De Minister van Justitie en Veiligheid
De Minister voor Rechtsbescherming
Via https://www.internetconsultatie.nl/wgs/reageren/

**Onderwerp**
Advies conceptwetsvoorstel
Gegevensverwerking door
Samenwerkingsverbanden (concept WGS)

**Datum**
14 september 2018

Geachte heren Grapperhaus en Dekker,

Het Platform Bescherming Burgerrechten heeft kennis genomen van het concept WGS en heeft besloten om op een aantal punten te reageren. Daarbij dient te worden opgemerkt dat een reactie op een consultatie zich niet leent om het veelvoud van twijfelachtige aannames die schuilgaan achter dit concept WGS uitputtend te adresseren.

## Recht op privacy

Artikel 8 EVRM beoogt het privéleven van de burger te beschermen tegen ongeoorloofde inmengingen van buitenaf en doet dit door hiervoor een grondslag in de wet te eisen, de maatregel te toetsen aan het beginsel van evenredigheid en het beperken van het aantal doelen waar maatregels van de overheid voor kunnen worden ingezet, ook wel doelcriteria geheten. Dit leidt in de regel ertoe dat in de wet wordt omschreven onder welke voorwaarden de overheid een inbreuk mag maken op het recht op privacy en welke waarborgen er worden gesteld in de wet, zodat de overheid geen misbruik maakt van deze bevoegdheid, waardoor de burger wordt beschermd tegen willekeur. In het vervolg van deze reactie wordt naar Artikel 8 EVRM gerefereerd als het recht op privacy. Deze bepaling in artikel 7 van het Handvest van de Grondrechten van de Europese Unie (hierna 'Handvest') waarin de term 'correspondentie' is vervangen voor 'communicatie', maar dat volgens artikel 52 lid 3 Handvest qua bescherming en beperkingen een gelijke inhoud en reikwijdte kent als artikel 8 EVRM. Artikel 8 Handvest voorziet in het recht op bescherming van persoonsgegevens. Het recht op bescherming van de persoonlijke levenssfeer is nationaal geregeld in artikel 10 lid 1 van de Gw.

## Zwaarte van de inbreuk

De zwaarte van de inbreuk is van belang voor de eisen die worden gesteld in de wetgeving aan de nauwkeurigheid van de bepalingen waarin overheidsbevoegdheden zijn vastgelegd en aan de waarborgen, waaronder toezicht, waarmee de inzet van de bevoegdheden gepaard moeten gaan. Hoe zwaarder de inbreuk des te nauwkeuriger de wetgever te werk moet gaan en des te steviger de waarborgen moeten zijn om de burger te beschermen tegen de overheidsmacht die door middel van deze bevoegdheden kunnen worden ingezet. De Hoge Raad bevestigde dit in 2017 door te beslissen dat een beperkte inbreuk op de persoonlijke levenssfeer kon plaatsvinden op basis van een algemene bevoegdheid, maar een meer dan beperkte inbreuk waarbij een 'min of meer compleet beeld is verkregen van bepaalde aspecten van het persoonlijke leven' vereist een specifiek op deze inbreuk

toegesneden wettelijke bepaling met bijbehorend toezicht.[1] Bij de zwaarte van de inbreuk op het recht op privacy wordt door het Europees Hof voor de Rechten van de Mens (hierna 'EHRM') en het Hof van Justitie van de EU (hierna 'HvJEU') gelet op de context van de verwerking van persoonsgegevens en de aard van de gegevens. Bij de context moet in dit kader onder andere worden gedacht aan nadelige gevolgen van de gegevensverwerking voor de burger, de redelijke verwachting van privacy (vertrouwelijkheid), de hoeveelheid personen die het raakt en hoe het doel van de nieuwe verwerking zich verhoudt tot het oorspronkelijke doel van de verwerking. De context waarin de gegevens worden verwerkt kan invloed hebben op de aard van de gegevens.

Ondanks het feit dat het concept WGS nog niet rept van een specifieke toepassing kan op voorhand worden vastgesteld dat het concept WGS zeer zware inbreuken op het recht op privacy mogelijk maakt met een minimum aan afbakening en een volledig gebrek aan betekenisvolle waarborgen. De soorten gegevens die terecht kunnen komen in een samenwerkingsverband zijn niet afgebakend. Zo is het bijvoorbeeld onduidelijk of deze kaderwet in combinatie met de wijzigingen in de AVG die betrekking hebben op doelbinding het mogelijk maken dat een aanbieder van een openbaar elektronisch communicatienetwerk op basis van artikel 11.2 jo 11.2a sub d Telecommunicatiewet (wettelijke basis) zich kan aansluiten bij een samenwerkingsverband en op systematische wijze gegevens hieraan kan aanleveren indien dit gebeurt binnen een samenwerkingsverband voor een doel van zwaarwegend algemeen belang dat bij AMvB is vastgesteld. Het wordt in het concept WGS in ieder geval niet uitgesloten.

De overheid permitteert zich om op basis van een AMvB samenwerkingsverbanden aan te gaan met private partijen waarbij gegevens systematisch worden verwerkt, waaronder het combineren, structureren, profileren en analyseren valt (artikel 6 lid 3 concept WGS), teneinde onder andere registers risicomeldingen in te richten waar de burger in kan belanden op basis van geheime algoritmen en zelfs de toepassing van kunstmatige intelligentie. Dit maakt het mogelijk omeen zeer indringend beeld van de burger te krijgen dat bovendien voortdurend wordt bijgewerkt.

## Legaliteitsvereiste

### Basis in de wet

Volgens de Nederlandse Grondwet vereist een inmenging in het recht op de bescherming van de persoonlijke levenssfeer een formeel-wettelijke grondslag. Gegevens liggen aan de basis van informatie en informatie ligt aan de basis van de uitoefening van overheidsmacht.[2] De macht van de overheid is rechtens gelegitimeerde macht en deze macht moet gebonden zijn aan het recht. De indruk van deze kaderwet is dat deze de informatiemacht tracht los te trekken van het recht, door de formele wetgever praktisch buitenspel te zetten en de discretionaire bevoegdheid aangaande structurele samenwerkingsverbanden bij de bevoegde minister(s) te leggen.

Hier neemt het concept WGS een interessante wending:

---

[1] HR 04-04-2017, ECLI:NL:2017:584.

[2] Paragraaf 2 van de 'Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', Strasbourg, 28-1-1981. Zie https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800ca434, laatst gezien 4-9-2018.

*'Op grond van vaste jurisprudentie van het Europees Hof van Justitie geldt echter dat een verordening van de Europese Unie boven het nationale recht en dus ook de grondwet gaat. De AVG vergt anders dan artikel 10 van de Grondwet geen formeel-wettelijke grondslag voor beperkingen van het recht op eerbiediging van de persoonlijke levenssfeer. De grondslag voor gegevensverwerking vloeit immers direct voort uit de AVG. Voor de WGS en de krachtens deze wet vast te stellen AMvB's voor de gegevensverwerking in specifieke samenwerkingsverbanden is deze grondslag te vinden in artikel 6, eerste lid, onder c en e van die verordening.'*[3]

De opstellers menen onder de werking van de Grondwet uit te kunnen komen door een beroep te doen op de AVG. Voor de rechtsgrond van de verwerking wordt verwezen naar artikel 6 lid 1 sub c en e AVG vallen, respectievelijk, de wettelijke verplichting en de verwerking voor de behartiging van een taak van algemeen belang. In artikel 6 lid 3 jo 4 AVG wordt echter voorzien in de mogelijkheid om af te wijken van het doelbindingsvereiste indien deze verwerking is vastgesteld bij 'lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is'. De opstellers van het concept WGS menen ten onrechte dat de AVG een wettelijke grondslag creëert voor de beoogde samenwerkingsverbanden op basis van een AMvB, echter, de AVG geeft slechts de ruimte aan de wetgever van de lidstaat om een rechtsgrond vast te stellen in het recht zoals dit geldt binnen die lidstaat. Met andere woorden, de AVG geeft een instructie aan de nationale wetgever, maar zij creëert niet een nieuwe bevoegdheid. Een rechtsgrond vastgesteld bij Nederlands recht moet nog steeds voldoen aan de Grondwet. Daarnaast is een AMvB geen geschikt instrument voor het vastleggen van vergaande bevoegdheden die grote stelselmatige inbreuken op de grondrechten van burgers faciliteren, omdat op deze wijze de uitvoerende macht ten onrechte op de stoel van de wetgevende macht plaatsneemt. De formele wetgever is bij uitstek de partij is die beslissingen dient te nemen aangaande maatschappelijk omstreden fenomenen waarin tegenstrijdige belangen een rol spelen en waar inmengingen plaatsvinden met de grond- en mensenrechten van burgers.

