

aan Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Directie Constitutionele Zaken en Wetgeving
Per email en via <https://www.internetconsultatie.nl/wbmv/b1>

ons kenmerk SPF20261011

datum 11 oktober 2026

onderwerp Commentaar Privacy First op concept-wetsvoorstel voor de Wet
bescherming nationale veiligheid door de inlichtingen- en
veiligheidsdiensten

Geachte heer/mevrouw,

Op 28 augustus jl. verzocht u Stichting Privacy First om een reactie te geven op het concept-wetsvoorstel voor de Wet bescherming nationale veiligheid door de inlichtingen- en veiligheidsdiensten (Wbmv). Privacy First is u erkentelijk voor uw verzoek en voorziet u hierbij graag van ons huidige commentaar. Onze voornaamste aandachtspunten hebben wij tevens ingebracht bij de rondetafelbijeenkomst met de Ministeries van Binnenlandse Zaken, Defensie, Algemene Zaken en Justitie & Veiligheid d.d. 6 oktober jl. Nadere inbreng van onze kant zal volgen tijdens het verdere parlementaire proces.

Algemeen

Het concept-wetsvoorstel bevat een zeer omvangrijke uitbreiding van de bevoegdheden in samenhang met een beperking van de bestaande waarborgen en toezicht. In veel gevallen zijn de bevoegdheden onvoldoende gelimiteerd en gespecificeerd, waardoor de bevoegdheden in de huidige vorm niet zullen voldoen aan de eisen van voorzienbaarheid die nodig zijn om de talloze beperkingen van het recht op privacy te kunnen legitimeren. Grootschalige massa-surveillance ligt in het verschiet. De balans tussen privacy en de gestelde doelen rond nationale veiligheid is daarbij dusdanig ver afgedreven van het fundamentele recht op privacy dat het wetsvoorstel in zichzelf een bedreiging kan gaan vormen voor de democratische rechtsstaat en het democratisch proces. Het huidige concept-wetsvoorstel komt daarmee, in de woorden van het Europees Hof voor de Rechten van de Mens, neer op “destroying democracy on the ground of defending it”. Met name in crisis- en conflictsituaties zal het de basis kunnen vormen voor misbruik door toekomstige, minder rechtsstatelijke Nederlandse regeringen. Ook door andere landen zal het huidige concept-wetsvoorstel kunnen worden gekopieerd en misbruikt. Het huidige voorstel dient daarom grondig te worden herzien.

1. Inleiding

- 1.1. Ons actuele commentaar is allereerst toegespitst op de artikelen 22 (bijzondere persoonsgegevens), 33 (automatisering, AI en algoritmen), 55-56 (zwarte lijsten met “vogelvrije targets”), 62 (OSINT en aanschaf bulkdata), 65 & 82 (bulkdata-interceptie en bevraging), 76-77 (hackbevoegdheid), 87 e.v. (vorderen van gegevens), 138-146 (internationale gegevensuitwisseling), 72 & 97 (strafbare feiten).
- 1.2. Kernpunt is dat op deze onderdelen de wettelijke voorzienbaarheid en de onafhankelijke toetsing van de inzet onvoldoende zijn verzekerd. Dit raakt rechtstreeks aan de eisen die voortvloeien uit artikel 8 EVRM. Het Europees Hof voor de Rechten van de Mens (EHRM) verlangt bij geheime surveillance dat de wet die de bevoegdheden regelt toegankelijk en voorzienbaar moet zijn en effectieve waarborgen tegen willekeur en misbruik bevat, met oog op de wijze waarop de verschillende fasen van verwerving, selectie, raadpleging, gebruik, opslag, verstrekking en vernietiging gezamenlijk zijn gereguleerd.¹
- 1.3. Privacy First maakt zich in algemene zin grote zorgen om de afname aan onafhankelijke ex ante toetsing en toezicht bij de inzet van bijzondere bevoegdheden. Dit kan ernstige consequenties hebben voor de privacy van de bevolking in het algemeen en individuele personen in het bijzonder, zoals bij het hacken van devices, bulk interceptie en analyse van (o.a. bijzondere) persoonsgegevens. Toestemming kan vaak worden verleend door de Minister voor zes maanden (voorheen drie maanden), bij spoed mondeling. Die toestemming kan zelfs worden gemandateerd aan een afdelingshoofd en verder de organisatie in, waardoor externe toetsing volledig uit het zicht verdwijnt.
- 1.4. In het concept-wetsvoorstel worden de huidige Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) en de Toetsingscommissie Inzet Bevoegdheden (TIB) terecht samengevoegd tot het nieuwe College van Toetsing en Toezicht Inlichtingen- en Veiligheidsdiensten (CTT). Deze samenvoeging dient te zorgen voor algehele versterking i.p.v. (zoals nu dreigt te gebeuren) verzwakking van toetsing en toezicht. Privacy First vraagt zich hierbij tevens af in hoeverre het institutioneel geheugen en de precedentwerking van het reeds bestaande *acquis* van CTIVD en TIB dreigen te verdwijnen; zie in dit verband art. 48 lid 3 van het concept-wetsvoorstel. Hoe onafhankelijk en effectief zal het CTT in de praktijk kunnen functioneren, ook qua capaciteit? Onze suggestie: maak van het CTT een Hoog College van Staat.
- 1.5. Tevens uiten wij later in dit commentaar onze zorgen over de notificatieplicht, verschoningsgerechtigden, (gebrek aan) actieve openbaarheid, informanten, het

