in figuur 1). Ten aanzien van bulkdatasets die met algemene bevoegdheden zijn verkregen, moeten de diensten periodiek beoordelen of er noodzaak tot verwijdering bestaat. Bulkdatasets die met bijzondere bevoegdheden zijn verkregen, mogen anderhalf jaar worden bewaard en gebruikt. Als de diensten een bulkdataset na anderhalf jaar toch nog langer willen gebruiken, dan moeten zij daarvoor toestemming vragen aan de betrokken minister. De

toestemming voor een nieuwe gebruikstermijn geldt voor de duur van een (1) jaar en mag slechts worden gegeven als dat noodzakelijk, proportioneel en subsidiair is.

- Hoofdstuk 8 gaat over de **verwijdering en vernietiging** van gegevens uit bulkdatasets (stap 7 in figuur 1).

- Hoofdstuk 9 bevat de conclusies en aanbevelingen van dit rapport.

In elk volgend hoofdstuk van dit rapport worden bevindingen weergegeven; het betreft de *blauwe cursieve zinnen*.

Daarnaast bevat het rapport blauwe, groene en paarse tekstkaders. De blauwe kaders beschrijven de betekenis van begrippen die in het rapport worden gebruikt. In de groene kaders worden de wettelijke vereisten weergegeven waaraan de CTIVD in dit rapport heeft getoetst. Tenslotte staan in de paarse kaders de aanbevelingen van de CTIVD.

In dit rapport wordt rekening gehouden met het staatsgeheime karakter van het werk van de diensten. Omdat dit rapport openbaar toegankelijk is, wordt in een aantal gevallen de werkwijze van de diensten met een zekere abstractie weergegeven. Alle onrechtmatigheden en onzorgvuldigheden die de CTIVD in het onderzoek heeft geconstateerd, zijn in dit rapport opgenomen. Van dit rapport is géén staatsgeheime versie en er is géén staatsgeheime bijlage.

2.6 Toelichting op de gebruikte onderzoeksmethodes

Gedurende dit onderzoek heeft de CTIVD verschillende onderzoekshandelingen verricht. De CTIVD heeft haar bevindingen allereerst gebaseerd op zelfstandig onderzoek dat zij heeft uitgevoerd in de systemen van de diensten. In dit kader heeft de CTIVD interne stukken bestudeerd, zoals overzichten, beleid en besliskaders over bulkdatasets. Daarnaast heeft zij verzoeken en toestemmingen voor de verdere verwerking van bulkdatasets onderzocht. Hierbij kan worden gedacht aan voorstellen voor het plaatsen van een bulkdataset in een toegangsregime of verzoeken voor het vaststellen van een nieuwe eindtermijnen voor het bewaren van een bulkdataset (gebruikstermijnen). Verder heeft zij ook wettelijke meldingen over bulkdatasets door de diensten aan de CTIVD onderzocht.

In de tweede plaats heeft de CTIVD gesprekken gevoerd met de diensten en (schriftelijke) vragen gesteld. Ten slotte heeft de CTIVD aan de hand van een risicogestuurde steekproef bulkdatasets geselecteerd voor een casestudie. Aan de hand van deze casestudie heeft de CTIVD beoordeeld of de diensten de toepasselijke wet- en regelgeving ook daadwerkelijk in de praktijk hebben nageleefd bij de verdere verwerking van de geselecteerde bulkdatasets. Daartoe heeft de CTIVD de verdere verwerking van deze bulkdatasets in verschillende fases van de levenscyclus van de bulkdatasets onderzocht.

3 Het technisch voortraject

Hoofdstuk 3 – Het technische voortraject



3.1 Inleiding en wettelijke criteria

Voordat de gegevens uit bulkdatasets door de diensten kunnen worden gebruikt in de onderzoeken die zij verrichten, is er onder meer een technisch voortraject nodig waarbij de gegevens beschikbaar worden gemaakt op de daarvoor bedoelde ICT-systemen. Dit hoofdstuk heeft betrekking op de toetsing van de wettelijke criteria die hierbij gelden.

Het is in eerste instantie van belang dat de diensten scherp hebben of een dataset die zij verkrijgen, voldoet aan de wettelijke definitie van bulkdataset (zie kader). Als een dataset voldoet aan de definitie van bulkdataset, gelden niet alleen de algemene regels voor gegevensverwerking, maar ook de specifieke regels voor bulkdatasets. Het bepalen of een verkregen dataset kwalificeert als een bulkdataset is onderdeel van het technische voortraject. In paragraaf 3.2.1. wordt hier nader op ingegaan.

Bulkdataset

Een bulkdataset is een omvangrijke gegevensverzameling waarbij het merendeel van de gegevens betrekking heeft op organisaties en/of personen die geen onderwerp van onderzoek van een dienst zijn en dat ook niet worden.

(Artikel 1 van de Tijdelijke regeling)

Wanneer vaststaat dat een gegevensverzameling een bulkdataset betreft, is het vervolgens van belang dat de diensten niet méér gegevens uit de bulkdataset beschikbaar maken op hun systemen dan nodig is voor de goede uitvoering van hun wettelijke taken. Dit betekent in de praktijk dat er vóór het beschikbaar maken van de gegevens uit datasets een datareductieslag dient plaats te vinden. Bij deze datareductieslag moet worden gewaarborgd dat de diensten geen

data behouden die valt onder één van de verboden categorieën. De diensten mogen op grond van de wet in beginsel géén informatie verwerken die iets zegt over iemands gezondheid, godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging of seksuele leven. Ook is het van belang dat de diensten in dit stadium onderzoeken of er gegevens voorkomen in de bulkdataset die betrekking hebben op de vertrouwelijke communicatie van advocaten. Deze gegevens mogen namelijk alleen worden verwerkt met voorafgaande toestemming van de Rechtbank Den Haag. In paragraaf 3.2.2 wordt nader ingegaan op de datareductieslag die moet plaatsvinden in het technische voortraject.

Verwerking van gegevens uitsluitend in het kader van wettelijke taken

De verwerking van gegevens vindt slechts plaats voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering van deze wet of de Wet veiligheidsonderzoeken.

(Artikel 18 lid 1 van de Wiv 2017)

Verbod op verwerking van onder meer medische gegevens

De verwerking van persoonsgegevens wegens iemands godsdienst of levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid en seksuele leven vindt niet plaats.

De verwerking van persoonsgegevens die bstrekking hebben op de in het derde lid bedoelde kenmerken vindt slechts plaats in aanvulling op de verwerking van andere gegevens en slechts voor zover dat voor het doel van de gegevensverwerking onvermijdelijk is.

(Artikel 19 lid 3 en 4 van de Wiv 2017)

Verwerking van gegevens die betrekking hebben op vertrouwelijke communicatie tussen een advocaat en diens client

Gegevens die betrekking hebben op de vertrouwelijke communicatie van een advocaat en diens cliënt en verkregen zijn door de uitoefening van een bijzondere bevoegdheid (...), worden terstond vernietigd, tenzij de verdere verwerking van de gegevens noodzakelijk is voor het onderzoek in het kader waarvan de gegevens zijn verworven en de Rechtbank Den Haag daartoe toestemming heeft verleend. (...)

(Artikel 27 lid 2 van de Wiv 2017)

Wanneer vaststaat dat een gegevensverzameling een bulkdataset betreft en de juiste stappen met betrekking tot datareductie zijn doorlopen, kunnen de gegevens beschikbaar worden gemaakt op de ICT-systemen van de diensten. Hierbij is van belang dat de diensten hun datahuishouding zo inrichten dat de verwerking van gegevens uit bulkdatasets op zorgvuldige

wijze plaatsvindt. Op dit onderdeel van het technische voortraject wordt nader ingegaan in paragraaf 3.2.3.

Behoorlijke en zorgvuldige gegevensverwerking

De verwerking van gegevens geschiedt in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze.

(Artikel 18 lid 2 van de Wiv 2017)

3.2 Beoordeling van het technisch voortraject

3.2.1 Het bepalen of sprake is van een bulkdataset

Het is allereerst van belang dat de diensten scherp hebben of een dataset die zij hebben verkregen, voldoet aan de wettelijke definitie van bulkdataset. Als daarvan sprake is, zijn de specifieke regels over bulkdatasets van toepassing. Dit zijn maatregelen die de diensten moeten treffen waarmee wordt gewaarborgd dat de privacyinbreuk bij deze gegevensverwerking niet onnodig groot is en in verhouding staat tot het beoogde doel.

De definitie van bulkdatasets is niet in alle gevallen gemakkelijk toepasbaar.
In de praktijk is het doorgaans redelijk eenvoudig vast te stellen welke datasets als bulkdatasets kwalificeren. In sommige gevallen is het onderscheid tussen bulkdatasets en datasets anders dan bulkdatasets echter minder eenvoudig te maken. Er zijn vier aspecten van de definitie van bulkdatasets (zie pagina 13), waardoor in de praktijk soms twijfel kan bestaan of een dataset als een bulkdataset moet worden beschouwd:

1) Wanneer is sprake van persoonsgegevens?
   Het begrip *persoonsgegevens* is een belangrijk onderdeel van de definitie van bulkdatasets. Een dataset kan geen bulkdataset zijn, als deze géén persoonsgegevens bevat. Persoonsgegevens zijn alle gegevens die gekoppeld zijn of kunnen worden aan een bepaald persoon (zie kader op pagina 7). In de praktijk is het soms echter lastig om vast te stellen of de gegevens in een dataset persoonsgegevens zijn, of dat het gaat om (technische) gegevens die niet aan individuele natuurlijke personen kunnen worden gekoppeld. Twee voorbeelden zijn telefoonnummers en IP-adressen. Hierbij is het afhankelijk van de context of het om persoonsgegevens gaat. Telefoonnummers kunnen niet in gebruik zijn of juist worden gebruikt door meerdere personen of organisaties, maar zij kunnen ook zijn gekoppeld aan een fysiek object. Ook voor IP-adressen geldt dat zij kunnen toebehoren aan (interne) routers van een netwerk. Telefoonnummers en IP-adressen zijn daarom niet altijd te koppelen aan een natuurlijk persoon.

2) Hoe moet worden vastgesteld wat het merendeel is?
Het kan ook ingewikkeld zijn om te bepalen of een dataset voor het *merendeel* gegevens bevat van mensen/organisaties waar de dienst geen interesse in heeft. Bijvoorbeeld als het gaat om datasets met veel verschillende technische categorieën van data, maar waarin ook persoonsgegevens voorkomen. Het is dan soms lastig om te bepalen of er genoeg duidelijke persoonsgegevens zijn om te kunnen spreken van een bulkdataset.

3) Wanneer betreffen het gerichte onderzoeksgegevens en wanneer gaat het om gegevens van mensen die niet onderzocht (zullen) worden?
Het is soms moeilijk te beoordelen of een dataset gerichte onderzoeksgegevens bevat, of dat het gaat om gegevens van mensen die niet onderzocht (zullen) worden. Alleen in dat laatste geval kan sprake zijn van een bulkdataset. Een bijkomende moeilijkheid is dat in de definitie van bulkdataset gesproken wordt over *"personen en/of organisaties"* die geen onderwerp van onderzoek zijn of zullen worden. Dit roept de vraag op of sprake is van een bulkdataset bij een gegevensverzameling die betrekking heeft op een organisatie waar een dienst onderzoek naar doet, maar ook de persoonsgegevens bevat van mensen die misschien wel bij de organisatie horen, maar zeker niet allemaal worden onderzocht.

4) Wanneer is sprake van een afgebakende bulkdataset?
Op basis van de definitie wordt niet duidelijk wanneer sprake is van een afgebakende bulkdataset. Het is daardoor lastig te bepalen in welke gevallen (kleine) bulkdatasets (administratief) mogen worden samengevoegd tot een enkele bulkdataset, of juist moeten worden opgesplitst in meerdere bulkdatasets. De vraag of een bepaalde gegevensverzameling moet worden gezien als één, of als verschillende bulkdatasets, kan relevant zijn voor het vaststellen van de toegangsregimes (zie hoofdstuk 4) en het bewaken van eindtermijnen voor het gebruik (zie hoofdstuk 8).

Omdat de definitie van een bulkdataset in de praktijk niet altijd makkelijk toepasbaar is, ontstaat er soms onduidelijkheid, zowel bij de diensten als bij de CTIVD, of een bepaalde dataset als een bulkdataset moet worden behandeld. Ook kan er onduidelijkheid bestaan of bepaalde gegevens als één, of als meerdere bulkdatasets moet worden beschouwd. Deze onduidelijkheden zijn problematisch, omdat als een gegevensverzameling ten onrechte niet wordt aangemerkt als een bulkdataset, de wettelijke waarborgen en regels voor de verdere verwerking van bulkdatasets niet worden toegepast. In dat geval is er wel sprake van een vergaande privacyinbreuk door de verwerking van de gegevensverzameling, maar ontbreekt de passende bescherming.

De AIVD en de MIVD hebben gezamenlijk beleid om te waarborgen dat datasets ten onrechte niet worden aangemerkt als bulkdataset, toch blijven er risico's bestaan.