## Voorzienbaarheid

Het vereiste van voorzienbaarheid is ontwikkeld in de rechtspraak van het EHRM als één van de 'quality-of-law' criteria. Het vereiste bepaalt dat regelgeving voldoende precies dient te zijn en een indicatie moet geven van de omstandigheden en voorwaarden waaronder een inmenging met de rechten van burgers mag plaatsvinden door de inzet van bevoegdheden van de overheid. De wet moet duidelijk maken wat de reikwijdte van de bevoegdheid is en de voorwaarden waaronder deze mag worden ingezet. Als burger moet je de vraag kunnen stellen 'Waarom ik?'. De regels hoeven niet zo precies te zijn dat deze geen flexibiliteit bieden in de praktijk. Het EHRM heeft in het verleden vastgesteld dat de precisie waarmee dit moet worden aangegeven onder meer afhangt van de inhoud van de maatregel, het terrein waarop het van toepassing is en de status en hoeveelheid personen op wie het van toepassing is.[4] Het is door de directe werking van het EVRM ook in Nederland van toepassing.

In het concept WGS wordt bepaald dat aan deze eisen ook kan worden voldaan door een AMvB.[5] Dit veronderstelt dat de wet waaronder de AMvB hangt een bevoegdheid mag creëren die niet voldoet aan het voorzienbaarheidsvereiste. Dit is maar zeer de vraag. Zeker nu niet op voorhand kan worden

[3] Concept WGS, blz. 21
[4] *Vogt v Germany* App no 17851/91 (EHRM, 26 september 1995).
[5] Concept WGS, blz. 20.

uitgesloten dat de inhoud van de maatregel, met name bij de systematische verwerkingen onder artikel 6 concept WGS, kan bestaan uit geheime surveillance. Het is vaste rechtspraak dat bij geheime surveillance het voorzienbaarheidsvereiste strikt worden toegepast en in het licht van de voortschrijdende verfijning van technologie zijn heldere en gedetailleerde regels een vereiste.[6] Voor het lichtere middel van stelselmatige observatie met een technisch hulpmiddel, waarvan ook sprake kan zijn in een samenwerkingsverband (tal van apparaten en technisch middelen (pinpas, ov-pas) kunnen dienen als een zodanig technisch hulpmiddel. Over de inzet van dergelijke middelen door de sociale recherche heeft de Centrale Raad van Beroep onlangs nog bepaald dat deze moet berusten op een voldoende duidelijke, voorzienbare en met waarborgen omklede wettelijke grondslag.[7] Een algemene bepaling in de WWB werd nadrukkelijk onvoldoende geacht en in plaats daarvan werd aansluiting gezocht bij de waarborgen uit artikel 126 Wetboek van Strafvordering waarin tussenkomst van de officier van justitie is vereist en waarop het bevel tot observatie onder meer het misdrijf, een zo nauwkeurig mogelijke aanduiding van de verdachte, de feiten of omstandigheden op basis waarvan er sprake is van een verdenking en de geldigheidsduur van het bevel staat. Wat de rechter hierbij van belang achtte was dat het middel geschikt was om een 'min of meer compleet beeld te verkrijgen van bepaalde aspecten van het persoonlijke leven van de betrokkenen, zoals in dit geval de woonsituatie'.[8] Hierbij dient opgemerkt te worden dat het beeld dat kan worden verkregen van burgers op basis van de voorziene samenwerkingsverbanden nog vele malen indringender kan zijn. De aard van de gegevens kan op zichzelf variëren van minder intiem tot zeer intiem. Minder intieme gegeven kunnen door het systematische karakter van de verwerking en de hoeveelheid van de gegevens toch intiem van aard worden, doordat ze alsnog een indringend beeld van een persoon geven.[9] Hier kan bijvoorbeeld worden gedacht aan een slimme meter die ieder kwartier het stroomgebruik van een huishouden vastlegt. De 96 metingen op één dag geven een beperkt beeld van een huishouden, maar de metingen over een spanne van een maand geven een zeer indringend beeld van een huishouden waarbij zelfs gevoelige eigenschappen als religie uit de gegevens kan worden afgeleid.

Het concept WGS beoogt een blanco bevoegdheid te creëren, waarbij de inbreuken op het recht op privéleven nauw samenhangen met het subjectieve besluit van bestuursorganen of private partijen om deel te nemen aan een samenwerkingsverband. De enige drempel die wordt opgeworpen is dat dit moet worden vastgelegd in een AMvB en dat het een doel van zwaarwegend algemeen belang moet dienen. De overige voorwaarden waaronder een samenwerkingsverband mag worden opgezet zijn niet duidelijk afgebakend.

In de eerste plaats mist er een duidelijk omschreven doel waarvoor een samenwerkingsverband kan worden ingezet. De lijst van doelen opgenomen in artikel 2 lijkt niet als doel te hebben om de beoogde bevoegdheid af te bakenen, maar om het mogelijk te maken om deze in te zetten in iedere sfeer waarin de overheid actief is.

In de tweede plaats ontbreekt er een duidelijk omschreven werkwijze. De omschreven bevoegdheid wordt in zeer algemene bewoordingen gevat en in principe wordt praktisch alles overgelaten aan de opsteller(s) van de AMvB. Ook in zaken rond dataretentie, zoals Digital Rights Ireland, is door het HvjEU

---

[6] *Huvig v France* App no 11105/84 (EHRM, 24 april 1990), para 32, 34.
[7] CRvB 15-08-2017, ECLI:NL:CRVB:2017:2807, § 4.7.7.
[8] ibid, § 4.7.6.
[9] *MM v The United Kingdom* App no 24029/07 (ECtHR, 13 November 2012), § 200.

erkend dat er criteria voor toegang tot gegevens moeten worden opgenomen in de wetgeving die de bewaring van deze gegevens vereisen.[10] Dit werd opgemerkt ondanks het feit dat lidstaten wel de instructie kregen om te waarborgen dat alleen overeenkomstig de (inmiddels vernietigde) dataretentierichtlijn (2006/24/EG) 'bewaarde gegevens alleen in welbepaalde gevallen, en in overeenstemming met nationale wetgeving, aan de bevoegde nationale autoriteiten worden verstrekt' (artikel 4), waarbij in artikel 1 het bewaren van de gegevens werd gekoppeld aan het doel om ernstige criminaliteit te onderzoeken en op te sporen.

In de derde plaats ontbreken categorieën van gegevens in het concept WGS. Deze worden pas ingevuld in de AMvB. Er zijn zelfs geen gegevens die expliciet buiten de scope worden gehouden. Hoewel in de toelichting wordt gezegd dat bijzondere persoonsgegevens niet vallen onder de verplichting om gegevens te verstrekken die is vastgelegd in artikel 5, wordt daarbij aangetekend dat op dergelijke gegevens de AVG, UAVG en andere wetten van toepassing zijn. De relatie tussen artikel 5 WGS en de UAVG wordt niet verder toegelicht. Het blijft daarom onduidelijk wat precies de gevolgen hiervan zijn. Zo zijn er regelingen in de AVG (artikel 9 lid 2 sub g) en de UAVG (artikel 23 sub c) die de verwerking van bijzondere gegevens toestaat voor redenen van zwaarwegend algemeen belang op grond van lidstatelijk recht, waarbij de evenredigheid moet worden gewaarborgd en specifieke maatregelen te bescherming van de fundamentele rechten van de betrokkene moeten worden genomen. Is het de bedoeling van de opstellers van de WGS dat een AMvB als een dergelijke grond van lidstatelijk recht kan dienen of is dit nadrukkelijk niet de bedoeling? Dit dient te worden opgehelderd.

Daarnaast stelt de MvT van het concept WGS dat er in deze wet aanvullende uitzonderingen op het verwerkingsverbod zijn opgenomen voor politiegegevens, strafrechtelijke en justitiële gegevens. Dit kunnen alle bijzondere categorieën van persoonsgegevens betreffen, zie artikel 23 sub c UAVG. Volgens deze bepaling is het verbod om bijzondere categorieën van persoonsgegevens te verwerken, gelet op artikel 9 lid 2 sub g (grondslag uitzondering lidstatelijk recht voor doel van zwaarwegend algemeen belang), niet van toepassing indien 'de verwerking noodzakelijk is in aanvulling op de verwerking van persoonsgegevens van strafrechtelijke aard voor de doeleinden waarvoor deze gegevens worden verwerkt'. Er zijn geen beperkingen van het soort bijzondere categorieën in deze bepaling opgenomen. Het lijkt er daarom op dat bijvoorbeeld ook dna vallen dat door de politie is afgenomen. De doeleinden, zoals bedoeld in artikel 23 sub c UAVG, waarvoor deze gegevens mogen worden verwerkt worden in het concept WGS uitgebreid onder zowel de Wpg als de Wjsg naar samenwerkingsverbanden. Deze bepalingen uit de UAVG, de AVG en dit concept WGS tezamen voorzien in de mogelijkheid om bijzondere persoonsgegevens op systematische basis binnen samenwerkingsverbanden te verwerken. De MvT van het concept stelt nadrukkelijk dat de nieuwe bepalingen in dit voorstel 'niet alleen de bevoegdheid maar ook een plicht regelen tot verstrekking'.[11]

Bovendien kan in de 'Consultatie Wet bevorderen samenwerking en rechtmatige zorg' worden gevonden dat in de samenwerkingsverbanden die binnen dit concept worden beoogd de mogelijkheid bestaat om gegevens verder te verwerken indien 'enig wettelijk voorschrift tot de bekendmaking verplicht' (artikel 2.6 lid 2 sub a Wet bevorderen samenwerking en rechtmatige zorg.[12] Dit roept de

---

[10] Gevoegde zaken C-293/12 en C-594/12 Digital Rights Ireland EU:C:2014:238, para 60.

