Bijlage I

Toetsingskader

bij het toezichtsrapport over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en de MIVD

CTIVD nr. 55

28 december 2017

Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten

Commissie van Toezicht
op de Inlichtingen- en
Veiligheidsdiensten

CTIVD nr. 55

TOEZICHTSRAPPORT

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

Inhoudsopgave

CTIVD nr. 55

INLEIDING

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

In deze bijlage wordt het toepasselijk toetsingskader met betrekking tot op internet aangeboden bulkdatasets uitgewerkt. Het toetsingskader wordt gevormd door de wet, jurisprudentie, eerdere toezichtsrapporten van de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (hierna: CTIVD), de door de ministers in dat kader overgenomen aanbevelingen en het interne beleid van Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst (hierna: AIVD respectievelijk MIVD, tezamen: de diensten). Hierbij wordt zowel de huidige Wet op de inlichtingen- en veiligheidsdiensten 2002 (hierna: Wiv 2002) als de naar verwachting toekomstige Wet op de inlichtingen- en veiligheidsdiensten 2017 (hierna: Wiv 2017) meegenomen. Met betrekking tot het interne beleid zijn twee beleidsnotities van belang die door de diensten zijn opgesteld. Deze beleidsnotities gaan over het verwerven en ontsluiten van door derden op internet aangeboden bulkdatasets onder de Wiv 2002. Deze zullen hierna worden aangehaald als “de beleidsnotities”.

Van belang zijn in dit rapport de grondrechten met betrekking tot de eerbiediging van de persoonlijke levenssfeer en de bescherming van persoonsgegevens, neergelegd in de artikelen 10 en 13 van de Grondwet. Daarnaast heeft het Europees Verdrag voor de Rechten van de Mens (hierna: EVRM) rechtstreekse werking in de Nederlandse rechtsorde. Met name de jurisprudentie met betrekking tot artikel 8 van het EVRM, gewezen door zowel het Europees Hof voor de Rechten van de Mens (hierna: EHRM) als nationale gerechten, geeft nader inzicht in de reikwijdte en interpretatie van deze grondrechten. Ook het Hof van Justitie van de Europese Unie (hierna: HvJEU) heeft arresten gewezen die richting geven aan de reikwijdte en invulling van genoemde grondrechten.

Allereerst wordt in deze bijlage vastgesteld in welke mate de verwerking van gegevens van door derden op internet aangeboden bulkdatasets een inmenging in het recht op privacy (8 EVRM) inhoudt (paragraaf 1). Deze door derden op internet aangeboden bulkdatasets zijn veelal afkomstig uit beveiligingslekken of ‘hacks’ bij bedrijven of instellingen. Vervolgens wordt in paragraaf 2 besproken op welke grondslag en onder welke voorwaarden deze inmenging plaats mag vinden. In paragraaf 3 worden de vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit uitgewerkt en wordt aangegeven wat dit betekent voor de motivering van de concrete verwerving en verwerking van een bulkdataset.

CTIVD nr. 55

TOEZICHTSRAPPORT

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

1 De privacy-inmenging

Uit jurisprudentie van het EHRM kan worden afgeleid dat het opslaan en verder verwerken van persoonsgegevens een inmenging in het recht op privacy vormt.[1] Persoonsgegevens zijn gegevens die betrekking hebben op een identificeerbare of geïdentificeerde individuele, natuurlijke personen.[2] Bij de beoordeling van de vraag of gegevens als persoonsgegeven moeten worden aangemerkt is van belang of de gegevens alleen of in combinatie met andere gegevens zó kenmerkend zijn voor een natuurlijke persoon dat deze daarmee kan worden geïdentificeerd. Daarbij worden alle middelen betrokken waarvan mag worden aangenomen dat daarmee redelijkerwijs tot identificatie kan worden gekomen.[3] De verwerking van gegevens die geen persoonsgegeven zijn, levert geen privacy-inmenging op.

Voor de waardering van de zwaarte van de privacy-inmenging zijn de factoren van belang die het EHRM in jurisprudentie heeft ontwikkeld met betrekking tot de verwerking van gegevens. Kort gezegd, moet op grond van deze jurisprudentie rekening worden gehouden met (1) de context waarin de gegevens worden verzameld, (2) de aard van de gegevens en (3) de wijze waarop de gegevens verder worden verwerkt en gebruikt.[4] Daarbij duidt een verdere verwerking van de persoonsgegevens op een zwaardere privacy-inmenging.[5]

---

1 Zie bijvoorbeeld EHRM 18 februari 2000, nr. 27798/95 *(Amann t. Zwitserland)*, par 65, EHRM 4 mei 2000, nr. 28341/95 *(Rotaru t. Roemenië)*, par. 43, EHRM 28 januari 2003, nr. 44647/98 *(Peck t. Het Verenigd Koninkrijk)*, par. 63-63, EHRM 17 juli 2003, nr. 63737/00 *(Perry t. Het Verenigd Koninkrijk)*, par. 38 en 40-41 en EHRM 17 december 2009, nr. 16428/05 *(Gardel t. Frankrijk)*, par. 62.

2 Artikel 1, onder e, van de Wiv 2002 en de Wiv 2017. Deze definitie is overeenkomstig de definitie in het Toezichtsrapport nr. 39 over de rechtmatigheid van het onderzoek op sociale media door de AIVD (2014) en de definitie uit de Wet bescherming persoonsgegevens. Identificeerbaar betekent in deze context dat de gegevens met een redelijke inspanning naar een natuurlijke persoon zijn te herleiden.

3 Zie ook HvJEU 19 oktober 2016, C-582-14 *(Breyer t. Duitsland)*, Raad van State 26 juli 2017, ECLI:NL:RVS:2017:2008, r.o. 5.1, de Artikel 29 Werkgroep opinie 4/2007 over het begrip persoonsgegevens van 20 juni 2007 en overweging 26 van de Algemene Verordening Gegevensbescherming van 27 april 2016, OJ L 119/1.

4 EHRM 4 december 2008, nr. 30562/04 en 30566/04 (*S. en Marper t. Het Verenigd Koninkrijk*), par. 67.

5 Zie ook EHRM 28 januari 2003, nr. 44647/98 (*Peck t. Het Verenigd Koninkrijk*) par. 62-63 en EHRM 2 september 2010, nr. 35623/05 (*Uzun t. Duitsland*), par. 45: *"Further elements which the Court has taken into account in this respect include the question whether there has been compilation of data on a particular individual, whether there has been processing or use of personal data or whether there has been publication of the material concerned in a manner or degree beyond that is normally foreseeable"*.

Voor de invulling van deze factoren moet ook worden gekeken naar andere jurisprudentie die rechtstreeks in de Nederlandse rechtsorde doorwerkt.[6] Uit de uitspraken van het HvJEU omtrent dataretentie, kan worden afgeleid dat het preventief opslaan van grote hoeveelheden passagiers- of telecommunicatieverkeersgegevens, waarvan de betrokkenen in meerderheid niet in relatie staan tot het doel (zoals de bestrijding van zware criminaliteit of terrorisme), een ernstige inmenging met het recht op privacy vormt.[7] De aangehaalde jurisprudentie is veelal afkomstig uit andere rechtsgebieden en heeft betrekking op andere gevallen dan het in het kader van de nationale veiligheid verwerven van op internet aangeboden bulkdatasets. Bovendien betreft het een ander type gegevens. Deze uitspraken zijn daarmee niet zonder meer toepasbaar. Wel kunnen uit deze uitspraken relevante factoren en omstandigheden worden afgeleid om de privacy-inmenging in onderhavige context te beoordelen. De drie eerder genoemde factoren uit EHRM-jurisprudentie worden hieronder toegepast op de onderhavige context.

1.1 De context waarin de gegevens worden verzameld

In het geval van door derden op internet aangeboden bulkdatasets gaat het om publiekelijk beschikbare informatie. Deze gegevens worden eenmalig door de diensten verworven. De privacy-verwachting die de betrokkenen bij publiekelijk toegankelijke informatie (open bron) mogen hebben is redelijkerwijs beperkter dan bij gegevens uit gesloten bronnen.[8] Aan de andere kant is de verwerving ingrijpender dan bij volledig open bronnen. Het gaat immers om gegevens die door de betrokkenen niet zelf publiek zijn gemaakt (zoals IP-adressen). De betrokken zijn zich er ook vaak niet van bewust dat deze informatie over hen beschikbaar wordt gesteld. Van een deel van de datasets is bekend dat deze door middel van het plegen van een strafbaar feit, zoals hacken, in de openbaarheid zijn gekomen.

1.2 De aard van de gegevens

De verworven bulkdatasets kunnen miljoenen gebruikersgegevens bevatten. Deze datasets bevatten gegevens zoals (gebruikers)namen, (gehashte) wachtwoorden, e-mailadressen en gelogde IP-adressen. Hoewel dit persoonsgegevens betreffen, moet de inhoud van de datasets minder gevoelig worden geacht dan de in de aangehaalde jurisprudentie genoemde gegevens. Uit DNA-, passagiers- of telecommunicatieverkeersgegevens kunnen immers een min of meer gedetailleerd beeld van bepaalde delen van het privéleven of gedragspatronen worden afgeleid. Uit de gegevens uit de datasets kan slechts beperkt informatie over de gebruiker worden afgeleid, zoals een accountnaam of e-mailadres. Aan de andere kant moet ook worden vastgesteld dat de bulkdatasets in overgrote meerderheid gegevens over personen bevatten die geen aanleiding hebben gegeven in de aandacht van de diensten staan. De gegevens worden daarmee (voornamelijk) voor toekomstig gebruik opgeslagen.