De AIVD en de MIVD hebben een gezamenlijk beleid over het technisch voortraject bij bulkdatasets die verzameld en verwerkt worden door de diensten. In dit beleid is bepaald dat medewerkers van de inlichtingenteams die betrokken zijn bij het verwerven van een dataset, deze kunnen aanmelden bij een speciaal team dat verantwoordelijk is voor het technische voortraject van datasets. Dit team beoordeelt onder meer of aangemelde datasets moeten worden gekwalificeerd en behandeld als bulkdataset. Naar het oordeel van de CTIVD blijven ten aanzien van dit aanmeldproces twee risico's bestaan. Deze risico's zorgen ervoor dat datasets alsnog ten onrechte niet als bulkdatasets worden aangemerkt of dat deze beoordeling van datasets inconsistent is:

1) De medewerkers van de verschillende teams moeten in een voortraject van een dataset zelf aangeven of er een vermoeden bestaat dat het om een bulkdataset kan gaan. Daardoor is sprake van een sterke afhankelijkheid van de individuele inschattingen van deze medewerkers.
2) Niet alle datasets die de diensten verwerken, worden onderworpen aan een aanmeldproces waarvoor de diensten gezamenlijk beleid hebben opgesteld. Met name bij de MIVD werden bij een aantal (oudere) datasets, mede in verband met compartimentering, andere werkwijzen gehanteerd.

Aanbeveling 1
Zorg voor nadere maatregelen die voorkomen dat datasets ten onrechte niet als bulkdatasets in beeld komen, bijvoorbeeld doordat deze niet worden aangemeld.

Aanbeveling 2
Verduidelijk de definitie van bulkdatasets, of de wijze waarop deze moet worden toegepast, in beleid of regelgeving om ervoor te zorgen dat alle gegevensverzamelingen die het inbreukmakende karakter van een bulkdataset hebben, volgens de regels voor bulkdatasets worden verwerkt en in passende waarborgen wordt voorzien.

3.2.2 Datareductie vooraf

In 3.1.1. is uiteengezet dat een belangrijk uitgangspunt voor gegevensverwerking is dat de diensten niet meer gegevens mogen verwerken dan nodig is voor de uitvoering van hun wettelijke taken.

De diensten hebben gezamenlijk beleid op basis waarvan datareductie plaatsvindt voordat bulkdatasets kunnen worden gebruikt voor de uitvoering van wettelijke taken.

Op de bulkdatasets die de CTIVD heeft onderzocht, hebben de diensten een datareductieslag toegepast vóórdat de gegevens uit deze sets beschikbaar zijn gemaakt voor inlichtingenonderzoek. Deze datareductieslag maakt deel uit van het technische voortraject waar bulkdatasets aan onderhevig zijn.

Voordat de gegevens beschikbaar worden gemaakt op de daarvoor bedoelde ICT-systemen bepaalt het team dat verantwoordelijk is voor het technische voortraject, in samenspraak met het betrokken inlichtingenteam, welke (categorieën) gegevens nodig zijn voor het inlichtingenonderzoek en welke niet. Alleen de noodzakelijke gegevens worden beschikbaar gemaakt. De overige gegevens worden op termijn verwijderd en vernietigd (zie hoofdstuk 8). Ook vindt op deze plek in het proces een check plaats op de aanwezigheid van gegevens die de diensten niet (zomaar) mogen verwerken, zoals medische gegevens en gegevens die betrekking hebben op communicatie tussen een advocaat en diens cliënt.

Bij sommige bulkdatasets waarmee de diensten werken, is de hierboven beschreven aanmeldprocedure niet gevolgd. Bijvoorbeeld omdat het oudere bulkdatasets betreft, of bulkdatasets waarmee, omwille van de structuur van de gegevens, op een afwijkende manier wordt gewerkt. De CTIVD heeft een aantal van deze gevallen onderzocht en ook bij deze gevallen heeft een data-reductieslag plaatsgevonden.

De CTIVD heeft in een steekproef geen verboden (categorieën) gegevens in bulkdatasets aangetroffen.
De CTIVD heeft in een steekproef (zie paragraaf 2.3) geen (categorieën van) gegevens aangetroffen in bulkdatasets die de diensten op basis van de wet in beginsel niet mogen verwerken. Daarbij gaat het om gegevens die betrekking hebben op iemands godsdienst, levensovertuiging, ras, lidmaatschap van een vakvereniging, gezondheid en seksuele leven. Ook heeft de CTIVD in deze steekproef geen ongeoorloofde verwerking van gegevens geconstateerd die betrekking hebben op de vertrouwelijke communicatie van een advocaat en diens cliënt.

3.2.3 Technische ontsluiting van de bulkdataset op de systemen

Er is sprake van een versnipperd datalandschap met betrekking tot bulkdatasets, waarop onvoldoende centrale regie wordt gevoerd.
Uit onderzoek van de CTIVD blijkt dat de diensten op verschillende plekken en manieren werken met bulkdatasets. Ook zijn de bulkdatasets op verschillende manieren toegankelijk gemaakt op de systemen van de diensten. Dit kan deels worden verklaard door verschillen zoals:

- of het een oude of een wat nieuwere bulkdataset betreft;
- of het om een bulkdataset gaat die uitsluitend door de AIVD, de MIVD of misschien wel door beide diensten wordt gebruikt; en
- verschillen in de structuur van de gegevens uit bulkdatasets.

Het gebruik van bulkdatasets is in de loop der jaren significant toegenomen. Ook worden bulkdatasets via de inzet van verschillende bevoegdheden verworven, waardoor op steeds meer plekken binnen de diensten met deze sets wordt gewerkt. Als gevolg daarvan is een versnipperd datalandschap ontstaan waarop geen centrale regie wordt gevoerd. Hierdoor zijn er verhoogde risico's op onrechtmatigheden, die zich in sommige gevallen ook verwezenlijken. Dit is het geval bij gegevensverzamelingen die niet in beeld zijn als bulkdatasets (zie paragraaf 3.2.1), situaties waarin er onvoldoende zicht is op het verstrijken van beoordelingstermijnen voor individuele bulkdatasets (zie paragraaf 7.2.1) of situaties waarin verschillende afdelingen binnen de diensten verschillende werkwijzen hanteren om aan regelgeving te voldoen, en daarin soms ook tekortschieten (zie paragraaf 6.2.2.). Ook is het versnipperde datalandschap en het bestaan van bepaalde ICT-legacy hierbinnen, een belangrijke oorzaak voor de in dit rapport geconstateerde problemen op het gebied van toegangsmanagement (zie paragraaf 5.2.2).

De diensten zijn tijdens het onderzoek van de CTIVD reeds gestart met het doorvoeren van verbeteringen met betrekking tot het versnipperde datalandschap en het voeren van een centrale regie op de verdere verwerking van bulkdatasets.
De diensten hebben tijdens het onderzoek van de CTIVD reeds ingezet op verbeteringen met betrekking tot het versnipperde datalandschap en het voeren van een centrale regie op de verdere verwerking van bulkdatasets. Op een aantal vlakken is gewerkt aan dataconvergentie (d.w.z het bij elkaar brengen van data) en het verplaatsen van bulkdatasets naar ICT-systemen die beter zijn ingericht om te kunnen voldoen aan de specifieke regels voor bulkdatasets. Ook hebben de diensten gewerkt aan een verbetering van het overzicht van de bulkdatasets die zij verwerken. Tot slot hebben de diensten gewerkt aan nieuwe beleidsplannen waarin de processen voor bulkdatasets (beter) zijn vastgelegd.

Aanbeveling 3
Werk verder aan de reeds ingezette dataconvergentie en de versterking van de centrale regie die wordt gevoerd op de verdere verwering van bulkdatasets.

4 Bepalen van het toegangsregime

Hoofdstuk 4 – Bepalen van het toegangsregime



4.1 Inleiding en wettelijke criteria

De diensten zijn verplicht om een inhoudelijke beoordeling te maken van de mate waarin het gebruik van een bulkdataset een privacyinbreuk met zich meebrengt. Op basis van deze beoordeling moeten de diensten een bepaald toegangsregime voorstellen, dat van toepassing zal zijn op de desbetreffende bulkdataset. Voor elk van de drie mogelijke toegangsregimes gelden nadere regels voor het verdere gebruik van de bulkdataset die op onderdelen van elkaar verschillen. De diensten mogen een bulkdataset pas gebruiken voor de uitvoering van wettelijke taken als het voorgestelde toegangsregime is vastgesteld door de minister.

In dit hoofdstuk wordt het proces bij de diensten van het beoordelen van de privacyinbreuk van bulkdatasets en het vaststellen van toegangsregimes getoetst.

Beoordeling van toegangsregimes voor bulkdatasets
De dienst beoordeelt in welke mate de verdere verwerking van een bulkdataset een beperking oplevert van het recht op de bescherming van de persoonlijke levenssfeer.
(Artikel 3 lid 1 van de Tijdelijke regeling)

Bij het maken van deze beoordeling moeten de diensten een aantal criteria wegen. Allereerst moeten de diensten beoordelen in welke mate de bulkdataset de volgende type gegevens bevat:

1) **Identificerende gegevens**
   Identificerende gegevens zijn gegevens die zicht geven op de identiteit van een persoon. De privacyinbreuk van een bulkdataset is groter, naarmate deze meer (verschillende soorten) identificerende gegevens bevat. Een combinatie van identificerende gegevens geeft namelijk een completer beeld van een persoon. Ook is de aanwezigheid van

sommige (combinaties van) identificerende gegevens, meer inbreukmakend dan van andere. Een Burgerservicenummer (BSN) in combinatie met de voor-en achternaam van een persoon vormt bijvoorbeeld een grotere inbreuk op de privacy van die persoon dan alleen een telefoonnummer of een adres in combinatie met een technisch kenmerk omdat het meer zicht geeft op de identiteit van de persoon.

2) Locatiegegevens
Locatiegegevens zijn gegevens die iets zeggen over de geografische locatie van een persoon. Bij de beoordeling van de privacyinbreuk in dit kader spelen de frequentie en nauwkeurigheid een rol. Adresgegevens zijn bijvoorbeeld statisch van aard en zeggen weinig over waar de bewoner zich op een bepaald moment bevindt. Met locatiegegevens van een mobiele telefoon kan een locatie van de gebruiker nauwkeuriger worden vastgesteld.

3) Netwerkgegevens
Netwerkgegevens zijn gegevens waarmee het (sociale) netwerk waarin een persoon zich bevindt, in kaart kan worden gebracht. Zo kan bijvoorbeeld aan de hand van telefoniegegevens worden vastgesteld dat er telefonisch contact is (geweest) tussen personen en met welke frequentie dit contact plaatsvindt of heeft plaatsgevonden.

4) Vertrouwelijke inhoudelijke gegevens
Hierbij gaat het om de inhoud van mail- of chatverkeer, of om bijvoorbeeld privéberichten op sociale media. Ook kan het gaan om andere typen gegevens die inzicht geven op inhoudelijke aspecten van iemands privéleven.

Naast een beschouwing van de hierboven genoemde criteria, moeten de diensten meewegen in welke mate de gegevens uit de bulkdataset openbaar toegankelijk zijn. De toegankelijkheid zegt iets over de inspanning die moet worden verricht om de gegevens te kunnen raadplegen. Gegevens die gemakkelijk door iedereen te raadplegen zijn, worden geacht doorgaans minder vertrouwelijk van aard te zijn, waardoor de privacyinbreuk als minder zwaar wordt beschouwd.

Wegingscriteria bij de beoordeling van de privacyinbreuk bij het gebruik van bulkdatasets

Bij de beoordeling (...) worden in ieder geval de volgende criteria betrokken:

a. *De mate waarin een bulkdataset inzicht geeft in bepaalde aspecten van het privéleven, waaronder identificerende gegevens, locaties, netwerk en vertrouwelijke inhoudelijke gegevens;*
b. *De mate waarin een bulkdataset voor eenieder toegankelijk is.*

(Artikel 3 lid 2 van de Tijdelijke regeling)

De diensten moeten het resultaat van hun beoordeling motiveren in een voorstel voor het plaatsen van een bulkdataset in het betreffende toegangsregime. Dit voorstel moet door de verantwoordelijke minister worden vastgesteld. Een bulkdataset mag pas worden gebruikt zodra een toegangsregime is vastgesteld. Het voorstel omvat het resultaat en verantwoording van de beoordeling van de privacyinbreuk die de verdere verwerking oplevert. De vaststelling van een toegangsregime moet aan de CTIVD worden gemeld, zodat de CTIVD dit in haar toezicht kan betrekken.

Er zijn drie mogelijke toegangsregimes: *standaard*, *beperkt* of *strikt beperkt*. Het gekozen toegangsregime is bepalend voor welke regels gelden voor het verdere gebruik van de bulkdataset. Allereerst zegt het toegangsregime iets over welke (groepen) functionarissen binnen de diensten gebruik mogen maken van de bulkdataset. Hoofdstuk 5 gaat verder in op de toetsing van de implementatie van (technische) maatregelen waarmee de toegang tot deze toegangsregimes wordt beperkt. Ook is het toegangsregime van een bulkdataset onder meer bepalend voor de termijn waarbinnen een beoordeling moet worden gemaakt of er een noodzaak bestaat om de gegevens in kwestie te verwijderen en te vernietigen. Hier gaat hoofdstuk 7 nader op in.

Standaard, beperkt en strikt beperkt toegangsregime

Aan de hand van de beoordeling van de wegingscriteria (zie vorige groene kader) stelt de minister vast of de verdere verwerking van een bulkdataset onderworpen wordt aan een:

a. Standaard toegangsregime
b. Beperkt toegangsregime
c. Strikt beperkt toegangsregime

(Artikel 3 lid 3 van de Tijdelijke regeling)

4.2 Beoordeling van het proces omtrent de bepaling van het toegangsregime

4.2.1 Het beoordelen van de inbreuk op de privacy

De diensten hebben gezamenlijk beleid voor het beoordelen van bulkdatasets en het toekennen van toegangsregimes.

De diensten voeren een gezamenlijk beleid voor de wijze waarop het beoordelen van bulkdatasets en het toekennen van toegangsregimes plaatsvindt. De toepassing van de maatregelen uit dit beleid dragen bij aan de positieve bevindingen die in dit hoofdstuk worden besproken. Verderop komt onder meer aan bod dat de beoordelingen die door beide diensten zijn uitgevoerd inhoudelijk consistent zijn, en bovendien navolgbaar zijn voor de CTIVD.