[11] Concept WGS, blz. 21.

[12] Het lijkt een cumulatieve voorwaarde, maar op de laatste bladzijde van de MvT (26) is te zien dat de bedoeling van de wetgever is dat deze voorwaarde alternatief is.

vraag op of de gegevens verkregen uit deze samenwerkingsverbanden dus ook onder de samenwerkingsverbanden beoogd onder het concept WGS vallen. Dit dient wel verhelderd te worden, zodat we tenminste met zekerheid kunnen vaststellen dat het de bedoeling is van de opstellers om het medisch beroepsgeheim bij het oud vuil te zetten.

Ten slotte komen we nog kort terug op de systematische verwerking van gegevens in samenwerkingsverbanden waarbij er feitelijk sprake kan zijn van heimelijke observatie. In dergelijke zaken heeft het EHRM bepaald dat duidelijk dient te zijn:

a. 'Welke activiteiten of overtredingen aanleiding kunnen geven voor heimelijke surveillance;
b. Welke categorieën van personen kunnen worden getroffen door heimelijke surveillance;
c. Wat de maximale duur is van de surveillancebevoegdheid;
d. Welke procedure moet worden gevolgd om de verkregen gegevens te mogen onderzoeken, gebruiken en opslaan;
e. Welke voorzorgsmaatregelen moeten worden getroffen bij het gebruik van de gegevens en het verschaffen daarvan aan derde partijen; en
f. De omstandigheden waaronder de gegevens moeten worden gewist of vernietigd.'[13]

Bij deze systematische verwerkingen gaat het niet langer slechts over heimelijke observatie, maar ook de heimelijke profilering die hieruit volgt. Dit alles op basis van algoritmes en mogelijk kunstmatige intelligentie waarvan de partijen die het gebruiken zelfs grip verliezen op wat de uitkomsten zijn. Wanneer de uitvoerende macht niet meer begrijpt op basis waarvan de macht wordt uitgevoerd, behoort het voorzienbaarheidsvereiste tot het verleden en gaat een belangrijke bouwsteen van de 'rule of law' of rechtstaat verloren. De waarborgen omtrent het bekend maken van de onderliggende logica bieden ook geen soelaas, omdat deelnemers zich tegen die bekendmaking van verzetten.

### Toegankelijkheid

De AMvB's zullen worden gepubliceerd in het Staatsblad. Op deze manier kan het doel van het samenwerkingsverband worden vastgesteld. Het is de vraag of alle deelnemers hier ook in zullen verschijnen. Het project *Finpro*, waarnaar ook in het concept WGS wordt verwezen, kan worden gezien als een samenwerkingsverband avant la lettre, maar dan met als doel 'wetenschappelijk onderzoek'. De private partijen die aan dit 'wetenschappelijk onderzoek' deelnamen wilden dit feit graag privé houden, terwijl ze de persoonsgegevens van hun klan ten afstonden aan een privaat onderzoeksbureautje. Hiervoor lieten ze een non-disclosure agreement tekenen, waardoor tot op de dag van vandaag nog steeds niet duidelijk is welke private partijen aan Finpro hebben deelgenomen.[14] Het is niet duidelijk of er binnen de samenwerkingsverbanden beoogd door dit wetsvoorstel ook voor dergelijke wensen vanuit deelnemers ruimte is.

### Effectieve waarborgen

Effectieve waarborgen worden onder de rechtspraak soms gecategoriseerd onder het legaliteitsvereiste, maar hangen zeker ook samen met het proportionaliteitsvraagstuk. Onder de rechtspraak van het EHRM wordt er, zeker bij geheime surveillance, veelal de nadruk gelegd op de invulling van de reikwijdte van de bevoegdheid en bestaat er dus een sterk verband met het voorzienbaarheidsvereiste. Minimumeisen

---

[13] Van de dagvaarding in de SyRI-zaak, zie . EHRM Weber en Saravia (n-o), 29 juni 2006, 54934/00, par. 95.
[14] Aanhangsel Handelingen 2015-2016, nr. 2958. Zie https://bit.ly/2oGJPdN, laatst gezien 5 september 2018.

die worden gesteld om de misbruik van bevoegdheden tegen te gaan zijn: de aard, reikwijdte en termijn van inzet van surveillancemaatregelen, de redenen waarvoor ze kunnen worden opgelegd, de bevoegde autoriteiten om ze toe te staan, uit te voeren en om toezicht te houden (hier wordt onder de paragraaf 'Toezicht' op ingegaan)en het soort 'remedy' dat onder het nationale recht wordt geboden.[15] Het HvJEU is eerder geneigd de waarborgen onder de proportionaliteitstoets te scharen (zie oa het arrest Digital Rights Ireland).

De bedoeling van deze waarborgen is om de burger te beschermen tegen misbruik van recht en willekeur. Het EHRM heeft bepaald dat het essentiële doel van artikel 8 EVRM is om de burger te beschermen tegen willekeurige inmenging door publieke autoriteiten. De hierboven besproken waarborgen ontbreken in het concept WGS. Met in het achterhoofd de verwijdering van waarborgen en bescherming waarin de WGS voorziet, kan hierover de conclusie niet anders luiden dan dat deze kaderwet de burger in aanmerkelijke mate blootstelt aan willekeurige machtsuitoefening door overheid én bedrijfsleven.

## Nut, noodzaak en doel

Gezien het feit dat de WGS een kaderwet betreft is het niet gemakkelijk om de nut en noodzaak van deze wet op voorhand vast te stellen. Wat de WGS beoogt te doen is, in de woorden van de Werkgroep Verkenning kaderwet gegevensuitwisseling, is het wegnemen van generieke knelpunten met betrekking tot gegevensuitwisseling in bestaande wetgeving. Met andere woorden, de kaderwet beoogt de mogelijkheid te creëren om de verschillende verboden om gegevens verder te verwerken en bepalingen die nadere toetsing vereisen die volgt uit verschillende wetten op basis van deze kaderwet ongedaan te maken. De doelcriteira voor zo'n samenwerkingsverband zijn zo breed geschetst dat het moeilijk is om een doel binnen de overheidssfeer te formuleren dat hier niet binnen valt, zolang het maar voor de samenleving van meer dan gewone betekenis is.

De opstellers van de MvT geven wel het volgende weg:

> 'Pas wanneer sprake is van *een behoefte* bij de ene overheidsinstantie aan gegevens waarover een andere overheidsinstantie beschikt en dus aan het uitwisselen van gegevens tussen overheidsinstanties, ontstaat de noodzaak een dergelijke uitwisseling van gegevens van een adequate juridische grondslag te voorzien.'[16]

Wat opvalt is de woordkeuze 'een behoefte'. Het EHRM heeft aangegeven dat noodzakelijk niet hetzelfde betekent als 'onmisbaar', 'absoluut noodzakelijk' of 'strikt noodzakelijk', maar ook niet flexibel is als 'nuttig', 'toelaatbaar', 'redelijk' of 'wenselijk'.[17] Het bestaan van een behoefte in de samenleving is daarom onvoldoende om dit wetsvoorstel te legitimeren. In de rechtspraak van het EHRM is vastgesteld dat een maatregel een 'dringende maatschappelijke behoefte' moet vervullen. Hierbij moet er worden gekeken naar de omstandigheden van het geval. Dit is geen vrijblijvende toets en dient gebaseerd zijn op een redelijke waardering van de relevante feiten. In de WGS wordt verwezen

---

[15] *Shimovolos v Russia* App no 30193/09 (EHRM, 21 juni 2011), para 68.

[16] Ministerie van Justitie en Veiligheid, Conceptwetsvoorstel gegevensverwerking door samenwerkingsverbanden (WGS) *Internetconsultatieversie*, https://www.internetconsultatie.nl/wgs, blz. 7.