¹ Zie bijv. EHRM 4 dec. 2015, *Zakharov/Rusland*, nr. 47143/06, par. 231-236; EHRM 25 mei 2021, *Big Brother Watch and Others/Verenigd Koninkrijk*, nrs. 58170/13 e.a., par. 334-339 en 347-364.

klachtrecht, de verwante Wet op de Defensiegereedheid, oorlogspropaganda en *peaceful use of outer space*.

2. Artikel 22: bijzondere persoonsgegevens

- 2.1. Artikel 22 beschrijft in passieve vorm onder welke omstandigheden bijzondere persoonsgegevens worden verwerkt, namelijk wanneer dat voor het (niet nader gespecificeerde) doel “onvermijdelijk” zou zijn. Hoewel aangenomen kan worden dat hiermee een bevoegdheid van de diensten wordt bedoeld, is onduidelijk waarom deze kritische bevoegdheid niet specifiek aan een van de relevante actoren die voorkomen in de wet (de diensten, medewerkers van de diensten, een Minister, de krijgsmacht, CTT etc.) is toebedeeld. Uit de memorie van toelichting (MvT) bij de Wbmv blijkt niet waarom het noodzakelijk kan zijn om (bulk)gegevens omtrent ras, vakverenigingslidmaatschap, gezondheid of seksuele leven van (groepen) personen te verwerken. Onder de AVG is de verwerking van dergelijke bijzondere persoonsgegevens verboden, behoudens uitzonderingsgevallen. Dit geldt eveneens onder de nieuwe Conventie 108+ van de Raad van Europa die (ook blijkens par. 14.2.4 in de MvT) bovendien onverkort geldt in het domein nationale veiligheid.
- 2.2. Artikel 22 Wbmv staat verwerking van gegevens over godsdienst, ras, vakbondslidmaatschap, gezondheid en seksueel leven toe “voor zover dat voor het doel van de gegevensverwerking onvermijdelijk is”, zonder dat een orgaan wordt aangewezen dat hierover beslist of nadere criteria worden gesteld. De MvT verklaart dit summier met de stelling dat doelbinding bij bulkgegevens pas in een later bewerkingsstadium vaststaat.
- 2.3. Deze formulering roept in het licht van artikel 8 EVRM vragen op over de **voorzienbaarheid en kwaliteit van de wettelijke regeling**. Het EHRM beschouwt het enkele bewaren van persoonsgegevens die betrekking hebben op het privéleven al als een inmenging in artikel 8 EVRM. Bij de beoordeling zijn onder meer de aard van de gegevens, de wijze waarop zij worden gebruikt en verwerkt en de gevolgen die daaruit kunnen voortvloeien relevant.²
- 2.4. Voor gegevens waaruit politieke opvattingen kunnen worden afgeleid, is de bescherming nog pregnanter. Het EHRM heeft uitdrukkelijk geoordeeld dat persoonsgegevens die politieke opvattingen onthullen tot een categorie van **bijzonder gevoelige gegevens** behoren die een verhoogd beschermingsniveau

² In *S. and Marper/Verenigd Koninkrijk* (4 dec. 2008), nrs. 30562/04 en 30566/04, par. 67, 103 en 107 benadrukte het EHRM bovendien het belang van doelbinding en passende waarborgen bij het bewaren van persoonsgegevens.

vereisen.³ Het Hof stelde bovendien vast dat de opslag en verwerking van informatie over politieke activiteiten onder omstandigheden ook de artikelen 10 en 11 EVRM kan raken.

- 2.5. Dit is relevant voor de keuze in artikel 22 Wbmv om politieke gezindheid niet als afzonderlijke categorie van bijzonder beschermde persoonsgegevens te behandelen. Anders dan bij de AVG is het EVRM daarbij niet afhankelijk van een formele categorisering van gegevens: beslissend is mede welke informatie uit de verwerking kan worden afgeleid en welke gevolgen dat heeft voor de persoonlijke levenssfeer en de uitoefening van andere verdragsrechten. Gegevens die politieke opvattingen onthullen dienen een verhoogde bescherming te genieten.⁴
- 2.6. Daar komt bij dat artikel 22 onvoldoende concrete criteria bevat voor het moment waarop gegevens als “onvermijdelijk” mogen worden verwerkt. De jurisprudentie van het EHRM verlangt juist dat de wet de omvang van de bevoegdheid en de wijze waarop die mag worden uitgeoefend voldoende duidelijk afbakt. Het ontbreekt in het concept-wetsvoorstel aan de nodige minimumwaarborgen, waaronder regels over de categorieën van personen, de duur van de maatregel, het onderzoeken en gebruiken van verkregen gegevens, verstrekking aan derden en vernietiging.⁵
- 2.7. Artikel 22 verdient daarom een aanzienlijk concretere wettelijke normering. De wet zou niet uitsluitend moeten bepalen dat verwerking “onvermijdelijk” moet zijn, maar tevens moeten vastleggen onder welke omstandigheden dergelijke gegevens mogen worden geselecteerd, geraadpleegd, verder verwerkt, bewaard en verstrekt. Daarbij zou de wet expliciet rekening moeten houden met gegevens die politieke opvattingen, politieke activiteiten of andere constitutioneel beschermde activiteiten kunnen onthullen.
- 2.8. Als overige categorieën persoonsgegevens zijn genoemd ras, vakverenigingslidmaatschap, gezondheid of seksuele leven. Het is onduidelijk waarop deze selectie van categorieën persoonsgegevens (uit het geheel van de AVG-definitie) berust en waarom het noodzakelijk en proportioneel kan zijn om (bulk)gegevens van die categorieën te verwerken.

