Eerste Kamer der Staten-Generaal **I**

Vergaderjaar 2026-2027

36 263 Tijdelijke regels inzake specifieke wettelijke voorzieningen voor het uitvoeren van onderzoeken door de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen alsmede voorzieningen inzake de mogelijkheid tot vaststelling van een nieuwe eindtermijn voor gebruik door de diensten van in het kader van hun taakuitvoering met bijzondere bevoegdheden verworven bulkdatasets en de invoering van een bindende toets ex ante van verleende toestemmingen voor de real time interceptie van verkeers- en locatiegegevens (Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkdatasets en overige specifieke voorzieningen)

U **VERSLAG VAN EEN SCHRIFTELIJK OVERLEG**
Vastgesteld 5 november 2026

De vaste commissie voor Binnenlandse Zaken[1] heeft schriftelijk overleg gevoerd met de minister van Binnenlandse Zaken en Koninkrijksrelaties en de minister van Defensie over **het CTIVD-rapport nr. 84 over bulkdatasets door AIVD en MIVD.** Bijgaand brengt de commissie hiervan verslag uit. Dit verslag bestaat uit:

- De uitgaande brief van 29 september 2026.
- De antwoordbrief van 2 november 2026.

De griffier van de vaste commissie voor Binnenlandse Zaken,

Bergman

[1] Samenstelling:
Beukering (Fractie-Beukering), Dessing (FVD), Dittrich (D66), Doornhof (CDA), Fiers (PRO), Van Gasteren (Fractie-Van Gasteren), Van der Goot (OPNL), Griffioen (D66), Van Gurp (PRO), Van Hattem (PVV), Janssen (SP), Janssen-van Helvoort (PRO), Karaaslan (D66), Kroon (BBB), Lagas (BBB) (voorzitter), Van Langen-Visbeek (BBB), Lievense (BBB), Meijer (VVD) (ondervoorzitter), Moonen (D66), Nicolaï (PvdD), Perin-Gopie (Volt), Recourt (PRO), Van Rooijen (50PLUS), Roovers (PRO), Van de Sanden (Fractie-Van de Sanden), Schalk (SGP), Straus (VVD), Talsma (ChristenUnie), Van Toorenburg (CDA), Visseren-Hamakers (Fractie-Visseren-Hamakers), Walenkamp (Fractie-Walenkamp)

BRIEF VAN DE VOORZITTER VAN DE VASTE COMMISSIE VOOR BINNENLANDSE ZAKEN

Aan de minister van Binnenlandse Zaken en Koninkrijksrelaties

Den Haag, 29 september 2026

De leden van de vaste commissie voor Binnenlandse Zaken hebben met belangstelling kennisgenomen van uw brief van 1 juli 2026, die u mede namens de minister van Defensie stuurde, inzake de aanbieding van (de beleidsreactie op) het rapport nummer 84 van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (verder CTIVD) over verwerking van bulkdatasets door de AIVD en MIVD (verder CTIVD rapport nr. 84).[2]
Naar aanleiding hiervan hebben de leden van de fractie van **PRO**, mede namens de leden van de fractie van de **PvdD**, een aantal nadere vragen en opmerkingen.

Vragen en opmerkingen door de fractieleden van PRO, mede namens de leden van de fractie van de PvdD.

Onrechtmatigheden
In rapport 84 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, die zich in sommige gevallen hebben verwezenlijkt”.[3]

Hieronder enkele bevinden uit het rapport:
- “De diensten gebruiken bulkdatasets ter ondersteuning van de taakuitvoering zonder dat daarbij de regels en waarborgen voor bulkdatasets worden nageleefd. Dit is onrechtmatig”.[4]
- “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]
- “De CTIVD heeft in het onderzoek een aantal A-bulkdatasets aangetroffen waarbij de periodieke beoordeling van de noodzaak tot verwijdering niet (op tijd) heeft plaats gevonden. Dit is onrechtmatig”.[6]
- "Verscheidene bulkdatasets hadden geen geldige eindtermijn; dit is onrechtmatig”.[7]

In de reactie van de regering lezen we dat er “winst te behalen is” en dat er sprake is van "compliance-incidenten".[8] Het woord ‘onrechtmatig(heden)’ komt, zo lezen de leden van de fractie PRO, in de brief niet voor.

Vraag 1
Onderschrijft u de conclusies van de CTIVD over de geconstateerde onrechtmatigheden? Deze leden ontvangen graag een toelichting, per constatering, waarom wél of niet, en vragen u expliciet in te gaan op het oordeel onrechtmatig. Kunt u hierbij ook graag aangeven welke consequenties hieraan volgens u verbonden moeten worden?

[2] *Kamerstukken I* 2025/26, 36263, S.
[3] Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, ‘*Toezichtrapport over verwerking van bulkdatasets door de AIVD en MIVD*’, CTIVD nr. 84, 11 juni 2026, pagina 3 (verder CTIVD-rapport nr. 84).
[4] CTIVD-rapport nr. 84, pagina 37.
[5] CTIVD-rapport nr. 84, pagina 53.
[6] CTIVD-rapport nr. 84, pagina 55.
[7] CTIVD-rapport nr. 84, pagina 48 en 49.
[8] *Kamerstukken* I 2025/26, 36263, S, pagina 2.

U ziet oorzaken in "administratieve druk" en "menselijke fouten".[9] De CTIVD wijst, niet voor het eerst, op structurele technische en procedurele tekortkomingen.

Vraag 2
Is er volgens u sprake van structurele technische en procedurele tekortkomingen? Zo ja, op welke onderdelen? Zo nee, waarom niet?

Patroon en doorschuiven
Deze leden constateren dat meerdere knelpunten eerder door de CTIVD gesignaleerd zijn: het niet als zodanig behandelen van bulkdata, het te lang bewaren en niet tijdig vernietigen, de versnipperde datahuishouding en de vertaling van beleid naar praktijk.

Vraag 3
Herkent u dit patroon van terugkerende knelpunten? Zo nee, waarom niet? Zo ja, hoe beoordeelt u de herhaling gezien de eerdere toezeggingen om de knelpunten aan te pakken, en wat is volgens u de oorzaak?

Vraag 4
Kunt u een overzicht geven van alle toezeggingen sinds 2018 over bulkdata (naar aanleiding van onder meer de rapporten 55, 70, 71, 79 en 84 en de voortgangsrapportages), met per toezegging de status, de verantwoordelijke en de datum van uitvoering?

Ook ten aanzien van het ‘doorschuiven’ van oplossingen voor de onrechtmatigheden en onzorgvuldigheden naar de toekomst is volgens deze leden sprake van een patroon. Terugkerende knelpunten werden eerder doorgeschoven naar de komst van de resultaten van de evaluatiecommissie (2020), daarna naar de komst van de Tijdelijke Wet (2023) en nu (2026) naar de komst van de nieuwe wet.

Vraag 5
Herkent u dit patroon van doorschuiven? Zo nee, waarom niet. Zo ja, hoe gaat u voorkomen dat de knelpunten steeds doorgeschoven blijven worden?

Omvang van de bulkdata en het aandeel Nederlanders
Het CTIVD-rapport nr. 84 beschrijft bulkdatasets als omvangrijke verzamelingen persoonsgegevens met soms miljoenen regels en stelt dat verreweg de meeste betrokkenen niets met spionage of terrorisme te maken hebben. Het bezit van al die data brengt ook risico’s met zich mee. Daarom hebben de aan het woord zijnde leden enkele vragen om zicht te krijgen op de omvang van deze data, het aandeel data over Nederlanders en de bijbehorende risico’s.