In het beleid is bepaald dat het inlichtingenteam waarvoor de bulkdataset wordt verworven, een voorstel schrijft voor de vaststelling van het toepasselijke toegangsregime. Dit gebeurt aan de hand van een sjabloon. Het voorstel bevat een beoordeling van de zwaarte van de privacyinbreuk die de verwerking van de bulkdataset met zich meebrengt. De diensten voeren de beoordeling uit aan de hand van een aantal vuistregels die invulling geven aan de elementen van het eerste wettelijke criterium (de mate waarin een bulkdataset inzicht geeft in bepaalde aspecten van het privéleven). Het tweede wettelijke criterium (de mate waarin de bulkdataset voor eenieder toegankelijk is) wordt ook meegenomen in de beoordeling.

Nadat het inlichtingenteam het voorstel heeft geschreven, wordt de afdeling Juridische Zaken betrokken. Zij kan eventueel nog wijzigingen in het voorstel doorvoeren. Het definitieve voorstel wordt in de vorm van een toestemmingsnota voorgelegd aan de dienstleiding en ter vaststelling aan de verantwoordelijke minister.

Er ontbreken duidelijke beleidsmatige uitgangspunten voor wanneer bulkdatasets in samenhang moeten worden beoordeeld.
In beginsel wordt elke bulkdataset afzonderlijk beoordeeld en wordt niet beschouwd of er samenhang is met andere bulkdatasets waarover de diensten beschikken. In enkele gevallen worden afzonderlijke bulkdatasets wel in samenhang beoordeeld. In de beslissing om bulkdatasets in samenhang te beoordelen lijken criteria zoals overlap in soort gegevens, tijdstip en wijze van verwerving doorslaggevend. Hiervoor is echter geen duidelijk beleid.

Ondanks dat de classificatie per bulkdataset afzonderlijk wordt gemaakt, is het wel degelijk van belang om bulkdatasets in samenhang te bekijken. Bulkdatasets kunnen uiteindelijk binnen een inlichtingenonderzoek immers ook worden gecombineerd. Het inzicht in mogelijke samenhang en het effect van gecombineerd gebruik op de privacyinbreuk kan daarom relevant zijn bij de bepaling van de toegangsregimes. De wet bevat hierover geen bepalingen.

Aanbeveling 4
Zorg voor een besliskader om te bepalen of de verdere verwerking van meerdere bulkdatasets (al dan niet) in samenhang moet worden gewogen om de privacyinbreuk daarvan (goed) te kunnen beoordelen.

Er vindt structureel intern multidisciplinair overleg plaats over het toekennen van een toegangsregime.
De diensten hebben gedurende de onderzoeksperiode het proces van beoordeling van de beperking van de privacy nader vormgegeven en toegepast. Dit heeft ertoe geleid dat er structureel overleg plaatsvindt over de indeling van bulkdatasets in toegangsregimes. Bij dit overleg zijn verschillende functionarissen en disciplines betrokken. Hierdoor zijn zowel de technische als juridische aspecten meegenomen bij de beoordeling.

De diensten maken consistente beoordelingen van de privacyinbreuk van bulkdatasets aan de hand van vuistregels die in het beleid zijn opgenomen.

Het beleid van de diensten bevat vuistregels over de toetsing en weging van de in bulkdatasets aanwezige identificerende gegevens, locatiegegevens, netwerkgegevens en vertrouwelijke, inhoudelijke gegevens en in hoeverre de bulkdataset openbaar toegankelijk is. De CTIVD heeft geconstateerd dat de vuistregels uit het beleid consistent worden toegepast in de praktijk en worden gemotiveerd in de toestemmingsverzoeken voor het toekennen van toegangsregimes. De vuistregels laten ruimte om, afhankelijk van de omstandigheden van het geval, af te wijken.

Uit het overzicht van alle bulkdatasets en toegangsregimes is ook gebleken dat voor zover de AIVD en de MIVD dezelfde bulkdatasets hebben beoordeeld, zij afzonderlijk van elkaar dezelfde toegangsregimes hebben voorgesteld.

De invulling en weging van het criterium voor openbare toegankelijkheid is discutabel.
Zoals hiervoor al is toegelicht, wordt ook meegewogen of een bulkdataset openbaar beschikbaar is (geweest). De uitkomst hiervan kan invloed hebben op het toe te kennen toegangsregime. Wanneer niet duidelijk is of gegevens openbaar beschikbaar zijn (geweest), proberen de diensten dit te achterhalen. Als dit niet mogelijk is, wordt door de diensten gesteld dat het onbekend is of de gegevens openbaar toegankelijk waren of wordt deze afweging gemaakt op basis van de aard van de gegevens. Dit doet zich bijvoorbeeld voor wanneer gegevens zijn ontvangen van een partnerdienst.

In die gevallen kiezen de diensten er soms voor de bulkdataset als openbaar toegankelijk aan te merken, terwijl zij dit niet met zekerheid hebben kunnen vaststellen. Op de vraag of is overwogen om gegevens van een partnerdienst daarom structureel als *niet openbaar* aan te merken, was het antwoord van de diensten dat niet de wijze van verwerven (verkrijging van een partnerdienst) centraal staat, maar de waarschijnlijke herkomst van de gegevens. Dit betekent dat bulkdatasets, die verkregen zijn van partnerdiensten, soms worden aangemerkt als openbaar toegankelijk terwijl de diensten niet hebben kunnen vaststellen of dit ook feitelijk klopt.

Ook zijn er gevallen waarin de diensten bulkdatasets die (kortstondig) op het internet (tegen betaling) werden aangeboden als openbaar toegankelijk beschouwen. Uit CTIVD-rapport nr. 79 (2024) blijkt reeds dat de privacyinbreuk van dergelijke bulkdatasets heel groot kan zijn, bijvoorbeeld omdat het kan gaan om *gegevens uit een datalek.* Hoewel het niet onrechtmatig is om deze bulkdatasets als openbaar toegankelijk aan te merken, is de CTIVD van oordeel dat de weging van het criterium voor openbare toegankelijkheid weinig zegt over de privacyinbreuk van de verwerking van dergelijke bulkdatasets.

Gegevens uit een datalek

Gegevens uit een datalek kunnen bijvoorbeeld gestolen zijn uit de interne systemen van bedrijven en instellingen bij een hack. Dergelijke gegevens worden soms commercieel op het internet aangeboden. Het betreft echter gegevens die door de oorspronkelijke eigenaar niet vrijwillig op het internet gezet.

Bulkdatasets die afkomstig zijn van commerciële partijen die tegen betaling worden verworven, worden soms ook gezien als openbaar toegankelijk. Gedurende het onderzoek van de CTIVD werd geen onderscheid gemaakt ten aanzien van de hoogte van het bedrag van de betaling.

Aanbeveling 5
Merk gegvens aan als niet openbaar toegankelijk wanneer niet feitelijk kan worden vastgesteld of de verworven gegevens openbaar toegankelijk zijn (geweest).

Scherp in regelgeving of beleid aan hoe dit criterium moet worden betrokken bij de beoordeling van de privacyinbreuk van bulkdatasets. Houd hierbij rekening met de omstandigheid dat gegevens uit een datalek openbaar toegankelijk kunnen zijn, maar doorgaans niet door de betrokkenen zelf openbaar zijn gemaakt.

De openbaarheid van gegevens is niet altijd bepalend voor de aard van de gegevens noch voor de mate van privacyinbreuk die de verwerking van deze gegevens met zich meebrengt.

4.2.2 Het vaststellen van toegangsregimes en melding daarvan aan de CTIVD

Het merendeel van de vastgestelde toegangsregimes is op tijd gemeld bij de CTIVD.
De diensten hebben gedurende de onderzoeksperiode in bijna alle gevallen de vaststelling van een toegangsregime terstond gemeld bij de CTIVD. In minder dan 5% van de gevallen meldden de diensten na meer dan acht dagen. Ook voldeden de meldingen aan de juiste vereisten. Alle vaststellingen waren bijvoorbeeld voorzien van een handtekening door de minister.

De inhoudelijke beoordeling van bulkdatasets en het gekozen toegangsregime was steeds navolgbaar voor de CTIVD.
De CTIVD beoordeelt sinds de invoering van de Tijdelijke regeling verdere verwerking bulkdatasets 2017 de meldingen van vastgestelde toegangsregimes. In verreweg de meeste gevallen is de inhoudelijke beoordeling van de privacyinbreuk en het gekozen toegangsregime navolgbaar voor de CTIVD. In enkele gevallen is de CTIVD het gesprek aangegaan met de diensten.

5 Toegangsmanagement bij bulkdatasets

Hoofdstuk 5 – Toegangsmanagement bij bulkdatasets



5.1 Inleiding en wettelijke criteria

Wanneer de diensten het toegangsregime voor een bulkdataset hebben vastgesteld, is het vervolgens van belang dat het toegangsregime wordt afgedwongen met behulp van technische maatregelen. Het proces voor het implementeren van deze maatregelen wordt in dit rapport toegangsmanagement genoemd. In dit hoofdstuk wordt het toegangsmanagement voor bulkdatasets binnen de diensten getoetst.

Toegangsmanagement

Toegangsmanagement is het treffen van maatregelen die toegang (of uitsluiting) tot gegevens afdwingen.

In hoofdstuk 4 is toegelicht dat bulkdatasets kunnen worden ingedeeld in een standaard, beperkt of strikt beperkt toegangsregime. Het standaard toegangsregime is de lichtste categorie. Alle medewerkers van de AIVD en de MIVD mogen toegang krijgen tot gegevens uit deze bulkdatasets, mits dat uit hoofde van hun functie nodig is voor de goede uitvoering van hun taken.

Standaard toegangsregime

De verkrijging van in bulkdatasets met een standaard toegangsregime opgenomen gegevens is uitsluitend toegestaan door binnen de dienst of ingevolge van artikel 91 van de wet ten behoeve van de AIVD werkzame ambtenaar onderscheidenlijk ingevolge artikel 92 ten behoeve van de MIVD werkzame ambtenaar, voor zover dat nodig is voor een goede uitvoering van de aan de betreffende ambtenaar opgedragen taak.

(Artikel 5 van de Tijdelijke regeling).

Het beperkte toegangsregime houdt in dat een beperkter aantal medewerkers binnen de diensten toegang mag hebben tot de gegevens dan bij het standaard toegangsregime. Het verkrijgen van gegevens is enkel toegestaan voor teams met een geldige teamtoestemming. Ook kan de data worden ingezien door medewerkers van bepaalde door het hoofd van een dienst aangewezen functiegroepen.

Beperkt toegangsregime

De verkrijging van in een bulkdatasets met een beperkt toegangsregime opgenomen gegevens is uitsluitend toegestaan door:

a. *Daartoe door het hoofd van de dienst aangewezen functiegroepen;*
b. *Een daartoe door het hoofd van de dienst aangewezen team op een daartoe strekkend verzoek van het unithoofd onderscheidenlijk het afdelingshoofd en na advies van de betrokken afdeling juridische zaken. Het verzoek bevat de reden waarom verkrijging van de in de bulkdataset opgenomen gegevens door het betreffende team noodzakelijk is. Een toestemming wordt verleend voor de duur van ten hoogste 12 maanden en kan telkens op een daartoe strekkend verzoek worden verlengd.*

(Artikel 6 van de Tijdelijke regeling)

Het strikt beperkt toegangsregime is het meest exclusieve toegangsregime voor bulkdatasets. Dit toegangsregime geldt voor bulkdatasets waarbij de inbreuk op grondrechten het grootst is. Gegevens uit bulkdatasets met een strikt beperkt toegangsregime mogen alleen worden geraadpleegd door medewerkers van teams met een geldige teamtoestemming. Verder mag de data slechts worden geraadpleegd op basis van naslagen. Hiervoor moet eerst een gemotiveerd naslagverzoek worden goedgekeurd door het teamhoofd, de teamleider of het bureauhoofd. Daarnaast kan de data worden ingezien door medewerkers van bepaalde daartoe door het hoofd van een dienst aangewezen functiegroepen. Net als bij het beperkte toegangsregime worden deze functiegroepen doorgaans aangewezen omdat deze medewerkers de gegevens nodig hebben voor ondersteunende taken die niet rechtstreeks bijdragen aan het inlichtingenproces (zie paragraaf 6.2.2).

Strikt beperkt toegangsregime

1. *De verkrijging van in bulkdatasets met een strikt beperkt toegangsregime opgenomen gegevens is uitsluitend toegestaan door:*
   a. *Daartoe door het hoofd van de dienst aangewezen functiegroepen.*
   b. *Een daartoe door het hoofd van de dienst aangewezen team op een daartoe strekkend verzoek van het unithoofd onderscheidenlijk het afdelingshoofd en na advies van de betrokken afdeling juridische zaken. Het verzoek bevat de reden waarom verkrijging van de in de bulkdataset opgenomen gegevens door het betreffende team noodzakelijk is.*

Een toestemming wordt verleend voor de duur van ten hoogste 12 maanden en kan telkens op een daartoe strekkend verzoek worden verlengd.

2. *De verkrijging van de gegevens door een ingevolge het eerste lid, onder b, aangewezen team, vindt slechts plaats op basis van kenmerken gerelateerd aan het desbetreffende onderzoek die door het teamhoofd onderscheidenlijk de teamleider dan wel het bureauhoofd zijn vastgesteld. Kenmerken worden voorzien van een toereikende motivering in relatie tot het onderzoek waarvoor ze dienen te worden toegepast.*

(Artikel 6 van de Tijdelijke regeling)

De hierboven beschreven regels hebben specifiek betrekking op het toegangsbeheer voor gegevens uit bulkdatasets. Deze regels bestaan uit algemene vereisten om onbevoegde gegevensverwerking, verlies en aantasting van gegevens te voorkomen. Zo moeten de diensten ook op basis van de zorgplicht uit artikel 24 van de Wiv 2017 maatregelen treffen van technische en organisatorische aard om verlies en aantasting van gegevens te voorkomen. Ook moeten zij maatregelen treffen tegen onbevoegde gegevensverwerking. Binnen dit scala aan maatregelen kan bijvoorbeeld worden gedacht aan de automatische registratie van het raadplegen van gegevens door medewerkers (gegevenslogging).