3. Artikel 33: automatisering, AI en algoritmen

- 3.1 De bevoegdheid tot automatiseren in artikel 33 Wbmv is te breed en ongericht opgesteld, te meer omdat automatiseren in het wetsvoorstel niet is gedefinieerd. Dit

³ EHRM 24 jan. 2019, *Catt/Verenigd Koninkrijk*, nr. 43514/15, par. 112-123.

⁴ Zie bijv. EHRM 28 juni 2022, *M.D. and Others/Spanje*, nr. 36584/17, par. 55.

⁵ Vergelijk EHRM *Zakharov/Rusland* (2015), *supra* noot 1.

zet de deur open voor het experimenteren met risicotoepassingen (tools waarvan de output onbekend is), lees algoritmen en AI, op privacygevoelige informatie, door deze uit te zonderen onder lid 2 als zijnde gebruik dat “in het maatschappelijk verkeer gebruikelijk is”.

3.2 Het is bovendien onduidelijk waarom maatschappelijk gebruik op zichzelf een criterium is voor enige risicobeoordeling, aangezien daarbij de context – van heimelijk verzamelde persoonsgegevens en de bevoegdheid om te hacken – niet is meegenomen. Er worden daarbij vanwege de vage definities geen serieuze waarborgen of veiligheidseisen gesteld aan de inzet van (al dan niet algoritmische) technologie zoals gebruikelijk bij het verwerken van persoonsgegevens, inclusief effectieve menselijke tussenkomst.

3.3 De begrippen rond automatisering en risicotoepassing zouden nader moeten worden gespecificeerd en opgedeeld in afzonderlijke verwerkingslagen met eigen waarborgen afhankelijk van de mate van inmenging in de privacy, waaronder op basis van gevoeligheid van de gegevens en de omvang van datasets. Verder ontbreekt bij de inzet van risicotoepassingen voldoende onafhankelijke toetsing.

4. Artikelen 55–56: zwarte lijsten met “vogelvrije targets”

4.1 Voor onderzoek naar personen betrokken bij de onder artikel 55 en 56 bedoelde organisaties (“opponentenregime”) vervallen überhaupt alle waarborgen: de Minister kan groepen op een geheime zwarte lijst plaatsen en vervolgens kunnen de diensten zonder voorafgaande toetsing alle bijzondere bevoegdheden inzetten tegen deze (groepen) mensen. Hoe groot zijn in dit verband de risico’s van een nieuwe Koude Oorlog met vogelvrije binnenlandse “vijanden”?

5. Artikel 62: OSINT en aanschaf bulkdata

5.1 De diensten mogen via artikel 62 persoonlijke data *scrapen* van het openbare internet en inzetten voor onderzoek. Voor de betrokken persoon betekent dit dat een dossier kan worden opgebouwd uit allerlei informatie die de persoon niet onder controle heeft door bijvoorbeeld het publiceren van data door derden, door algoritmen, of de verkeerde interpretatie van anders bedoelde uitingen. De diensten hoeven hiervoor geen enkele verantwoording af te leggen. Door deze online (massa)surveillance kan een dusdanig grote inbreuk op de online privacy worden gepleegd dat het onbegrijpelijk is dat het gaat om een algemene bevoegdheid zonder additionele waarborgen en specifiekere voorzienbaarheid.

5.2 Realiseren de diensten zich dat dit mogelijk zal leiden tot het “ondergronds gaan” van mensen en groeperingen en dat de OSINT-bevoegdheid van de diensten bij de

eerstvolgende crisis zal kunnen leiden tot een maatschappelijk *chilling effect* (zoals tijdens de recente Corona-crisis reeds merkbaar was)?

5.3 Volledig uit balans onder art. 62 is de door de wetgever gelegitimeerde praktijk van de AIVD om bulkdatasets met gelekte persoonsgegevens op het *dark web* te kopen van cybercriminelen,⁶ waarmee de dienst bijdraagt aan een onveiligere online omgeving.