---

[6] De regulering van bevoegdheden van inlichtingen- en veiligheidsdiensten is expliciet aan de EU-Lidstaten zelf overgelaten. Zie: artikel 4 lid 2 van het Verdrag betreffende de Europese Unie. Het Handvest van Grondrechten van de Europese Unie biedt wel bescherming als de "kern" van het recht op bescherming van persoonsgegevens en het recht op privacy in het geding is. Zie HvJEU 21 december 2016, C-203/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB t. Post -och telestyrelsen*), par. 72-73 en 91.

[7] Zie HvJEU 8 april 2014, C-293/12 (*Digital Rights Ireland t. Ierland*) en C-594/12, ECLI:EU:C:2014:238 (*Seitlinger, Tschohl e.a. t. Kärtner Landsregierung*), HvJEU 21 december 2016, C-203/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB t. Post-och telestyrelsen*) en HvJEU 26 juli 2017, ECLI:EU:C:2017:592. Het recht op privacy is neergelegd in artikel 7 van het Europees Handvest voor de Rechten van de Mensen en het recht op bescherming van persoonsgegevens in artikel 8.

[8] Zie in vergelijkbare zin EHRM 25 september 2001, nr. 44787/98 (*P.G. en J.H. t. Het Verenigd Koninkrijk*), par. 57 en EHRM 17 juli 2003, nr. 63737/00 (*Perry t. Het Verenigd Koninkrijk*), par. 38.

1.3 De verdere verwerking van de gegevens

De gegevens uit de verworven bulkdatasets worden opgeslagen en ontsloten ten behoeve van het inlichtingenproces van beide diensten. De informatie kan, al dan niet in combinatie met andere gegevensbestanden, worden gebruikt om (nieuwe) targets te identificeren of hun inloggegevens te achterhalen. Uit EHRM-jurisprudentie volgt dat elke verdere verwerking van persoonsgegevens een meer ernstige privacy-inmenging meebrengt.

Om deze reden is het van belang dat bij de ontsluiting van een dataset, in het geval deze voor de overgrote meerderheid uit persoonsgegevens bestaat van personen die geen aanleiding tot onderzoek geven, de buitenbak-binnenbakprocedure (zie paragraaf 2.5) wordt toegepast. Op deze wijze wordt uitvoering gegeven aan het need-to-knowbeginsel en de vereisten van functie- en/of taakscheiding. Ten slotte wordt in de interne beleidsnotities een bewaartermijn vastgesteld.

Deze nadere voorwaarden voor de ontsluiting en het gebruik van de gegevens beperken de mate waarin gegevens verder worden verwerkt. Daarmee zijn in het ontsluitingsproces mechanismen ingebouwd om de privacy van de personen die in de datasets voorkomen te waarborgen.

1.4 Conclusie

Bij de verwerving van datasets met persoonsgegevens vindt een meer ernstige privacy-inmenging plaats. De verklaringen daarvoor zijn (1) de context waarin de gegevens worden verzameld (enerzijds publiekelijk beschikbare informatie waarvan de betrokkenen anderzijds niet verwachten dat deze openbaar is), (2) de aard van de informatie (beperkt per betrokkene, maar wel over miljoenen personen) en (3) het verder verwerken van de gegevens.

2 Wettelijke basis, voorzienbaarheid en waarborgen

Als sprake is van een inmenging, vereist artikel 8 EVRM dat deze bij de wet is voorzien. Dit betekent dat een privacy-inmenging een basis dient te hebben in nationale wetgeving.[9] Bovendien moet de kwaliteit van de wet zodanig zijn dat deze waarborgen tegen misbruik biedt.[10] Hoe ernstiger de privacy-inmenging is, hoe gedetailleerder wetgeving met procedurele waarborgen het EHRM vereist.[11]

Het EHRM heeft bijvoorbeeld geoordeeld dat een algemene bevoegdheid van een belastingautoriteit om relevante documenten op te vragen ten behoeve van een belastingaanslag en de inspectie daarvan een voldoende wettelijke basis vormde, voor zover daaraan beperkingen werden gesteld en deze vergezeld ging van voldoende effectieve en adequate waarborgen.[12] Ook oordeelde de Belastingkamer van de Hoge Raad in februari 2017 dat het (*'real time'*) verzamelen, vastleggen, bewerken en jarenlang bewaren van gegevens over de bewegingen van voertuigen op diverse plaatsen in Nederland (zogenoemde ANPR-gegevens) een ernstige privacy-inmenging inhoudt.[13] Vanwege deze ernstige privacy-inmenging kon het verzamelen van deze gegevens niet op de algemene taakomschrijving en bevoegdheid van de Belastingdienst om inlichtingen in te winnen worden gebaseerd.[14] Daarnaast oordeelde de Strafkamer van de Hoge Raad in 2014 dat het toezenden van voor de gebruiker van de telefoon niet-waarneembare sms-berichten als zodanig niet in een daarop toegesneden wettelijke bepaling was geregeld.[15] De algemene taakstelling van de politie was in dit concrete geval echter een voldoende grondslag, omdat daarmee maar een beperkte inbreuk werd gemaakt op de grondrechten van de verdachte.[16] Daarbij vond de Hoge Raad het wel van belang dat op basis van een intern beleid de officier van justitie een bevel moest afgeven voor de inzet van de bevoegdheid en dat de verbalisering van de inzet van het opsporingsmiddel op orde was.[17] Bovengenoemde zaken zijn illustratief voor de algemene regel dat naarmate de privacy-inmenging ernstiger is, het EHRM meer gedetailleerde wetgeving met procedurele waarborgen vereist.

De wettelijke grondslag voor de toepassing van de bevoegdheid moet toegankelijk zijn en de betrokkene moet daarbij kunnen voorzien wat de consequenties van de wettelijke bepaling zijn in het specifieke geval.[18] Aangenomen wordt dat regelgeving in het kader van de nationale veiligheid, vanwege het heimelijke karakter, niet dezelfde duidelijkheid en nauwkeurigheid kan bieden als regelgeving op andere terreinen.[19] Deze beperking van de voorzienbaarheid brengt echter een risico van willekeur en misbruik met zich mee. Daarom gelden een aantal minimumvoorwaarden waaraan de toepassing van heimelijke maatregelen moet voldoen. Zo dient duidelijk te zijn wanneer heimelijke bevoegdheden kunnen worden ingezet en welke procedurele waarborgen daarbij in acht worden genomen.[20] De

---

9 Het EHRM vereist niet dat dit een formele wet is, maar artikel 10 van de Grondwet wel.

10 Zie bijvoorbeeld EHRM 25 september 2001, nr. 44787/98 (*P.G. & J.H.t. Verenigd Koninkrijk*), par. 44 en 61, EHRM 1 juli 2008, nr. 58243/00 (*Liberty e.a. t. Het Verenigd Koninkrijk*), par. 62, EHRM 2 september 2010, nr. 35623/05 (*Uzun t. Duitsland*), par. 61 en EHRM 21 juni 2011, nr. 30194/09 (*Shimovolos t. Rusland*), par. 68.

11 Zie bijvoorbeeld EHRM 25 september 2001, nr. 44787/98 (*P.G. & J.H.t. Verenigd Koninkrijk*), par. 44, EHRM 4 december 2008, nr. 30562/04 en 30566/04 (*S. en Marper t. Het Verenigd Koninkrijk*), par. 96 en EHRM 26 oktober 2000, nr. 30985/96 *(Hasan en Chaush t. Bulgarije*), par. 84

12 EHRM 14 maart 2014, nr. 24117/08 (*Bernh Larsen Holding AS e.a. t. Noorwegen*), par. 134.

13 HR 24 februari 2017, ECLI:NL:HR:2017:286, r.o. 2.3.4 t/m 2.3.6.

14 HR 24 februari 2017, ECLI:NL:HR:2017:286, r.o. 2.3.4.

15 HR 1 juli 2014, ECLI:NL:HR:2014:1563. Zie ook HR 1 juli 2014, ECLI:NL:HR:2014:1562 (over het gebruik van de IMSI-catcher door de politie op grond van de algemene taakstelling in artikel 3 van de Politiewet).

16 HR 1 juli 2014, ECLI:NL:HR:2014:1563, r.o. 2.4.

17 HR 1 juli 2014, ECLI:NL:HR:2014:1563, r.o. 2.5.

18 EHRM 26 maart 1987, nr. 9248/81 (*Leander t. Zweden*), par. 51.

19 EHRM 26 maart 1987, nr. 9248/81 (*Leander t. Zweden*), par. 51.

20 EHRM 29 juni 2006, nr. 54934/00 (*Weber en Saravia t. Duitsland*), par. 93-94.

afweging of er voldoende waarborgen zijn, is afhankelijk van alle omstandigheden van het geval, waaronder de aard, het bereik en de duur van de inzet van de bevoegdheid, de grond op basis waarvan de bevoegdheid mag worden ingezet, de autoriteiten die bevoegd zijn toestemming te verlenen, de autoriteiten die bevoegd zijn de bevoegdheid uit te oefenen en de autoriteiten op die op de uitvoering toezicht houden.[21]

De CTIVD stelt vast dat het in de context van het onderhavige onderzoek om drie juridische bases kan gaan: (1) het verzamelen van gegevens uit een voor ieder toegankelijke informatie bron (open bron), (2) de informantenregeling en (3) de agentenregeling. In meer concrete termen moet bij de eerste optie worden gedacht aan het verzamelen van datasets met bulkgegevens via internet, waarbij de gegevens zonder meer en zonder drempel aan een ieder worden aangeboden, bijvoorbeeld via een website. Bij de informantenregeling moet worden gedacht aan de situatie dat een natuurlijk persoon een dataset via internet op vrijwillige basis aan een medewerker van de AIVD of MIVD ter beschikking stelt. Bij de agentregeling moet in deze context worden gedacht aan de situatie dat een medewerker onder dekmantel en onder instructie en aansturing van de AIVD of de MIVD een dataset voor die dienst verwerft.