[17] *Handyside v The United Kingdom* App no 5493/72 (EHRM, 7 December 1976) para 48.

naar het EVRM en de dringende maatschappelijke behoefte, maar er wordt ten onrechte gesteld dat de aanwezigheid hiervan wordt getoetst door te kijken naar de noodzakelijkheid en relevantie van een maatregel.[18] Dit zou ertoe leiden dat de gepercipieerde noodzakelijkheid tot gegevensuitwisseling door de bevoegde ministers wordt gehanteerd als een criterium voorgesteld om vast te stellen of sprake is van een dringende maatschappelijke behoefte. Dit is juridisch onjuist. De vraag of is voldaan aan het vereiste van noodzakelijkheid behoort mede aan de hand van het vervullen van een dringende maatschappelijke behoefte moet worden beantwoord.[19] Bovendien moet er volgens het EHRM worden gekeken naar het belang dat tegen de inbreuk wordt beschermd en de aard van de inbreuk.[20] Hier wordt geen woord aan gewijd in het concept WGS, terwijl de keerzijde van de medaille van het probleemoplossend potentieel dat deze wet beoogt te introduceren, ligt in het gevaar van een overheid die al haar bevoegdheden op het vlak van informatie mag gebruiken in alle hoedanigheden die zij bezit.

De proportionaliteit en subsidiariteit van de maatregel zijn in relatie tot concrete samenwerkingsverbanden makkelijker te beoordelen dan in het kader van het concept WGS. Er kunnen, echter, wel kanttekeningen worden gezet bij de beoogde verwerkingen in de samenwerkingsverbanden. In artikel 6 is vastgelegd dat de gegevens systematisch worden verwerkt (combineren, structureren, profileren en analyseren) met als doel om 'noodzakelijke informatie af te leiden en vast te leggen'. Uit de MvT wordt duidelijk dat dit risico's betreft die worden verbonden aan bepaalde personen in bepaalde contexten die worden vastgelegd in zwarte lijsten.[21] Dit staat niet in deze woorden in de MvT, maar hier komt het feitelijk op neer. Dit lijkt te duiden op een geautomatiseerde uitwisseling waarbij naar alle waarschijnlijkheid autonoom communicerende databases gegevens uitwisselen die met behulp van (geheime) algoritmes dit soort lijsten zullen produceren. Het systematisch karakter van de verwerking en daarmee gepaard gaande inbreuken op het recht op privacy draaien de bescherming van artikel 8 EVRM op de kop. Waar deze uitgaat van het recht op respect voor het recht op privacy als de regel en de inbreuk als de uitzondering ('there shall be no interference ... except such as is in accordance.....'), creëert de kaderwet de mogelijkheid om op systematische basis een uitzondering op de regel te maken.[22] Het is niet duidelijk waarom het huidige instrumentarium voor de overheid niet volstaat. De huidige samenwerkingsverbanden die bestaan worden al gebruikt om misstanden op te sporen en lijken het al mogelijk te maken voor de overheid om in samenwerkingsverbanden te opereren. Al mogen hierbinnen niet de gegevens van de verschillende deelnemers door de anderen worden gebruikt voor operationele doeleinden, de ontdekte patronen en groepsprofielen mogen wel worden gebruikt 'binnen de grenzen van zijn wettelijke taken en bevoegdheden [om] te matchen met gegevens waarover hijzelf rechtmatig beschikt, om daaruit bijvoorbeeld lijsten te destilleren van personen die bepaalde risico's op het desbetreffende taakgebied vertonen', aldus de MvT van het concept WGS.[23] Voor uitzonderlijke gevallen, als hier een aanleiding voor bestaat, mogen gegevens verder worden verwerkt voor onverenigbare doeleinden en wordt ook voor dergelijke gevallen voorzien in uitzonderingen op de geheimhouding. Het huidige wettelijke kader voor gegevensuitwisseling kent de

---

[18] ibid, blz. 20.

[19] Ursula Kilkelly, *The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention of Human Rights* (Human Rights Handbook, No. 1, Council of Europe 2003), blz. 31.

[20] *Dudgeon v The United Kingdom* App no 7525/76 (ECtHR, 22 oktober 1981). Kilkelly, blz. 32.

[21] Concept WGS, blz. 13.

[22] Zie ook Gevoegde zaken C-203/15 and C-698/15 Tele2 Sverige EU:C:2016:970, para 89. Gevoegde zaken C-293/12 en C-594/12 Digital Rights Ireland EU:C:2014:238, para 57 en 58.

[23] Concept WGS, blz. 13.

overheid al brede bevoegdheden toe en er wordt niet duidelijk gemotiveerd waar de noodzaak in bestaat om het huidige wettelijke kader nog verder uit te breiden.

In het huidige systeem dient de uitzondering op de regel een aanleiding te hebben die verband houdt met de persoon van de betrokkene. Het concept WGS beoogd om deze uitzondering te maken los van de persoon van de betrokkene. In het samenwerkingsverband wordt de inbreuk op de bescherming van privacy en persoonsgegevens de regel in plaat van de uitzondering. De AMvB, zoals voorzien in de WGS, voorziet in algemene en ongedifferentieerde verwerking van een niet nader omlijnde hoeveelheid gegevens.[24]

## Doel

Er wordt een overkoepelend doel aangegeven, zoals al eerder opgemerkt, is dit het creëren van een kaderwet teneinde de verschillende verboden om gegevens verder te verwerken en bepalingen die nadere belangenafwegingen vereisen die volgen uit verschillende wetten ongedaan te maken. Dit wordt door de opstellers van dit concept en de eerdere Werkgroep consequent geduid met het eufemisme 'knelpunten oplossen'. De gevolgen voor de rechtsbescherming van burgers, echter, is dat deze compleet en blijvend dreigt te worden tenietgedaan door deze wet. Een kritische lezer zou kunnen opmerken dat het doel van deze kaderwet is om de rechtsbescherming van de burger tegen de concentratie van informatiemacht van de overheid en bedrijfsleven buitenspel te zetten. Het doel om de rechtsbescherming van de burger teniet te doen is niet legitiem. Een brief van toenmalig Minister van der Steur aan de Tweede Kamer illustreert dat de Nederlandse regering in Brussel bij de onderhandelingen over de tekst van de AVG actief heeft ingezet op het ondermijnen van deze rechtsbescherming.[25]

De WGS beoogd de inzet van samenwerkingsverbanden nader af te grenzen door de eis te stellen dat het een doel van 'zwaarwegend algemeen belang' moet dienen. In hoeverre dit extra bescherming biedt hangt ervan af hoe dit criterium in de praktijk wordt toegepast. Eerdere uitlatingen van de wetgever waarin werd gesteld dat een verwerking een algemeen belang dient zodra deze voor de samenleving van betekenis is en een zwaarwegend algemeen belang 'indien die voor de samenleving van meer dan gewone betekenis is', is uiterst subjectief en lijkt onbruikbaar als praktisch criterium om de inzet van een samenwerkingsverband te beperken.[26] Het criterium van 'zwaarwegend algemeen belang' kan volgens de MvT van de Wpg worden herleid tot artikel 8 lid 4 Richtlijn 95/46/EG, dat in de Engelse versie een 'substantial public interest' is.[27] Voorbeelden die hier worden genoemd is het melden van het vermoeden van kindermishandeling (blz. 16), maar ook partijen zoals Bureau Jeugdzorg en bepaalde landelijke inspecties om hun toezichthoudende taak uit te voeren (blz. 73).

Nadere afgrenzing van de doelen wordt voorzien door aansluiting te zoeken bij de doelcriteria van artikel 8 EVRM waarin het recht op bescherming van de privacy is vastgelegd. Het doel van het samenwerkingsverband dient één of meer van de in het EVRM genoemde belangen te vertegenwoordigen.[28] Deze belangen zijn zeer breed geformuleerd in de tweede paragraaf van artikel 8

---

[24] Tele2 Sverige, para 97.
[25] *Kamerstukken II* 2015/2016, 32 761, nr. 91, https://zoek.officielebekendmakingen.nl/dossier/32761/kst-32761-91.
[26] *Kamerstukken II* 2005/06, 30 327, nr. 3, blz. 74.
[27] Ibid, blz. 73.
[28] Concept WGS, blz. 21.