5.4 Privacy First vraagt zich in dit verband af: beschikken de diensten reeds over een formeel ethisch kompas voor goed inlichtingenwerk, vergelijkbaar met de bestaande Waardenkaart voor Goed Politiewerk?

6. Artikelen 65, 82: bulkdata-interceptie en bevraging

6.1. De diensten houden onder artikel 82 de bevoegdheid om bulkdata te verzamelen, met als enige specificatie dat deze plaatsvindt aan de hand van de kenmerken die zien op het doel van de interceptie. Het huidige zwaarbevochten criterium “zo gericht mogelijk” verdwijnt echter uit de wet, in strijd met de wens van de Nederlandse bevolking en het parlement na het “Sleepwet-referendum” en in strijd met de Europeesrechtelijke vereisten van noodzaak, proportionaliteit en subsidiariteit. De bevoegdheid tot het massaal verwerken van persoonsgegevens is in het concept-wetsvoorstel dusdanig breed en ongericht geformuleerd dat deze ook niet in lijn is met de mensenrechtelijke vereisten van wettelijke voorzienbaarheid. Enige waarborg is dat het CTT toestemming voor bulkinterceptie dient te geven voor een jaar, welke vervolgens jaarlijks kan worden verlengd, met een bewaartermijn van drie jaar. Deze bewaartermijn is erg lang, aangezien het gaat om bulkdata en de noodzaak van het bewaren van die grote hoeveelheden persoonlijke data niet hoeft te worden aangetoond.

6.2. De summiere beschrijving in het huidige concept-wetsvoorstel schiet ernstig tekort in termen van voorzienbaarheid en waarborgen voor subsidiariteit en proportionele verwerking van bulkdata.⁷ In de wet dient tenminste te worden omschreven hoe de interceptie in zijn werk gaat, met duidelijke end-to-end omlijning en waarborgen bij de volledige keten van verwerkingen, te meer omdat er met behulp van algoritmen analyses kunnen worden gedraaid op in bulk verzamelde data. Het EHRM heeft ten aanzien van de verwerking van bulkdata uitgelegd dat de volledige keten

⁶ Zie bijv. CTIVD, *Toezihtsrapport 55 over het verwerven van door derden op internet aangeboden bulkdatasets door de AIVD en MIVD* (2018), <https://www.ctivd.nl/documenten/2018/02/13/index>; CTIVD, *Toezihtsrapport 79 over de inzet van virtuele agenten door de AIVD en de MIVD* (2024), <https://www.ctivd.nl/documenten/2024/09/09/index>; CTIVD, *Toezihtsrapport 84 over verwerking van bulkdatasets door de AIVD en MIVD* (2026), <https://www.ctivd.nl/documenten/2026/06/24/toezicht-rapport-84-bulk>.

⁷ Vergelijk EHRM *Brother Watch and Others/Verenigd Koninkrijk* (2021), *supra* noot 1.

nauwkeurig moet worden omschreven, inclusief de bijbehorende waarborgen. Het feit dat ook de eerder aangehaalde bijzondere persoonsgegevens in bulk kunnen worden getapt en geanalyseerd maakt dat de regeling in de huidige vorm een grootschalige inbreuk zal maken op de privélevens van grote groepen mensen.

- 6.3. Bovendien is onduidelijk hoe de bevoegdheid om bulkdata te verzamelen van telecomaandieners zich verhoudt tot de Europeesrechtelijke privacyvereisten bij het verwerken van telecomgegevens.
- 6.4. Artikel 65 maakt bevraging van gewone (niet-bijzondere) bulkgegevens mogelijk op basis van uitsluitend jaarlijkse ministeriële toestemming, zonder onafhankelijke voorafgaande toetsing. Deze lacune is moeilijk te verenigen met de recente EHRM-rechtspraak over bulkinterceptie. Het Hof benadrukte dat de noodzakelijkheid en proportionaliteit niet uitsluitend bij de oorspronkelijke verzameling mogen worden beoordeeld, maar bij de verschillende fasen van het proces. Het Hof achtte het ontbreken van onafhankelijke autorisatie aan het begin van de bulkinterceptie, het ontbreken van voldoende regels rond selectors en het ontbreken van voorafgaande autorisatie voor bepaalde persoonsgerichte selectors wezenlijke tekortkomingen.
- 6.5. De omstandigheid dat de gegevens reeds zijn verzameld betekent niet zonder meer dat een afzonderlijke bevraging geen nieuwe en zelfstandige inmenging kan vormen. Juist wanneer een algemene bulkdataset door een gerichte zoekopdracht wordt ontsloten kan de intensiteit van de inmenging te sterk worden.
- 6.6. Het gehele proces van bulkverwerving en -verwerking moet zijn omgeven door voldoende waarborgen.⁸ Ook de Afdeling bestuursrechtspraak van de Raad van State heeft in de context van de Wiv 2017 reeds bevestigd dat de proportionaliteits- en gerichtheidstoets op bulkinterceptie moet zien op “het geheel aan waarborgen tijdens de verschillende fasen van de interceptieketen”.⁹
- 6.7. Een regeling die deze cruciale fase in de keten volledig buiten onafhankelijke voorafgaande toetsing laat, is daarom in strijd met het recht op privacy zoals uitgelegd door het EHRM. Dat geldt temeer wanneer de bevraging door selectors of andere zoekcriteria de overgang vormt van algemene verzameling naar gegevens over concrete personen, groepen of activiteiten. Privacy First adviseert daarom om artikel 65 onder artikel 47 te brengen, dan wel een afzonderlijke wettelijke voorziening te creëren voor onafhankelijke ex ante toetsing van ingrijpende bulkbevragingen.