Vraag 6
Kunt u aangeven wat de actuele omvang is van de bulkdatasets, uitgedrukt in (a) aantal sets, (b) aantal regels (rijen), (c) opslagvolume (bijvoorbeeld in terabytes) en (d) aantal unieke personen, zo nodig bij benadering/ in bandbreedtes (bijvoorbeeld minder dan een miljoen, een tot tien miljoen, meer dan honderd miljoen)?

[9] *Kamerstukken* I 2025/26, 36263, S, pagina 2.

Vraag 7
Kunt u een schatting geven van het aandeel Nederlanders, of van gegevens van Nederlanders? Dit bijvoorbeeld via een vertrouwelijke steekproef door de CTIVD? Kunt u dit toelichten?

Vraag 8
Kunt u aangeven hoeveel sets, regels of volume gebruikt worden ‘ter ondersteuning van de taakuitvoering’, en welk deel daarvan persoonsgegevens bevat? Indien u deze gegevens niet openbaar wil maken, ontvangen deze leden graag een inhoudelijke onderbouwing. Indien volgens u geheimhouding van toepassing is, kunt u dan motiveren welk specifiek geheimhoudingsbelang publicatie van geaggregeerde cijfers in de weg staat?

Risico's van de dataopslag
Het bezit van grote bulkdatasets kent risico's. Het CTIVD-rapport nr. 84 beschrijft volgens deze leden onder meer onbevoegde toegang van binnenuit, te lang bewaren en gebruik buiten de waarborgen van het bulkdatasetregime. Daarnaast zijn er andere risico's, zoals hacks en datalekken en misbruik door medewerkers.

Vraag 9
Welke risico's ziet u bij de opslag van grote bulkdatasets? Graag een volledige opsomming met toelichting per risico.

Vraag 10
Hoe groot of klein schat u deze risico's in? Bestaat er een formele risicoanalyse voor bulkdata? Zo ja, door wie is die opgesteld en door wie getoetst?

Vraag 11
Hoeveel beveiligingsincidenten, gevallen van onbevoegde toegang en vermoedens van misbruik zijn er volgens u de afgelopen vijf jaar geregistreerd bij bulkdatasets, en wat waren de gevolgen?

Bronnen van bulkdata en het criterium ‘openbaar toegankelijk’
Het CTIVD-rapport nr. 84 noemt de invulling en weging van het criterium openbare toegankelijkheid “discutabel” en het is volgens de CTIVD daarbij niet onrechtmatig om zulke sets als openbaar aan te merken, maar die weging zegt weinig over de privacy inbreuk. [10] Het gaat onder meer om sets van partnerdiensten, om kortstondig en tegen betaling op internet aangeboden sets (soms uit datalekken) en om commercieel aangeboden sets. In uw brief staat dat u het oordeel "discutabel" niet herkent waarbij u verwijst naar de toelichting bij het nieuwe Wetboek van Strafvordering.[11]
In het rapport nummer 74 van de CTIVD ‘Automated OSINT: tools en bronnen voor openbronnenonderzoek’ (verder CTIVD rapport nr. 74) stelde de CTIVD dat verwerking van gegevens uit gelekte datasets een grotere inbreuk op fundamentele rechten meebrengt.[12] De strafbaarstelling sinds 1 maart 2019 van het wederrechtelijk overnemen of doorgeven van niet-openbare gegevens uit een geautomatiseerd werk (art. 138c Sr) en van heling van niet-openbare gegevens (art. 139g Sr) noemde zij daarbij indicatief voor hoe naar het overnemen van gegevens uit gelekte datasets wordt gekeken.[13] Artikel 139g Sr stelt onder meer het verwerven of voorhanden

[10] CTIVD-rapport nr. 84, pagina 53.
[11] *Kamerstukken* I 2025/26, 36263, S, pagina 4.
[12] CTIVD, ‘*Toezichtrapport Automated OSINT: tools en bronnen voor openbronnenonderzoek’*, CTIVD nr. 74, 22 december 2021, pagina 5 (verder CTIVD-rapport nr. 74).
[13] CTIVD-rapport nr. 74, pagina 21.

hebben van niet-openbare gegevens strafbaar als men wist of redelijkerwijs moest vermoeden dat die door een misdrijf zijn verkregen, en kent een uitzondering voor het algemeen belang.
Een lager toegangsregime betekent volgens de aan het woord zijde leden onder meer een ruimere kring van gebruikers en, bij A-sets, geen bindend toezicht van de CTIVD.

Vraag 12
Aangaande het overzicht van de bronnen, kunt u aangeven wat het aandeel per herkomst (overheid, informanten, buitenlandse diensten, commercieel, gelekt of openbaar aangeboden, hack, agent, interceptie) is, en welk aandeel als ‘openbaar toegankelijk’ aangemerkt is en daarom in een lager toegangsregime geplaatst?

Vraag 13
Aangaande het criterium ‘openbaar toegankelijk’, kunt u aangeven wat het aandeel per herkomst (overheid, informanten, buitenlandse diensten, commercieel, gelekt of openbaar aangeboden, hack, agent, interceptie) is? Hoeveel sets zijn als ‘openbaar toegankelijk’ aangemerkt, uitgesplitst naar partnerdienst, gelekt of gehackt en commercieel? Hoeveel daarvan staan in het standaardregime, en welke bewaar- en beoordelingstermijnen gelden daar?

Vraag 14
Erkent u dat een set die door de betrokkenen nooit zelf openbaar is gemaakt, niet minder ingrijpend wordt doordat deze (tijdelijk) openbaar was/is? Kunt u aangeven waarom "openbaar’ dan een weegfactor is die tot een lager regime kan leiden?

Vraag 15
Bent u bereid het criterium te beperken tot gegevens die de betrokkene zelf openbaar maakte of redelijkerwijs openbaar mocht achten, en gelekte of illegaal verkregen gegevens daarvan uit te sluiten? Zo nee, waarom niet?

Vraag 16
Kunt u aangeven welke concrete criteria de diensten hanteren sinds de beleidsreactie om vast te stellen of een set openbaar is? Worden bestaande sets daarop herbeoordeeld en worden die herbeoordelingen aan de CTIVD gemeld?

Gelekte en gestolen data
Vraag 17
U verwijst naar de toelichting bij het nieuwe Wetboek van Strafvordering, waarin bronnen met een financiële drempel als publiek toegankelijk gelden. Kunt u aangeven waarom een strafvorderlijke uitleg passend is voor inlichtingendiensten? Hanteert u voor ‘openbaar toegankelijk’ dezelfde betekenis als het strafrecht voor ‘niet-openbare gegevens’ in artikel 138c en 139g Sr? Zo ja, hoe kan een set die na een datalek breed circuleert dan als ‘openbaar’ gelden in de zin van de Wet op de inlichtingen- en veiligheidsdiensten (verder Wiv)? Zo nee, waarom wordt een andere maatstaf gehanteerd?

Vraag 18

Kunt u aangeven op welke rechtsgrond de diensten niet-openbare gegevens kunnen verwerven of voorhanden hebben waarvan zij weten of redelijkerwijs moeten vermoeden dat deze door een misdrijf zijn verkregen? En geldt die rechtsgrond ook voor het kopen van zulke sets, voor sets van partnerdiensten en voor het gebruik ervan? Wordt daarbij per geval een afweging gemaakt en door wie?

Vraag 19
Kunt u toelichten welke toets voorafgaat aan het kopen van gestolen of gelekte datasets en wie beslist? Is er een ministeriële toestemming? Hoe wordt het risico op financiering van criminaliteit gewogen?