De voorzienbaarheid van deze drie wettelijke grondslagen voor het verzamelen van bulkdatasets en de bijbehorende waarborgen worden hierna behandeld.

2.1 Het verzamelen van publiekelijk toegankelijke gegevens (open bron)

Publiekelijk toegankelijke gegevens zijn gegevens uit een informatiebron die voor een ieder toegankelijk is. Onder de Wiv 2002 en Wiv 2017 worden de termen 'open bron' en 'openbare bronnen' als synoniem gebruikt. Het verzamelen van gegevens uit open bronnen wordt als één van de minst ingrijpende bevoegdheden van de AIVD en de MIVD beschouwd. Op grond van het subsidiariteitsbeginsel moet daarom eerst worden nagegaan of gegevens niet uit een open bron kunnen worden vergaard, alvorens bijzondere bevoegdheden zoals het tappen van een telefoon of het hacken van een computer worden toegepast.[22]

In het hiernavolgende wordt het wettelijk kader voor het vergaren van gegevens uit publiekelijk toegankelijke informatiebronnen ('openbronnenonderzoek') in de Wiv 2002 en de Wiv 2017 besproken.

2.1.1 Openbronnenonderzoek onder de Wiv 2002

De Wiv 2002 biedt de diensten een algemene bevoegdheid bij de uitvoering van hun taak, dan wel ter ondersteuning daarvan, gegevens te verzamelen.[23] Hoewel dit niet direct uit de wettekst zelf is af leiden, wordt dit wel in de toelichting op de wet expliciet gemaakt. In de toelichting staat bijvoorbeeld aangegeven dat gegevens kunnen worden vergaard door kennisneming van voor een ieder toegankelijke bronnen, zoals kranten of tijdschriften.[24] Een ieder toegankelijke bronnen worden onder de Wiv 2002 ook wel "*open bronnen*" genoemd.[25]

---

21 EHRM 2 september 2010, nr. 35623/05 (*Uzun t. Duitsland*), par. 63.

22 Zie artikel 31 en 32 Wiv 2002 en artikel 25 Wiv 2017.

23 Artikel 6,7 12 en 31 Wiv 2002 en *Kamerstukken II* 2000/01 25877, nr. 15, p. 5

24 *Kamerstukken II* 1997/98, 25877, nr. 3, p. 22. Zie ook Koops e.a., 'Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdiensten Wiv 20XX', 12 februari 2016, p. 59.

25 *Kamerstukken II* 1997/98, 25877, nr. 3, p. 19.

Een bron is "open", wanneer de verspreider (het medium) de informatie publiekelijk toegankelijk heeft gemaakt. Het maakt hierbij niet uit of moet worden ingelogd of dat voor de informatie moet worden betaald. Als de verspreider het iedereen toestaat te betalen of een inlogaccount aan te maken, is de bron publiekelijk toegankelijk.[26]

Voor het verzamelen van gegevens uit open bron gelden geen toestemmingsvereisten.

2.1.2 Openbronnenonderzoek onder de Wiv 2017

In artikel 25 Wiv 2017 is een algemene bepaling opgenomen met een opsomming van bronnen waaruit de diensten in ieder geval gegevens kunnen verzamelen.[27] In het artikel wordt aangegeven dat de diensten onder meer bevoegd zijn gegevens te verzamelen (1) uit voor een ieder toegankelijke informatiebronnen (open bron), (2) uit informatiebronnen waarvoor de dienst een recht op kennisneming van de aldaar berustende gegevens is verleend[28] en (3) via de raadpleging van informanten.[29] Het verzamelen van gegevens uit deze drie bronnen vindt plaats op basis van de algemene bevoegdheid, waarvoor geen bijzondere toestemmingsvereisten gelden.[30] De informantenregeling is in artikel 39 Wiv 2017 verder uitgewerkt.

Voor zover het verzamelen van de gegevens uit open bronnen *niet-stelselmatig* van karakter is, worden de gegevens verzameld op basis van de algemene bevoegdheid om gegevens te verzamelen uit een voor ieder toegankelijke informatiebron. Dit heeft een wettelijke basis in artikel 25 lid 1 sub a van de Wiv 2017. In de toelichting op de wet staat dat voor het raadplegen van 'voor een ieder toegankelijke informatiebronnen' wordt gedoeld op "*alle bronnen die zonder meer kunnen worden geraadpleegd en waarvoor geen drempels bestaan*". Deze bronnen worden in het kader van de Wiv 2017 ook wel 'open bronnen' of 'openbare bronnen' genoemd. De voorbeelden die daarvan worden genoemd zijn kranten, tijdschriften en (het openbare deel van) het internet.

In de toelichting op de Wiv 2017 wordt niet goed uitgelegd wat moet worden verstaan onder een 'drempel' bij het begrip 'voor een ieder toegankelijke informatiebron'. De CTIVD begrijpt dat onder een drempel niet per definitie registratie of betaling wordt verstaan, omdat voor de aankoop van een krant of tijdschrift op internet ook vaak registratie en betaling noodzakelijk is en deze bronnen als open bron worden beschouwd. De toelichting maakt wel duidelijk dat informatie op gesloten profielen op sociale media niet als open bron moet worden gezien.[31]

De CTIVD leidt hieruit af dat informatie die personen op sociale media expliciet niet kenbaar willen maken, door hun profiel gesloten te houden en de informatie alleen aan 'vrienden' zichtbaar te maken, als gesloten bron moet worden aangemerkt. Informatie op sociale media op internet wordt als open bron beschouwd als deze voor een ieder raadpleegbaar is, ook als daar betaling of registratie voor nodig is. In de context van sociale media kan hierbij worden gedacht aan profielinformatie of

---

[26] Zie ook Toezichtsrapport nr. 39 over de rechtmatigheid van het onderzoek op sociale media door de AIVD (2014), p. 16.

[27] Dit is geen limitatieve opsomming. Als het noodzakelijk is dat de diensten uit nog andere informatiebronnen gegevens verzamelen, kan de minister daar toestemming voor verlenen. Zie artikel 25, tweede lid, Wiv 2017.

[28] In de context van dit onderzoek gaat het niet om informatiebronnen waarvoor de dienst een recht op kennisneming van de aldaar berustende gegevens is verleend. In de memorie van toelichting worden daarvan als voorbeeld politiegegevens genoemd. Het toetsingskader voor deze bron wordt om deze reden niet verder uitgewerkt.

[29] Tevens kunnen gegevens worden verzameld (4) met uitoefening van bijzondere bevoegdheden en (5) in het kader van de samenwerking tussen de diensten en andere instanties. Gelet op de scope van dit onderzoek (de verwerving van gegevens door de diensten zelf op grond van de algemene bevoegdheid), zijn deze laatste twee bronnen voor dit toezichtsrapport niet relevant.

[30] Het betreft immers bevoegdheden die uitgeoefend kunnen worden bij alle taakonderdelen.

[31] *Kamerstukken II* 2016/17, 34588, nr. 3, p. 63.

informatie in 'groepen' die zichtbaar zijn na registratie op de sociale mediawebsite.[32] Een open bron op internet betreft ook voor een ieder (na registratie) zichtbare informatie op online forums en online marktplaatsen. In deze zin is het begrip 'open bron' en 'publiekelijke toegankelijke informatiebron' niet gewijzigd ten opzichte van de situatie onder de Wiv 2002.

Voor het niet-stelselmatig verzamelen van gegevens uit open bron, zoals bedoeld in artikel 25 van de Wiv 2017, geldt geen specifiek toestemmingsvereiste.

2.1.3 Stelselmatig verzamelen van persoonsgegevens uit open bron

In de 'Privacy Impact Assessment' (PIA) van de Wiv 2017 is opgemerkt dat ook bij het verzamelen van gegevens uit open bronnen een privacy-inmenging plaatsvindt. Het werd door de auteurs van de PIA wenselijk geacht openbronnenonderzoek aan het gegevensverwerkingskader uit de Wiv 2017 te onderwerpen. Om deze reden is expliciet in de wet op genomen dat de diensten bevoegd zijn tot het verzamelen van publiekelijk toegankelijke gegevens.[33] Wanneer de gegevens op 'stelselmatige wijze' worden vergaard vindt een meer dan geringe inmenging met de rechten van en vrijheden van de betrokkene plaats en moet een nieuwe bevoegdheid uit artikel 38 Wiv 2017 worden ingezet.[34]

Het *stelselmatig* verzamelen van gegevens omtrent personen uit open bronnen is geregeld in artikel 38 Wiv 2017. Voor het, al dan niet met een technisch hulpmiddel, stelselmatig verzamelen van deze gegevens moet de betrokken minister of het hoofd van de desbetreffende dienst toestemming geven. Het geven van toestemming van de bevoegdheid kan op basis van mandaat ook lager in de organisatie worden belegd. Het verzamelen van gegevens is stelselmatig, indien een min of meer volledig beeld van bepaalde aspecten van het privéleven van een persoon wordt verkregen. In de context van dit onderzoek is dit wetsartikel echter in beginsel niet van toepassing. Bij het verwerven van bulkdatasets gaat het immers niet om het langdurig verzamelen van gegevens over specifieke personen, maar om het eenmalig verwerven van een dataset met informatie over een groot aantal personen.

2.1.4 Resumerend

In de context van dit onderzoek betekent het voorgaande dat datasets die op openbare websites worden aangeboden als publiekelijk toegankelijke informatie worden beschouwd. Toepassing van de algemene bevoegdheid tot het verzamelen van gegevens uit open bronnen is daarbij als juridische grondslag aangewezen.

Gesloten delen van het internet waarvoor registratie en/of betaling noodzakelijk is, worden ook als publiekelijk toegankelijk beschouwd, voor zover deze zonder meer voor een ieder toegankelijk zijn. Datasets die daarop worden aangeboden kunnen dus ook uit 'open bron' worden vergaard.