⁸ Zie ook EHRM 25 mei 2021, *Centrum för rättvisa/Zweden*, nr. 35252/08.

⁹ ABRvS 9 mei 2025, ECLI:NL:RVS:2025:2351, ro. 14.

7. Artikelen 76–77: hackbevoegdheid

- 7.1. Artikel 76 regelt de bevoegdheid om geautomatiseerde werken binnen te dringen, al dan niet via derde partijen en het doorbreken van beveiliging. Hieronder kan worden verstaan de mogelijkheid om bijvoorbeeld smartphones, laptops, tablets, webcams, “smart devices” (IoT), camera-deurbellen, modems, routers en zelfs boordcomputers in voertuigen etc te hacken van personen die het doelwit zijn of toevallige derde partijen (ook in de vitale sector), met alle risico’s van dien. Eenmaal binnengedrongen op een device krijgen de diensten verregaande bevoegdheden waaronder het installeren van spyware (*technisch hulpmiddel*) op iemands toestel, het uitlezen van data en het aftappen van communicatie. Het heimelijk hacken en aftappen van persoonlijke communicatiemiddelen is evident een dusdanig grove inmenging in de privésfeer dat de specifieke situaties waarin deze bevoegdheden kunnen worden ingezet een zeer nauwkeurige beschrijving vereisen en vooraf onafhankelijk getoetst moeten kunnen worden.
- 7.2. Artikel 76 maakt het binnendringen van een geautomatiseerd werk mogelijk, al dan niet via een derde persoon of organisatie, en artikel 77 regelt de voorbereidende positionering. Van de drie fasen van de hackbevoegdheid is uitsluitend de uitwinningsfase (art. 78) onderworpen aan voorafgaande onafhankelijke toetsing door het CTT (art. 47 sub e); het binnendringen zelf en de voorbereiding daarvan staan niet op die lijst.
- 7.3. Dit betekent dat juist de stap waarmee feitelijk toegang tot een geautomatiseerd werk wordt verkregen zonder voorafgaande onafhankelijke toetsing kan plaatsvinden. De regeling is tevens onvoldoende duidelijk en onvoldoende specifiek ten aanzien van de aard, reikwijdte, duur en intensiteit van inzetbaarheid om willekeurige toepassing te kunnen voorkomen.
- 7.4. Voor de hackbevoegdheid is daarnaast van belang dat het binnendringen in een geautomatiseerd werk niet noodzakelijk beperkt blijft tot gegevens die reeds als relevant kunnen worden geïdentificeerd. Het kan toegang verschaffen tot een zeer grote hoeveelheid persoonlijke informatie, waaronder communicatie, foto’s, locatiegegevens, gezondheidsinformatie en gegevens over politieke of sociale activiteiten.
- 7.5. De precieze afbakening van het begrip “geautomatiseerd werk” is direct bepalend voor de intensiteit van de inbreuk ¹⁰ op het recht op privacy en daarom noodzakelijk. De verwerving van gegevens uit bijvoorbeeld individuele e-mailboxen vergroot de inbreuk op de persoonlijke levenssfeer. De Wbmv definieert dit begrip onvoldoende specifiek, wat het risico op geschillen over de reikwijdte van de

¹⁰ Zie bijv. ABRvS 22 april 2026, ECLI:NL:RVS:2026:2939.

bevoegdheid vergroot, terwijl juist de toegangsverlening zelf niet vooraf onafhankelijk wordt getoetst.

- 7.6. Tegen deze achtergrond ligt het voor de hand om niet alleen de uitwinningfase, maar ook de beslissing tot daadwerkelijk binnendringen in een geautomatiseerd werk aan onafhankelijke voorafgaande toetsing te onderwerpen. Daarnaast verdient het begrip “geautomatiseerd werk” een duidelijkere wettelijke afbakening die voldoende duidelijk maakt welke typen systemen en toegangen onder artikel 76 vallen.