Vraag 20
Weet u hoeveel sets er de afgelopen vijf jaar verworven zijn uit datalekken of via criminele marktplaatsen en welk bedrag daarvoor betaald is, zo nodig als bandbreedte?

Vraag 21
Onderzoekt u of en wanneer betrokkenen van wie gegevens zijn verworven uit een datalek daarover geïnformeerd kunnen worden, bijvoorbeeld via bestaande meldkanalen?

Partnerdiensten
Vraag 22
Kunt u aangeven hoeveel bulkdatasets ontvangen zijn van buitenlandse diensten? Is bekend hoe die sets zijn verworven (hack, interceptie, koop) en vragen de diensten dat na?

Vraag 23
Als een partnerdienst een set met bijzondere bevoegdheden verwierf, borgt u dan dat in Nederland niet alsnog een lichter regime geldt dan bij eigen verwerving?

Commerciële data
Vraag 24
Kunt u toelichten welke commerciële data verwerkt worden en op welke wettelijke grondslag?

Vraag 25
De CTIVD noemt in rapport 74 de reikwijdte van art. 25 lid 1 onder b Wiv 2017 onduidelijk.[14] Hanteert u een drempelbedrag of een andere norm om aan te nemen dat een betaalde set niet meer openbaar is?

Het schaduwarchief
Vraag 26
Acht u het mogelijk dat de diensten via gekochte, gelekte of ontvangen sets gegevens raadplegen die zij anders alleen na toestemming en toetsing per geval zouden mogen verwerven? Zo ja, hoe voorkomt u dat dit de bestaande toetsing en toezicht omzeilt? Hoeveel raadplegingen vinden per jaar plaats in sets in het standaardregime en kan de CTIVD dankzij de verbeterde logging achteraf controleren wie wat heeft geraadpleegd?

[14] CTIVD-rapport nr. 74, pagina 16.

De leden van de vaste commissie voor Binnenlandse Zaken zien uw reactie met belangstelling tegemoet en ontvangen deze graag zo spoedig mogelijk, maar uiterlijk binnen vier weken na dagtekening van deze brief.

I.M. Lagas MDR
Voorzitter van de vaste commissie voor Binnenlandse Zaken

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 2 november 2026

Onrechtmatigheden
In rapport 84 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, die zich in sommige gevallen hebben verwezenlijkt”.

Hieronder enkele bevinden uit het rapport:
• “De diensten gebruiken bulkdatasets ter ondersteuning van de taakuitvoering zonder dat daarbij de regels en waarborgen voor bulkdatasets worden nageleefd. Dit is onrechtmatig”.
• “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”.
• “De CTIVD heeft in het onderzoek een aantal A-bulkdatasets aangetroffen waarbij de periodieke beoordeling van de noodzaak tot verwijdering niet (op tijd) heeft plaats gevonden. Dit is onrechtmatig”.
• "Verscheidene bulkdatasets hadden geen geldige eindtermijn; dit is onrechtmatig”.

In de reactie van de regering lezen we dat er “winst te behalen is” en dat er sprake is van "compliance-incidenten". Het woord ‘onrechtmatig(heden)’ komt, zo lezen de leden van de fractie PRO, in de brief niet voor.

Vraag 1
Onderschrijft u de conclusies van de CTIVD over de geconstateerde onrechtmatigheden? Deze leden ontvangen graag een toelichting, per constatering, waarom wél of niet, en vragen u expliciet in te gaan op het oordeel onrechtmatig. Kunt u hierbij ook graag aangeven welke consequenties hieraan volgens u verbonden moeten worden?

Vraag 2
Is er volgens u sprake van structurele technische en procedurele tekortkomingen? Zo ja, op welke onderdelen? Zo nee, waarom niet?

Antwoord op vragen 1 en 2
Van ‘onrechtmatige gegevensverwerking’ is sprake wanneer de diensten gegevens verwerken zonder daarbij het geheel van geldende wet- en regelgeving (volledig of correct) toe te passen. Daarvan is bijvoorbeeld sprake als er geen wettelijke grondslag bestaat voor de gegevensverwerking, wanneer zonder de juiste toestemmingen toegang wordt verkregen tot gegevens, of wanneer wettelijke waarborgen niet of onvoldoende worden toegepast. Wij onderschrijven dat de hierboven genoemde bevindingen van de CTIVD onrechtmatigheden betreffen.
Een groot deel van de bevindingen en aanbevelingen van de CTIVD is te herleiden naar tekortkomingen in het technisch beheer van bulkdatasets, het bijbehorend datamanagement en de (interne) controle op wie toegang heeft (gehad) tot welke data. Dat op deze gebieden sprake is (geweest) van structurele technische en procedurele tekortkomingen, erkennen wij. Een deel van de daarmee samenhangende risico’s en kwetsbaarheden zijn door de diensten voorafgaand aan en tijdens het onderzoek van de CTIVD reeds zelfstandig geïdentificeerd. In verschillende gevallen hebben deze risico’s daadwerkelijk geleid tot complianceincidenten, die voorafgaand en tijdens het onderzoek aan de CTIVD zijn gemeld.
Naar aanleiding van deze incidenten hebben de diensten direct maatregelen getroffen om dergelijke incidenten te detecteren, mitigeren en in de toekomst te voorkomen, dan wel het risico dat dit soort incidenten zich voordoen aanzienlijk te verkleinen. Het betreft hier maatregelen op het gebied van autorisatiebeheer en toegangsmanagement, alsook maatregelen die zien op het verder vergroten van het bewustzijn bij medewerkers rondom het belang van compliant werken. De eerste belangrijke stappen zijn zodoende al gezet.

Ten aanzien van sets ter ondersteuning van de taakuitvoering wensen wij te benadrukken dat het ontbreken van een wettelijke grondslag voor de werkwijze van de diensten niet betekent dat de diensten geen passende waarborgen hebben toegepast op dit type sets. De diensten hebben sinds geruime tijd intern beleid ten aanzien van de verwerking van gegevens die noodzakelijk zijn ter ondersteuning van de taakuitvoering. Daarin zijn nadere regels gesteld aan en waarborgen opgenomen voor het gebruik van verrijkingsdata, testdata, data t.b.v. technisch/cryptologisch onderzoek en gegevens die noodzakelijk zijn voor de uitvoering van (bijzondere) bevoegdheden. Zo mag dit type gegevens niet in bulk beschikbaar worden gesteld aan het inlichtingenproces en mogen deze gegevens enkel worden verwerkt indien het om een geringe privacyinbreuk gaat. De CTIVD heeft dit beleid bestempeld als een 'redelijke waarborg' om de privacyinbreuk te beperken.[15]

Uiteraard dient iedere vorm van gegevensverwerking door de diensten een deugdelijke wettelijke grondslag te hebben, ook als het gaat om gegevens ter ondersteuning van de taakuitvoering. Het wetsvoorstel voor de Wet bescherming nationale veiligheid door de inlichtingen- en veiligheidsdiensten (Wbnv), zoals die onlangs in consultatie is gegaan, voorziet in deze wettelijke grondslag. Nu dit wetsvoorstel nog in voorbereiding is en in ieder geval de nodige tijd zal vergen, werken de diensten aan de implementatie van een voorlopige oplossing die past binnen het huidig wettelijk kader en tevens tegemoetkomt aan de specifieke aard van sets ter ondersteuning van de taakuitvoering. Over deze werkwijze zijn de diensten in overleg met de CTIVD.