EVRM en sluiten wat dit betreft aan bij de brede doelclausulering in artikel 2 van de concept WGS. Nationale en openbare veiligheid, economisch welzijn van het land, voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen. Door al deze belangen op één hoop te vegen creëert de wetgever een onmetelijke brede basis om de concentratie van gefragmenteerde informatiemacht in samenwerkingsverbanden te rechtvaardigen. Het is juist deze opeenstapeling van doelen die in het kader van de toetsing van de noodzakelijkheid problematisch is. Door al deze doelen a priori van belang te achten creëert de wetgever een voorwendsel om de invoering van de zeer vergaande bevoegdheden in de kaderwet te rechtvaardigen. De noodzaak van een maatregel vaststellen is alleen mogelijk wanneer er een duidelijk doel is vastgesteld. Een duidelijk doel ontbreekt in het concept WGS.

## Toezicht

De gegevensverwerkingen die op basis van het concept WGS plaatsvinden veroorzaken inbreuken op het recht op de eerbiediging van het privéleven bij de verwerking van persoonsgegevens op drie verschillende momenten. Het eerste is bij de verstrekking van gegevens aan het samenwerkingsverband door een deelnemer. Op dit moment vindt er al een doorbreking van het doelbindingsbeginsel plaats. Het tweede moment is de verwerking van de gegevens binnen het samenwerkingsverband, waarbij de gegevens kunnen worden gecombineerd en op basis hiervan profielen kunnen worden opgemaakt. Het derde moment is de verstrekking van de resultaten aan de diverse deelnemers, aangezien deze resultaten tot stand zijn gekomen door een veelvoud van gegevens waar deze deelnemers oorspronkelijk geen toegang toe hadden. Daarnaast liggen deze resultaten aan de basis van de vervolgacties en interventies van de deelnemers.

Het is vaste rechtspraak van het EHRM dat de geheime verwerking van persoonsgegevens vraagt om adequate en effectieve waarborgen tegen misbruik van bevoegdheid. De AMvB wordt weliswaar gepubliceerd, maar het is niet waarschijnlijk dat de informatie die hierin wordt vermeld ook daadwerkelijk houvast biedt voor betrokkenen om te begrijpen dat hun gegevens worden verwerkt en wat deze verwerking voor gevolgen heeft. Daarnaast blijven de algoritmen en de risicomodellen geheim. Kortom, de openbaarmaking van de AMvB lijkt geen adequate en effectieve waarborg tegen misbruik. Het EHRM eist in het geval van geheime surveillance onafhankelijk en effectief toezicht. Hiervoor hoeft het toezicht niet door een rechter te worden uitgeoefend, maar de toezichthoudende instantie moet wel effectief en onafhankelijk zijn. In het concept WGS is er niets geregeld omtrent toezicht.

## Recht op bescherming van persoonsgegevens en AVG

Het recht op bescherming van persoonsgegevens zoals vastgelegd in artikel 8 Handvest wordt herhaald en er wordt bepaald dat de WGS en de krachtens de WGS vast te stellen AMvB's voorzien in de gerechtvaardigde grondslag. De overige vereisten uit het Handvest worden ingevuld door de AVG en de UAVG. Hieronder wordt ingegaan op de doelbinding, waarin de grootste verandering plaatsvindt. Het gegevensbeschermingsrecht, zoals al eerder werd aangegeven, moet in overeenstemming met artikel 8 EVRM worden uitgelegd.[29]

---

[29] Gevoegde zaken C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-04989, para 68. HR 09-09-2011, LJN: BQ8097, NJ 2011, 595 m. nt. E.J. Dommering.

## Doelbinding

In artikel 2 wordt de doelbinding voor de samenwerkingsverbanden vastgelegd. In de AMvB moet het doel van het samenwerkingsverband uitdrukkelijk omschreven, welbepaald en gerechtvaardigd zijn. Deze beschrijving van het doel beslaat het eerste element van de doelbinding. Het tweede element, ook wel het vereiste van verenigbaarheid genoemd, is dat gegevens niet verder mogen worden verwerkt voor doeleinden die met het oorspronkelijke doeleinde onverenigbaar zijn.

Dit beginsel is één van de hoekstenen van het gegevensbeschermingsrecht. Het is ook vastgelegd in de AVG. Hierin wordt het, mede dankzij de inzet van Nederland tijdens de trioloog-onderhandelingsfase, zodanig ingekaderd dat de lidstaten de mogelijkheid krijgen om het middels de wetgever buitenspel te zetten. In artikel 6 lid 3 wordt toegestaan dat doelbinding kan worden 'aangepast' in het lidstatelijk recht op basis waarvan gegevens worden verwerkt en in lid 4 dat onverenigbare verwerkingen zijn toegestaan zolang deze zijn voorzien in het lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is. De beperkingsclausule in artikel 13 Richtlijn 95/46/EG en artikel 23 AVG zijn gekoppeld aan de beperkingsclausule van artikel 8 lid 2 EVRM (artikel 7 jo 52 Handvest), er mogen op bepaalde regels uitzonderingen worden gemaakt als dit noodzakelijk is voor één van de genoemde publieke belangen, en het volgt uit vaste rechtspraak van het HvJEU dat de bescherming van het recht op privéleven 'vereist dat de uitzonderingen op de bescherming van persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven'.[30] EVRM en Handvest voorzien niet in een basis om systematische uitwisseling van de persoonsgegevens van een niet nader omschreven groep, voor een niet nader omschreven categorie van delicten dan wel overtredingen, mogelijk te maken. Het gegevensbeschermingsrecht moet in overeenstemming met artikel 8 EVRM worden uitgelegd. Dit volgt uit de Nederlandse, alsmede Europese jurisprudentie.[31] Het concept WGS is hiermee onverenigbaar.

Het concept WGS beoogt het mogelijk te maken om brede doelen in te stellen op basis waarvan alle deelnemers van een samenwerkingsverband gegevens kunnen verstrekken, ook als dit onverenibaar is met het oorspronkelijke doel. In het concept staat weliswaar dat de doelen uitdrukkelijk, welbepaald en gerechtvaardigd moeten zijn, maar in de praktijk worden doelen lang niet altijd welbepaald geformuleerd.[32] In het concept WGS is het niet duidelijk wat er nu precies gebeurt met de resultaten verkregen uit de gegevensverwerkingen en is het daarom al moeilijk te zeggen of het doel welbepaald is. In het concept WGS wordt gesteld dat de grondslag voor de verstrekking aan het verband ook geldt voor de verwerking binnen dat verband, dit specifiek in relatie tot private partijen, en dat het verband deze gegevens kan verwerken 'tot voor een deelnemer noodzakelijke informatie' (blz. 15). Het is onduidelijk welke partij op basis van wat voor criteria bepaalt wat kwalificeert als 'noodzakelijke informatie'.

De effectiviteit van de rechtsbescherming die volgt uit het gegevensbeschermingsrecht hangt nauw samen met de toepassing van de doelbinding en het feit dat andere belangrijke eisen die volgen uit dit

---

[30] Gevoegde zaken C-293/12 and C-594/12 *Digital Rights Ireland* [2014] OJ C175/6, para 52 en de rechtspraak die hierin wordt genoemd.

[31] Gevoegde zaken C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-04989, para 68. HR 09-09-2011, LJN: BQ8097, NJ 2011, 595 m. nt. E.J. Dommering.

[32] Zie bijv. artikel 64 lid 1 Wet SUWI waarin drie breed geformuleerde doelen voor gegevensverwerkingen in samenwerkingsverbanden worden geformuleerd: 'de voorkoming en bestrijding van onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen op het terrein van de sociale zekerheid en de inkomensafhankelijke regelingen, de voorkoming en bestrijding van belasting- en premiefraude en het niet naleven van de arbeidswetten'.

recht, zoals datamininmalisatie, alleen in samenhang met de doelbinding kunnen worden toegepast. Het minimaliseren van de verwerkte gegevens kan alleen als er een welbepaald doel is in relatie waar tot de verwerkte gegevens kunnen worden afgestemd.[33]

Het concept WGS plaatst nog een kanttekening bij de mogelijkheden om van de doelbinding af te wijken. 'Daarmee is niet gezegd dat het wenselijk is dit principe voor samenwerkingsverbanden te allen tijde buiten toepassing te laten.'[34] Alleen als er een 'duidelijke noodzaak bestaat' kunnen gegevens worden verstrekt voor een ander doel dan waarvoor zij zijn verzameld, aldus de opstellers. Het toetsen van deze noodzaak zal dan gebeuren in de gegevensbeschermingseffectbeoordeling die plaatsvindt ter voorbereiding van de AMvB. De invulling van dit noodzakelijkheidsvereiste dient te gebeuren aan de hand van artikel 8 EVRM en de hierop gebaseerde rechtspraak, en in navolging hiervan artikel 7 Handvest en de rechtspraak van het HvJEU. Met het gevaar om in de herhaling te vallen, het dient om uitzonderlijke gevallen te gaan en dit verhoudt zich hierom niet met het karakter van de beoogde samenwerkingsverbanden waarin systematische uitwisseling van gegevens centraal staat.

