Afdeling Nederland
Keizersgracht 177
Postbus 1968
1000 BZ Amsterdam

T
F
E
I www.amnesty.nl

Aan
de Minister van Justitie en Veiligheid

Datum
14 september 2018

Onderwerp
Inbreng Amnesty International consultatie conceptvoorstel WGS

Ons kenmerk Uw kenmerk

Geachte heer Grapperhaus,

Amnesty International Nederland maakt graag gebruik van de consultatie met betrekking tot het conceptwetsvoorstel voor de Wet gegevensverwerking door samenwerkingsverbanden (WGS).

Het conceptwetsvoorstel beoogt in de wet te verankeren dat samenwerkingsverbanden gezamenlijk gegevens mogen verwerken en aan welke voorwaarden die verwerking moet voldoen. Deze nieuwe bevoegdheid zal vooral zien op gemeenschappelijke casusanalyses en data-analyses door de samenwerkende partijen. Dit kan resulteren in zogenoemde risicoprofielen: de identificatie van personen, organisaties of bedrijven die zich mogelijkerwijs schuldig zullen gaan maken aan fraude, aantasting van de veiligheid of strafbare feiten.

In de memorie van toelichting wordt weliswaar kort gereflecteerd op de mogelijke effecten van de nieuwe bevoegdheid op het recht op eerbiediging van de persoonlijke levenssfeer, en in het bijzonder het recht op bescherming van persoonsgegevens. Een grondige mensenrechtenanalyse van zowel deze als andere mensenrechten ontbreekt echter.

In dit document treft u Amnesty's inbreng aan in het kader van de consultatie op het voorliggende voorstel.

Hierbij gaan we op het volgende in:

- De conceptwet is onvoldoende voorzienbaar
- De 'dringende maatschappelijke behoefte' is onvoldoende onderbouwd
- Sterkere waarborgen voor het recht op non-discriminatie zijn nodig
- Procedurele rechten staan onder druk
- Toezicht moet sterker geregeld worden

Uiteraard lichten we onze bijdrage graag aan u toe.

Met vriendelijke groet,

Amnesty International IVL

Inbreng in het kader van de consultatie conceptvoorstel Wet gegevensverwerking door samenwerkingsverbanden

Amnesty International Nederland, 14 september 2018

Het conceptwetsvoorstel voor de Wet gegevensverwerking door samenwerkingsverbanden (WGS) beoogt in de wet te verankeren dat samenwerkingsverbanden gezamenlijk gegevens mogen verwerken en aan welke voorwaarden die verwerking moet voldoen. Daarbij worden gegevens van verschillende van in elk geval bestuursorganen maar ook private partijen samengebracht en verwerkt. De gegevensverwerking zal vooral gericht zijn op gemeenschappelijke casusanalyses en data-analyses door de samenwerkende partijen. Dit kan resulteren in zogenoemde risicoprofielen: de identificatie van personen, organisaties of bedrijven die zich mogelijkerwijs schuldig zullen gaan maken aan fraude, aantasting van de veiligheid of strafbare feiten. Daarmee past het wetsvoorstel in een bredere en verontrustende trend waarin de overheid steeds meer 'pre-crime'-initiatieven neemt om toekomstige risico's en gevaren uit te sluiten of te verkleinen. Personen die nog geen strafbare handelingen hebben gepleegd of voorbereid, maar op basis van dergelijke analyses tot 'risicovol' zijn bestempeld, kunnen onderwerp worden van vergrote overheidscontrole en bestuursbesluiten die soms gepaard gaan met indringende beperkingen van hun mensenrechten. Dergelijke initiatieven kunnen haaks staan op het onschuldbeginsel. Ook kunnen ze gepaard gaan met minder en zwakkere waarborgen dan onder het strafrecht gebruikelijk zijn. Het conceptwetsvoorstel biedt daarom indirect ook een kader voor bestuursbesluiten met indringende gevolgen voor de mensenrechten.