Patroon en doorschuiven
Deze leden constateren dat meerdere knelpunten eerder door de CTIVD gesignaleerd zijn: het niet als zodanig behandelen van bulkdata, het te lang bewaren en niet tijdig vernietigen, de versnipperde datahuishouding en de vertaling van beleid naar praktijk.

Vraag 4
Kunt u een overzicht geven van alle toezeggingen sinds 2018 over bulkdata (naar aanleiding van onder meer de rapporten 55, 70, 71, 79 en 84 en de voortgangsrapportages), met per toezegging de status, de verantwoordelijke en de datum van uitvoering?

Antwoord op vraag 4
Het opvolgen van de aanbevelingen van de CTIVD wordt gemonitord door de Compliance Offices van de AIVD en de MIVD. Hiervoor wordt onder andere een overzicht bijgehouden van de status per aanbeveling naar aanleiding van de monitoring. Voor de aanbevelingen ten aanzien van bulkdatasets uit de rapporten van de CTIVD is er per aanbeveling de status met toelichting toegevoegd. In het overzicht is rapport 84 niet opgenomen gezien er op dit moment uitvoering wordt gegeven aan de desbetreffende aanbevelingen. De Directeur-Generaal van de AIVD en de Directeur van de MIVD zijn verantwoordelijk voor het uitvoeren van de overgenomen aanbevelingen.

Overzicht opvolging aanbevelingen ten aanzien van Bulkdatasets

Rapport 70 - Het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan door de AIVD en de MIVD (2020)

Aanbeveling 70.4
Maak overkoepelend beleid voor bulkdatasets ongeacht de bevoegdheid waarmee deze zijn verkregen. Leg hierin eenduidig vast welke waarborgen van toepassing zijn, waar de verantwoordelijkheid voor de naleving daarvan is belegd en hoe deze waarborgen in de praktijk tot uiting komen.

Status Opgevolgd.

[15] Zie CTIVD rapport nr. 84 over de verwerking van bulkdatasets door de AIVD en MIVD (2026), p. 33.

Toelichting Er is gezamenlijk beleid vastgesteld ten aanzien van bulkdatasets. Daarnaast zijn de werkwijzen voor een eenduidige toepassing van de waarborgen vastgelegd in werkinstructies.

Aanbeveling 70.7
Vernietig de bulkdatasets die integraal als relevant zijn beoordeeld.

Status Aanbeveling niet overgenomen.

Toelichting Destijds is in de beleidsreactie aangegeven dat de bulkdatasets niet vernietigd zouden worden, omdat de ministers van oordeel waren dat de wijze waarop de diensten de bulkdatasets op relevantie hadden beoordeeld, met inachtneming van het wettelijk kader, rechtmatig was. Uiteindelijk zijn de bulkdatasets alsnog vernietigd na een bindend oordeel van de afdeling klachtbehandeling van de CTIVD.

Aanbeveling 70.7
Realiseer effectieve afstand, inclusief fysieke afstand, tussen data-analisten met 'buitenbakrechten' en het inlichtingenteam waaraan zij zijn verbonden.
- Richt een gestandaardiseerde procedure in voor periodieke controle van buitenbakautorisaties van data-analisten.
- Het (geautomatiseerd) vastleggen van buitenbakbevragingen door dataanalisten dient op basis van artikel 18 en 24 Wiv 2017 nadrukkelijk ook gericht te zijn op interne en externe controledoeleinden.
- De diensten dienen ten slotte de (door)ontwikkeling van rapportages over de bevragingen van bulkdatasets een hoge prioriteit toe te kennen, nu deze randvoorwaardelijk zijn voor een rechtmatige verwerking.

Status Opgevolgd.

Toelichting Er is gezamenlijk beleid vastgesteld ten aanzien van bulkdatasets. Daarnaast zijn de werkwijzen voor een eenduidige toepassing van de waarborgen vastgelegd in werkinstructies.

Rapport 71 - Het verzamelen en verder verwerken van passagiersgegevens van luchtvaartmaatschappijen door de AIVD en de MIVD

Aanbeveling 71.1
De AIVD en de MIVD hebben de API-gegevens niet aangemerkt als een bulkdataset. Dit dient zo spoedig mogelijk te gebeuren. Aanbevolen wordt aan beide diensten om te inventariseren of er meer bulkdatabestanden aanwezig zijn en daarop het beleid toe te passen.

Status Opgevolgd.

Toelichting De API-gegevens zijn aangemerkt als bulkdataset waardoor de waarborgen die voortvloeien uit de Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017 worden toegepast.

Aanbeveling 71.2
De AIVD en de MIVD dienen alsnog een schriftelijke toets op de noodzakelijkheid, proportionaliteit en subsidiariteit uit te voeren voor het verzamelen van API-gegevens, conform het beleid voor bulkdatasets. Bovendien moet deze toets periodiek (jaarlijks) worden herhaald gezien de voortdurende verzameling van de passagiersgegevens.

Status Opgevolgd.

Toelichting De API-gegevens zijn aangemerkt als bulkdataset waardoor de

waarborgen die voortvloeien uit de Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017 worden toegepast.

Aanbeveling 71.3
De CTIVD beveelt aan dat de beide diensten onderzoeken op welke wijze de autorisaties voor het gebruik van de applicatie voor de verdere verwerking van API-gegevens strikter ingeregeld kunnen worden, waarbij rekening wordt gehouden met de verschillende functies en bijbehorende taken binnen de AIVD en de MIVD.

Status Opgevolgd.

Toelichting De API-gegevens zijn aangemerkt als bulkdataset waardoor de waarborgen die voortvloeien uit de Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017 worden toegepast.

Aanbeveling 71.4
De diensten dienen een zodanige vastlegging van de verdere gegevensverwerkingen te bewerkstelligen dat een adequate interne controle en effectief extern toezicht mogelijk is.

Status Opgevolgd.
Toelichting De interne logging wordt uitgebreid door de AIVD en MIVD naar aanleiding van rapport 84 om compliant werken te monitoren en incidenten in de toekomst zo veel mogelijk te kunnen voorkomen, sneller te kunnen detecteren en beter te kunnen mitigeren.

Aanbeveling 71.5
De CTIVD beveelt de AIVD en de MIVD aan periodiek na te gaan of de opgeslagen gegevens nog betekenis hebben en of eerder verworven datasets (passagiersgegevens) nog noodzakelijk zijn voor het doel waarvoor zij zijn verzameld.

Status Opgevolgd.

Toelichting De API-gegevens zijn aangemerkt als bulkdataset waardoor de waarborgen die voortvloeien uit de Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017 worden toegepast.

Aanbeveling 71.6
De diensten dienen een zodanige adequate interne controle te bewerkstelligen dat hiermee wordt voldaan aan de eisen die de zorgplicht uit artikel 24 Wiv 2017 stelt.

Status Opgevolgd.

Toelichting Er is een intern compliance-stelsel ingericht die bijdraagt aan het controleren en monitoren van de zorgplicht uit artikel 24 Wiv 2017. De compliancefunctie wordt in het nieuwe wetsvoorstel verder bestendigd.

Aanbeveling 71.7
De AIVD dient in samenspraak met de MIVD nader invulling te geven aan het beleid en de wettelijke vereisten voor gegevensverwerkingen in de vorm van concrete procesbeschrijvingen, werkinstructies, en implementatie in de technische systemen, waarbij oog is voor de aard en de omvang van de

gegevens en de inbreuk die de verzameling en de verdere verwerking daarvan met zich meebrengt.

Status Opgevolgd.

Toelichting Er is gezamenlijk beleid vastgesteld ten aanzien van bulkdatasets. Daarnaast zijn de werkwijzen voor een eenduidige toepassing van de waarborgen vastgelegd in werkinstructies.