Zorgplicht voor onder meer het voorkomen van onbevoegde gegevensverwerking

1. *De hoofden van de diensten dragen er voorts zorg voor dat de technische, personele en organisatorische maatregelen in verband met de verwerking van gegevens in overeenstemming zijn met hetgeen bij of krachtens deze wet is bepaald.*
2. *Tot de maatregelen behoren in ieder geval:*
   a. *(...)*
   b. *De nodige voorzieningen van technische en organisatorische aard ter beveiliging van de gegevensverwerking tegen verlies of aantasting van gegevens, alsmede tegen onbevoegde gegevensverwerking*
   c. *De aanwijzing van personen die bij uitsluiting van anderen bevoegd zijn tot de bij aanwijzing vermelde werkzaamheden in het kader van de verwerking van gegevens.*

(Artikel 24 van de Wiv 2017)

5.2 Beoordeling van toegangsmanagement bij bulkdatasets

5.2.1 Toegangsmanagement bij bulkdatasets met een standaard toegangsregime

De diensten hebben toereikende maatregelen getroffen om ervoor te zorgen dat slechts medewerkers die dat nodig hebben voor de goede uitvoering van hun taak, toegang hebben tot gegevens uit bulkdatasets met een standaardtoegangsregime.

Uit het onderzoek van de CTIVD blijkt dat het toegangsmanagement van de diensten ten aanzien van bulkdatasets met een standaard toegangsregime toereikend is. De diensten dwingen op technische wijze af dat binnen het standaard toegangsregime slechts (inlichtingen)medewerkers toegang hebben tot bijzondere onderzoeksgegevens als zij dat nodig hebben voor hun taken. Ten aanzien van het toegangsmanagement bij bulkdatasets in het standaard toegangsregime heeft de CTIVD in het onderzoek geen onrechtmatigheden geconstateerd.

Hoewel het standaard regime het lichtste toegangsregime voor bulkdatasets betreft, betekent dit niet dat alle dienstmedewerkers toegang mogen krijgen tot deze gegevens. Toegang mag slechts worden verkregen als dat nodig is voor de goede taakuitvoering van de medewerker. Een belangrijke constatering hierbij is dat niet alle (inlichtingen)medewerkers toegang tot gegevens uit bulkdatasets die met een bijzondere bevoegdheid zijn verworven, nodig hebben voor de goede uitvoering van hun taken. Een voorbeeld is de Unit Veiligheidsonderzoeken (UVO). De UVO mag bij de uitvoering van veiligheidsonderzoeken géén gebruik maken van bijzondere bevoegdheden. Uit het onderzoek van de CTIVD is niet gebleken dat de UVO naslagen vericht in bulkdatasets die met een bijzondere bevoegdheid zijn verworven.

Veiligheidsonderzoeken

Veiligheidsonderzoeken worden uitgevoerd om te controleren of een persoon geschikt is om een vertrouwensfunctie uit te voeren. Een vertrouwensfunctie is een functie die de mogelijkheid biedt de nationale veiligheid te schaden, bijvoorbeeld als een persoon in zijn vertrouwensfunctie toegang heeft tot staatsgeheime informatie.

5.2.2 *Toegangsmanagement bij bulkdatasets met een beperkt en strikt beperkt toegangsregime*

De maatregelen die de diensten hebben getroffen om ervoor te zorgen dat slechts daartoe bevoegde dienstmedewerkers gegevens uit een bulkdataset met een (strikt) beperkt toegangsregime kunnen raadplegen zijn ontoereikend. De getroffen maatregelen vormen risico's en houden kwetsbaarheden in stand die onbevoegde gegevensverwerking mogelijk maken. Dit is onzorgvuldig.

De CTIVD heeft onderzocht op welke wijze de toegang wordt afgedwongen tot gegevens uit bulkdatasets met een beperkt en strikt beperkt toegangsregime. Daaruit bleek dat de wijze waarop de diensten dit technisch en procedureel hebben geïmplementeerd, risico's bevat die onbevoegde gegevensverwerking mogelijk maken. Concreet bestaat het risico dat dienstmedewerkers van teams zonder geldige teamtoestemming en/of zonder geldig naslagverzoek, onder bepaalde omstandigheden toch toegang kunnen krijgen tot gegevens uit (strikt) beperkte toegangsregimes. In een aantal gevallen hebben deze risico's zich ook daadwerkelijk verwezenlijkt (zie volgende bevinding).

Gedurende de onderzoeksperiode zijn er meerdere gevallen aan het licht gekomen waarbij dienstmedewerkers toegang hadden tot gegevens uit bulkdatasets met een (strikt) beperkt toegangsregime, terwijl zij daartoe niet (langer) bevoegd waren. Deze voorvallen zijn onrechtmatig.
Tijdens de onderzoeksperiode zijn er verschillende gevallen aan het licht gekomen waarbij bleek dat dienstmedewerkers toegang hadden tot gegevens uit bulkdatasets met een (strikt) beperkt toegangsregime, terwijl zij daartoe niet bevoegd waren. Deze voorvallen beschouwt de CTIVD als onrechtmatig. Er was immers sprake van onbevoegde gegevensverwerking.

Deels hebben deze incidenten te maken met de structurele gebreken in de wijze waarop toegangsmanagement technisch en procedureel is ingeregeld (zie vorige bevinding). Deels gaat het ook om incidenten die op zichzelf staan en meer te maken hebben met het versnipperde ICT-landschap op het gebied van bulkdatasets, zoals besproken in paragraaf 3.2.3. Het merendeel van de incidenten is zelfstandig door de diensten onderkend en gemeld bij de CTIVD.

Aanbeveling 6
De wijze waarop toegangsmanagement voor bulkdatasets met een (strikt) beperkt toegangsregime technisch en procedureel is geïmplementeerd, moet worden verbeterd op een manier die het risico op onrechtmatige gegevensverwerking mitigeert.

5.2.3 Logging van toegang en gebruik van gegevens

De technische wijze waarop wordt bijgehouden welke medewerkers toegang hebben gehad tot welke gegevens (gegevenslogging), is toereikend als maatregel tegen verlies of aantasting van gegevens.
Door middel van logging kan worden nagegaan wie toegang heeft gehad tot welke gegevens. Als er bijvoorbeeld sprake zou zijn van een datalek, dan kan met behulp van deze logging onderzocht worden wie de gegevens heeft opgevraagd. Hoewel dit de verloren data waarschijnlijk niet zal veiligstellen, kan hiermee wel de oorzaak van het datalek worden ontdekt.

De technische wijze waarop wordt bijgehouden welke medewerkers toegang hebben gehad tot welke gegevens (gegevenslogging) als maatregel tegen onbevoegde gegevensverwerking is niet toereikend. Dit is onzorgvuldig.
Hoewel kan worden nagegaan wie welke data heeft bevraagd, kan niet goed worden gecontroleerd of de toegang tot bepaalde gegevens op dat moment terecht was. De huidige manier van logging maakt het maar tot op zekere hoogte mogelijk om vast te stellen of iemand die toegang heeft gehad tot bepaalde gegevens, daartoe de juiste autorisaties had en/of deze terecht waren toegekend. Er kan dus niet worden vastgesteld of er in situaties onbevoegde gegevensverwerking heeft plaatsgevonden. Dit ziet de CTIVD als een onzorgvuldigheid.

Daarnaast is het op basis van de logging moeilijk te achterhalen wanneer de gegevens door medewerkers verder zijn verwerkt (en dus niet alleen opgevraagd in een zoekslag) en of dit gebruik bevoegd was. Dit onderscheid wordt niet gemaakt in de logging.

Een oorzaak van deze problemen is dat de regels voor autorisaties soms wijzigen. Hierdoor is het niet duidelijk welke autorisatieregels gebruikt werden op het moment van dataverwerking. Ook wisselen medewerkers van afdeling. Hierdoor is het niet meer te achterhalen of de medewerker op een bepaald moment in tijd al dan niet terecht toegang had tot bepaalde data.

Aanbeveling 7

De logging van de toegang tot bulkdatasets moet worden verbeterd. Daarnaast moeten wijzigingen in autorisaties beter inzichtelijk worden gemaakt. Achteraf moet beter kunnen worden vastgesteld wie al dan niet terecht toegang heeft gehad tot een bulkdataset en daarvan gebruik heeft gemaakt.

6 Gebruik van bulkdatasets

Hoofdstuk 6 – Gebruik van bulkdatasets



6.1 Inleiding en wettelijke criteria

De diensten gebruiken gegevens uit bulkdatasets bij de onderzoeken die zij uitvoeren in het kader van hun taakuitvoering, zoals de onderzoeken naar dreigingen uit andere landen en terrorisme. Daarnaast worden gegevens uit bulkdatasets volgens de diensten gebruikt ter ondersteuning van hun taakuitvoering. Hierbij kan bijvoorbeeld worden gedacht aan het gebruik van gegevens voor de verbetering van modellen of applicaties of ter ondersteuning van de inzet van bevoegdheden. De diensten zijn bevoegd tot het verwerken van gegevens uit bulkdatasets op basis van hun algemene wettelijke bevoegdheid tot gegevensverwerking.

Bevoegdheid tot gegevensverwerking

De diensten zijn bevoegd tot het verwerken van gegevens met inachtneming van de eisen die bij of krachtens deze wet of de wet veiligheidsonderzoeken daaraan zijn gesteld.

(Artikel 17 van de Wiv 2017)

Bulkdatasets kunnen verschillende soorten gegevens bevatten en worden daardoor op verschillende manieren door de diensten gebruikt. Bulkdatasets kunnen bijvoorbeeld identificerende gegevens bevatten. Dergelijke gegevens slaan op feitelijke kenmerken die beschrijven wie of wat je bent. Gedacht kan worden aan postcodes, geboortedata en paspoortnummers. In het rapport van de Evaluatiecommissie Wiv 2017 worden een aantal voorbeelden gegeven van bulkdatasets met identificerende gegevens die door de diensten worden gebruikt: 1) een verzameling van e-mailadressen, 2) een bulkregister van een telecommunicatie-aanbieder met abonneegegevens, 3) het Handelsregister van de Kamer van Koophandel (KvK) en 4) het kentekenregister (Basisregistratie Voertuigen) van de RDW.

De diensten kunnen dergelijke bulkdatasets gebruiken om kenmerken van personen of organisaties na te slaan, om zo nieuwe informatie te ontdekken die waardevol is voor het onderzoek van de diensten. Met het uitvoeren van een naslag kan bijvoorbeeld worden vastgesteld welk telefoonnummer wordt gebruikt door welke persoon of welk persoon op een bepaald moment zich op een bepaalde locatie bevond.

Naast (statische) identificerende gegevens kunnen bulkdatasets ook complexere gegevens bevatten. Een voorbeeld zijn de passagiersgegevens van luchtvaartmaatschappijen die zij verplicht moeten delen met de Koninklijke Marechaussee. De diensten hebben ook de beschikking over deze gegevens in de vorm van een bulkdataset (zie toezichtrapport nr. 71 (2020) dat betrekking heeft op dit onderwerp). De passagiersgegevens bevatten naast identificerende gegevens ook gegevens over reisbewegingen van personen. Bulkdatasets met dergelijke meer complexe gegevens kunnen bijvoorbeeld door middel van data-analyse worden gebruikt om dreigingen te identificeren en te onderkennen die de diensten nog niet eerder in beeld hadden.

Voorbeelden van het gebruik van bulkdatasets

Gebruik registers van Nederlandse medeoverheden of organisaties
De diensten maken ook gebruik van register-bulkdata van Nederlandse medeoverheden zoals de Basisregistratie Personen (BRP). De BRP bevat persoonsgegevens van Nederlandse ingezetenen en van personen die Nederland hebben verlaten. De AIVD gebruikt deze gegevens bijvoorbeeld bij het uitbrengen van een ambtsbericht over een persoon, om de naam en geboortedatum van een persoon te kunnen onderbouwen. Op deze wijze is voor de ontvanger, bijvoorbeeld het Openbaar Ministerie, direct te verifiëren over wie een ambtsbericht gaat. De diensten maken gebruik van bulkdatasets van het RDW en KVK. De diensten gebruiken betreffende bulkdatasets niet alleen voor inlichtingenonderzoek, maar bijvoorbeeld ook voor veiligheidsonderzoeken ten behoeve van het afgeven van een Verklaring Geen Bezwaar (VGB) wat o.a, het personeel van de diensten nodig heeft om hier werkzaam te zijn. Daarnaast kan het KvK bijvoorbeeld gebruikt worden om financiële en eigendomsgegevens van een bedrijf dat in opdracht van defensie werkt (defensie-industrie) te kunnen onderzoeken.

In dit hoofdstuk wordt het gebruik van gegevens uit bulkdatasets door de diensten voor de (ondersteuning van de) taakuitvoering getoetst aan de daaraan te stellen wettelijke vereisten. Belangrijk hierbij zijn de vereisten van doelbinding en een behoorlijke en zorgvuldige gegevensverwerking op basis van artikel 18 van de Wiv 2017. Doelbinding houdt in dat gegevens alleen voor een bepaald doel in het kader van de uitvoering van de wet, en dus niet zomaar, mogen worden verwerkt.