In het conceptwetsvoorstel wordt nauwelijks stilgestaan bij het effect van de nieuwe bevoegdheid op verschillende mensenrechten. Er wordt weliswaar kort gereflecteerd op de mogelijke effecten op het recht op eerbiediging van de persoonlijke levenssfeer, en in het bijzonder het recht op bescherming van persoonsgegevens. Maar een grondige analyse hiervan, ook in relatie tot relevante Europese en nationale jurisprudentie, ontbreekt. Ook een analyse van andere mensenrechten die in het geding kunnen zijn bij de beoogde gegevensverwerking ontbreekt, zoals het recht om niet gediscrimineerd te worden en de zogenoemde procedurele rechten: het recht op een effectief rechtsmiddel en het recht op een eerlijk proces. Mede gezien de technologische ontwikkelingen op het gebied van big data-analyses[1] en de huidige internationale en nationale discussies over de gevolgen van die ontwikkelingen voor mensenrechten had een uitgebreidere toelichting van de effecten van de WGS verwacht mogen worden.

De conceptwet had bescherming van mensenrechten bij (geautomatiseerde) gegevensverwerking, profilering en (geautomatiseerde) besluitvorming uniform kunnen regelen. Dat gebeurt niet. De beschrijving en uitwerking van het mensenrechtenkader en de mate waarin de concept-wet voldoet aan de daaruit voortvloeiende mensenrechtelijke eisen is uiterst summier, vooral in het licht van de huidige technologische ontwikkelingen en discussies.

Hieronder komen de volgende mensenrechtenzorgen aan de orde:

[1] Er is geen uniforme definitie van 'big data'. Gerards e.a. schrijven dat big data vaak beschreven wordt aan de hand van kenmerken van de gebruikte data en de daarop toegepaste analysemethodes. Deze kenmerken zijn de hoeveelheid data, de verscheidenheid aan data en de snelheid van verzameling en analyse. Zie *Grondrechten en algoritmes*, J. Gerards, R. Nehmelman en M. Vetzo, Universiteit Utrecht, maart 2018, p. 5.

1. De conceptwet is onvoldoende voorzienbaar

De conceptwet maakt direct inbreuk op het recht op bescherming van de persoonlijke levenssfeer. In het verlengde daarvan zijn er risco's voor in elk geval het recht op non-discriminatie, het recht op toegang tot een effectief rechtsmiddel dan wel de rechter en het recht op een eerlijke proces.

Het recht op bescherming van de persoonlijke levenssfeer is geregeld in artikel 10 lid 1 van de Grondwet. Lid 2 en 3 geven vervolgens een specifieke instructie aan de wetgever om de omgang met persoonsgegevens te regelen en daarmee de persoonlijke levenssfeer te beschermen. In artikel 13 van de Grondwet zijn het brief-, telefoon- en telegraafgeheim vastgelegd. In artikel 8 van het Europees Verdrag van de Rechten van de Mens (EVRM) is het recht op respect voor privé- en familieleven, de woning en correspondentie vastgelegd. Dit is ook te vinden in artikel 7 van het Handvest van de Grondrechten van de Europese Unie (Handvest).[2] Artikel 8 van het Handvest voorziet in het recht op bescherming van persoonsgegevens. Het recht op privacy wordt vaak gebruikt als een verzamelnaam voor de domeinen privé- en familieleven, de woning en communicatie.

Artikel 8 lid 2 van de EVRM bepaalt dat een beperking van het recht op privacy bij wet moet zijn voorzien en noodzakelijk moet zijn in een democratische samenleving. Daarbij moet sprake zijn van een legitiem doel, een dringende maatschappelijke behoefte (*pressing social need*), voldaan worden aan de eisen van proportionaliteit en subsidiariteit en er moeten effectieve waarborgen zijn tegen misbruik en willekeur.