Daarbij moet als vuistregel worden aangehouden dat toepassing van de algemene bevoegdheid voor het verzamelen van gegevens uit open bron ophoudt, wanneer de handelingen van de diensten overgaan in het met de aanbieder van de bulkdatasets interacteren om de benodigde gegevens te vergaren. In dat geval is de informantenregeling of de agentenregeling van toepassing.

---

[32] Zie in deze zin ook *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 39 en *Kamerstukken II* 2016/17, 34588, nr. 18, p. 53.

[33] Zie Koops e.a., 'Privacy Impact Assessment Wiv 20XX', p. 62-65.

[34] Zie ook *Kamerstukken II* 2016/17, 34588, nr. 3, p. 63 en *Kamerstukken II* 2016/17, 34588, nr. 18, p. 53.

2.2 De informantenregeling

Een informant is een ieder die door de positie waarin hij verkeert dan wel de hoedanigheid die hij heeft over gegevens beschikt of kan beschikken die voor een goede taakuitvoering van de dienst van belang kunnen zijn.[35] In de onderhavige context gaat het om een door een derde op internet aangeboden bulkdataset. De aanbieder van de dataset kan in dat geval mogelijk als informant worden aangemerkt. In deze paragraaf wordt eerst kort de informantenregeling onder de Wiv 2002 besproken en daarna de informantenregeling in de Wiv 2017.

2.2.1 De informantenregeling onder de Wiv 2002

In artikel 17 Wiv 2002 staat dat de diensten bevoegd zijn bij de uitvoering van de taak, of ter ondersteuning van een goede taakuitvoering, zich te wenden tot bestuursorganen, ambtenaren en voorts een ieder die geacht wordt de benodigde gegevens te kunnen verstrekken. Voor de inzet van artikel 17 Wiv 2002 gelden geen bijzondere toestemmingsvereisten.

Als een persoon informatie wil verstrekken die voor de taakuitvoering, of ter ondersteuning van de taakuitvoering, van belang is, kunnen de diensten deze op grond van artikel 17 Wiv 2002 verwerven. Een persoon die op grond van deze bevoegdheid gegevens verstrekt, wordt ook wel een 'informant' genoemd. De informant onderscheidt zich van een 'agent' doordat een informant niet door de AIVD of de MIVD wordt 'gestuurd'. Informanten krijgen van de diensten dan ook geen instructie tot het verzamelen van gegevens. Dit wil zeggen dat het kennisnemen of het verstrekken van de gegevens binnen de normale hoedanigheid of werkzaamheden van de informant moet vallen. De informantenregeling schept voor de medewerkers van de diensten een algemene bevoegdheid gegevens te verzamelen door te interacteren, zolang daarbij niet 'sturend' wordt opgetreden.[36] Interacteren houdt in dat er sprake is van meer dan het enkel registreren of betalen, zoals communiceren over een specifieke betalingswijze. Een medewerker van de dienst mag in deze interactie dus wel een alias of valse naam gebruiken, maar zich in de communicatie niet actief opstellen.[37]

Ook zijn de diensten op grond van artikel 17 van de Wiv 2002 (nevengeschikt) bevoegd zich te wenden tot een verantwoordelijke voor een gegevensverwerking. In dat geval is de medewerker van de dienst verplicht zich te legitimeren aan de hand van een daartoe verstrekt legitimatiebewijs. De legitimatieplicht is in artikel 17 Wiv 2002 geïntroduceerd om de Wet bescherming persoonsgegevens voor de verantwoordelijke buiten toepassing te verklaren.[38] Het gevolg van deze bepaling is dat de verantwoordelijke voor een gegevensverwerking niet hoeft na te gaan wat de inhoud van de verstrekking behelst, de betrokkene niet hoeft te informeren over de gegevensverstrekking aan de AIVD en de MIVD en de verantwoordelijke de gedane verstrekking niet hoeft vast te leggen (protocolplicht).[39] De ratio van deze bepaling is aldus gelegen in het bieden van een vorm van vertrouwen aan een gegevensverantwoordelijke die zich aan de Wet bescherming persoonsgegevens gebonden acht. Dit is bij de aanbieders van de bulkdatasets doorgaans niet het geval, zeker niet wanneer het illegale (waarschijnlijk gelekte of gehackte) gegevens betreft. De legitimatieplicht is in deze context dus niet van toepassing.

---

35 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 64. Een bestuursorgaan kan ook als informant worden aangemerkt.

36 Zie *Kamerstukken II* 1997/98, 25877, nr. 3, p. 31 en *Kamerstukken II* 1999/2000, 25877, nr. 8, p. 59 en 124. Zie ook CTIVD rapport 8a en 8b inzake de inzet van informanten en agenten door de AIVD en MIVD, meer in het bijzonder in het buitenland.

37 Toezichtsrapport nr. 39 over de rechtmatigheid van het onderzoek op sociale media door de AIVD (2014), p. 8 en 11.

38 *Kamerstukken II* 1997/98, 25877, nr. 3, p. 23-24.

39 *Kamerstukken II* 1999/2000, 25877, nr. 8, p. 43.

2.2.2 De informantenregeling onder de Wiv 2017

In de Wiv 2017 is de regeling voor de inzet van informanten uitgebreid en neergelegd in artikel 39. In essentie wordt de informantenregeling van de Wiv 2002 gehandhaafd, aangevuld met de expliciete mogelijkheid dat de diensten geautomatiseerd (*online en real time*) toegang tot de gegevens mag worden verleend en met de mogelijkheid tot het rechtstreeks geautomatiseerd vergelijken van gegevens. In de Wiv 2002, stelde artikel 17 niets over de wijze van verstrekking en liet daarmee alle opties open. Deze toevoegingen zijn vanuit het oogpunt van kenbaarheid en rechtszekerheid opgenomen. Uit de toelichting blijkt dat deze nieuwe regeling met name van belang is in de gevallen waarbij het voorzienbaar is dat het in het kader van de goede taakuitoefening wenselijk is dat de diensten structureel de beschikking hebben over (actuele) gegevens die bij een persoon of instantie beschikbaar zijn.[40]

In artikel 39 Wiv 2017 behouden de AIVD en de MIVD de mogelijkheid een ieder te benaderen die geacht wordt de benodigde gegevens te kunnen verstrekken.[41] De informantenregeling schept nog steeds de bevoegdheid gegevens te verzamelen door met personen te interacteren, zonder dat daarbij 'sturend' wordt opgetreden. Als een persoon wel doelbewust door een dienst wordt ingezet om gericht gegevens te verzamelen moet de agentenregeling worden toegepast.[42]

In artikel 39 Wiv 2017 ontbreekt de nevengeschikte vermelding van de verantwoordelijke voor een gegevensverwerking, omdat een ieder ook tevens een verantwoordelijke kan zijn.[43] In die gevallen geldt de legitimatieplicht. Net als in de Wiv 2002 is de reden daarvoor is dat de verantwoordelijke zich kan vergewissen dat het verzoek rechtens door een dienst wordt gedaan en de geldende voorschriften voor de verantwoordelijke op het gebied van gegevensverwerking niet van toepassing zijn.[44]

De minister van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) heeft bij de behandeling van het wetsvoorstel in de Eerste Kamer toegezegd dat, indien de diensten derden om gegevens verzoeken of rechtstreekse toegang daartoe vragen, altijd het niveau van waarborgen van toepassing is dat geldt op het moment dat de diensten die bevoegdheden rechtstreeks zouden inzetten zonder de hulp van deze derden. Als voor het door de diensten eigenstandig verwerven van inzage in databases een bijzondere bevoegdheid nodig zou zijn, dient in deze gevallen op het niveau en onder de vereisten van de desbetreffende bevoegdheid toestemming te worden gevraagd.[45] Dit onderzoek richt zich echter op een ander onderwerp, namelijk de verwerving en ontsluiting van reeds op internet aangeboden bulkdatasets.

Voor de inzet van de informantenregeling van artikel 39 Wiv 2017 geldt geen specifiek toestemmingsvereiste.

---

40 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 58.

41 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 64.

42 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 64.

43 Een verantwoordelijke is de natuurlijke persoon, rechtspersoon of een ieder ander die of het bestuursorgaan dat, alleen of tezamen met anderen, het doel van en de middelen voor de verwerking van gegevens vaststelt (artikel 1 sub d Wet bescherming persoonsgegevens).

44 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 56 t/m 58.

45 Zie ook Bits of Freedom, 'Wat is de toezegging van Plasterk waard?', 19 juli 2017, voor het maatschappelijk debat hieromtrent.

2.2.3 Resumerend

De diensten mogen op grond van artikel 17 lid 1 sub a Wiv 2002 en artikel 39 lid 1 Wiv 2017 gegevens van een informant afnemen. Met betrekking tot het onderwerp van dit onderzoek gaat het daarbij om een informant die via internet een dataset met bulkgegevens aan een ieder, waaronder de AIVD en de MIVD, aanbiedt.

2.3 De agentenregeling

Een agent is een natuurlijke persoon die doelbewust door een dienst wordt ingezet om gericht gegevens te verzamelen die voor de taakuitvoering van die dienst van belang kunnen zijn. Zoals opgemerkt in paragraaf 2.2, wordt daarbij door de diensten 'sturend' opgetreden. Een agent kan een derde, maar ook een medewerker van de dienst zijn. In de onderhavige context is het denkbaar dat een medewerker van een dienst in de hoedanigheid van agent zich via internet een informatiepositie verschaft waardoor deze een bulkdataset kan verwerven. Daarbij kan worden gedacht aan het infiltreren in een gesloten webforum waarop bulkdatasets worden verkocht. In deze paragraaf wordt eerst kort de agentenregeling in de Wiv 2002 en daarna de agentenregeling in de Wiv 2017 besproken.