Daarnaast zijn de diensten verplicht ervoor zorg te dragen dat gegevens behoorlijk en zorgvuldig verwerkt worden. Het criterium van behoorlijkheid is verbonden met de uitvoering van het proportionaliteitsvereiste. Om te voldoen aan het behoorlijkheidsvereiste moet de beperking in

de fundamentele rechten die plaatsvindt bij de verwerking van gegevens in verhouding staan tot het beoogde doel. Zorgvuldige gegevensverwerking heeft betrekking op het waarborgen van de juistheid en actualiteit van de gegevens die worden verwerkt. Het waarborgen van de juistheid en actualiteit van gegevens is van belang voor de betrouwbaarheid van inlichtingen.

Doelbinding en behoorlijke en zorgvuldige gegevensverwerking

1. *De verwerking van gegevens vindt slechts plaats voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering van deze wet of de wet veiligheidsonderzoeken.*
2. *De verwerking van gegevens van gegevens geschiedt in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze.*

(Artikel 18 lid 1 en 2 van de Wiv 2017)

6.2 Beoordeling van het gebruiken van bulkdatasets

6.2.1 Gebruik van bulkdatasets bij de uitvoering van wettelijke taken

Bulkdatasets zijn van groot belang voor de goede uitvoering van de wettelijke taken van de diensten.
In het onderzoek heeft de CTIVD in een casestudie een select aantal bulkdatasets van de diensten nader onderzocht. Daarnaast houdt de CTIVD toezicht in het kader van de Tijdelijke Wet wanneer er door de minister een nieuwe eindtermijn wordt vastgesteld voor bulkdatasets die met een bijzondere bevoegdheid zijn verworven (zie hoofdstuk 7). Aan de hand van zowel de casestudie van de CTIVD als het toezicht op het vaststellen van nieuwe gebruikstermijnen van bulkdatasets heeft de CTIVD een algemeen beeld opgedaan over het belang van de verwerking van de gegevens uit bulkdatasets door de diensten. De motivatie van de diensten van de noodzakelijkheid en opbrengst van het gebruik van de betreffende bulkdatasets in de toestemmingsnota's heeft aangetoond dat het gebruik van bulkdatasets van groot belang is voor de uitvoering van hun wettelijke taken.

Voorbeelden van opbrengst uit bulkdatasets

De diensten kunnen gegevens uit (gelekte) bulkdatasets gebruiken om informatie over hun targets te krijgen en om bestaande informatie te verrijken. Door diverse gegevens te combineren, kunnen diensten vaststellen of een persoon gelieerd is aan een statelijke actor of terroristische groepering. Dit kan de diensten in staat stellen om bijzondere bevoegdheden, zoals een tap, juist spaarzamer en gerichter in te zetten, in plaats van deze breed toe te passen.

Bij het monitoren van Russische dreigingen — waarbij complexe netwerken van spionage en sabotage worden ingezet — worden bulkdatasets gebruikt voor de eerste validatie van

vermoedelijke betrokkenen. Daarnaast is bulkdata van groot belang voor de veiligheid van vitale infrastructuur, zoals de Noordzee. Hierbij wordt de data gebruikt om patronen te analyseren, bijvoorbeeld om de aard en intentie van buitenlandse scheepvaartbewegingen te begrijpen.

Het belang van het gebruik van bulkdatasets voor het werk van de diensten in het kader van nationale veiligheid kwam al aan bod in het rapport van de evaluatiecommissie Wiv 2017 uit 2020 (pagina's 40 t/m 42). In één voorbeeld van de opbrengst van een bulkdataset wist de AIVD Nederlandse uitreizigers die zich hadden aangesloten bij IS te onderkennen op basis van locatie metadata uit een bulkdataset. Een ander voorbeeld betreft een casus waarin gegevens uit een bulkdataset door de MIVD gebruikt zijn om Nederlandse militairen in Afghanistan te beschermen.

De wijze waarop binnen het inlichtingenonderzoek wordt gewerkt met bulkdatasets voldoet aan het principe van behoorlijke gegevensverwerking.

In de onderzochte gevallen was sprake van de verwerking van identificerende gegevens uit bulkdatasets. Deze bulkdatasets worden door de diensten in het inlichtingenproces onderzocht door middel van naslagen. Dit betekent dat er gericht gezocht wordt in deze bulkdatasets op specifieke kenmerken. Het is daarmee niet zo dat alle gegevens uit de bulkdataset worden onderzocht. De inbreuk op fundamentele rechten wordt door deze manier van werken geminimaliseerd. Dit draagt bij aan de proportionaliteit van het verwerken van de gegevens en daarmee aan behoorlijke gegevensverwerking.

De CTIVD heeft bij het onderzoek voor dit rapport het gebruik van een aantal bulkdatasets door de diensten nader onderzocht aan de hand van de eerdergenoemde casestudie. In de casestudie is onder meer gekeken naar de logging van het gebruik van de bulkdatasets. Uit zowel de logging als de overige bevindingen uit de casestudie blijkt dat er geen sprake was van afwijkend gebruik van de bulkdatasets. Er zijn geen onregelmatigheden of bijzonderheden geconstateerd in het gebruik van de gegevens. Zo zijn er bijvoorbeeld geen aanwijzingen gevonden voor het gebruik van onbehoorlijke algoritmen bij de analyse van de gegevens door de diensten. De CTIVD heeft geen signalen geconstateerd die duiden op onbehoorlijk of onzorgvuldig gebruik.

Bij het gebruik van bulkdatasets zijn verbeteringen mogelijk om de opbrengst uit bulkdatasets beter in kaart te brengen.

Het is om verschillende redenen van belang dat de diensten in beeld hebben (of kunnen krijgen) wat de opbrengst is van bulkdatasets in het inlichtingenproces. Dit kan enerzijds van belang zijn om de doeltreffendheid van het werk te vergroten (doordat men inzicht krijgt in wat werkt en wat niet). Anderzijds is het ook van belang voor de rechtmatigheid van het werk van de diensten. Dit inzicht is namelijk van belang om te kunnen beargumenteren waarom het gebruik van bulkdatasets noodzakelijk is. Noodzakelijkheid is een belangrijk rechtmatigheidscriterium dat op verschillende plaatsten in dit rapport aan bod komt.

Bij het gebruik van bulkdatasets in het inlichtingenproces door de AIVD en MIVD zijn verbeteringen mogelijk bij het in kaart brengen van de opbrengst. Concreet kunnen er nadere stappen worden gezet op het gebied van (al dan niet geautomatiseerde) *datalineage*. Hiermee zou op geautomatiseerde wijze in beeld kunnen worden gebracht in hoeverre welke bulkdatasets bijdragen aan het inlichtingenproces. Ook zou inzichtelijk kunnen worden gemaakt welke feiten in inlichtingenproducten zoals inlichtingenanalyses of -berichten onderbouwd zijn met gegevens uit bulkdatasets.

Datalineage

Het (via een geautomatiseerd systeem) inzichtelijk maken van de volledige levenscyclus van gegevens binnen een organisatie. Hiermee worden de herkomst van de data, de verwerking en de uiteindelijke bestemming in kaart gebracht.

Aanbeveling 8

Onderzoek de state-of-the-art mogelijkheden voor de toepassing van (geautomatiseerde) datalineage. Voer op basis hiervan verbeteringen door in de huidige wijze van datalineage.

6.2.2 Gebruik van bulkdatasets ter ondersteuning van de uitvoering van wettelijke taken

De diensten gebruiken bulkdatasets ter ondersteuning van de taakuitvoering zonder dat daarbij de regels en waarborgen voor bulkdatasets worden nageleefd. Dit is onrechtmatig.

De CTIVD constateert dat bepaalde afdelingen van de diensten gebruikmaken van bulkdatasets zonder daarbij de regels en waarborgen voor bulkdatasets na te leven. Het betreft gevallen waarbij volgens de diensten bulkdatasets niet rechtstreeks ten behoeve van inlichtingen, maar ter ondersteuning van de taakuitvoering worden gebruikt.

Gegevensverwerking ter ondersteuning van de taakuitvoering

De diensten maken onderscheid tussen gegevensverwerking in het kader van hun wettelijke taken en *ter ondersteuning van hun taakuitvoering*. In dit tweede geval worden de gegevens niet rechtstreeks in het inlichtingenproces gebruikt. In plaats daarvan worden ze gebruikt voor ondersteunende activiteiten zoals de verbetering van modellen of applicaties. Ook stellen de diensten in bepaalde gevallen dat als zij gegevens gebruiken ter ondersteuning van de inzet van bevoegdheden dat dit moet worden gezien als gegevensverwerking ter ondersteuning van de taakuitvoering.

De diensten hebben hiermee een onderscheid tussen bulkdatasets gecreëerd op grond waarvan zij de bulkdatasets die ter ondersteuning van de taakuitvoering worden gebruikt uitzonderen van

de gebruikelijke regels en waarborgen voor bulkdatasets. Dit heeft tot gevolg dat bij deze verwerking van bulkdatasets de toepasselijke regels niet worden nageleefd. Als gevolg hiervan worden wettelijke bewaartermijnen en het datareductiestelsel niet toegepast en geen toegangsregimes bepaald. Wel wijzen de diensten erop dat als gegevens ter ondersteuning van de taakuitvoering worden verwerkt, er op basis van functiescheiding slechts een beperkt aantal medewerkers toegang heeft tot de gegevens.

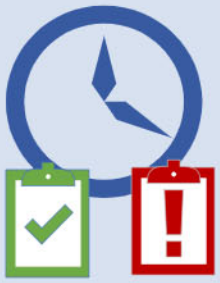
Hoewel de functiescheiding die de diensten hebben aangebracht in de praktijk een redelijke waarborg is om de daarmee gemoeide privacyinbreuk in te perken, constateert de CTIVD dat er geen wettelijke grondslag bestaat om de verwerking van bulkdatasets ter ondersteuning van de taakuitvoering anders te behandelen dan reguliere verwerking. De Tijdelijke regeling stelt bijvoorbeeld dat alle bulkdatasets moeten worden beoordeeld en ingedeeld in een toegangsregime. Daarop worden geen uitzonderingen gemaakt. Ook maakt de wet geen uitzonderingen voor bewaartermijnen van bulkdatasets die met een bijzondere bevoegdheid zijn verworven (Tw) en de verplichting om gegevens die met bijzondere bevoegdheid zijn verworven zo spoedig mogelijke op relevantie te beoordelen (artikel 27 van de Wiv 2017). Voorop dient te worden gesteld dat ook wanneer bulkdatasets ter ondersteuning van de taakuitvoering worden verwerkt, er sprake is van een privacyinbreuk.

Aanbeveling 9

Zorg ervoor dat gegevens uit bulkdatasets ter ondersteuning van de taakuitvoering ook rechtmatig verder worden verwerkt. Overweeg om bij de herziening van de Wiv 2017, een wettelijke grondslag te creëren indien het noodzakelijk blijkt om ter ondersteuning van de taakuitvoering bulkdatasets te verwerken. Specifieer nader welke verwerkingsdoeleinden kunnen worden aangemerkt als ter ondersteuning van de taakuitvoering. Het gebruiken van gegevens bij de inzet van bevoegdheden zou ook gewoon als taakuitvoering gezien kunnen worden. Leg naast het creëren van een grondslag wettelijk vast welke eisen gelden om te voorzien in passende waarborgen die recht doen aan de privacyinbreuk. Functiescheiding zoals in onderhavige gevallen is ingericht, kan hiervan een onderdeel zijn.

7 Beoordeling noodzaak tot verwijdering en nieuwe gebruikstermijnen

Hoofdstuk 7 – Periodieke beoordeling & Gebruikstermijnen



7.1 Inleiding en wettelijke criteria

Het bewaren en gebruiken van persoonsgegevens door de diensten vormt een inbreuk op het recht op privacy van de betrokken personen. Er zijn daarom wettelijke regels die bepalen hoe lang de diensten gegevens mogen bewaren en gebruiken, waarna deze moeten worden vernietigd. Voor bulkdatasets gelden specifieke regels voor bewaartermijnen. De naleving van deze regels wordt in dit hoofdstuk getoetst.

Welke wettelijke criteria aangaande de bewaartermijn van een bulkdataset van toepassing zijn, hangt af van de wijze waarop deze door een dienst is verworven. Er gelden twee verschillende wettelijke regimes, enerzijds voor bulkdatasets die met de inzet van een *algemene bevoegdheid* van een dienst zijn verworven en anderzijds voor bulkdatasets die met een *bijzondere bevoegdheid* zijn verworven. In dit rapport worden deze respectievelijk aangeduid als A-bulkdatasets en B-bulkdatasets.

Gegevensverzameling op grond van algemene en bijzondere bevoegdheden

De diensten hebben op grond van artikel 25 van de Wiv 2017 een algemene bevoegdheid om (persoons)gegevens te verzamelen. Hierbij gaat het om openbaar toegankelijke gegevens, (commercieel) aangekochte gegevens, gegevens afkomstig van informanten, waaronder andere overheidsorganisaties, en gegevens verkregen van buitenlandse inlichtingendiensten.

De wet kent ook bijzondere bevoegdheden toe aan de diensten waarmee zij gegevens kunnen verzamelen. Hierbij gaat het om de bevoegdheden genoemd in paragraaf 3.2.5. van de Wiv 2017. Gedacht kan worden aan de inzet van agenten (artikel 41), de hackbevoegdheid (artikel 45) en de tap-bevoegdheid (artikel 47).

Een bijzondere bevoegdheid wordt door de wetgever gezien als een zwaarder middel dan de inzet van een algemene bevoegdheid. Bij de meeste bijzondere bevoegdheden is vooraf toestemming van de minister en/of een rechtmatigheidstoets van de Toetsingscommissie Inzet Bevoegdheden (TIB) vereist.