Rapport 79 - De inzet van Virtuele Agenten door de AIVD en MIVD (2024)

Aanbeveling 79.3
Indien virtuele agenten worden aangestuurd op het verwerven van bulkdatasets dient dit vastgelegd te worden in de aanvraag voor de inzet van de agentbevoegdheid waarin het doel van de inzet wordt beschreven. Tevens dient direct na de verwerving van een bulkdataset te worden beoordeeld of alle (typen) gegevens daadwerkelijk noodzakelijk zijn om de in de motivering aangegeven doelen te bereiken. Gegevens die niet noodzakelijk zijn, moeten worden vernietigd. Dit dient te worden meegewogen in de proportionaliteitstoets bij de verwerving van een bulkdataset.

Status Opgevolgd.

Toelichting Aanbeveling deels overgenomen. In het toestemmingsverzoek voor de inzet van de agentenbevoegdheid wordt opgenomen wanneer het doel van de inzet het verwerven van een bulkdataset is. Het tweede gedeelte van de aanbeveling voor het zo spoedig mogelijk na de verwerving van een bulkdataset te beoordelen of alle (typen) gegevens daadwerkelijk noodzakelijk zijn om de in de motivering aangegeven doelen te bereiken is niet overgenomen. Dit deel van de aanbeveling is niet uitvoerbaar gezien de aard van een bulkdataset. Dit is uitgebreid toegelicht in de beleidsreactie.

Ook ten aanzien van het ‘doorschuiven’ van oplossingen voor de onrechtmatigheden en onzorgvuldigheden naar de toekomst is volgens deze leden sprake van een patroon. Terugkerende knelpunten werden eerder doorgeschoven naar de komst van de resultaten van de evaluatiecommissie (2020), daarna naar de komst van de Tijdelijke Wet (2023) en nu (2026) naar de komst van de nieuwe wet.

Vraag 3
Herkent u dit patroon van terugkerende knelpunten? Zo nee, waarom niet? Zo ja, hoe beoordeelt u de herhaling gezien de eerdere toezeggingen om de knelpunten aan te pakken, en wat is volgens u de oorzaak?
Vraag 5
Herkent u dit patroon van doorschuiven? Zo nee, waarom niet. Zo ja, hoe gaat u voorkomen dat de knelpunten steeds doorgeschoven blijven worden?

Antwoord op vragen 3 en 5
De CTIVD heeft eerder vergelijkbare tekortkomingen ten aanzien van het gebruik van bulkdatasets gesignaleerd. Zo heeft de CTIVD in toezichtsrapporten nr. 70 en 71 over de verwerking van passagiersgegevens van luchtvaartmaatschappijen en het verzamelen van bulkdatasets met de hackbevoegdheid en de verdere verwerking daarvan onder meer aandacht gevraagd voor de naleving van de waarborgen voor de verdere verwerking van bulkdatasets. Naar aanleiding van deze rapporten hebben onze ambtsvoorgangers de Tijdelijke regeling verdere verwerking bulkdatasets Wiv 2017 geïntroduceerd, met daarin aanvullende waarborgen en maatregelen die meer recht doen aan de bescherming van de fundamentele rechten van burgers en de operationele waarde van bulkdatasets voor de diensten. De CTIVD stelt nu vast dat in de uitvoering en (technische) implementatie van die waarborgen nog winst valt te behalen. Zoals de CTIVD ook

heeft vastgesteld in haar onderzoek, staat de (verdere) verbetering van de omgang met bulkdatasets bij de diensten hoog op de agenda. Gezien de aard van de tekortkomingen en de complexiteit van het onderwerp is structurele verbetering echter een kwestie van de lange adem. De benodigde technische verbetermaatregelen vergen aanpassingen, bijvoorbeeld in de IT-systemen, die tijd en capaciteit kosten. De realisatie van deze structurele verbeteringen zal daarom een langdurige en consistente inspanning vergen waar, gelet op het belang van het thema, intern op wordt gestuurd.

Wij herkennen ons derhalve in het door de CTIVD geschetste beeld van terugkerende knelpunten en zetten het reeds ingezette verbetertraject de komende tijd voort. Wij herkennen ons niet in een patroon van doorschuiven. Tijdens het opstellen van het conceptwetsvoorstel van de Wbnv is expliciet aandacht geweest voor de knelpunten die zijn geïdentificeerd ten aanzien van de verwerking van bulkdatasets. Dit nieuwe wetsvoorstel beoogt een duidelijk stelsel te creëren ten aanzien van de verwerking van bulkdatasets, dat recht doet aan de noodzakelijke slagkracht voor de diensten en tegelijkertijd voorziet in voldoende waarborgen. Vanzelfsprekend wisselen wij graag te zijner tijd van gedachten met uw Kamer over dit wetsvoorstel.

Omvang van de bulkdata en het aandeel Nederlanders
Het CTIVD-rapport nr. 84 beschrijft bulkdatasets als omvangrijke verzamelingen persoonsgegevens met soms miljoenen regels en stelt dat verreweg de meeste betrokkenen niets met spionage of terrorisme te maken hebben. Het bezit van al die data brengt ook risico's met zich mee. Daarom hebben de aan het woord zijnde leden enkele vragen om zicht te krijgen op de omvang van deze data, het aandeel data over Nederlanders en de bijbehorende risico's.

Vraag 6
Kunt u aangeven wat de actuele omvang is van de bulkdatasets, uitgedrukt in (a) aantal sets, (b) aantal regels (rijen), (c) opslagvolume (bijvoorbeeld in terabytes) en (d) aantal unieke personen, zo nodig bij benadering/ in bandbreedtes (bijvoorbeeld minder dan een miljoen, een tot tien miljoen, meer dan honderd miljoen)?

Vraag 7
Kunt u een schatting geven van het aandeel Nederlanders, of van gegevens van Nederlanders? Dit bijvoorbeeld via een vertrouwelijke steekproef door de CTIVD? Kunt u dit toelichten?

Vraag 8
Kunt u aangeven hoeveel sets, regels of volume gebruikt worden 'ter ondersteuning van de taakuitvoering', en welk deel daarvan persoonsgegevens bevat? Indien u deze gegevens niet openbaar wil maken, ontvangen deze leden graag een inhoudelijke onderbouwing. Indien volgens u geheimhouding van toepassing is, kunt u dan motiveren welk specifiek geheimhoudingsbelang publicatie van geaggregeerde cijfers in de weg staat?

Antwoord op vragen 6, 7 en 8
Gelet op de wettelijke plicht tot geheimhouding wordt in het openbaar niet ingegaan op de bronnen, het actuele kennisniveau en de modus operandi van de diensten. Bronbescherming is een van de hoogste prioriteiten van de diensten, en is ook van toepassing op het verwerven en verder verwerken van bulkdatasets. We doen derhalve geen uitspraken over aantallen. De diensten kunnen hun wettelijke taak uitsluitend binnen een zekere mate van geheimhouding uitoefenen.
Het geven van inzicht daarin gaat ten koste van het goed functioneren van de diensten en daarmee ten koste van de bescherming van de nationale veiligheid.

Risico's van de dataopslag
Het bezit van grote bulkdatasets kent risico's. Het CTIVD-rapport nr. 84 beschrijft volgens deze leden onder meer onbevoegde toegang van binnenuit, te lang
bewaren en gebruik buiten de waarborgen van het bulkdatasetregime. Daarnaast zijn er andere risico's, zoals hacks en datalekken en misbruik door medewerkers.