Uit de EVRM, het EU Handvest en jurisprudentie blijkt dat een inbreuk op privacy, en op andere mensenrechten, slechts gerechtvaardigd is indien die is voorzien van een voldoende duidelijke en precieze wettelijke basis. De wet moet toegankelijk en 'voorzienbaar' zijn. Dat wil zeggen dat in de wet voldoende duidelijk en nauwkeurig moet zijn aangegeven onder welke omstandigheden en voorwaarden autoriteiten via een maatregel inbreuk mogen maken op de persoonlijke levenssfeer. Daardoor kan de burger weten in welke situaties of bij welke vormen van gedrag hij of zij te maken kan krijgen met de toepassing van de maatregel.[3] Bovendien moet de wet voldoende waarborgen tegen misbruik en willekeur bevatten. Volgens Amnesty International is hier in het conceptwetsvoorstel niet aan voldaan.

- *Heimelijke gegevensverwerking vraagt om sterkere waarborgen*

In sommige gevallen kan volgens de conceptwet de gegevensverwerking in een samenwerkingsverband geheel aan het zicht van de betrokken individuen onttrokken zijn. Vooral in de context van strafvordering, waarin vertrouwelijke of geclassificeerde informatie verwerkt kan worden, zullen er al snel grenzen worden gesteld aan de openbaarheid van gegevensverwerking. Dit roept de vraag op of de minimumvereisten voor heimelijke surveillance niet ook van toepassing zouden moeten zijn op (delen van) de WGS. Voor gevallen waarin sprake is van heimelijke surveillance heeft het Europees Hof voor de Rechten van de Mens (EHRM) minimumvereisten geformuleerd om misbruik van bevoegdheden te voorkomen. Immers, zo redeneert het EHRM, juist wanneer een bevoegdheid die bij de uitvoerende macht rust heimelijk kan worden ingezet, zijn de risico's evident.[4] Zo moet uit de wet blijken welke activiteiten of overtredingen aanleiding kunnen zijn voor de surveillance, welke categorieën mensen kunnen worden getroffen, wat de maximale duur is van de surveillancebevoegdheid, welke procedure gevolgd moet worden om de verkregen gegevens te mogen onderzoeken, gebruiken en opslaan en welke voorzorgsmaatregelen moeten worden getroffen wanneer de gegevens aan derde partijen verschaft worden. Ook moeten de omstandigheden waaronder de gegevens moeten worden gewist of vernietigd erin staan.[5] Het conceptwetsvoorstel voldoet hier niet aan: het is erg breed en vaag geformuleerd, geeft weinig handvatten voor de inrichting van een rechtmatige gegevensverwerking in een concrete situatie, en kent nauwelijks voorzorgsmaatregelen om de rechten van betrokkenen te beschermen.

---

[2] Artikel 52 lid 3 van het Handvest bepaalt dat rechten uit het Handvest die overeenkomen met rechten uit de EVRM gelijk zijn qua inhoud en reikwijdte.

[3] EHRM 2 augustus 1984, *Malone/Verenigd Koninkrijk*, nr. 8691/79, r.o. 67; EHRM 24 april 1990, nr. 11801/85, *Kruslin/Frankrijk*, r.o. 30; *Zakharov/Rusland*, r.o. 229; EHRM 12 januari 2016, nr. 37138/14, *Szabó en Vissy/Hongarije*, r.o. 59.

[4] Weber en Saravia/Duitsland, r.o. 93; Zakharov/Rusland, r.o. 229; Szabó en Vissy/Hongarije, r.o. 62.

[5] Weber en Saravia/Duitsland, r.o. 95; Zakharov/Rusland, r.o. 231; Szabó en Vissy/Hongarije, r.o. 56.