8. Artikel 87 e.v.: bevoegdheid tot het vorderen van gegevens van financiële instellingen, telecom providers en online platforms

- 8.1. Eén van de meest Orwelliaanse bepalingen in het concept-wetsvoorstel is artikel 94: de algemene vorderingsbevoegdheid onder dreiging van gevangenisstraf, met zwijgplicht. Het concept-wetsvoorstel kent in art. 87 e.v. vergelijkbare bevoegdheden toe om gegevens te vorderen van financiële instellingen, telecom providers en online platforms. In dit verband kan tevens een decryptiebevel (met zwijgplicht) worden opgelegd, ook dit op straffe van hechtenis bij weigering om daaraan te voldoen.
- 8.2. Financiële en digitale gegevens kunnen, ook wanneer zij niet de inhoud van communicatie bevatten, gezamenlijk een zeer gedetailleerd beeld van iemands privéleven opleveren. Uit betaal- en rekeninggegevens kunnen onder meer sociale relaties, reisbewegingen, medische behandelingen, religieuze activiteiten, politieke betrokkenheid en consumptiepatronen worden afgeleid. Gegevens van online platforms kunnen daarnaast inzicht geven in contacten, locatie, interesses, communicatie, zoek- en gebruikspatronen en deelname aan maatschappelijke of politieke activiteiten. Het EHRM heeft herhaaldelijk benadrukt dat dergelijke gegevens binnen de reikwijdte van artikel 8 EVRM vallen en dat de bescherming niet afhankelijk is van de vraag of de gegevens de inhoud van communicatie betreffen. Communicatiegegevens (telecom metadata) kunnen door hun aard en combinatie een gedetailleerd beeld van iemands sociale relaties, locatie, internetgebruik en communicatiepatronen opleveren, en de verwerking daarvan vereist vanwege die privacygevoeligheid terughoudendheid en sterke wettelijke waarborgen.¹¹

¹¹ Zie bijv. EHRM 28 mei 2024, *Pietrzak and Bychawska-Siniarska and Others/Polen*, nr. 72038/17 & 25237/18. Deze jurisprudentie heeft directe betekenis voor de wijze waarop de vorderingsbevoegdheid in de Wbnv moet worden afgebakend.

- 8.3. Niet kan worden volstaan met een algemene bevoegdheid om gegevens te vorderen van financiële instellingen, telecomproviders of online platforms. De wet dient voldoende concreet te bepalen welke categorieën gegevens, van welke personen, over welke periode, voor welke doeleinden en onder welke noodzakelijkheids- en proportionaliteitsvoorwaarden mogen worden verkregen. Daarbij moet worden onderscheiden tussen gegevens die slechts identificerend van aard zijn en gegevens die door hun inhoud, omvang of duur een indringend beeld van iemands privéleven kunnen opleveren. Een rekeningnummer of klantgegevens kan niet zonder meer op één lijn worden gesteld met meerdere jaren aan betaaltransacties; evenmin kan een beperkt accountgegevens op één lijn worden gesteld met historische gegevens over contacten, locatie, zoekgedrag en interacties op een online platform.
- 8.4. Voor de beoordeling van de proportionaliteit moet bovendien niet alleen naar afzonderlijke gegevenscategorieën worden gekeken, maar ook naar de combinatiemogelijkheden. Gegevens die afzonderlijk als weinig gevoelig kunnen worden beschouwd, kunnen door koppeling met andere datasets alsnog een zeer nauwkeurig profiel van een persoon opleveren. De EHRM-jurisprudentie ondersteunt juist een dergelijke contextuele benadering van de privacy-inbreuk: de intensiteit van de inmenging hangt mede af van de aard, hoeveelheid, duur en wijze van verwerking van de gegevens en van de informatie die daaruit kan worden afgeleid. De Wbmv zou daarom uitdrukkelijk moeten bepalen dat bij noodzakelijkheids- en proportionaliteitstoetsing rekening wordt gehouden met de mogelijkheid dat gegevens uit verschillende bronnen worden gecombineerd of aan reeds beschikbare gegevens worden gekoppeld.
- 8.5. Dit is in het bijzonder van belang bij financiële gegevens. Een afzonderlijke betaling kan weinig zeggen over iemands privéleven, maar een historische transactiedataset kan een vrijwel volledig gedragsprofiel opleveren, met informatie over verblijfplaatsen, sociale contacten, gezondheidszorg, religieuze of politieke activiteiten en andere persoonlijke omstandigheden. Hetzelfde geldt voor online platforms. Een afzonderlijk accountgegevens kan beperkt gevoelig zijn, terwijl een verzameling van historische locatie-, contact-, zoek- en interactiegegevens een zeer gedetailleerd beeld van iemands persoonlijke en sociale leven kan opleveren. De wetgever dient daarom niet uitsluitend te categoriseren naar de bron van de gegevens, maar ook naar de informatiewaarde en potentiële cumulatieve gevoeligheid ervan.
- 8.6. Een tweede aandachtspunt betreft de onafhankelijke voorafgaande toetsing. Voor omvangrijke, historische of gecombineerde gegevensvorderingen ligt een zwaardere waarborg voor de hand dan voor beperkte identificerende gegevens. Naarmate de vordering meer gegevens omvat, een langere periode bestrijkt of het mogelijk maakt verschillende gegevensbronnen aan elkaar te koppelen, neemt het risico toe dat de overheid een gedetailleerd profiel van een persoon kan

reconstrueren. In dergelijke gevallen zou voorafgaande onafhankelijke toetsing van de noodzakelijkheid en proportionaliteit moeten worden voorgeschreven. De wet zou daarbij expliciet moeten voorzien in een afzonderlijke proportionaliteitsbeoordeling wanneer de gevorderde gegevens, al dan niet in combinatie met reeds beschikbare gegevens, inzicht kunnen geven in bijzondere persoonlijke omstandigheden of in de uitoefening van door het EVRM beschermde rechten, zoals de vrijheid van meningsuiting, vereniging en vergadering.