2.3.1 De agentenregeling in de Wiv 2002

De agentregeling is neergelegd in artikel 21 Wiv 2002. Agenten zijn natuurlijke personen die, al dan niet onder dekmantel van een aangenomen identiteit of hoedanigheid, onder de verantwoordelijkheid en met instructie van een dienst gericht gegevens verzamelen. In tegenstelling tot informanten worden agenten aangestuurd om op zoek te gaan naar informatie. De taak van een agent is om een informatiepositie jegens een bepaalde persoon of organisatie te verwerven en deze – eenmaal verworven – ook te behouden.[46] De grens van de informantenregeling wordt overschreden als een medewerker van de dienst, die zich van een valse identiteit bedient, zich daartoe *actief* opstelt en interactie met anderen aangaat.[47]

In artikel 21 lid 3 Wiv 2002 wordt aangegeven dat een agent, onder instructie van een dienst, bevoegd is tot het plegen van een strafbaar feit. In de instructie van de diensten staat onder welke omstandigheden deze handelingen mogen worden gepleegd die een strafbaar feit tot gevolg kunnen hebben of waarbij een strafbaar feit wordt gepleegd.[48] Ook wordt de wijze beschreven waarop de handelingen moeten worden uitgevoerd, voor zover deze bij het geven van de instructie zijn voorzien. Daarbij mag de agent niet het Tallon-criterium overtreden, hetgeen inhoudt dat de agent niet een ander persoon mag brengen tot het beramen of plegen van andere strafbare feiten dan waarop het opzet van de desbetreffende persoon is gericht.

De inzet van een agent is een bijzondere bevoegdheid. Toestemming daarvoor wordt versterkt door de betrokken minister, de directeur-generaal van de AIVD of de directeur MIVD. De toestemming kan op basis van het Mandaatbesluit worden gemandateerd aan een lager niveau. Bij de AIVD mag een teamhoofd, unithoofd of directeur daarvoor toestemming geven. Alleen indien de agent een persoon met een bepaalde maatschappelijke functie betreft, ligt het toestemmingsniveau hoger, te weten op

---

[46] Zie *Kamerstukken II* 1997/98, 25877, nr. 3, p. 31 en *Kamerstukken II* 1999/2000, 25877, nr. 8, p. 59 en 124. Zie ook CTIVD rapport 8a en 8b inzake de inzet van informanten en agenten door de AIVD en MIVD, meer in het bijzonder in het buitenland.

[47] Toezichtsrapport nr. 39 over de rechtmatigheid van het onderzoek op sociale media door de AIVD, p. 17.

[48] In de memorie van toelichting is aangegeven dat niet elk strafbaar feit mag worden gepleegd. De minister maakte indertijd duidelijk dat geen enkel belang van de dienst kan nopen tot het plegen van moord (*Kamerstukken II* 1997/98, 25877, nr. 3, p. 34).

dat van de directeur-generaal of de minister.[49] Bij de MIVD moet voor de initiële inzet van de agent de minister toestemming geven. Voor zover geen sprake is van een principieel beleidsmatig of politiek gevoelig karakter is de directeur van de MIVD bevoegd toestemming te verlenen voor de verlenging van de inzet.[50] De toestemming voor de inzet van een agent wordt ingevolge artikel 19, derde lid, Wiv 2002 verleend voor een periode van ten hoogste drie maanden en kan telkens op een daartoe strekkend verzoek worden verlengd voor eenzelfde periode.

Ook kan toestemming worden gegeven tot het plegen van strafbare feiten. Daarbij kan worden gedacht aan betrokkenheid bij het schenden tussen geheimen, zoals staatsgeheimen van bondgenoten en intellectueel eigendom.[51] Een andere mogelijkheid, die in de beleidsnotities ook wordt genoemd en is het plegen van heling. De bulkdatasets kunnen immers door middel van 'hacking' (computervredebreuk) zijn verkregen. In het strafrecht worden gegevens echter in principe niet als goed beschouwd. Dit maakt dat het traditionele artikel dat heling strafbaar stelt niet van toepassing is. Het beschikbaar stellen en daarmee helen van door middel van computervredebreuk buitgemaakte gegevens is om deze reden (nog) niet strafbaar.

De Wet computercriminaliteit III brengt hier mogelijk verandering in. In het wetsvoorstel Computercriminaliteit III, dat thans ter beoordeling in de Eerste Kamer ligt, wordt heling van gegevens strafbaar gesteld in artikel 139g van het Wetboek van Strafrecht. Dat willen zeggen: het beschikbaar stellen, verwerven, of voorhanden hebben van niet-openbare gegevens.[52] Bij deze heling van gegevens moet worden gedacht aan gegevens die uit een datalek of computervredebreuk zijn verkregen.[53] Het van het internet downloaden van voor het publiek toegankelijke (en daarmee openbare) gegevens, is niet strafbaar.[54]

2.3.2 De agentregeling in de Wiv 2017

De inzet van agenten vindt in de Wiv 2017 plaats op grond van artikel 41. De regeling is in essentie hetzelfde als de oude regeling van artikel 21 Wiv 2002, met de toevoeging dat de toestemmingsduur verlengd is naar een jaar.[55] De instructie die aan een agent wordt gegeven moet schriftelijk worden vastgelegd.[56] Dit biedt de mogelijkheid het optreden van de agent achteraf te kunnen toetsen en evalueren en is van belang voor het rechtmatigheidstoezicht van de CTIVD.[57] In de toelichting op de nieuwe Wiv 2017 wordt expliciet gemaakt dat in de praktijk de Landelijke Officier van Justitie Terrorismebestrijding advies wordt gevraagd over de instructie met betrekking tot het plegen van strafbare feiten. Deze gaat na of een adequate aanduiding van de te plegen strafbare feiten wordt gegeven.[58] Deze regeling komt overeen met de praktijk onder de Wiv 2002.

---

49 Artikel 4 van het Mandaatbesluit AIVD. Dit besluit is niet openbaar.

50 Artikel 4 onder a sub 1 van de Mandaatregeling Defensie Wet op de inlichtingen- en veiligheidsdiensten 2002 en Wet veiligheidsonderzoeken.

51 Zie respectievelijk artikelen 98c jo. 98 en 273 van het Wetboek van Strafrecht.

52 In 2009 had de wetgever al aan de Tweede Kamer toegezegd heling van gegevens strafbaar te stellen (*Kamerstukken II* 2008/09, 28864, nr. 232, p. 4). Op het helen van gegevens staat maximaal een jaar gevangenisstraf of een geldboete van de vierde categorie.

53 *Kamerstukken II* 2015/16, 34372, nr. 3, p. 62.

54 *Kamerstukken II* 2015/16, 34372, nr. 3, p. 66-67.

55 In tegenstelling tot bij andere bijzondere bevoegdheden is geen voorafgaande autorisatie door de Toetsingscommissie Inzet Bevoegdheden vereist. Zie daarvoor artikel 32 Wiv 2017.

56 Artikel 41 lid 7 Wiv 2017.

57 Zie ook *Kamerstukken II* 2016/17, 34588, nr. 3, p. 65.

58 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 66.

2.3.3 Resumerend

Er is sprake van een agent als een natuurlijk persoon onder instructie en aansturing van een dienst gericht gegevens verzameld. De agentregeling in de Wiv 2002 komt grotendeels overeen met de agentregeling uit de Wiv 2017.

2.4 Het verwerven van grote hoeveelheden gegevens (bulk)

Voor de verwerving van datasets met bulkgegevens op internet zijn drie juridische grondslagen toepasselijk. Dit zijn: het verzamelen van gegevens uit een open bron, het verwerven van gegevens van een informant en het verwerven van gegevens via een agent. De vraag dringt zich op of de algemene bevoegdheid (open bron of informant) en de agentregeling ook een voldoende voorzienbare grondslag bieden voor het vergaren van gegevens in *bulk*, waarbij het in enkele gevallen gaat om bestanden met miljoenen persoonsgegevens die op internet worden aangeboden.

Uit de wetsgeschiedenis blijkt dat de algemene bevoegdheid (een open bron of informant) of de inzet van de bijzondere bevoegdheid van een agent een voldoende precieze grond is voor het verwerven van ook grote gegevensverzamelingen.[59] Dit uitgangspunt heeft de CTIVD in eerdere rapporten overgenomen.[60] Daarbij wordt niet uitgesloten dat gegevens ongericht worden verworven. Dat wil zeggen dat op het moment van verwerving nog niet precies kan worden aangegeven waarop of op wie de gegevens betrekking hebben. Bij het ongericht verwerven gaat het doorgaans om zeer grote hoeveelheden gegevens (bulk). Op voorhand kan dikwijls worden ingeschat dat de bulkgegevens in overgrote meerderheid informatie bevatten die niet relevant is voor de goede taaktuitvoering van de diensten, gegeven de aard van het te verwerven volume aan gegevens.[61] Ook in de strafrechtspraak wordt niet uitgesloten dat op grond van een algemene bevoegdheid grote hoeveelheden gegevens worden opgeslagen.[62]

De wet geeft bovendien in grote lijnen aan in welke gevallen de bevoegdheid mag worden ingezet. De reikwijdte van de bevoegdheid wordt beperkt tot de taakstelling van de diensten en tot de in artikel 13 Wiv 2002 en artikel 19 Wiv 2017 omschreven personen. In het vijfde lid van artikel 19 Wiv 2017 is expliciet aangegeven dat de diensten bevoegd zijn gegevens te verwerken omtrent andere personen (dan targets), indien die gegevens een logisch en onlosmakelijk onderdeel vormen van de door de diensten te verwerven of verworven gegevensbestanden. Deze aanvulling is in het kader van de rechtszekerheid toegevoegd, om elke twijfel weg te nemen dat met bevoegdheden grote hoeveelheden gegevens (bulk) kunnen worden verzameld.[63]

2.5 Intern beleid over het verwerven van de datasets

In de interne beleidsnotities van de diensten aangaande het verwerven van op internet aangeboden bulkdatasets worden de drie mogelijke grondslagen voor de verwerving van de gegevens allemaal genoemd. Deze grondslagen betreffen: het verzamelen van gegevens uit open bron (artikel 17 Wiv 2002), de informantenregeling (artikel 17 Wiv 2002) en de agentenregeling in artikel 21 Wiv 2002.