Vraag 9
Welke risico's ziet u bij de opslag van grote bulkdatasets? Graag een volledige opsomming met toelichting per risico.

Vraag 10
Hoe groot of klein schat u deze risico's in? Bestaat er een formele risicoanalyse voor bulkdata? Zo ja, door wie is die opgesteld en door wie getoetst?

Antwoord op vragen 9 en 10
Er bestaat een formele risicoanalyse voor bulkdata. Deze is opgesteld door het Compliance & Risk Office.

Zoals reeds genoemd is een groot deel van de bevindingen en aanbevelingen van de CTIVD te herleiden naar tekortkomingen in het technisch beheer van bulkdatasets, het bijbehorend datamanagement en de (interne) controle op wie toegang heeft (gehad) tot welke data. Hier zitten tevens de grootste risico's en kwetsbaarheden, die in verschillende gevallen daadwerkelijk hebben geleid tot compliance-incidenten die voorafgaand en tijdens het onderzoek aan de CTIVD zijn gemeld. Gelet op de wettelijke plicht tot geheimhouding kunnen wij niet ingaan op de inhoud van deze compliance-meldingen. Wel benadrukken wij dat de diensten naar aanleiding van deze maatregelen direct maatregelen hebben getroffen om dergelijke incidenten te detecteren, mitigeren en in de toekomst te voorkomen, dan wel het risico dat dit soort incidenten zich voordoen aanzienlijk te verkleinen. Het betreft hier maatregelen op het gebied van autorisatiebeheer en toegangsmanagement, alsook maatregelen die zien op het verder vergroten van het bewustzijn bij medewerkers rondom het belang van compliant werken.
Wij onderstrepen evenwel dat de benodigde technische verbetermaatregelen aanpassingen vergen, bijvoorbeeld in de IT-systemen, die tijd en capaciteit kosten. De realisatie van deze structurele verbeteringen zal daarom een substantiële en consistente inspanning vergen. De diensten zullen de CTIVD periodiek op de hoogte houden van de ontwikkelingen en vorderingen op dit gebied.

Tijdens het opstellen van het conceptwetsvoorstel van de Wbnv is expliciet aandacht geweest voor de knelpunten die zijn geïdentificeerd ten aanzien van de verwerking van bulkdatasets. Dit nieuwe wetsvoorstel beoogt een duidelijk stelsel te creëren ten aanzien van de verwerking van bulkdatasets, dat recht doet aan de noodzakelijke slagkracht voor de diensten en tegelijkertijd voorziet in voldoende waarborgen. Vanzelfsprekend wisselen wij graag te zijner tijd van gedachten met uw Kamer over dit wetsvoorstel.

Vraag 11
Hoeveel beveiligingsincidenten, gevallen van onbevoegde toegang en vermoedens van misbruik zijn er volgens u de afgelopen vijf jaar geregistreerd bij bulkdatasets, en wat waren de gevolgen?

Gelet op de wettelijke plicht tot geheimhouding wordt in het openbaar niet ingegaan op de bronnen, het actuele kennisniveau en de modus operandi van de diensten. We doen derhalve geen uitspraken over aantallen. De diensten kunnen hun wettelijke taak uitsluitend binnen een zekere mate van geheimhouding uitoefenen. Het geven van inzicht daarin gaat ten koste van het goed functioneren van de diensten en daarmee ten koste van de bescherming van de nationale veiligheid.

Bronnen van bulkdata en het criterium 'openbaar toegankelijk'
Het CTIVD-rapport nr. 84 noemt de invulling en weging van het criterium openbare toegankelijkheid "discutabel" en het is volgens de CTIVD daarbij niet onrechtmatig om zulke sets als openbaar aan te merken, maar die weging zegt weinig over de privacy inbreuk. Het gaat onder meer om sets van partnerdiensten, om kortstondig en tegen betaling op internet aangeboden sets (soms uit datalekken) en om commercieel aangeboden sets. In uw brief staat dat u het oordeel "discutabel" niet herkent waarbij u verwijst naar de toelichting bij het nieuwe Wetboek van Strafvordering.

In het rapport nummer 74 van de CTIVD 'Automated OSINT: tools en bronnen voor openbronnenonderzoek' (verder CTIVD rapport nr. 74) stelde de CTIVD dat verwerking van gegevens uit gelekte datasets een grotere inbreuk op fundamentele rechten meebrengt. De strafbaarstelling sinds 1 maart 2019 van het wederrechtelijk overnemen of doorgeven van niet openbare gegevens uit een geautomatiseerd werk (art. 138c Wetboek van Strafrecht, hierna: Sr) en van heling van niet-openbare gegevens (art. 139g Sr) noemde zij daarbij indicatief voor hoe naar het overnemen van gegevens uit gelekte datasets wordt gekeken.
Artikel 139g Sr stelt onder meer het verwerven of voorhanden hebben van nietopenbare gegevens strafbaar als men wist of redelijkerwijs moest vermoeden dat die door een misdrijf zijn verkregen,

en kent een uitzondering voor het algemeen belang. Een lager toegangsregime betekent volgens de aan het woord zijnde leden onder meer een ruimere kring van gebruikers en, bij A-sets, geen bindend toezicht van de CTIVD.

Vraag 12
Aangaande het overzicht van de bronnen, kunt u aangeven wat het aandeel per herkomst (overheid, informanten, buitenlandse diensten, commercieel, gelekt of openbaar aangeboden, hack, agent, interceptie) is, en welk aandeel als 'openbaar toegankelijk' aangemerkt is en daarom in een lager toegangsregime geplaatst?

Vraag 13
Aangaande het criterium 'openbaar toegankelijk', kunt u aangeven wat het aandeel per herkomst (overheid, informanten, buitenlandse diensten, commercieel, gelekt of openbaar aangeboden, hack, agent, interceptie) is? Hoeveel sets zijn als 'openbaar toegankelijk' aangemerkt, uitgesplitst naar partnerdienst, gelekt of gehackt en commercieel? Hoeveel daarvan staan in het standaardregime, en welke bewaar- en beoordelingstermijnen gelden daar?

Antwoord op de vragen 12 en 13
Gelet op de wettelijke plicht tot geheimhouding wordt in het openbaar niet ingegaan op de bronnen, het actuele kennisniveau en de modus operandi van de diensten. Bronbescherming is een van de hoogste prioriteiten van de diensten, en is ook van toepassing op het verwerven en verder verwerken van bulkdatasets.
We doen derhalve geen uitspraken over aantallen. De diensten kunnen hun wettelijke taak uitsluitend binnen een zekere mate van geheimhouding uitoefenen. Het geven van inzicht daarin gaat ten koste van het goed functioneren van de diensten en daarmee ten koste van de bescherming van de nationale veiligheid.

Vraag 14
Erkent u dat een set die door de betrokkenen nooit zelf openbaar is gemaakt, niet minder ingrijpend wordt doordat deze (tijdelijk) openbaar was/is? Kunt u aangeven waarom "openbaar' dan een weegfactor is die tot een lager regime kan leiden?

De Tijdelijke regeling schrijft voor dat de diensten, bij het bepalen van de privacyinbreuk die wordt gemaakt door een bulkdataset, meewegen in hoeverre de bulkdataset voor eenieder toegankelijk is. Volgens de CTIVD is de invulling en weging van dit openbaarheidscriterium echter discutabel. In dat verband wijst de CTIVD erop dat de diensten bulkdatasets soms aanmerken als openbaar toegankelijk als zij niet kunnen vaststellen of dit feitelijk klopt, de gegevens afkomstig zijn uit een datalek of door commerciële partijen tegen betaling worden aangeboden (ongeacht het gevraagde bedrag). Tegen deze achtergrond doet de CTIVD de aanbeveling om bulkdatasets als niet openbaar toegankelijk aan te merken wanneer niet feitelijk kan worden vastgesteld of de verworven gegevens openbaar toegankelijk zijn (geweest), en in regelgeving of beleid aan te scherpen hoe dit criterium moet worden betrokken bij de beoordeling van de privacyinbreuk van bulkdatasets.