- 8.7. Aanbevolen wordt daarom om de vorderingsbevoegdheden in de Wbnv te differentiëren naar de aard, gevoeligheid, omvang, duur en combineerbaarheid van de gegevens. Voor beperkte identificerende gegevens kan een lichtere procedure gelden, maar voor omvangrijke historische gegevensverzamelingen en gegevensvorderingen die door hun aard of combinatie een gedetailleerd beeld van het privéleven kunnen opleveren, dienen aanvullende wettelijke criteria en ex ante (en eventueel ex post) onafhankelijke toetsing te gelden. Tevens dient de wet expliciet te bepalen dat gegevens niet als privacy-ongevoelig kunnen worden aangemerkt uitsluitend omdat zij afzonderlijk gezien geen bijzondere persoonsgegevens of communicatie-inhoud bevatten. De wetgever moet voorkomen dat de Wbnv door een gefragmenteerde benadering van gegevenscategorieën de cumulatieve privacy-inbreuk buiten beeld laat.

9. Artikelen 138–146: internationale gegevensuitwisseling

- 9.1. De uitwisseling van ongeëvalueerde bulkdata met buitenlandse partnerdiensten is Privacy First altijd een doorn in het oog geweest. Anno 2026 gelden die zorgen voornamelijk voor de Verenigde Staten. Ook in de huidige concept-Wbnv is het gebrek aan specifieke end-to-end waarborgen bij internationale uitwisseling van persoonsgegevens immer problematisch. Zo dienen er in de eerste plaats waarborgen te worden geëist van de ontvangende staat die misbruik en disproportionele inmenging voorkomen, waaronder waarborgen voor veilige opslag en beperking van verdere verstrekking.¹² Ook ontbreekt in het concept-wetsvoorstel een wettelijke verplichting om bij verstrekking aan buitenlandse partners de privacybelangen van betrokken personen mee te wegen.¹³ Bovendien kan een waarborg die uitsluitend op een eerder moment in de keten wordt toegepast, onvoldoende zijn wanneer later een nieuwe en intensievere verwerking plaatsvindt.
- 9.2. Het vertrouwensbeginsel tussen partnerdiensten zou niet moeten betekenen dat iedere latere gegevensverstrekking of verwerking automatisch buiten onafhankelijke controle valt. De wet zou tenminste moeten voorzien in duidelijke

¹² Zie EHRM *Big Brother Watch/VK* (2021), *supra* noot 1.

¹³ Zie EHRM *Centrum för rättvisa/Zweden* (2021), *supra* noot 8.

criteria voor uitzonderingssituaties, herbeoordeling bij gewijzigde omstandigheden, beperking van verdere verstrekking en effectieve onafhankelijke controle. Tevens dienen U-bocht constructies (waarbij buitenlandse diensten illegaal verkregen gegevens verstrekken of buitenwettelijke activiteiten voor de Nederlandse diensten uitvoeren) te worden voorkomen en wettelijk te worden verboden.

- 9.3. Voor structurele samenwerkingsrelaties kan worden overwogen de wegingsnotitie aan een onafhankelijke toets te onderwerpen, analoog aan de toetsing van de aanwijzing van organisaties onder artikel 57. Daarnaast verdient het aanbeveling wettelijk vast te leggen dat bij verstrekking van gegevens aan buitenlandse partners expliciet rekening wordt gehouden met de privacybelangen en andere verdragsrechten van de betrokken personen.

10. Artikelen 72, 97: strafbare feiten

- 10.1 Onder de huidige Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) werd de bevoegdheid voor medewerkers en agenten om strafbare feiten te kunnen plegen vrijwel ongemoeid gelaten en niet nader juridisch ingekaderd. Dit ondanks de eerder bestaande (maar nooit uitgevoerde) opdracht in de vroegere Wiv 2002 om deze bevoegdheid alsnog van juridische waarborgen te voorzien middels een algemene maatregel van bestuur (AMvB).
- 10.2 Ook de vroegere commissie Dessens achtte dergelijke nadere normering – terecht – wenselijk. Desondanks werd de grondslag voor de betreffende AMvB bij invoering van de Wiv 2017 afgeschaft. Het plegen van strafbare feiten door medewerkers en agenten bleef daarmee grotendeels plaatsvinden in een juridisch vacuüm.
- 10.3 Privacy First heeft dit altijd onwenselijk, riskant en ronduit gevaarlijk geacht. Hoe ethisch is deze bevoegdheid en hoe ver reikt deze de afgelopen decennia reeds in de praktijk? Denk hierbij bijvoorbeeld ook aan de inzet van agenten-provocateurs t.b.v. “anti-radicalisering”, contra-terrorisme etc.