---

59 *Kamerstukken II* 2005/06, 30553, nr. 3, p. 13 e.v.

60 Toezichtsrapport nr. 38 inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD (2014), p. xi, en 59 e.v. en Toezichtsrapport nr. 39 over de rechtmatigheid van het onderzoek op sociale media door de AIVD (2014), p. 13 met verwijzing naar *Kamerstukken II* 2005/06, 30553, nr. 3, p. 13 e.v.

61 Toezichtsrapport nr. 39 over de rechtmatigheid van het onderzoek op sociale media door de AIVD (2014), p. 13.

62 Parket bij de Hoge Raad 9 september 2014 ECLI:PHR:2014:1963, r.o. 4.3 en 4.8

63 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 34.

Hierbij wordt geen expliciete keuze gemaakt welke grondslag per verworven dataset van toepassing wordt verklaard.

In het interne beleid is aangegeven dat de verwerving van de bulkdatasets in beginsel plaatsvindt op basis van artikel 17 Wiv 2002, mogelijk in combinatie met artikel 21, derde lid Wiv 2002. In de beleidsnotities wordt opgemerkt dat van de agentenregeling sprake is als een medewerker van de dienst, die zich van een valse identiteit bedient, zich bij de verwerving van bulkdatasets actief gaat opstellen. De verwijzing naar de agentregeling artikel 21 lid 3 Wiv 2002 is opgenomen, omdat mogelijk sprake is van het plegen van een strafbaar feit, waarvoor toestemming moet worden gegeven.[64] In de beleidsnotitie staat dat mogelijk sprake is van het delict heling.

De CTIVD merkt hierbij op dat de toepasselijkheid van een strafbaar gestelde gedraging niet per definitie tot gevolg heeft dat in alle gevallen de agentregeling moet worden toegepast. Het is inherent aan de informantenregeling dat de diensten daarbij ook niet-openbare gegevens kunnen verzamelen.[65] Indien een medewerker in het kader van de taakuitvoering onder de algemene bevoegdheid niet-openbare gegevens verwerft, wordt echter in het kader van de uitvoering van een wettelijk voorschrift gehandeld. Het expliciet geven van toestemming voor het 'helen van gegevens' is dan ook niet noodzakelijk en kan zelfs beter achterwege worden gelaten als geen sprake is van de inzet van een agent. Het geven van toestemming voor het plegen van een strafbaar feit, terwijl geen sprake is van een agentsituatie, schept immers onduidelijkheid over welke bevoegdheid precies is ingezet en daarmee welke waarborgen van toepassing zijn.

In de interne beleidsnotitie worden extra waarborgen voorgeschreven ten opzichte van de toepassing van de algemene bevoegdheid. Op grond van de interne beleidsnotities moet voor de verwerving van bulkdatasets *zonder persoonsgegevens* toestemming worden gegeven op het niveau van unithoofd van de JSCU. Voor het verwerven van op internet aangeboden bulkdatasets *met persoonsgegevens* is toestemming nodig op het niveau van de directeur-generaal van de AIVD en de directeur van de MIVD. In het geval de aard van de gegevens of de mate van inbreuk op de privacy een toestemming op hoger niveau noodzakelijk maakt, wordt de aanvraag ook nog aan de minister voorgelegd.

2.6 De verdere verwerking van gegevens

Als de gegevens op een van de voornoemde grondslagen (open bron, via raadpleging van een informant of de inzet van een agent) zijn verworven, worden deze ten behoeve van het inlichtingenproces verder verwerkt. De wet stelt enkele belangrijke voorwaarden aan de verwerking van gegevens. De verwerking van gegevens mag slechts plaatsvinden voor een bepaald doel en slechts voor zover dat noodzakelijk is voor de goede taakuitvoering van de diensten. De verwerking van gegevens moet bovendien op een behoorlijke en zorgvuldige wijze plaatsvinden met een verwijzing naar de betrouwbaarheid van de gegevens of de bron waaraan de gegevens zijn ontleend.[66]

Tevens moeten voorzieningen worden getroffen ter bevordering van de juistheid en volledigheid van de gegevens die worden verwerkt.[67] Met de invoering van de Wiv 2017 wordt tevens de zorgplicht voor de kwaliteit van de gegevensverwerking van kracht. Deze zorgplicht houdt in dat de hoofden

---

64 In de beleidsnotitie van de MIVD is vermeld dat in dat geval ook de Landelijk Officier van Justitie wordt ingelicht.

65 Zie ook Toezichtsrapport nr. 38 inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD (2014), p. 63.

66 Artikel 12 Wiv 2002 en 18 Wiv 2017. Bij de verwerking van gegevens uit de datasets worden geen bijzondere gegevens verwerkt. Artikel 13 lid 3 Wiv 2002 en 19 lid 3 Wiv 2017 zijn dus niet van toepassing.

67 Artikelen 16 Wiv 2002 en artikel 24 Wiv 2017.

van de diensten zorg moeten dragen voor de technische, personele en organisatorische maatregelen ter bevordering van de kwaliteit van de gegevensverwerking. Daaronder worden ook de daarbij gehanteerde algoritmen en modellen begrepen.

Zolang de gegevens in de dataset niet op hun relevantie voor de taakuitvoering zijn beoordeeld, zijn aanvullende voorwaarden noodzakelijk. Dit betekent dat aandacht moet worden besteed aan het wettelijk vereiste dat slechts toegang wordt gegeven tot gegevens voor zover dat noodzakelijk is voor een goede taakuitvoering van de aan de desbetreffende medewerker opgedragen taken (need-to-knowbeginsel). Met name indien een bulkdataset hoofdzakelijk persoonsgegevens bevat van personen die niet in de aandacht van de dienst staan, dient aan de toegang daartoe tevens de nadere voorwaarden van functie- en/of taakscheiding te worden verbonden. Daarnaast is in dat geval gewenst dat een bewaartermijn wordt vastgesteld, bij afloop waarvan de bulkdataset moet worden vernietigd.[68]

Ten slotte stelt de wet verplichtingen omtrent de verwijdering en vernietiging van gegevens. Gegevens die hun betekenis hebben verloren moeten worden verwijderd en vernietigd, tenzij wettelijke regels omtrent bewaring daaraan aan de weg staan.[69] Deze verplichting houdt onder de huidige wet ook in dat gegevens die als niet-relevant worden beoordeeld nooit betekenis hebben gehad en dus moeten worden vernietigd.[70] Onder de Wiv 2017 is in aanvullende zin nieuw dat bij gegevens die op basis van een bijzondere bevoegdheid worden verworven, zoals de agentregeling, een relevantietoets moet worden uitgevoerd. Deze toets houdt in dat zo spoedig mogelijk, en in ieder geval binnen een jaar, moet worden onderzocht of de gegevens relevant zijn voor enig onderzoek van de diensten. Gegevens die niet-relevant worden bevonden of gegevens die niet binnen de bewaartermijn worden beoordeeld, moeten terstond worden vernietigd.[71]

2.7 Intern beleid over het verder verwerken van datasets

Met betrekking tot de verdere verwerking van gegevens is in het beleid vastgelegd dat een bijzondere procedure wordt toegepast op het moment dat een dataset voor het merendeel uit persoonsgegevens bestaat van personen die geen aanleiding tot onderzoek geven. Deze zogenoemde buitenbak-binnenbakprocedure is een uitwerking van het beginsel van need-to-know en de vereisten van functie- en taakscheiding. De procedure houdt in dat de gehele dataset voor een vastgestelde bewaartermijn in de buitenbak wordt gezet, waardoor de operationele teams daar niet bij kunnen. De buitenbak is alleen direct toegankelijk voor een klein aantal technische beheerders en een deel van de data-analisten van de AIVD. Ook een select aantal medewerkers van de MIVD heeft toegang tot de buitenbak.

Als een medewerker van een operationeel team kennis wil nemen van de gegevens in de buitenbak, moet een zogenoemde naslagprocedure worden doorlopen. In een aanvraag moet het operationeel team gemotiveerd aangeven waarom zij bepaalde kenmerken, zoals een naam of een e-mailadres, willen laten naslaan in de buitenbak. Deze aanvraag moet bij de AIVD door het desbetreffende teamhoofd worden goedgekeurd. Bij de MIVD is daarvoor toestemming van de directeur noodzakelijk. Daarna maakt de JSCU de resultaten van de naslag voor het operationele team beschikbaar. Dit kan worden gezien als het verplaatsen van de gegevens van de buitenbak naar de binnenbak. Het verplaatsen van

---

[68] Bijlage II van het Toezichtsrapport nr. 53 over de inzet van de hackbevoegdheid door de AIVD en de MIVD (2017), p. 18.

[69] Artikel 43 Wiv 2002 en artikel 20 Wiv 2017.

[70] Bijlage II van het Toezichtsrapport nr. 53 over de inzet van de hackbevoegdheid door de AIVD en de MIVD (2017), p. 19.

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

gegevens naar de binnenbak maakt dat deze voor een groot aantal operationele medewerkers, ook van andere dan het verzoekende team, rechtstreeks raadpleegbaar worden.