De Raad van Europa publiceerde in 2017 richtlijnen ter bescherming van individuen bij big data-verwerkingen en stelde daarin dat persoonsgegevens *niet* verder mogen worden verwerkt in strijd met de doelbinding als de betrokkene dit onverwachts, ongepast of bezwaarlijk zou achten.[35]

### Voorgestelde aanpassing doelbinding in andere wetgeving

In het concept WGS zijn er wijzigingen van zes Nederlandse wetten voorgesteld die de aanpassing van doelbinding op sectoraal niveau beogen. Deze worden kort per geval hieronder besproken.

In artikel 9 wordt aan artikel 20 Wet politiegegevens (hierna 'Wpg') een lid 3 toegevoegd, wordt de mogelijkheid gecreëerd voor de verwerkingsverantwoordelijke die deelneemt aan een samenwerkingsverband als bedoeld in de WGS om aan dit verband politiegegevens te verstrekken. Een politiegegeven is elk persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt (artikel 1 sub a Wpg), inhoudende zowel politie als Koninklijke marechaussee. Op dit moment voorziet de Wpg al in de mogelijkheid om deze gegevens uit te wisselen met private partijen in het kader van samenwerkingsverbanden, echter, de doelclausulering is een stuk beperkter dan die wordt voorgesteld in het concept WGS. Daarnaast mag deze verstrekking aan derden nu alleen plaatsvinden 'indien het doel van de verstrekking overeenstemt of verenigbaar is met de politietaak'.[36] Artikel 3 lid 3 Wpg voorziet expliciet in het doelbindingsvereiste. De toevoeging van dit derde lid in de Wpg zou als gevolg hebben dat de doelbinding die volgt uit de eerste twee leden van artikel 20 Wpg buitenspel worden gezet, namelijk de doelclausulering wordt uitgebreid met de doelen in het concept WGS én de politiegegevens mogen voor onverenigbare doeleinden worden verwerkt.

Artikel 10 concept WGS voorziet in een soortgelijke wijziging van de Wet justitiële en strafvorderlijke gegevens (hierna 'Wjsg'). Artikel 3 lid 3 Wjsg verbiedt verwerkingen die onverenigbaar zijn met het doel

---

[33] Article 29 Data Protection Working Party, 'Opinion 03/2013 on purpose limitation'(Adopted on 2 April 2013 00569/13/EN WP 203, The Article 29 Working Party 2013) <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf >, 14-15.

[34] Concept WGS, blz. 12.

[35] Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, *Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data*, Straatsburg 23 januari 2017, blz. 4.

[36] *Kamerstukken II* 2005/06, 30 327, nr. 3, blz. 77.

waarvoor de gegevens zijn verkregen. Deze onverenigbaarheid wordt opgeheven door aansluiting bij de WGS.[37] Daarnaast lijkt het uit de Aanwijzing Wet justitiële en strafvorderlijke gegevens te volgen dat de bevoegdheden om gegevens te verstrekken zien op individuele gevallen, waarbij belangenafwegingen worden gemaakt tussen de ontvanger en de belangen van de betrokkene (blz. 3).

Ook worden er wijzigingen beoogd van een aantal wetten die zien op de financiële markten met het oogmerk om de gegevens die de toezichthouders op basis van deze wetten verkrijgen verder te verwerken in samenwerkingsverbanden. Het gaat om de Wet op het financieel toezicht, de Wet toezicht accountantorganisaties en de Wet toezicht trustkantoren 2018.

Ook wordt er een wijziging beoogd in de Wet ter voorkoming van witwassen en financieren van terrorisme. Ook deze wet stelt in artikel 34a expliciet de verenigbaarheidstoets in voor verdere verwerkingen en geeft bovendien aan dat verwerkingen niet mogen plaatsvinden voor commerciële doeleinden. De beoogde wijziging moet het mogelijk maken voor de toezichthoudende partijen om gegevens die zijn verstrekt of ontvangen of van een buitenlandse toezichthouder zijn ontvangen te verstrekken aan een samenwerkingsverband. Gezien de ernst van de materie waarop deze wet ziet rijst de vraag of een unilaterale wijziging van de Nederlandse wet die zo'n drastische verandering in het gebruik van gegevens die worden verkregen van buitenlandse toezichthouders op deze wijze mag worden doorgevoerd. Dit is sowieso in strijd met artikel 22 lid 2 sub c van deze wet. Deze bepaling vereist dat verstrekking zich verdraagt met de Nederlandse wet, hetgeen niet het geval is nu het de Grondwet niet respecteert (zie verder de sub-paragraaf 'Basis in de wet'). Daarnaast wordt in artikel 22 lid 2 sub d en f voorzien in de eis dat er voldoende moet zijn gewaarborgd dat de gegevens geheim worden gehouden en niet voor andere doelen worden gebruikt dan waarvoor deze zijn verstrekt. Deze geheimhouding beoogd het voorgestelde artikel 23b ongedaan te maken en de verwerking voor andere doeleinden volgt expliciet uit het concept WGS.

### Informatieplicht

Artikel 8 lid 3 sub b geeft impliciet invulling aan de informatieplicht door te stellen dat het 'register risicomeldingen' er is 'om subjecten van risicomeldingen op aanvraag te informeren of het register hun gegevens bevat', hetgeen betekent dat het feit dat ze zijn opgenomen in dit register niet standaard aan hen wordt gemeld. Daarbij lijkt de beoogde informatie die wordt verstrekt binair van aard te zijn, een 'ja' of een 'nee'. Ook mist er een bewaartermijn voor de risicomelding, in tegenstelling tot zijn evenknie die wordt gecreëerd in SyRI-samenwerkingsverbanden waarbij een termijn van twee jaar geldt. Artikel 8 lid 4 WGS bepaalt dat, indien het samenwerkingsverband systematisch gegevens verwerkt, zoals bedoeld in artikel 6 lid 3 WGS, het samenwerkingsverband voorziet in 'op een voor het publiek toegankelijke wijze informatie over:

a. de toepassing en het doel van deze verwerkingswijze;
b. nuttige informatie over de onderliggende logica [van geautomatiseerde besluitvorming, inclusief profilering];
c. de eventuele toepassing van artificiële intelligentie bij de verwerking, en
d. de in de aanhef bedoelde maatregelen [om de kwaliteit van de gegevensverwerking te waarborgen.'

[37] Voor nadere onderbouwing hiervan zie Concept WGS, blz. 13.

Het is niet duidelijk hoe deze informatie toegankelijk wordt gemaakt. Voorts geeft artikel 8 lid 4 WGS de ruimte om van deze informatieplicht af te wijken indien naar het oordeel van een deelnemer 'zwaarwegende redenen zich daartegen verzetten'. Er lijkt hiermee invulling te worden gegeven aan de uitzonderingen op de informatieplicht die zijn vastgelegd in artikel 14 lid 5 sub b en c AVG. Sub b van deze bepaling stelt, nochtans, als voorwaarde dat het vervullen van de informatieplicht de verwezenlijking van de doeleinden van die verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen. Deze bewoording duidt op een concreet gevaar en is een objectievere maatstaf dan het oordeel van een deelnemer over de aanwezigheid van zwaarwegende redenen. De voorwaarden in de WGS wijken dus af, ten nadele van de rechtsbescherming van betrokkene, van de voorwaarden vastgelegd in de AVG. Deze hebben directe werking en hiervan mag niet worden afgeweken.

Bovendien, stelt sub b hierbij als eis dat de verwerkingsverantwoordelijke in dit geval passende maatregelen neemt om de rechten, vrijheden en belangen van de betrokkene te beschermen, 'waaronder het openbaar maken van informatie'.[38] In sub c is voorzien in een uitzondering in het geval dit uitdrukkelijk is voorgeschreven in het lidstatelijk recht en 'dat recht voorziet in passende maatregelen zijn genomen om de gerechtvaardigde belangen van de betrokkene te beschermen'. Dit lidstatelijk recht moet in de Nederlandse rechtsorde een formeel-wettelijke grondslag hebben en de passende maatregelen dienen daarom in de WGS te worden geconcretiseerd. Zelfs indien verder onderzoek zou uitwijzen dat de Grondwet niet van toepassing is, kan worden betoogd dat het onvoldoende is om deze waarborgen op te nemen in de AMvB. De uitzondering wordt opgenomen in de WGS en de passende maatregelen om de belangen van de betrokkene te beschermen zouden daarom ook op dit niveau moeten worden vastgesteld.