De inzet van alle bevoegdheden door de diensten moet op basis van artikel 26 van de Wiv 2017 voldoen aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. Dat betekent dat de diensten alleen bevoegdheden mogen inzetten als dat echt nodig is (noodzakelijkheid), als het in verhouding staat tot het beoogde doel (proportionaliteit) en dat het lichtste middel in termen van inbreuk op fundamentele rechten eerst wordt ingezet (subsidiariteit).

7.1.1 Wettelijk regels bij A-bulkdatasets

Gegevens die de diensten hebben verzameld, moeten worden verwijderd wanneer zij, gelet op het doel waarvoor zij worden verwerkt, geen betekenis (meer) hebben (artikel 20 lid 1. van de Wiv 2017). De verwijderde gegevens worden vernietigd, tenzij wettelijke regels omtrent bewaring daaraan in de weg staan. Voor A-bulkdatasets gelden er vaste termijnen waarna er door het hoofd van de betreffende dienst moet worden beoordeeld of er een noodzaak tot verwijdering bestaat. De termijnen zijn gekoppeld aan de verschillende toegangsregimes die voor bulkdatasets worden ingesteld.

Bulkdatasets met een standaard, beperkt en strikt beperkt toegangsregime moeten na respectievelijk 36, 24 en 12 maanden worden beoordeeld op de noodzaak tot verwijdering. In paragraaf 4.1 is beschreven dat het toegangsregime van de bulkdataset door de diensten bepaald moet worden op basis van de mate waarin de verwerking ervan een privacy-inbreuk voor de betrokkenen met zich meebrengt, gelet op de inhoud van de bulkdataset.

Periodieke beoordeling noodzaak tot verwijdering bulkdatasets

Onverminderd het bepaalde in artikel 20 lid 1 van de Wiv 2017, wordt door het hoofd van de dienst, nadat de set betekenis heeft gekregen in de zin van artikel 20 van de wet, periodiek beoordeeld of de betreffende bulkdataset dient te worden verwijderd. Deze beoordeling vindt plaats:

a. ten aanzien van een bulkdataset met een standaard toegangsregime na ten hoogste 36 maanden;
b. ten aanzien van een bulkdataset met een beperkt toegangsregime na ten hoogste 24 maanden;
c. ten aanzien van een bulkdataset met een strikt beperkt toegangsregime na ten hoogste 12 maanden;

(Artikel 8 van de Tijdelijke regeling)

7.1.2 Wettelijk regels bij B-bulkdatasets

Voor B-bulkdataset zijn andere wettelijke regels op de bewaar- en gebruikstermijnen van toepassing als voor A-bulkdatasets. De Tijdelijke wet bepaalt dat de eindtermijn voor het gebruik van gegevens uit B-bulkdatasets anderhalf jaar is. Na afloop van deze termijn worden de gegevens in de bulkdataset vernietigd. Van de vernietiging wordt terstond mededeling gedaan aan de CTIVD.

Als het nodig is de gegevens langer te bewaren, kan herhaaldelijk een nieuwe eindtermijn voor het gebruik van de dataset worden vastgesteld. Hierbij dient aan de minister te worden gemotiveerd dat een nieuwe eindtermijn noodzakelijk, proportioneel en subsidiair is. Wanneer de minister een nieuwe eindtermijn heeft vastgesteld, wordt hiervan melding gedaan aan de CTIVD. De CTIVD houdt vervolgens bindend toezicht op de nieuwe eindtermijn. Wanneer de CTIVD van oordeel is dat een nieuwe eindtermijn onrechtmatig is, kan zij daaraan het gevolg verbinden dat de bulkdataset (alsnog) moet worden vernietigd. De verantwoordelijke minister kan tegen het oordeel in beroep.

Nieuwe eindtermijn voor B-bulkdatasets in de Tijdelijke wet

1. *Onze minister kan (...) worden verzocht om te beoordelen of een nieuwe eindtermijn dient te worden vastgesteld voor het gebruik van een bulkdataset voor enig lopend onderzoek (...).*
2. *Een verzoek om toestemming omvat (...):*
   (....)
   d. de reden waarom een nieuwe eindtermijn voor gebruik van de bulkdatasets noodzakelijk is;
   e. de reden waarom een nieuwe eindtermijn voor gebruik van de bulkdatasets vanuit de daarmee gepaard gaande beperking van het recht op de persoonlijke levenssfeer van de personen wier gegevens in de bulkdataset zijn opgenomen proportioneel en subsidiair is;
   (...)

(Artikel 14ba van de Tijdelijk wet)

Waarom aparte wettelijke regels omtrent gebruik- en bewaartermijnen voor B-bulkdatasets?

De regelgeving voor bewaartermijnen van B-bulkdatasets kent een zekere voorgeschiedenis. Voor de inwerkintreding van de Tijdelijke wet was artikel 27 van de Wiv 2017 leidend voor de bewaartermijnen van B-bulkdatasets. Dit artikel bepaalt dat *alle gegevens die met een bijzondere bevoegdheid zijn verworven*, zo spoedig mogelijk, maar uiterlijk binnen 12 maanden, met een enkele mogelijke verlenging tot 18 maanden, moeten worden onderzocht op hun relevantie voor het onderzoek waarvoor zij zijn verworven.

Gegevens die niet relevant zijn voor het onderzoek of enig ander onderzoek van de diensten, moeten vervolgens terstond worden vernietigd. Op grond van dit artikel konden B-bulkdatasets

die niet binnen anderhalf jaar op hun relevantie waren beoordeeld, niet langer dan anderhalf jaar worden bewaard, terwijl dat soms wel voor de onderzoeken van de diensten noodzakelijk is. Dit is een van de knelpunten dat is opgelost met de invoering van de Tijdelijke Wet.

Met de Tijdelijke wet heeft de wetgever niet gekozen voor een uniforme set regels voor de bewaartermijnen van alle bulkdatasets, ongeacht de verwervingsgrond. In plaats daarvan heeft de wetgever slechts beoogd voorzieningen te treffen voor B-bulkdatasets om bij die gevallen de regelgeving beter aan te laten sluiten op de praktijk. Voor de bewaartermijnen van A-bulkdatasets bestond ditzelfde knelpunt niet, omdat artikel 27 van de Wiv 2017 geen betrekking heeft op gegevens die met algemene bevoegdheden zijn vergaard.

Op grond van de Tijdelijke wet is de betrokken minister bevoegd een nieuwe gebruikstermijn voor B-bulkdatasets vast te stellen. De Tijdelijke Wet regelt bovendien, in afwijking van artikel 27 van de Wiv 2017, dat B-bulkdatasets niet langer *zo spoedig mogelijk* op relevantie beoordeeld hoeven te worden. Beide punten passen beter bij de wijze waarop de diensten met bulkdatasets werken in de praktijk.

Bulkdatasets worden doorgaans gebruikt als naslagwerk, hetgeen betekent dat niet altijd op voorhand kan worden bepaald of bepaalde gegevens uit de bulkdataset relevant zijn voor een onderzoek van de diensten. Daarnaast kunnen bulkdatasets voor periodes van meerdere jaren bruikbaar zijn voor de onderzoeken van de diensten, waardoor het noodzakelijk kan zijn om bepaalde bulkdatasets langer dan anderhalf jaar te bewaren.

7.2 Beoordeling van de processen omtrent periodieke beoordelingen en nieuwe gebruikstermijnen

7.2.1 Periodieke beoordeling van de noodzaak tot verwijdering (bij A-bulkdatasets)

In paragraaf 7.1 is uitgelegd dat A-bulkdatasets door het hoofd van de betrokken dienst periodiek moeten worden beoordeeld op de vraag of verwijdering noodzakelijk is. Indien de bulkdataset geen betekenis meer heeft voor het onderzoek van de diensten, dient deze te worden verwijderd.

De diensten beschikken over een werkproces op basis waarvan de periodieke beoordeling van de noodzaak tot verwijdering van A-bulkdatasets wordt gemaakt en voorgelegd aan het betrokken diensthoofd.
De CTIVD stelt vast dat de diensten een werkproces hebben ingericht op basis waarvan de periodieke beoordeling van de noodzaak tot verwijdering van A-bulkdatasets wordt gemaakt en voorgelegd aan het betrokken diensthoofd. In de regel wordt dit proces nageleefd.

De CTIVD heeft in het onderzoek een aantal A-bulkdatasets aangetroffen waarbij de periodieke beoordeling van de noodzaak tot verwijdering niet (op tijd) heeft plaatsgevonden. Dit is onrechtmatig.

De CTIVD heeft onderzocht op basis van een steekproef of A-bulkdatasets van de diensten tijdig worden beoordeeld. In een aantal gevallen heeft de CTIVD een aantal A-bulkdatasets aangetroffen waarbij de herbeoordeling niet (op tijd) heeft plaatsgevonden. Dit is onrechtmatig.

Aanbeveling 10
Onderzoek welke A-bulkdatasets ten onrechte (nog) niet zijn onderworpen aan een periodieke beoordeling van de noodzaak tot verwijdering. Zorg ervoor dat de periodieke beoordeling alsnog plaatsvindt.

Aanbeveling 11
Tref nadere maatregelen om ervoor te zorgen dat de periodieke beoordeling van de noodzaak tot verwijdering van A-bulkdatasets tijdig plaatsvindt.

De CTIVD heeft in het onderzoek geen voorbeelden aangetroffen waarbij de uitkomst van de beoordeling van de noodzaak tot verwijdering van een A-bulkdataset naar het oordeel van de CTIVD onnavolgbaar was.
De CTIVD heeft op basis van een steekproef onderzocht of de beoordeling van de noodzaak tot verwijdering van A-bulkdatasets inhoudelijk goed gemotiveerd is. De CTIVD heeft geen voorbeelden aangetroffen waarbij de motivering naar het oordeel van de CTIVD onnavolgbaar was.

De CTIVD ziet de meerwaarde van de periodieke herbeoordeling. De periodieke beoordeling heeft in sommige gevallen geleid tot de vernietiging van bulkdatasets.

7.2.2 Nieuwe gebruikstermijnen (bij B-bulkdatasets)

De CTIVD heeft sinds de invoering van de Tijdelijke wet geen gebruik gemaakt van haar bindende bevoegdheid ten aanzien van nieuwe eindtermijnen voor B-bulkdatasets.
Op 1 juli 2024 is de Tijdelijke Wet inwerking getreden. Op basis van deze wet beoordeelt de CTIVD de rechtmatigheid van nieuwe eindtermijnen voor B-bulkdatasets die door de minister worden vastgesteld. Bij een nieuwe eindtermijn moet de noodzakelijkheid, proportionaliteit en subsidiariteit door de diensten worden gemotiveerd. De CTIVD heeft tot nu toe geen gebruik gemaakt van haar bindende bevoegdheid om de vaststelling van een nieuwe eindtermijn als onrechtmatig te beoordelen en daaraan gevolgen te verbinden. In een geval zag de CTIVD aanleiding om haar bindende bevoegdheid in te zetten. De CTIVD heeft de betreffende dienst hiervan op de hoogte gesteld naar aanleiding waarvan de betreffende dienst besloot het verzoek voor een nieuwe eindtermijn in te trekken en de data niet langer te bewaren dan de oorspronkelijke bewaartermijn toestond. Hiermee was de noodzaak voor de CTIVD voor het inzetten van haar bindende bevoegdheid weggenomen. Dit geval heeft aangetoond dat de bindende bevoegdheid van de CTIVD van wezenlijk belang is ter voorkoming van onrechtmatige gegevensverwerking door de diensten.

7.2.3 Procesverloop bij dynamische bulkdatasets (A en B)

De wet maakt onvoldoende onderscheid tussen "bulkdatasets" en "de gegevens in bulkdatasets". Hierdoor is onduidelijkheid ontstaan over de eindtermijnen van dynamische bulkdatasets.

Artikel 14b van de Tijdelijke wet bepaalt dat de eindtermijn van het gebruik van de *gegevens uit bulkdatasets* die met een bijzondere bevoegd zijn verkregen, anderhalf jaar bedraagt. Hierbij gaat het nadrukkelijk om de *gegevens* uit bulkdatasets. In artikel 14ba, eerste lid van de Tijdelijke Wet wordt bepaald dat de minister kan worden verzocht om te beoordelen of een nieuwe eindtermijn voor het *gebruik* van een B-bulkdataset moet worden vastgesteld. Hierbij gaat het nadrukkelijk om het gebruik van de bulkdataset, niet om de gegevens daarin.

In de praktijk is door dit verschil in typering op enig moment onduidelijkheid ontstaan bij de diensten en bij de CTIVD over hoe de diensten om moeten gaan met de eindtermijnen van zogenaamde *dynamische bulkdatasets* die met een bijzondere bevoegdheid zijn verzameld. Een dynamische bulkdataset is een bulkdataset waarbij de gegevens periodiek aangevuld of overschreven worden. Indien bij dynamische bulkdatasets de *ouderdom van de gegevens* bepalend zou zijn voor de eindtermijn, dan kan het gebeuren dat er nooit een eindtermijn verstrijkt omdat de gegevens steeds tussentijds overschreven zijn. Daar staat tegenover dat indien de ouderdom van de bulkdataset als geheel bepalend is voor de eindtermijn, de situatie kan ontstaan dat de eindtermijn van dynamische bulkdataset verstrijkt terwijl (een deel van) de gegevens daarin slechts kort daarvoor zijn verworven.