2.8 Conclusie

Het op internet verwerven van door derden aangeboden bulkdatasets kan onder de algemene bevoegdheid tot het verzamelen van gegevens uit open bron plaatsvinden, indien de gegevens zonder meer en zonder drempel aan een ieder worden aangeboden, bijvoorbeeld via een website. Deze grondslag kent zijn begrenzing daar waar de diensten overgaan tot het interacteren met de aanbieder van de bulkdataset. Interacteren houdt in dat er sprake is van meer dan het enkel registreren of betalen, zoals communiceren over een specifieke betalingswijze. Onder de informantenregeling mogen medewerkers van de diensten (al dan niet onder een valse naam) met de aanbieder van de dataset interacteren, voor zover daarbij niet sturend wordt opgetreden. Als een medewerker, die zich van een valse identiteit bedient, of een derde onder aansturing en instructie van de dienst een bulkdataset verwerft, is de agentregeling van toepassing. Het is de diensten toegestaan met deze bevoegdheden grote hoeveelheden gegevens (bulk) te verzamelen.

In de interne beleidsnotitie worden extra (bovenwettelijke) waarborgen voorgeschreven. Op grond van de interne beleidsnotities moet voor de verwerving van bulkdatasets *zonder persoonsgegevens* toestemming worden gegeven op het niveau van unithoofd van de JSCU. Voor het verwerven van op internet aangeboden bulkdatasets *met persoonsgegevens* is toestemming nodig op het niveau van de directeur-generaal van de AIVD en de directeur van de MIVD. In het geval de aard van de gegevens of de mate van inbreuk op de privacy een toestemming op hoger niveau noodzakelijk maakt, wordt de aanvraag ook nog aan de minister voorgelegd.

Bij het verder verwerken van de gegevens zijn mechanismen ingebouwd om de privacy van de personen die in de datasets voorkomen te beschermen. Dit omvat regels omtrent de toegang tot en het bewaren van de gegevens. Het toepassen van de buitenbak-binnenbakprocedure is een invulling van vereisten van functie- en taakscheiding gericht op het need-to-knowbeginsel en het vaststellen van een bewaartermijn.

Naar het oordeel van de CTIVD voorzien de Wiv 2002 en de Wiv 2017 in een voorzienbare en adequate wettelijke basis voor de verwerving van datasets met bulkgegevens op internet, in combinatie met de waarborgen zoals geformuleerd in de interne beleidsnotities. Een kanttekening daarbij is wel dat een deel van de procedurele waarborgen niet publiekelijk toegankelijk is en daarmee niet kenbaar is, omdat zij alleen in intern beleid staan beschreven.

3 Noodzakelijkheid, proportionaliteit en subsidiariteit

Nu is vastgesteld dat het verwerven van bulkdatasets een voldoende voorzienbare wettelijke basis heeft in de toegekende bevoegdheden van de diensten, betekent dit niet dat de verwerving van een bulkdataset ook altijd gerechtvaardigd is. Daartoe dient de daarmee gemaakte inmenging noodzakelijk, proportioneel en subsidiair te zijn om een gerechtvaardigd doel te kunnen bereiken. In het geval van de AIVD en de MIVD is dit een doel in het belang van de nationale veiligheid.

Om te kunnen voldoen aan het noodzakelijkheidscriterium dient volgens de jurisprudentie van het EHRM sprake te zijn van een dringende maatschappelijke behoefte. Het begrip noodzaak dient restrictief te worden geïnterpreteerd, wat in het geval van geheim onderzoek betekent dat de inmenging strikt noodzakelijk moet zijn.[72] De privacy-inmenging dient bij te dragen aan het doel waarvoor de bevoegdheid wordt ingezet. Tevens dient de inmenging in redelijke verhouding te staan tot het doel dat daarmee wordt beoogd (proportionaliteit).[73] De inmenging mag niet plaatsvinden als het doel ook met een lichter middel kan worden bereikt (subsidiariteit).[74]

Uit de uitspraken van het HvJEU is af te leiden dat het verwerven en het algemeen en ongedifferentieerd opslaan van grote hoeveelheden persoonsgegevens, waarbij op voorhand duidelijk is dat het overgrote deel van de persoonsgegevens betrekking heeft op personen die geen aanleiding tot onderzoek hebben gegeven, op gespannen voet staat met het noodzakelijkheids- en proportionaliteitsvereiste. Als deze gegevens toch door de diensten worden verworven en verwerkt, moet vooraf worden gemotiveerd wat het doel is en hoe dit in verhouding staat met de privacy-inmenging die plaatsvindt. Dit impliceert ook het toepassen van het beginsel van dataminimalisatie: het niet (langer) verwerken van meer gegevens dan strikt noodzakelijk. De keuzes omtrent het al dan niet verwerken van gegevens en de waarborgen in de verwerkingssystemen beïnvloedt de belangenafweging.[75]

In dit hoofdstuk wordt uitgewerkt welke eisen aan de verwerving van een individuele bulkdataset kunnen worden gesteld. Daartoe wordt de toets van noodzakelijkheid, proportionaliteit en subsidiariteit met betrekking tot het gebezigd juridisch kader uit de Wiv 2002 en Wiv 2017 in paragraaf 3.1 tot en met 3.4 verder geanalyseerd. Het antwoord op de vraag hoe deze toets praktisch moet worden ingevuld met betrekking tot de verwerving en ontsluiting van op internet aangeboden bulkdatasets wordt in paragraaf 3.5 behandeld.

3.1 De algemene bevoegdheid en de agentenregeling onder de Wiv 2002

De Wiv 2002 stelt enkele belangrijke voorwaarden aan de verwerking van de gegevens, waaronder de verwerving daarvan. De diensten mogen gegevens slechts verwerken voor een bepaald doel en voor zover dat noodzakelijk is voor een goede uitvoering van de wet.[76] De verworven gegevens moeten

---

[72] Zie EHRM 6 september 1978, nr. 5029/71 (*Klass e.a. t. Duitsland*), par. 48 en EHRM 4 mei 2000, nr. 28341/95 (*Rotaru t. Roemenië*), par. 47.

[73] EHRM 7 december 1976, nr. 5493/72 (*Handyside t. Verenigd Koninkrijk*), par. 49.

[74] EHRM 8 juli 2003, nr. 36022/97 (*Hatton e.a. t. Verenigd Koninkrijk*), par. 97.

[75] Zie HvJEU 8 april 2014, C-293/12 (*Digital Rights Ireland t. Ierland*), par. 63 en C-594/12, ECLI:EU:C:2014:238 (*Seitlinger, Tschohl e.a. t. Kärtner Landsregierung*) en HvJEU 21 december 2016, C-203/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB t. Post-och telestyrelsen*), par. 89. Het recht op privacy is neergelegd in artikel 7 van het Europees Handvest voor de Rechten van de Mensen en het recht op bescherming van persoonsgegevens in artikel 8.

[76] Artikel 12 Wiv 2002.

bovendien op een zorgvuldige en behoorlijke wijze worden verwerkt.[77] Behoorlijke gegevensverwerking optreden houdt onder meer in dat er sprake is van evenredigheid tussen de verwerking als zodanig en het beoogde doel daarvan (proportionaliteit).[78]

De agentenregeling van artikel 21 Wiv 2002 is een bijzondere bevoegdheid. Als gevolg daarvan mogen de diensten de bevoegdheid alleen inzetten wanneer dat noodzakelijk is voor de goede uitvoering van hun veiligheids- en/of inlichtingentaak. Bovendien moet de uitoefening van de bevoegdheid evenredig (proportioneel) zijn aan de boogde doelen. Tevens dient de inzet subsidiair te zijn.[79] Dit betekent dat de bevoegdheid niet mag worden ingezet als met een minder ingrijpende bevoegdheid kan worden volstaan. Daarbij is expliciet aangegeven dat de inzet van een bijzondere bevoegdheid alleen is geoorloofd als de daarmee beoogde gegevens niet kunnen worden verkregen op grond van de algemene bevoegdheid, dat wil zeggen door kennisneming van voor een ieder toegankelijke informatiebronnen (open bronnen) of informatiebronnen waartoe de diensten rechtens toegang is verleend.

3.2 De algemene bevoegdheid en de agentenregeling onder de Wiv 2017

Voor zowel de algemene bevoegdheid als de agentenregeling bepaalt artikel 18 lid 1 Wiv 2017 dat de gegevensverwerking slechts plaatsvindt voor een bepaald doel en slechts voor zover dat noodzakelijk is voor de goede uitvoering van de wet. In de memorie van toelichting wordt het noodzakelijkheidsvereiste helder toegelicht:

"Welke gegevens de diensten noodzakelijk achten te verzamelen zal in de praktijk primair worden bepaald door het onderzoeksonderwerp, het doel van het onderzoek en de reeds beschikbare informatie en dergelijke. Afhankelijk van het verloop van het onderzoek en de gegevens die daarin beschikbaar komen, zal tekens dienen te worden bezien welke informatie nog ontbreekt en op welke wijze ontbrekende informatie zou kunnen worden verzameld. Het is met andere woorden een dynamisch proces".[80]

Daarnaast is in de Wiv 2017 expliciet opgenomen dat zowel de inzet van de algemene bevoegdheid als de inzet van de agentenregeling subsidiair en proportioneel moet zijn.[81]

3.3 De interne beleidsnotities

In aanvulling op de wettelijke vereisten worden in de beleidsnotities enkele voorwaarden gesteld aan de verwerving en verwerking van op internet aangeboden bulkdatasets.

Het interne beleid benadrukt dat het binnenhalen van een volledig databestand slechts plaats mag vinden, voorzover dat noodzakelijk is voor de taakuitvoering. Daarbij wordt aangegeven dat de noodzaak, proportionaliteit en subsidiariteit van de verwerving moet worden gemotiveerd.