### Passende maatregelen ter bescherming van fundamentele rechten en vrijheden van betrokkene

In artikel 9 lid 2 sub g AVG is een uitzondering vastgelegd op het verbod om bijzondere persoonsgegevens te verwerken indien dit gebeurt op basis van lidstatelijk recht. Hieraan worden een aantal voorwaarden gesteld waaronder een evenredigheidstoets. Daarnaast moeten er passende en specifieke maatregelen worden getroffen ter bescherming van de grondrechten en de fundamentele belangen van de betrokkenen. De mogelijkheid dat bijzondere categorieën van persoonsgegevens in het samenwerkingsverband worden verwerkt wordt ten onrechte niet omschreven in de voorgestelde wettekst, terwijl uit de toelichting blijkt dat deze wel bestaat. Deze mogelijkheid zou niet mogen bestaan zonder dat er expliciet deze verplichting voor het treffen van passende en specifieke maatregelen worden genoemd en aangezien in de MvT al wordt toegelicht hoe de resultaten zullen worden gebruikt, kunnen ook al in de kaderwet specifieke en passende maatregelen worden geconcretiseerd.

Uit artikel 6 lid 3 WGS blijkt dat samenwerkingsverbanden kunnen profileren en uit de MvT blijkt impliciet dat dit ook kan leiden tot automatische besluitvorming. Er zijn al voorbeelden uit de praktijk bekend waarbij koppeling v an bestanden werd gevolgd door automatische besluitvorming. Zelfs als de besluitvorming die volgt op de profilering niet automatisch is, maar semi-automatische en daarbij sterk

[38] Het is alleen niet duidelijk op welke informatie wordt gedoeld in deze zin.

leunt op de resultaten uit het samenwerkingsverband, kan dit in feite neerkomen op automatische besluitvorming. In artikel 22 lid 2 sub b AVG is een uitzondering gemaakt op het verbod op automatische besluitvorming indien dit gebeurt op basis van een lidstaatrechtelijke bepaling die van toepassing is op de verwerkingsverantwoordelijke. Ditzelfde lid bepaalt dat in deze bepaling in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de betrokkene moet zijn voorzien. Er wordt in het concept WGS toegegeven dat de uitwisseling van informatie aan de basis ligt van vervolgacties en interventies, maar deze worden verder niet besproken in de WGS.[39] Aangezien de data-analyses die worden uitgevoerd op basis van de WGS voorzien in de resultaten die leiden tot beslissingen of besluiten, zouden passende maatregelen al in de WGS moeten worden opgenomen.

Het enige dat de burger hiervoor terugkrijgt aan rechtsbescherming tegen de slagkracht van de overheid is dat deze samenwerkingsverbanden zullen worden vastgelegd in AMvB's. Hierbij zal dan wel een PIA moeten worden uitgevoerd, maar daar gaat op zichzelf geen rechtsbescherming vanuit.

Naast een zeer brede doelclausulering worden de samenwerkingsverbanden voor het overige slechts beperkt door de voorschriften in de AMvB waarin:

- de deelnemers worden aangewezen (artikel 3);
- de gezamenlijke verwerkingsverantwoordelijkheid, werkwijze en rolverdeling wordt vastgelegd (artikel 4);
- de gegevenscategorieën die aan het samenwerkingsverband mogen worden verstrekt (artikel 5);
- regels omtrent de wijze waarop het samenwerkingsverband gegevens kan verwerken en of hier ook systematisch verwerken (waaronder combineren, structureren, profileren en analyseren) onder valt (artikel 6);
- verdere verstrekkingen van resultaten ook buiten het doel van het samenwerkingsverband (artikel 7);
- Voorwaarden en beperkingen aan alle verwerkingen binnen het samenwerkingsverband, waaronder waarborgen voor private partijen, maatregelen om de kwaliteit van de gegevensverwerking te waarborgen bij systematische verwerkingen, om informatie te verschaffen aan het publiek omtrent o.a. toepassing, doel en onderliggende logica van de verwerking (artikel 8 lid 1, 2, 3 en 4);
- Technische en organisatorische maatregelen inzake onderlinge toegang en afscherming om niet noodzakelijke verstrekking te voorkomen (artikel 8 lid 5).

Onder deze waarborgen wordt er maar weinig nader ingevuld en wat wordt ingevuld biedt weinig houvast voor de rechtsbescherming. Sterker nog, het lijkt meer ruimte te bieden om de rechtspositie van de betrokkene verder te ondermijnen. Het valt verder op dat het concept WGS niet voorziet in regels omtrent de algoritmes en ook niet omtrent de data (doelbinding, minimale gegevensverwerking, juistheid). Voorafgaand aan een AMvB zal een PIA moeten worden uitgevoerd, maar daar gaat op zichzelf geen rechtsbescherming vanuit.

## Andere mensenrechten en neveneffecten

[39] Concept WGS, blz. 13-14.

Er kunnen een belangrijke kanttekening worden geplaatst bij deze relativering van de bevoegdheid die de WGS in het leven roept. Zo wordt er, onder andere, aangegeven dat de WGS het mogelijk moet maken om middels de uitwisseling van gegevens lijsten van personen op te stellen voor 'operationele doeleinden' en kunnen zowel publieke als private partijen 'op basis van uitgewisselde informatie actie ondernemen of een interventie plegen die bijdraagt aan het voorkomen en bestrijden van criminaliteit'.[40] Kortom, er wordt toegegeven dat de uitwisseling van informatie aan de basis ligt van vervolgacties en interventies, maar deze worden buiten de reikwijdte van de WGS gehouden. Wat deze vervolgacties en interventies kunnen zijn en de voorwaarden die aan ze worden gesteld blijven derhalve volledig onder de regie van de individuele partijen die deelnemen aan het samenwerkingsverband. De vervolgacties en interventies kunnen onder andere in strijd komen met het gelijkheidsbeginsel en het recht op een eerlijk proces.

Het concept WGS spreekt haar eigen geringschatting van de te creëren bevoegdheid ook tegen wanneer het stelt dat 'gegevensverwerking altijd een centrale plaats heeft gehad bij de interne werkprocessen van veel overheidsinstanties en in de verhouding overheid-burger', alsmede dat gegevensverwerking 'een belangrijk onderdeel van en dienstbaar [is] aan de opgedragen taak van praktisch elke overheidsinstantie'.[41] Dit bagatelliseren staat in schril contrast tot wat het concept WGS mogelijk maakt, te weten de volledige ontschotting van de informatiemacht van overheid en bedrijfsleven middels een AMvB. De woorden van de MvT van de WBP waren destijds een stuk zorgvuldiger gekozen:

> 'Gegevens zijn een bron van informatie; informatie is de basis van kennis en kennis is macht. Deze macht kan ten goede, maar ook ten kwade worden aangewend.'[42]

In het concept WGS wordt wel degelijk voorzien in de mogelijkheid van gebruik van de uitkomsten middels registers van risicomeldingen, hetgeen neerkomt op zwarte lijsten. De ABRvS heeft bepaald dat het criterium om op een zwarte lijst te worden geplaatst voldoende duidelijk moest zijn omschreven, in dat specifieke geval in een convenant, omdat anders het risico op willekeur bestond.[43] Dit leverde strijd op met het beginsel van behoorlijke en zorgvuldige verwerking, dat nog steeds van kracht is onder de AVG (artikel 5 lid 1 sub a AVG). Bovendien geeft artikel 8 lid 3 sub b, zoals al behandeld onder de subparagraaf 'Informatieplicht', impliciet invulling aan de informatieplicht door te stellen dat deze er is 'om subjecten van risicomeldingen op aanvraag te informeren of het register hun gegevens bevat', hetgeen betekent dat het feit dat ze zijn opgenomen in dit register niet standaard aan hen wordt gemeld. Daarbij lijkt de beoogde informatie die wordt verstrekt binair van aard te zijn, een 'ja' of een 'nee'. Ook mist er een bewaartermijn voor de risicomelding, in tegenstelling tot zijn evenknie die is gecreëerd in SyRI-samenwerkingsverbanden waar de 'Wet structuur uitvoeringsorganisatie werk en inkomen' een bewaartermijn van twee jaar stelt.[44]

Ook is het maar zeer de vraag of de voorziene analyses en daaruit voortkomende profielen in de praktijk niet nauw of zelfs volledig zullen zijn verbonden met besluitvorming binnen de aangesloten organisaties. De bovengenoemde vervolgacties en interventies kunnen bestaan uit van alles en nog wat. De bevoegdheden van bestuursorganen en de beslissingsmacht van private partijen vormen in de regel

---

[40] Concept WGS, blz. 13-14.
[41] Ibid, blz. 7.
[42] Kamerstukken II 2008-2009, 29911, nr. 23, blz. 7.
[43] ABRvS 04-07-2007, ECLI:NL:RVS:2007:BA8742, § 2.4.5.
[44] Artikel 65 lid 5 Wet SUWI.

geen gevaar voor burgers die niks hebben gedaan, maar het is door de potentiële samensmelting van informatiemacht dat deze bevoegdheden tegen iemand kunnen worden uitgeoefend. Zeker in relatie tot publieke organisaties die in de vrijheid van de burger kunnen ingrijpen is dit een groot risico. Dat deze organisaties door deze datakoppelingen lijsten van burgers kunnen krijgen met een verhoogd risico wordt in de MvT toegegeven, echter, er wordt gesteld dat dit 'nog geen formele verdenking oplevert'. De zin hierna wordt dit gerelativeerd:

> 'Zeker als zo'n lijst met behulp van Big Data technologie louter correlatieve en geen causale verbanden laat zien, kan van een formele verdenking (nog) geen sprake zijn. Daarvoor dienen concrete feiten en omstandigheden met betrekking tot de desbetreffende persoon op tafel te komen die op fraude wijzen.'