11. Verschoningsgerechtigden

In het huidige concept-wetsvoorstel krijgen advocaten, journalisten, Kamerleden en CTT-medewerkers (terecht) extra bescherming middels voorafgaande toetsing door de rechtbank Den Haag bij de inzet van bijzondere bevoegdheden jegens hen. Privacy First adviseert om deze rechterlijke bescherming uit te breiden naar alle groepen verschoningsgerechtigden, waaronder medici, notarissen en geestelijken.

12. Notificatieplicht

Een “lichtpuntje” in het concept-wetsvoorstel is de handhaving van de (in de praktijk weliswaar nauwelijks nageleefde) notificatieplicht. Deze geldt echter immer slechts jegens individuen en niet jegens organisaties die (als zodanig) evengoed *targets* kunnen zijn geweest. Privacy First adviseert dan ook opnieuw om deze bepaling te wijzigen in de zin dat de notificatieplicht tevens voor organisaties zal gaan gelden.

13. Actieve openbaarheid

Privacy First adviseert tevens opnieuw om de Wbmv alsnog te voorzien van bepalingen ter actieve openbaarmaking van (historische) documenten van de diensten. De praktijk van “*declassification and transparency*” in andere landen (waaronder de vroegere Verenigde Staten) kan in dit opzicht een bron van inspiratie vormen.

14. Informanten

Privacy First adviseert ook opnieuw om de Wbmv alsnog te voorzien van een verbod om journalisten als agenten of informanten in te zetten. Dit in het belang van de persvrijheid en journalistieke bronbescherming. In het belang van een gezond maatschappelijk middenveld zou een dergelijk verbod eveneens kunnen worden ingevoerd (of tenminste onafhankelijke toetsing en toezicht moeten krijgen) met betrekking tot de inzet van agenten en informanten bij maatschappelijke (non-gouvernementele) organisaties.

15. Klachtrecht

Art. 189 concept-Wbmv bevat een klachtrecht bij het nieuwe CTT. Privacy First verzoekt u hierbij om in de wettekst en/of MvT te verduidelijken dat dit klachtrecht zowel geldt voor burgers als voor maatschappelijke organisaties (NGO's, zowel in hun eigen belang als in het algemeen of collectief belang), dit mede vanuit oogpunt van rechtsstatelijke effectiviteit en efficiency.

16. Zorgwekkende samenhang met nieuwe Wet op de Defensiegereedheid

Onder het huidige voorstel voor een Wet op de Defensiegereedheid (Wodg) zal eenieder die kritiek uit op Defensie als “gevaar voor de gereedstelling” van de krijgsmacht kunnen worden bestempeld en vervolgens met alle middelen kunnen worden onderzocht, gevolgd en mogelijk ook worden gemanipuleerd. Verzamelde (bijzondere) persoonsgegevens zullen bovendien met bondgenoten gedeeld kunnen worden. Privacy First ziet hier zorgwekkende parallellen met de concept-Wbmv en verzoekt u om hier paal en perk aan te stellen. Tevens wenst Privacy First in dit verband te vernemen hoe de samenwerking en afstemming tussen de Autoriteit Persoonsgegevens (beoogd toezichthouder voor de Wodg) en het CTT

zullen worden vormgegeven.

17. Oorlogspropaganda

In de MvT wordt diverse keren gerept over propaganda en desinformatie. In dit verband attendeert Privacy First u graag op het feit dat louter Nederland en 15 Westerse bondgenoten het internationale verbod op propaganda voor illegale agressie-oorlogen (art. 20 lid 1 IVBPR) tot op heden nooit hebben willen erkennen. (Nederland maakte daartoe eind jaren '70 een vrijwel onbeargumenteerd algemeen voorbehoud. In 2009 verzocht het VN Mensenrechtencomité de Nederlandse regering tevergeefs om dit voorbehoud in te trekken.) Hoe houdbaar is de Nederlandse weigering om dit wereldwijde verbod op oorlogspropaganda te erkennen anno 2026 nog?

18. *Peaceful use of outer space*

De MvT (p. 9) vermeldt dat "Defensie [werkt] aan de krijgsmacht van morgen" en dat daarbij "nadrukkelijker wordt ingezet op cyber, kunstmatige intelligentie, drones *en de ruimte*." Privacy First herinnert u hierbij graag aan het feit dat de ruimte in juridische zin geen militair domein is; hier geldt in het internationaal recht van oudsher het regime van *peaceful use of outer space*. De recente ontwikkeling richting militarisering en mogelijke bewapening van de ruimte is hiermee in strijd en brengt voor de gehele mensheid toekomstige existentiële gevaren met zich mee.

Tot slot

Voor nadere informatie of vragen met betrekking tot bovenstaande is Privacy First te allen tijde bereikbaar op telefoonnummer 020-8100279 of per email: info@privacyfirst.nl.

Hoogachtend,
namens Stichting Privacy First,

Vincent Böhre
directeur