---

77 Artikel 12 Wiv 2002. De onderzochte datasets bevatten geen gevoelige gegevens, waardoor het regime van artikel 13 Wiv 2002 buiten toepassing blijft.

78 Zie hiervoor de algemene behoorlijkheidsnormen: De Nationale ombudsman, 'Behoorlijkheidwijzer', 2015, te raadplegen via www.nationaleombudsman.nl.

79 Zie artikelen 18, 31 en 23 Wiv 2002.

80 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 40.

81 Artikel 26 Wiv 2017.

Aan de andere kant spreken de beleidsnotities ook over 'het stuiten op de bulkdatasets' en 'het binnenhalen van de bestanden in een *window of opportunity*'. Deze zinsneden duiden op een vooral praktische werkwijze, waarbij gegevens worden verworven op basis van de mate van beschikbaarheid.

3.4 De uitwerking

Voor de invulling van het noodzakelijkheids-, proportionaliteits- en subsidiariteitsvereiste moet in het geval van een individueel verwerving van op internet aangeboden bulkdataset aan de volgende vier vereisten worden gedacht: (1) een schriftelijke motivering, (2) een doelomschrijving met uitleg over de aansluiting met de taakgebieden en onderzoeksopdrachten, (3) een uitleg over de wijze waarop de verwerking van de datasets bijdraagt aan het bereiken van de geformuleerde doelen en (4) een afweging met het recht op privacy van de betrokkenen.

1. Schriftelijke motivering

De invulling van het noodzakelijkheidsvereiste en proportionaliteitsvereiste vraagt een schriftelijke motivering van de diensten met daarin de concrete relevante feiten en omstandigheden met betrekking tot de verwerving van de desbetreffende bulkdataset. Deze informatie is noodzakelijk voor de duiding van de privacy-inmenging. In ieder geval moet daarbij worden aangegeven wat de aard van de gegevens is, wat de context is waarin zij worden verworven en op welke wijze en voor welke doeleinden de gegevens zullen worden verwerkt.

2. Het doel

Om het doel van de verwerking voldoende concreet te maken, dienen de diensten in algemene bewoordingen aan te geven op welke taakgebieden en onderzoeksopdrachten informatie ontbreekt en op welke wijze de bulkdataset bijdraagt aan de verbetering van de informatiepositie. De verwerking kan ook geschieden met het oog op toekomstig onderzoek van de diensten. Daarbij moet dan wel expliciet worden gemaakt voor welke processen, zoals identificatie of verificatie van targets, de gegevens zullen worden gebruikt en hoe deze gegevens en processen aan deze doelen (naar verwachting) zullen bijdragen.[82]

3. De noodzaak

Ter uitvoering van het noodzakelijkheidsvereiste moeten de diensten ook motiveren in hoeverre de verwerving leidt tot het bereiken van de geformuleerde doelen. De term 'strikt noodzakelijk' impliceert databeperking, in die zin dat niet meer gegevens opgeslagen en verwerkt mogen worden dan noodzakelijk is voor de taak uitvoering. Deze databeperking kan plaatsvinden door bepaalde gegevens niet te verwerven, op te slaan of verder te verwerken, zoals gevoelige persoonsgegevens (gegevens omtrent godsdienst of levensovertuiging, ras, gezondheid en seksuele leven).[83] Ook kan worden gedacht aan het terstond na verwerving vernietigen van dat deel van de gegevens dat voor het te bereiken doel niet noodzakelijk is. Bovendien kan van de diensten worden verlangd dat zij – los van een eventuele bewaartermijn – periodiek nagaan of het verwerken van de gegevens nog steeds noodzakelijk is. In de motivering moet worden aangegeven op welke wijze in de uitvoering concreet invulling wordt gegeven aan het vereiste van dataminimalisatie.

---

[82] Zie ter vergelijking Parket bij de Hoge Raad 9 september 2014 ECLI:PHR:2014:1963, r.o. 4.13.

[83] Artikel 13 leden 3 en 4 Wiv 2002: het verwerken van deze gegevens dient immers onvermijdelijk te zijn.

4. De belangenafweging

Het beginsel van de proportionaliteit vraagt dat het belang van de diensten om in het kader van de nationale veiligheid hun doelen te bereiken moet worden afgewogen tegen de inmenging in de privacy van de betrokkenen. Een relevante factor voor de proportionaliteitstoets is de scherpte van de doelomschrijving. De verwerking van de datasets kan aan aanvaardbaarheid winnen als meer specifiek wordt omschreven voor welk doel de gegevens worden gebruikt, bijvoorbeeld door een beperking van de verwerking naar wettelijke taken. In het bijzonder kan dan worden gedacht aan het uitsluitend gebruiken van de gegevens voor de veiligheids- en inlichtingentaken. Dit zijn immers ook de taken waarvoor bijzondere bevoegdheden mogen worden toegepast. Een andere mogelijkheid is het alleen gebruiken van de gegevens voor bepaalde typen onderzoek, zoals de hiervoor genoemde identificatie en verificatie.

Een andere relevant element om te bepalen of een verwerking proportioneel is, is de duur van de bewaartermijn. Het hoeft geen betoog dat hoe korter die termijn is, hoe eerder de verwerking door de beugel kan. Bij het bepalen van de bewaartermijn moet in ogenschouw worden genomen hoe lang de gegevens relevant kunnen zijn voor het omschreven doel.[84] Daarnaast moeten bij het vaststellen van de bewaartermijn de risico's worden betrokken die met het opslaan van de gegevens gepaard gaan. Daarbij kan zowel worden gedacht aan risico's voor de dienst, als voor de betrokkenen. Een voorbeeld van het eerste is het risico op verlies van de actualiteit van de gegevens, waardoor deze niet meer betrouwbaar zijn. Bij het tweede kan worden gedacht aan het risico voor een ernstige privacy-inmenging of de kans op misbruik van de gegevens op het moment dat deze in handen komen van derden, bijvoorbeeld door een datalek. Het spreekt voor zich dat nadere interne procedures en het treffen van maatregelen ter beveiliging van de gegevens deze risico's kunnen verkleinen.[85]

Indien de bulkdataset naar verwachting in overgrote meerderheid gegevens bevat van of over personen die geen aanleiding geven tot onderzoek door de diensten, komt ook daaraan een groot gewicht toe. Dit betekent echter niet dat het belang van de diensten zo zwaar hoeft te zijn dat de verwerving en verwerking een verzwaarde proportionaliteitstoets (d.w.z. dat er aanwijzingen bestaan voor een direct gevaar van de nationale veiligheid) dienen te doorstaan.[86] Het inzetten van een algemene bevoegdheid is in beginsel immers minder inbreukmakend dan het aanwenden van een bijzondere bevoegdheid. Het stellen van dezelfde eisen als aan een bijzondere bevoegdheid, zou aan dit subsidiaire karakter van de algemene bevoegdheid onvoldoende recht doen.

In dit kader moet worden benadrukt dat het hier gaat om bulkdatasets die door een ieder kunnen worden vergaard. De gegevens in de datasets zijn reeds 'gestolen' of gelekt bij een organisatie en publiekelijk aangeboden. In deze zin heeft zich al een privacy-inmenging bij de betrokkenen voorgedaan, alleen niet door toedoen van de overheid. Wel moet worden gemotiveerd op welke gronden de meer ernstige privacy-inmenging kan worden gerechtvaardigd en welke specifieke waarborgen, zoals functie- en taakscheiding (zie paragrafen 2.6 en 2.7), worden toegepast om de inmenging zo klein mogelijk te houden. Bij de verwerving en verdere verwerking van deze bulkdatasets door de diensten, als onderdelen van de overheid, kan immers wederom een ernstige privacy-inmenging plaatsvinden,

---

84 Zie ter vergelijking Parket bij de Hoge Raad 9 september 2014 ECLI:PHR:2014:1963, r.o. 4.14.

85 Zie ter illustratie Algemene Verordening Gegevensbescherming, overweging 85.

86 De verzwaarde proportionaliteitstoets houdt in dat gemotiveerd moet worden dat de operationele belangen zwaarder moeten wegen dan de belangen van de personen of organisaties wier informatie in de gegevens voorkomen. Bij zwaarwegende operationele belangen kan in het geval van de inzet van bijzondere bevoegdheden gedacht worden aan situaties waarin sprake is van één of meer concrete aanwijzingen dat er een direct gevaar voor de nationale veiligheid bestaat. Zie Toezichtsrapport nr. 53 over de inzet van de hackbevoegdheid door de AIVD en MIVD (2017), p. 27, Toezichtsrapport nr. 38 inzake gegevensverwerking op het gebied van telecommunicatie door de AIVD en de MIVD (2014), p. 39 en Toezichtsrapport nr. 39 over de rechtmatigheid van het onderzoek op sociale media door de AIVD (2014), p. 14 en 26.

mede doordat politie, OM en andere overheidsorganen tot het treffen van maatregelen tegen personen en/of organisaties door de diensten kunnen worden aangezet door middel van een ambtsbericht.

3.5 Conclusie

Concluderend kan worden gesteld dat de hiervoor genoemde elementen in de wet, de toelichting daarop of de interne beleidsnotities weliswaar in het algemeen worden genoemd, maar een concrete uitwerking daarvan dikwijls ontbreekt. Dit betekent dat daarmee nog meer nadruk komt te liggen op de motivering die in het individuele, concrete geval van de verwerving van een bulkdataset wordt gegeven. Daarin moet overtuigend worden aangetoond dat de bulkdatasets niet worden verworven omdat deze nu eenmaal beschikbaar zijn, maar dat de verwerving tevens strikt noodzakelijk is voor de (ondersteuning van de) goede taakuitvoering van de diensten. Tevens moet daarin worden uitgelegd op welke wijze aan de hiervoor genoemde waarborgen invulling is gegeven.

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

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