De CTIVD heeft afgesproken met de diensten dat de ouderdom van de bulkdataset leidend is voor de eindtermijn van het gebruik. Dit betekent dat alle bulkdatasets die met een bijzondere bevoegdheid zijn verworven na anderhalf jaar een nieuwe gebruikstermijn moeten krijgen. Uiteraard geldt dit alleen als het met het oog op de nationale veiligheid noodzakelijk is om deze sets langer te bewaren. Dit geldt ook als de gegevens in die bulkdataset tussentijds zijn overschreven of aangevuld. Deze uitleg lijkt het meest aan te sluiten bij de bedoeling van de wetgever om voor alle B-bulkdatasets een dwingende bewaartermijn van anderhalf jaar in te stellen, waarbij steeds na een jaar kritisch wordt gekeken of de dataset moet worden behouden.

7.2.4 Overkoepelende bevindingen

Welke wettelijke regels van toepassing zijn op de verdere verwerking van bulkdatasets is afhankelijk van de verwervingsgrond.

In paragraaf 7.1 is het verschil tussen A-bulkdatasets en B-bulkdatasets uitgelegd. Hieruit blijkt dat het antwoord op de vraag welke wettelijke regels van toepassing zijn op de verdere verwerking van een bulkdataset afhangt van de manier waarop zij is verworven. Als een dienst een bulkdataset met een algemene bevoegdheid heeft verworven, gelden er andere (minder vergaande) eisen voor de verdere verwerking van die set dan voor de verdere verwerking van een set die met een bijzondere bevoegdheid is verworven. De wijze waarop een set is verworven zegt echter niet noodzakelijkerwijs iets over de aard van de gegevens en de mate waarin de verdere

verwerking daarvan een privacyinbreuk inhoudt. De mate van de privacyinbreuk zou daarom ook voorop moeten worden gesteld bij het bepalen welke waarborgen van toepassing zijn op de verdere verwerking van bulkdatasets. Om dit te bepalen is een inhoudelijk beoordeling van de gegevens noodzakelijk,

De wettelijke regels die van toepassing zijn op de verdere verwerking van B-bulkdatasets zijn strenger dan die voor A-bulkdatasets, terwijl A-bulkdatasets in de praktijk zelfs vaker gevoelige gegevens bevatten.

De CTIVD heeft onderzocht of de diensten B-bulkdatasets vaker in een beperkt of strikt beperkt toegangsregime plaatsen dan A-bulkdatasets. Het omgekeerde is echter het geval. A-bulkdatasets worden in de praktijk door de diensten juist vaker in een beperkt of strikt beperkt toegangsregime geplaatst dan B-bulkdatasets. Dit betekent dat A-bulkdatasets in de praktijk vaker (veel) gevoeligere data bevatten dan B-bulkdatasets en dat het verder verwerken van A-bulkdatasets in die gevallen dus een grotere privacyinbreuk meebrengt dan de verdere verwerking van B-bulkdatasets.

Dit is opmerkelijk, omdat de wettelijke regels voor de verdere verwerking voor B-bulkdatasets strenger zijn dan voor A-bulkdatasets. Voor B-bulkdatasets geldt een dwingende gebruikstermijn van anderhalf jaar en kan een nieuwe gebruikstermijn slechts door de minister worden vastgesteld. Ook is er bindend toezicht op nieuwe eindtermijnen van de CTIVD. Voor A-bulkdatasets gelden mogelijke termijnen van 36, 24 en 12 maanden, waarna de noodzaak tot verwijdering beoordeeld dient te worden door het hoofd van de betrokken dienst. Van bindend toezicht door de CTIVD is geen sprake.

Het onderscheid tussen A-bulkdatasets en B-bulkdatasets is ook relevant voor de Unit Veiligheidsonderzoeken (UVO) van de AIVD. De UVO maakt bij de uitvoering van veiligheidsonderzoeken géén gebruik van bijzondere bevoegdheden. Uit het onderzoek van de CTIVD is niet gebleken dat de UVO naslagen vericht in bulkdatasets die met een bijzondere bevoegdheid zijn verworven.

Aanbeveling 12
Overweeg bij de herziening van de Wiv 2017 om de regels voor de verdere verwerking van bulkdatasets, waaronder de regels voor bewaartermijnen, niet langer te baseren op de wijze van verwerving, maar op de inbreuk op grondrechten die de verdere verwerking van de bulkdataset door de diensten maakt. Om deze inbreuk te bepalen is een inhoudelijke beoordeling van de gegevens noodzakelijk.

8 Verwijdering en vernietiging van gegevens

Hoofdstuk 8 – Verwijdering en vernietiging van gegevens



8.1 Inleiding en wettelijke criteria

Op verschillende momenten in de levenscyclus van een bulkdataset is het noodzakelijk dat (gegevens uit) bulkdatasets door de diensten worden verwijderd en vernietigd.

Verwijderen en vernietigen van gegevens

De wet maakt onderscheid tussen het verwijderen en het vernietigen van gegevens. Verwijderen wil zeggen dat gegevens niet langer toegankelijk zijn voor de uitvoering van taken door de diensten. De gegevens worden in een zogenaamd *semi statisch archief* geplaatst en kunnen zo nodig weer toegankelijk worden gemaakt. Bij vernietiging verdwijnen de gegevens definitief en onomkeerbaar uit de systemen.

In hoofdstuk 3 is het technisch voortraject besproken waarbij bulkdatasets beschikbaar worden gemaakt op de systemen van de diensten. Met het oog op datareductie voorafgaand aan de verdere verwerking van bulkdatasets worden slechts de noodzakelijke delen van bulkdatasets beschikbaar gemaakt. De oorspronkelijke, volledige bulkdataset, wordt op enig moment verwijderd en vernietigd.

In hoofdstuk 7 zijn de processen voor de beoordeling van de noodzaak tot verwijdering van A-bulkdatasets en het vaststellen van eventuele nieuwe gebruikstermijnen van B-bulkdatasets beschreven. Aan bod kwam dat bij A-bulkdatasets periodiek de noodzaak tot verwijdering moet worden beoordeeld. Verwijderde gegevens moeten vervolgens worden vernietigd, tenzij wettelijke regels daaraan in de weg staan. Voor B-bulkdatasets geldt dat de gegevens uit de bulkdataset na afloop van de eindtermijn voor het gebruik van die gegevens moeten worden vernietigd, tenzij er een nieuwe eindtermijn voor het gebruik wordt vastgesteld. Wanneer een dienst de gegevens uit een B-bulkdataset heeft vernietigd na het verstrijken van de eindtermijn, moet daarvan melding worden gedaan aan de CTIVD.

In dit hoofdstuk worden de processen voor de concrete verwijdering en vernietiging van (gegevens uit) bulkdatasets door beide diensten getoetst en de naleving van die processen in de praktijk beoordeeld.

Verwijdering en vernietiging van gegevens die geen betekenis meer hebben

De gegevens die, gelet op het doel waarvoor zij worden verwerkt, geen betekenis hebben of hun betekenis zijn verloren, worden verwijderd. De verwijderde gegevens worden vernietigd, tenzij wettelijke regels omtrent bewaring daaraan in de weg staan.

(Artikel 20 lid 1 en 3 van de Wiv 2017)

Eindtermijnen bij B-bulkdatasets, vernietiging en melding aan de afdeling toezicht

In afwijking van (...) bedraagt de eindtermijn voor gebruik (...) van de gegevens in door de dienst verworven bulkdataset bij de uitoefening van een bijzondere bevoegdheid (...) anderhalf jaar. Na afloop van deze termijn worden de gegevens in de bulkdataset vernietigd. Van de vernietiging wordt terstond mededeling gedaan aan de afdeling toezicht van de commissie van toezicht.

(Artikel 14ba van de Tijdelijke Wet)

8.2 Beoordeling van de verwijdering en vernietiging van gegevens uit bulkdatasets

De verwijdering en vernietiging van gegevens is niet voor alle clusters en bronnen geautomatiseerd georganiseerd.

De diensten hebben geen overkoepelend beleid dat voor alle ICT-systemen geldt ten aanzien van de verwijdering en vernietiging van bulkdatasets. De wijze waarop gegevens worden verwijderd en vernietigd verschilt per ICT-systeem. Er zijn bijvoorbeeld systemen waarbij het verlopen van de bewaartermijn wordt gemonitord. Vervolgens wordt de bulkdataset handmatig ontoegankelijk gemaakt voor medewerkers van een inlichtingenteam. Er zijn echter ook systemen waarin de gegevens automatisch worden verwijderd na afloop van de bewaartermijn. Deze verschillen in systeeminrichting vergroten de foutgevoeligheid. Met name waar handmatige verwijdering is vereist, bestaat het risico dat gegevens niet tijdig, onvolledig of onjuist worden verwijderd.

Beleid over het verwijderen en vernietigen van bulkdatasets op fysieke gegevensdragers ontbreekt.

Bulkdatasets kunnen zowel digitaal als op fysieke gegevensdragers worden opgeslagen. De diensten hebben geen specifiek beleid voor het verwijderen en vernietigen van bulkdatasets op fysieke gegevensdragers. Binnen de diensten is een centrale afdeling aangewezen voor de registratie van fysieke gegevensdragers ten behoeve van bulkdatasets. Het procesverloop van het

verwijderen en vernietigen van gegevens op fysieke gegevensdragers, nadat de gegevens op de systemen van de diensten zijn gezet, is niet in alle gevallen hetzelfde.

De CTIVD werd niet altijd tijdig genotificeerd over de vernietiging van bulkdatasets.
Ten tijde van het onderzoek waren er nog geen afspraken over de meldingsprocedure voor de vernietiging van bulkdatasets vastgelegd. De diensten hebben niet altijd op eigen initiatief melding gemaakt van de vernietiging van bulkdatasets. Inmiddels zijn afspraken hierover geformaliseerd en wordt de CTIVD genotificeerd over de vernietiging van bulkdatasets.

Gegevens over verwijderde en vernietigde gegevens blijven beschikbaar, maar zijn beperkt toegankelijk.
De verwijdering van gegevens uit bulkdatasets houdt in de praktijk in dat de gegevens niet meer toegankelijk zijn voor medewerkers uit inlichtingenteams of andere medewerkers die de gegevens in onderzoeken van de diensten kunnen betrekken. De verwijderde gegevens blijven in een aantal gevallen wel beschikbaar voor medewerkers die betrokken zijn bij het technisch voortraject. In dit kader heeft de CTIVD twee bevindingen gedaan.

Ten eerste vindt er in het technisch voortraject (zie hoofdstuk 3) datareductie plaats. Tijdens dit proces worden gegevens waarvan op voorhand duidelijk is dat deze niet relevant zijn voor de taakuitvoering van de diensten uit de bulkdataset gefilterd, verwijderd en vernietigd. De ruwe data over deze vernietigde gegevens wordt echter disproportioneel lang bewaard. Hoewel deze ruwe data niet wordt ontsloten op de systemen en niet wordt betrokken in onderzoeken van de diensten, blijft de data wel beschikbaar voor een beperkt aantal medewerkers.

Ten tweede wordt door de diensten voorafgaand aan het beschikbaar maken van de gegevens op de daarvoor bedoelde ICT-systemen een zogenoemde *quickscan* gemaakt om informatie te krijgen over de inhoud en structuur van bulkdatasets. Dit is noodzakelijk om voorafgaand aan het beschikbaar maken van de data op de ICT-systemen een eerste inschatting te maken van de inhoud, noodzakelijkheid, proportionaliteit en subsidiariteit van de eventuele verwerving en verdere verwerking van de dataset. Aan de hand van de quickscan kan tevens een inschatting worden gemaakt of er sprake is van een bulkdataset. De quickscans blijven ook na verwijdering en vernietiging van een bulkdataset, bewaard.

Aanbeveling 13
Pas de bewaartermijn voor bulkdatasets in het technisch voortraject aan zodat er niet langer dan nodig inbreuk op de privacy wordt gemaakt.

Bulkdatasets bij de MIVD zijn niet tijdig verwijderd en vernietigd.
Tijdens het onderzoek bleek bij de MIVD dat er onrechtmatig (gegevens uit) bulkdatasets waren opgeslagen. Deze gegevens werden niet beheerd, waardoor bijvoorbeeld geen geldige einddatum voor het gebruik was vastgesteld terwijl dit wel had gemoeten. De CTIVD heeft niet kunnen vaststellen op welke bulkdatasets dit betrekking heeft. Verscheidene bulkdatasets

hadden geen geldige eindtermijn; dit is onrechtmatig. De MIVD heeft deze gegevens gedurende het onderzoek verwijderd en vernietigd.

9 Conclusie en overzicht van bevindingen

9.1 Conclusie

In dit rapport concludeert de CTIVD dat een aantal belangrijke waarborgen voor het gebruik van bulkdatasets door de AIVD en de MIVD niet op orde is. Daardoor bestaan verhoogde risico's op onrechtmatigheden en onzorgvuldigheden, die zich in sommige gevallen hebben verwezenlijkt. De diensten maken op grote schaal en op verschillende plekken in de organisatie gebruik van bulkdatasets. Uit hoofdstuk 3 blijkt dat het technisch voortraject een doorslaggevende rol speelt in de kwalificatie van bulkdatasets. Wanneer de diensten een dataset onterecht niet kwalificeren als bulkdataset heeft dit grote gevolgen voor de verdere verwerking van de gegevens. Ook blijft de verbetering van de technische en procedurele uitvoering van de verwerking van bulkdatasets noodzakelijk.

In het proces van de diensten rondom de bepaling van het toegangsregime (hoofdstuk 4) zijn weinig risico's of onrechtmatigheden geconstateerd. De inhoudelijke beoordelingen van bulkdatasets door de diensten zijn navolgbaar en de meldingen omtrent toegangsregimes worden tijdig gedaan aan de CTIVD. Wel is er een gebrek aan een besliskader waarbij aandacht is voor de mogelijk verhoogde inbreuk van het gebruiken van afzonderlijke bulkdatasets in samenhang. Dit geldt ook voor de invulling en weging van het criterium voor openbare toegankelijkheid.