De eerste zin impliceert dat bij gegevens die causale verbanden laten zien wél van een formele verdenking sprake kan zijn. Het is begrijpelijk dat de opstellers dit buiten de reikwijdte van hun voorstel houden, omdat men op deze manier onder de verantwoordelijkheid van het gebruik van de uitkomsten tracht uit te komen. De tweede zin die erop wijst dat er concrete feiten en omstandigheden boven tafel moeten komen probeert wederom een afstand te creëren tot het gebruik van de uitkomsten, terwijl aan deze uitkomsten data ten grondslag liggen die een 'proxy' vormen voor feiten en omstandigheden.[45] Met andere woorden, het is niet duidelijk waarom de gegevensuitwisseling binnen de samenwerkingsverbanden niet zouden kunnen leiden tot een formele verdenking. Het is niet duidelijk hoe een formele verdenking verschilt van een op data-analyse gebaseerde onderbouwing van een risico dat een bepaalde persoon een bepaald misdrijf heeft begaan. Hierbij dient in het oog te worden gehouden dat dit verdenkingen kan betreffen voor meer delicten dan alleen fraude. Het kan alles betreffen dat door het samenwerkingsverband het gewicht wordt toegekend van een 'zwaarwegend algemeen belang'. Daarnaast is het idee van een samenwerkingsverband dat dergelijke informatie wordt uitgewisseld met andere deelnemers, hoewel er mogelijkheden zijn voor de deelnemende partijen om de uitwisseling van gegevens te beperken. Het staat, nota bene, in artikel 2 sub d concept WGS dat de data kan worden gebruikt voor het 'vervolgen van strafbare feiten of de tenuitvoerlegging van straffen'. De ondoorzichtigheid van deze processen, alsmede de geheime algoritmes op basis waarvan uitkomsten tot stand komen, kunnen tot ongelijkwaardige procesposities leiden en raken daarom aan het recht op een eerlijk proces, specifieker 'equality of arms'. De ABRvS bepaalde in 2017 dat een systeem dat werd gebruikt om stikstofneerslag te meten dit deed op een wijze die 'niet inzichtelijk en controleerbaar is vanwege een gebrek aan inzicht in de gemaakte keuzes en de gebruikte gegevens en aannames', waardoor er bij het aanwenden van rechtsmiddelen tegen op het systeem gebaseerde besluiten 'een ongelijkwaardige procespositie van partijen [kan] ontstaan'.[46]

Daarnaast komt de onschuldpresumptie in het geding bij de massale gegevensverwerkingen waarin de gegevens, en dus ook de levens waar deze betrekking op hebben, van onschuldige burgers worden doorgespit. Er wordt aangegeven dat 'Voor opsporingsdiensten en OM kan dat betekenen dat men op basis van de verkregen informatie een voorbereidend onderzoek start.'[47] De vorderingsplicht die ingaat in de fase van verdenking wordt nauwkeurig buiten de scope gehouden. Nu het concept WGS nadrukkelijk stelt dat gegevens uit samenwerkingsverbanden aan OM en opsporingsdiensten mogen

---

[45] Zie ook Edward Snowden zijn uitspraak: 'Metadata is a proxy for content.'
[46] ABRvS 17-04-2017, ECLI:NL:RVS:2017:1259, § 14.3
[47] Concept WGS, blz. 16.

worden verstrekt 'in een fase waarin (nog) geen verdenking bestaat' is de vraag of hier niet ten onrechte aan de waarborgen uit het Wetboek van Strafvordering voorbij wordt gegaan.

## Mogelijke neveneffecten en contraproductieve effecten

Het concept WGS en het overboord zetten van de doelbinding betekent dat de informatiemacht die aanwezig is bij de overheid en bedrijfsleven kunnen fuseren. Nagenoeg alle gegevens die mensen over zichzelf opgeven kunnen nu in een onoverzichtelijk complex van contexten tegen hen worden gebruikt. Met andere woorden, de uiteindelijke WGS kan wel eens aan de basis liggen van een (verergerd) klimaat van wantrouwen dat een chilling effect kan hebben op de veel gepropageerde participatiesamenleving. Een overheid die zich vijandig opstelt richting haar burgers creëert een burgerij die zich terugtrekt in haar schulp, niet één die actief deelneemt aan de maatschappij, hetgeen de overheid juist in toenemende mate van haar burgers verlangt.

De grote hoeveelheid mogelijkheden om justitiële en strafvorderlijke gegevens verder te verwerken kan tot gevolg hebben dat mensen die hun straf al hebben uitgezeten, alsnog verder worden gestraft. Profielen kunnen discrimineren en de acties die hieruit voortvloeien, zoals een huisbezoek, kunnen stigmatiseren.

False positives kunnen problemen opleveren, zeker wanneer het moeilijk is te begrijpen hoe tot de positive is gekomen. De groteske vormen die dit aan kan nemen werden onlangs in de VS duidelijk waarin duizenden mensen hun uitkering verloren en waarin 93% van de gevallen bleek dat het om een vergissing ging.[48] In het boek *Kafka was een ZZP-er* wordt duidelijk dat we dezelfde problematiek ook dichter bij huis aantreffen.

Nu de WGS ook resultaten kan genereren die relevant zijn voor opsporingsdiensten is nog een waarschuwing op zijn plaats. Iedereen kent bijna wel het verhaal van Kowsoleea, de man wiens naam voor een jaar of acht was gebruikt door een criminele klasgenoot (?) die op een gegeven moment de gevangenis in ging en hierna was de heer Kowsoleea, die nog nooit in de gevangenis had gezeten, opeens het mikpunt van politieacties. Na onterecht van zijn bed te zijn gelicht probeerde hij recht te halen door zijn registratie in de politieregisters door te halen. Dit is, voor zover bekend, tot op heden nooit gelukt. Zelfs niet na ingrijpen van de ombudsman. Dit is een zaak die begon rond 2002.

De vraag is of je als bedrijf verplicht bent om mee te werken aan een samenwerkingsverband. Er is niets in het concept dat hierop wijst, maar in Artikel 3 wordt wel aangegeven dat de deelnemers bij AMvB worden aangewezen en het is niet duidelijk hoe deze aanwijzing zich verhoudt tot de wensen van private partijen.

## Conclusie

Dit wetsvoorstel leest eerder als een cross-over tussen Orwell en Kafka, dan als een document dat je zou verwachten van een overheid die optreedt als hoeder van de rechtstaat. Het concept WGS is een frontale aanval op de rechtstaat. Het is zeker waar dat het voortbouwt op een hele hoop kleine wijzigingen in een breed scala van wetten die inmiddels al zijn doorgevoerd, maar het is desalniettemin een radicale breuk met de oorspronkelijke benadering in het privacy- en gegevensbeschermingsrecht.

---

[48] https://www.theguardian.com/us-news/2016/dec/18/michigan-unemployment-agency-fraud-accusations

Met het terzijde stellen van de doelbinding valt de rechtsbescherming die de burger geniet in de tegen de informatiemacht van een in potentie alwetende overheid als een kaartenhuis in elkaar. Het vertrekpunt van het gegevensbeschermingsrecht is transparantie en een transparante relatie tussen de betrokkene (de burger) en de verwerkingsverantwoordelijke. Deze transparantie maakt het mogelijk om de macht te controleren. Het concept WGS met zijn samenwerkingsverbanden waarin geheime algoritmes en eventueel kunstmatige intelligentie een samenstel van categorieën van gegevens doorneust en hier informatieproducten uit vervaardigt die zijn verbonden aan ongeïnformeerde mensenlevens maakt een karikatuur van het gegevensbeschermingsrecht.

Uiteraard zijn wij bereid om bovenstaand standpunt nader toe te lichten en kunt u middels ons e-mail adres [redacted] :act met ons opnemen.

Met vriendelijke groet namens het Platform Bescherming Burgerrechten,

Platform Bescherming Burgerrechten