Deze aanbeveling is grotendeels overgenomen. Voortaan merken de diensten bulkdatasets aan als niet openbaar toegankelijk indien onduidelijk is of deze openbaar toegankelijk zijn (geweest). Ook hebben de diensten tijdens de onderzoeksperiode de regels rondom het openbaarheidscriterium in het beleid verduidelijkt en aangescherpt. Zo is inmiddels vastgelegd dat de hoogte van het bedrag dat wordt gevraagd voor de aanschaf van een bulkdataset aanleiding kan zijn om de bulkdataset niet langer als openbaar toegankelijk te beschouwen. De constatering van de CTIVD dat de invulling en weging van het openbaarheidscriterium discutabel is, herkennen wij nadrukkelijk niet. Bij de invulling van dit criterium hebben de diensten, in navolging van de CTIVD in rapport nr. 74 (2022), aansluiting gezocht bij de uitleg die aan openbronnenonderzoek wordt gegeven in de Memorie van Toelichting bij het Wetboek van Strafvordering. Op basis van de uitleg die wordt gegeven aan openbronnenonderzoek in CTIVD-rapport nr. 74 en de Memorie van Toelichting bij het Wetboek van Strafvordering, is niet uitgesloten dat bulkdatasets met daarin gegevens afkomstig uit een datalek en bulkdatasets die tegen betaling beschikbaar worden gesteld, aangemerkt kunnen worden als 'openbaar toegankelijk'.

De gedachte daarachter is dat de ernst van de privacy-inbreuk deels samenhangt met het bestaan van een gerechtvaardigde verwachting van privacy bij betrokkenen (in de jurisprudentie van het

EHRM ook wel aangeduid als de '*reasonable expectation of privacy')*[16]. Deze gerechtvaardigde verwachting van privacy zal doorgaans kleiner zijn bij gegevens die zich reeds in het publieke domein bevinden, ook als deze gegevens niet door betrokkenen zelf openbaar zijn gemaakt. Het verschil in privacy-inbreuk zit dus niet zozeer in de aard van de gegevens, maar in de gerechtvaardigde verwachting van privacy die doorbroken wordt.

Zoals benoemd in de beleidsreactie, wijst de praktijk uit dat, hoewel een openbaar karakter de diensten de mogelijkheid biedt een bulkdataset in een lager toegangsregime te plaatsen, de aard van de gegevens en de mate van privacyinbreuk die de verwerking van de gegevens met zich meebrengt (en niet het openbaarheidscriterium) doorslaggevend zijn voor het vaststellen van het toegangsregime. In de Wbnv is nadrukkelijk aandacht voor de invulling van het openbaarheidscriterium.

Vraag 15
Bent u bereid het criterium te beperken tot gegevens die de betrokkene zelf openbaar maakte of redelijkerwijs openbaar mocht achten, en gelekte of illegaal verkregen gegevens daarvan uit te sluiten? Zo nee, waarom niet?

In de beleidsreactie op het CTIVD-rapport hebben wij reeds aangegeven dat wij bij de invulling van het openbaarheidscriterium, in navolging van de CTIVD in rapport nr. 74, aansluiting hebben gezocht bij de uitleg die aan openbronnenonderzoek wordt gegeven in de Memorie van Toelichting bij het Wetboek van Strafvordering. Op basis van de uitleg die wordt gegeven aan openbronnenonderzoek in CTIVDrapport nr. 74 en de Memorie van Toelichting bij het Wetboek van Strafvordering, is niet uitgesloten dat bulkdatasets met daarin gegevens afkomstig uit een datalek en bulkdatasets die tegen betaling beschikbaar worden gesteld, aangemerkt kunnen worden als 'openbaar toegankelijk'. Aan deze invulling houden wij vast.

Vraag 16
Kunt u aangeven welke concrete criteria de diensten hanteren sinds de beleidsreactie om vast te stellen of een set openbaar is? Worden bestaande sets daarop herbeoordeeld en worden die herbeoordelingen aan de CTIVD gemeld?

Een bulkdataset is openbaar indien deze voor eenieder toegankelijk is, al dan niet na betaling. Volgens intern beleid kan de hoogte van het bedrag dat wordt gevraagd voor de aanschaf van een bulkdataset evenwel aanleiding zijn om de bulkdataset niet als openbaar toegankelijk te beschouwen. Naar aanleiding van het CTIVD-rapport hanteren de diensten tevens het uitgangspunt dat een set niet openbaar toegankelijk is indien onduidelijk is of deze openbaar toegankelijk is (geweest).
Een herbeoordeling van bestaande sets achten wij niet noodzakelijk. De praktijk wijst immers uit dat de aard van de gegevens en de mate van privacyinbreuk die de verwerking van de gegevens met zich meebrengt (en niet het openbaarheidscriterium) doorslaggevend zijn voor het vaststellen van het toegangsregime.

Gelekte en gestolen data

Vraag 17
U verwijst naar de toelichting bij het nieuwe Wetboek van Strafvordering, waarin bronnen met een financiële drempel als publiek toegankelijk gelden. Kunt u aangeven waarom een strafvorderlijke uitleg passend is voor inlichtingendiensten? Hanteert u voor 'openbaar toegankelijk' dezelfde betekenis als het strafrecht voor 'niet-openbare gegevens' in artikel 138c en 139g Sr? Zo ja, hoe kan een set die na een datalek breed circuleert dan als 'openbaar' gelden in de zin van de Wet op de inlichtingen- en veiligheidsdiensten (verder Wiv)? Zo nee, waarom wordt een andere maatstaf gehanteerd?

Vraag 18
Kunt u aangeven op welke rechtsgrond de diensten niet-openbare gegevens kunnen verwerven of voorhanden hebben waarvan zij weten of redelijkerwijs moeten vermoeden dat deze door een misdrijf zijn verkregen? En geldt die rechtsgrond ook voor het kopen van zulke sets, voor sets van partnerdiensten en voor het gebruik ervan? Wordt daarbij

[16] Zie bijvoorbeeld EHRM (GK) d.d. 5 september 2017, Barbulescu v. Roemenië, nr. 61496/08 en HR d.d. 11 november 2014, NJ2015/14, ECLI:NL:HR:2014:3145.

per geval een afweging gemaakt en door wie?

Vraag 19
Kunt u toelichten welke toets voorafgaat aan het kopen van gestolen of gelekte datasets en wie beslist? Is er een ministeriële toestemming? Hoe wordt het risico op financiering van criminaliteit gewogen?