Met betrekking tot toegangsmanagement zijn in hoofdstuk 5 ernstige risico's en onrechtmatigheden met betrekking tot de toegang van medewerkers tot bulkdatasets geconstateerd. Met name voor bulkdatasets waarop het beperkte of strikt beperkte toegangsregime van toepassing is, ziet de CTIVD (risico's op) onrechtmatigheden, zowel op technisch als procedureel gebied. Ook de logging van gegevens geeft onvoldoende inzicht die nodig is voor een goede beoordeling van processen.

Het onderzoek naar het gebruik van bulkdatasets wordt beschreven in hoofdstuk 6. De CTIVD onderschrijft het belang van het gebruik van bulkdatasets. Het gebruik van bulkdatasets ter ondersteuning van de taakuitvoering is onrechtmatig aangezien er hiervoor geen wettelijke grondslag bestaat. In deze gevallen wordt de toegang tot de bulkdatasets wel beperkt door de diensten. Dit neemt echter niet weg dat met de werkwijze van de diensten in dit kader geen wettelijke waarborgen worden toegepast die zien op periodieke beoordelingen en toegangsregimes.

De bevindingen over het langdurig gebruiken van bulkdatasets en het verschil tussen bulkdatasets verworven met een algemene (A-bulkdatasets) of met een bijzondere bevoegdheid (B-bulkdatasets) staan in hoofdstuk 7. De praktijk heeft aangetoond dat gevoelige bulkdatasets vaak worden verworven met de inzet van algemene bevoegdheden. De CTIVD ziet mede

daardoor geen reden voor het onderscheid tussen A- en B-bulkdatasets bij de verdere verwerking. De CTIVD is van oordeel dat de mate van inbreuk van de verdere verwerking van de gegevens leidend moet zijn bij de toepassing van waarborgen. Dit standpunt sluit aan op het toetsingskader van de Tijdelijke regeling, waarin de mate van privacyinbreuk doorslaggevend is voor de bepaling van toegangsregimes. Verder constateert de CTIVD dat periodieke beoordelingen niet altijd tijdig door de diensten worden uitgevoerd.

In hoofdstuk 8 zijn de bevindingen van het onderzoek naar de verwijdering en vernietiging van gegevens uit bulkdatasets opgenomen. Er doen zich voornamelijk risico's voor bij de handmatige vernietiging van bulkdatasets. Ook worden gegevens in het technisch voortraject langer bewaard dan noodzakelijk en proportioneel is. De MIVD heeft gedurende het onderzoek een aantal bulkdatasets vernietigd die ten onrechte werden bewaard.

9.2 Overzicht bevindingen en aanbevelingen

Hieronder volgt een overzicht van de bevindingen en aanbevelingen uit dit rapport:

Paragraaf	Bevindingen en aanbevelingen
3.2.1	1. De definitie van bulkdatasets is niet in alle gevallen makkelijk toepasbaar.
3.2.1	*2. De AIVD en de MIVD hebben gezamenlijk beleid om te waarborgen dat datasets ten onrechte niet worden aangemerkt als bulkdataset, toch blijven er risico's bestaan.*
3.2.1	**Aanbeveling 1:** Zorg voor nadere maatregelen die voorkomen dat datasets ten onrechte niet als bulkdatasets in beeld komen, bijvoorbeeld doordat deze niet worden aangemeld.
3.2.1	**Aanbeveling 2:** Verduidelijk de definitie van bulkdatasets, of de wijze waarop deze moet worden toegepast, in beleid of regelgeving om ervoor te zorgen dat alle gegevensverzamelingen die het inbreukmakende karakter van een bulkdataset hebben, volgens de regels voor bulkdatasets worden verwerkt en in passende waarborgen wordt voorzien.
3.2.2	3. De diensten hebben gezamenlijk beleid op basis waarvan datareductie plaatsvindt voordat bulkdatasets kunnen worden gebruikt bij de uitvoering van wettelijke taken.
3.2.2.	*4. De CTIVD heeft in een steekproef geen verboden (categorieën) gegevens in bulkdatasets aangetroffen.*
3.2.3	*5. Er is sprake van een versnipperd datalandschap met betrekking tot bulkdatasets, waarop onvoldoende centrale regie wordt gevoerd.*
3.2.3	*6. De diensten zijn tijdens het onderzoek van de CTIVD reeds gestart met het doorvoeren van verbeteringen met betrekking tot het versnipperde datalandschap en het voeren van een centrale regie op de verdere verwerking van bulkdatasets.*
3.2.3	**Aanbeveling 3:** Werk verder aan de reeds ingezette dataconvergentie en de versterking van de centrale regie die wordt gevoerd op de verdere verwering van bulkdatasets
4.2.1	*7. De diensten hebben gezamenlijk beleid voor het beoordelen van bulkdatasets en het toekennen van toegangsregimes.*
4.2.1	*8. Er ontbreken duidelijke beleidsmatige uitgangspunten voor wanneer bulkdatasets in samenhang moeten worden beoordeeld.*
4.2.1	**Aanbeveling 4:** Zorg voor een besliskader om te bepalen of de verdere verwerking van meerdere bulkdatasets (al dan niet) in samenhang moet worden gewogen om de privacyinbreuk daarvan (goed) te kunnen beoordelen.

4.2.1	9. Er vindt structureel intern multidisciplinair overleg plaats over het toekennen van een toegangsregime.
4.2.1	10. De diensten maken consistente beoordelingen van bulkdatasets aan de hand van vuistregels die in het beleid zijn opgenomen.
4.2.1	11. De invulling en weging van het criterium over openbare toegankelijkheid is discutabel.
4.2.1	Aanbeveling 5: Merk gegvens aan als niet openbaar toegankelijk wanneer niet feitelijk kan worden vastgesteld of de verworven gegevens openbaar toegankelijk zijn (geweest). Scherp in regelgeving of beleid aan hoe dit criterium moet worden betrokken bij de beoordeling van de privacyinbreuk van bulkdatasets. Houd hierbij rekening met de omstandigheid dat gegevens uit een datalek openbaar toegankelijk kunnen zijn, maar doorgaans niet door de betrokkenen zelf openbaar zijn gemaakt. De openbaarheid van gegevens is niet altijd bepalend voor de aard van de gegevens noch voor de mate van privacyinbreuk die de verwerking van deze gegevens met zich meebrengt.
4.2.2	12. Het merendeel van de vastgestelde toegangsregimes is op tijd gemeld bij de CTIVD.
4.2.2	13. De inhoudelijke beoordeling van bulkdatasets en het gekozen toegangsregime was steeds navolgbaar voor de CTIVD.
5.2.1	14. De diensten hebben toereikende maatregelen getroffen die zorgen dat slechts medewerkers die dat nodig hebben voor de goede uitvoering van hun taak, toegang hebben tot gegevens uit bulkdatasets met een standaardtoegangsregime.
5.2.2	15. De diensten gebruiken bulkdatasets ter ondersteuning van de taakuitvoering zonder dat daarbij de regels en waarborgen voor bulkdatasets worden nageleefd. Dit is onrechtmatig.
5.2.2.	16. Gedurende de onderzoeksperiode zijn er meerdere gevallen aan het licht gekomen waarbij dienstmedewerkers toegang hadden tot gegevens uit bulkdatasets met een (strikt) beperkt toegangsregime, terwijl zij daartoe niet (langer) bevoegd waren. Deze voorvallen worden door de CTIVD als onrechtmatigheden beschouwd.
5.2.2.	Aanbeveling 6: De wijze waarop toegangsmanagement voor bulkdatasets met een (strikt)

	beperkt toegangsregime technisch en procedureel is geïmplementeerd moet worden verbeterd op een manier die het risico op onrechtmatige gegevensverwerking mitigeert.
5.2.3.	17. De technische wijze waarop bijgehouden wordt welke medewerkers toegang hebben gehad tot welke gegevens (gegevenslogging), is toereikend als maatregel tegen verlies of aantasting van gegevens.
5.2.3	18. De technische wijze waarop bijgehouden wordt welke medewerkers toegang hebben gehad tot welke gegevens (gegevenslogging) als maatregel tegen onbevoegde gegevensverwerking is niet toereikend. Dit is onzorgvuldig.
5.2.3	Aanbeveling 7: De logging van de toegang tot bulkdatasets moet worden verbeterd. Daarnaast moeten wijzigingen in autorisaties beter inzichtelijk worden gemaakt. Achteraf moet beter kunnen worden vastgesteld wie al dan niet terecht toegang heeft gehad tot een bulkdataset en daarvan gebruik heeft gemaakt.
6.2.1	*19. Bulkdatasets zijn van groot belang voor de goede uitvoering van de wettelijke taken van de diensten.*
6.2.1	*20. De wijze waarop binnen het inlichtingenonderzoek wordt gewerkt met bulkdatasets voldoet aan het principe van behoorlijke gegevensverwerking.*
6.2.1	*21. Bij het gebruik van bulkdatasets zijn verbeteringen mogelijk om de opbrengst uit bulkdatasets beter in kaart te brengen.*
6.2.1	Aanbeveling 8: Onderzoek de state-of-the-art mogelijkheden voor de toepassing van (geautomatiseerde) datalineage. Voer op basis hiervan verbeteringen door in de huidige wijze van datalineage.
6.2.2	*22. Bepaalde afdelingen van de diensten gebruiken bulkdatasets ter ondersteuning van de taakuitvoering zonder dat daarbij de regels en waarborgen voor bulkdatasets worden nageleefd. Dit is onrechtmatig.*
6.2.2	Aanbeveling 9: Zorg ervoor dat gegevens uit bulkdatasets ter ondersteuning van de taakuitvoering ook rechtmatig verder worden verwerkt. Overweeg om bij de herziening van de Wiv 2017, een wettelijke grondslag te creëren indien het noodzakelijk blijkt om ter ondersteuning van de taakuitvoering bulkdatasets te verwerken. Specifieer nader welke verwerkingsdoeleinden kunnen worden aangemerkt als ter ondersteuning van de taakuitvoering. Het gebruiken van gegevens bij de inzet van bevoegdheden zou ook gewoon als taakuitvoering gezien kunnen worden. Leg naast het creëren van een grondslag wettelijk vast welke eisen gelden om te voorzien in passende waarborgen die recht doen aan de privacyinbreuk. Functiescheiding zoals in onderhavige gevallen is ingericht, kan hiervan een onderdeel zijn.
7.2.1.	23. De diensten beschikken over een werkproces waarbij de periodieke beoordeling van de noodzaak tot verwijdering van A-bulkdatasets wordt gemaakt en voorgelegd aan het betrokken diensthoofd.

7.2.1.	24. De CTIVD heeft in het onderzoek een aantal A-bulkdatasets aangetroffen waarbij de periodieke beoordeling van de noodzaak tot verwijdering niet (op tijd) heeft plaatsgevonden. Dit is onrechtmatig.
7.2.1.	**Aanbeveling 10:** Onderzoek welke A-bulkdatasets ten onrechte (nog) niet zijn onderworpen aan een periodieke beoordeling van de noodzaak tot verwijdering. Zorg ervoor dat de periodieke beoordeling alsnog plaatsvindt.
7.2.1	**Aanbeveling 11:** Zorg voor waarborgen in het proces die maken dat de periodieke beoordeling van de noodzaak tot verwijdering A-bulkdatasets tijdig plaatsvindt.
7.2.1	25. De CTIVD heeft in het onderzoek geen voorbeelden aangetroffen waarbij de uitkomst van de beoordeling van de noodzaak tot verwijdering van een A-bulkdataset naar het oordeel van de CTIVD onnavolgbaar was.
7.2.2.	*26. De CTIVD heeft sinds de invoering van de Tijdelijke wet geen gebruik gemaakt van haar bindende bevoegdheid ten aanzien van nieuwe eindtermijnen voor B-bulkdatasets.*
7.2.3.	*27. De wet maakt onvoldoende onderscheid tussen "bulkdatasets" en "de gegevens in bulkdatasets". Hierdoor is onduidelijkheid ontstaan over de eindtermijnen van dynamische bulkdatasets.*
7.2.4.	*28. Welke wettelijke regels van toepassing zijn op de verdere verwerking van bulkdatasets is afhankelijk van de verwervingsgrond.*
7.2.4	*29. De wettelijke regels die van toepassing zijn op de verdere verwerking van B-bulkdatasets zijn strenger dan die voor A-bulkdatasets, terwijl A-bulkdatasets in de praktijk zelfs vaker gevoelige gegevens bevatten.*
7.2.4.	**Aanbeveling 12:** Overweeg bij de herziening van de Wiv 2017 om de regels voor de verdere verwerking van bulkdatasets, waaronder de regels voor bewaartermijnen, niet langer te baseren op de wijze van verwerving, maar op de inbreuk op grondrechten die de verdere verwerking van de bulkdataset door de diensten maakt. Om deze inbreuk te bepalen is een inhoudelijke beoordeling van de gegevens noodzakelijk.
8.2	*30. De verwijdering en vernietiging van gegevens is niet voor alle clusters en bronnen geautomatiseerd georganiseerd.*
8.2	*31. Beleid over het verwijderen en vernietigen van bulkdatasets op fysieke gegevensdragers ontbreekt.*
8.2	*32. De CTIVD werd niet altijd tijdig genotificeerd over de vernietiging van bulkdatasets.*
8.2	*33. Gegevens over verwijderde en vernietigde gegevens blijven beschikbaar, maar zijn beperkt toegankelijk.*
8.2	**Aanbeveling 13:** Pas de bewaartermijn voor bulkdatasets in het technisch voortraject aan.
8.2	*34. Bulkdatasets bij de MIVD zijn niet tijdig verwijderd en vernietigd.*