Antwoord vragen 17, 18 en 19
Bij de invulling van het openbaarheidscriterium hebben de diensten, in navolging van de CTIVD in rapport nr. 74 (2022), aansluiting gezocht bij de uitleg die daaraan wordt gegeven in de Memorie van Toelichting bij het Wetboek van Strafvordering. Dit draagt bij aan een consistente uitleg van het begrip, maar betekent niet dat het strafvorderlijke kader rechtstreeks van toepassing is op de taakuitvoering van de diensten. Voor de beoordeling is onder meer relevant of de gegevens in beginsel voor eenieder onder gelijke voorwaarden beschikbaar zijn, dan wel of sprake is van een vorm van toegangscontrole of selectie waardoor degegevens slechts voor een beperkte kring toegankelijk zijn. Daarbij kunnen ook de aard van de gegevens en de wijze waarop deze worden aangeboden een rol spelen. Op basis van de uitleg die wordt gegeven aan openbronnenonderzoek in CTIVD-rapport nr. 74 en de Memorie van Toelichting bij het Wetboek van Strafvordering, is niet uitgesloten dat bulkdatasets met daarin gegevens afkomstig uit een datalek en bulkdatasets die tegen betaling beschikbaar worden gesteld, aangemerkt kunnen worden als 'openbaar toegankelijk'.

Het voorgaande laat onverlet dat de verwerving en verdere verwerking van openbaar toegankelijke gegevens door de diensten moet voldoen aan de eisen van de Wiv 2017, waaronder de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit. De openbare toegankelijkheid van gegevens betekent derhalve niet dat deze zonder nadere afweging door de diensten kunnen worden verwerkt.

De bevoegdheid van de diensten om (openbare en niet openbare) gegevens te verwerven en verwerken vloeit voort uit de Wiv 2017. Het enkele feit dat gegevens mogelijk door een derde op onrechtmatige of strafbare wijze zijn verkregen, betekent niet zonder meer dat de diensten deze gegevens niet zouden mogen verwerven of verwerken. Het kan in de praktijk dan ook voorkomen dat een bulkdataset wordt verworven op een (illegale) handelsplaats. In dat geval kan er sprake zijn van een strafbaar feit en dient de Landelijk Officier van Justitie en Terrorismebestrijding (LOvJ) toestemming te verlenen voor het mogen plegen van dat strafbare feit. Daarnaast dient er een reguliere toestemming te zijn voor de verwerving van een bulkdataset. Deze toestemming moet worden gegeven door het hoofd van de dienst of de verantwoordelijke minister. Een bijzonder aandachtspunt vormt het risico dat door betaling voor dergelijke gegevens criminele activiteiten direct of indirect worden gefinancierd of gestimuleerd. Dit risico wordt expliciet betrokken bij de afweging of de verwerving noodzakelijk, proportioneel en subsidiair is. Daarbij is tevens van aandacht voor de vraag of de aankoop kan bijdragen aan het ontstaan of in stand houden van een markt voor onrechtmatig verkregen gegevens.

Vraag 20
Weet u hoeveel sets er de afgelopen vijf jaar verworven zijn uit datalekken of via criminele marktplaatsen en welk bedrag daarvoor betaald is, zo nodig als bandbreedte?

Gelet op de wettelijke plicht tot geheimhouding wordt in het openbaar niet ingegaan op de bronnen, het actuele kennisniveau en de modus operandi van de diensten. Bronbescherming is een van de hoogste prioriteiten van de diensten, en is ook van toepassing op het verwerven en verder verwerken van bulkdatasets. We doen derhalve geen uitspraken over aantallen. De diensten kunnen hun wettelijke taak uitsluitend binnen een zekere mate van geheimhouding uitoefenen.
Het geven van inzicht daarin gaat ten koste van het goed functioneren van de diensten en daarmee ten koste van de bescherming van de nationale veiligheid.

Vraag 21
Onderzoekt u of en wanneer betrokkenen van wie gegevens zijn verworven uit een datalek daarover geïnformeerd kunnen worden, bijvoorbeeld via bestaande meldkanalen?

Op basis van de Wiv 2017 bestaat een dergelijke notificatieplicht niet. Desondanks kunnen zich situaties voordoen waarin de diensten het wenselijk achten om getroffen personen te informeren. In die gevallen zullen de diensten hen via de geëigende kanalen informeren.

Partnerdiensten

Vraag 22
Kunt u aangeven hoeveel bulkdatasets ontvangen zijn van buitenlandse diensten? Is bekend hoe die sets zijn verworven (hack, interceptie, koop) en vragen de diensten dat na?

Gelet op de wettelijke plicht tot geheimhouding wordt in het openbaar niet ingegaan op de bronnen, het actuele kennisniveau en de modus operandi van de diensten. Bronbescherming is een van de hoogste prioriteiten van de diensten, en is ook van toepassing op het verwerven en verder verwerken van bulkdatasets. We doen derhalve geen uitspraken over aantallen. De diensten kunnen hun wettelijke taak uitsluitend binnen een zekere mate van geheimhouding uitoefenen.
Het geven van inzicht daarin gaat ten koste van het goed functioneren van de diensten en daarmee ten koste van de bescherming van de nationale veiligheid.

Vraag 23
Als een partnerdienst een set met bijzondere bevoegdheden verwierf, borgt u dan dat in Nederland niet alsnog een lichter regime geldt dan bij eigen verwerving?

De Tijdelijke regeling verdere verwerking bulkdatasets is gebaseerd op twee uitgangspunten. Ten eerste het uitgangspunt dat de wijze van verwerving niet maatgevend is voor de beperking van het recht op bescherming van de persoonlijke levenssfeer die met de verdere verwerking van de bulkdataset gepaard gaat. Het tweede uitgangspunt is het principe dat naarmate de beperking van het recht op bescherming van de persoonlijke levenssfeer als gevolg van de verdere verwerking van de bulkdatasets groter is, dit gepaard dient te gaan met extra waarborgen. Dus niet de manier van verwerving, maar de aard en omvang van de beperking is bepalend voor de toepassing van één van de drie regimes met waarborgen voor het verkrijgen van inhoudelijke gegevens uit de bulkdatasets.

Commerciële data

Vraag 24
Kunt u toelichten welke commerciële data verwerkt worden en op welke wettelijke grondslag?

Wij kunnen in het openbaar niet ingaan op de vraag over welke commerciële data de diensten exact verwerken. Artikel 17 en 25 van de Wiv 2017 geven de diensten de grondslag om onder meer commerciële data te verwerven en te verwerken, met inachtneming van de eisen die bij of krachtens de Wiv 2017 of de Wvo zijn gesteld.

Vraag 25
De CTIVD noemt in rapport 74 de reikwijdte van art. 25 lid 1 onder b Wiv 2017 onduidelijk. Hanteert u een drempelbedrag of een andere norm om aan te nemen dat een betaalde set niet meer openbaar is?

Zoals gezegd hebben de diensten in intern beleid vastgelegd dat de hoogte van het bedrag dat wordt gevraagd voor de aanschaf van een bulkdataset aanleiding kan zijn om de bulkdataset niet langer als openbaar toegankelijk te beschouwen. Over een eventueel drempelbedrag doen wij geen uitspraak in de openbaarheid.

Het schaduwarchief

Vraag 26
Acht u het mogelijk dat de diensten via gekochte, gelekte of ontvangen sets gegevens raadplegen die zij anders alleen na toestemming en toetsing per geval zouden mogen verwerven? Zo ja, hoe voorkomt u dat dit de bestaande toetsing en toezicht omzeilt? Hoeveel raadplegingen vinden per jaar plaats in sets in het standaardregime en kan de CTIVD dankzij de verbeterde logging achteraf controleren wie wat heeft geraadpleegd?

De wettelijke waarborgen voor bulkdatasets zijn onverkort van toepassing op gekochte, gelekte of ontvangen bulkdatasets. De procedures zijn daar ook op ingericht. Van omzeiling van toestemming en toetsing per geval is dus geen sprake.

Over het aantal raadplegingen kunnen wij in het openbaar geen uitspraken doen.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

Pieter Heerma

De minister van Defensie,

Dilan Yesilgöz-Segerius