- *De doelomschrijving 'van zwaarwegend algemeen belang' is te ruim en vaag*

De vier brede doelcriteria ten aanzien waarvan een samenwerkingsverband opgericht kan worden uit artikel 2 van de WGS omvatten een zeer breed spectrum aan regelingen en beleidsterreinen van de overheid: van fraudebestrijding tot handhaving van de openbare orde en van toezicht tot opsporing en vervolging van strafbare feiten. Het lijkt moeilijk om een doel voor een samenwerkingsverband te formuleren dat hier niet binnen valt. Noch de conceptwet, noch de toelichting geven voorbeelden van de type situaties en vormen van gedrag waardoor individuen onderwerp zouden kunnen zijn van zo'n gegevensverwerking door samenwerkingsverbanden. Wel schrijft de conceptwet voor dat dit doel van 'zwaarwegend algemeen belang' moet zijn. Uit eerdere uitlatingen van de wetgever blijkt dat een gegevensverwerking 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'.[6] Maar hiermee biedt de conceptwet geenszins een voldoende precieze wettelijke grondslag, een vereiste die zowel uit Europese als Nederlandse jurisprudentie volgt.[7] De Afdeling Advies van de Raad van State heeft in het verleden ook gewezen op de onvoorzienbaarheid van een privacy-schendende maatregel als gevolg van een te ruime en vage doelomschrijving.[8]

- *Onbeperkte omvang van gegevensverwerking zonder sterke waarborgen*

Ook de aard en omvang van gegevensverwerking is weinig afgebakend in de conceptwet, terwijl dit van belang is voor een proportionaliteitsafweging in een concreet geval. Artikel 5 van de WGS bepaalt dat in de AMvB moet worden opgenomen welke categorieën van gegevens door de deelnemers aan een samenwerkingsverband verstrekt moeten worden aan dat samenwerkingsverband.[9] Er wordt niet toegelicht om wat voor gegevens het in de praktijk kan gaan. Op voorhand wordt geen enkele gegevenscategorie uitgesloten. Gezien de brede doelcriteria gaat het in potentie om een zeer grote variëteit aan gegevenscategorieën. Zelfs bijzondere categorieën van persoonsgegevens worden niet uitgesloten, zoals die waaruit bijvoorbeeld iemands ras of etnische afkomst, politieke opvattingen, religieuze overtuigingen of seksuele geaardheid blijken.[10] Conform de Algemene verordening gegevensbescherming (AVG) kan het verbod op de verwerking van dergelijke bijzondere persoonsgegevens weliswaar terzijde worden geschoven als de verwerking noodzakelijk is 'vanwege een zwaarwegend belang'. Maar daar waar de AVG voorschrijft dat dit alleen mag indien er passende maatregelen worden getroffen om de rechten van betrokkenen te beschermen,[11] licht de concept-WGS niet toe hoe deze uitzondering begrepen moeten worden en welke daarbij vereiste passende maatregelen getroffen moeten worden.

- *Doelbinding wordt doorbroken*

Ook mag het principe van doelbinding doorbroken worden. De toelichting op de conceptwet geeft aan dat doelbinding als knelpunt wordt ervaren door bestaande samenwerkingsverbanden. De wet beoogt daarom ruimte te bieden om hiervan af te wijken.[12] De AVG biedt onder strikte voorwaarden de mogelijkheid om van doelbinding af te wijken[13], maar het is opmerkelijk dat de conceptwet van de uitzondering de norm lijkt te maken. Het principe van doelbinding is immers een van de hoekstenen van het gegevensbeschermingsrecht: persoonsgegevens mogen alleen verwerkt worden voor het doel

---

[6] Kamerstukken II, 2005-2006, 30327, nr. 3, p. 74.

[7] Volgens de Hoge Raad moet daar wel sprake van zijn als door de (systematische) gegevensverwerking het privéleven van betrokkenen wordt geraakt. HR, 24 februari 2017, ECLI:NL:HR:2017:286, r.o. 2.3.4, HR, 24 februari 2017, ECLI:NL:HR:2017:287, r.o. 2.3.4, HR, 24 februari 2017, ECLI:NL:HR:2017:288, r.o. 2.3.4, CrvB, 15 augustus 2017, ECLI:NL:2017:2807, r.o. 4.7.

[8] Kamerstukken II, 2012-2013, 33579, nr. 4, p. 3.

[9] In het kader van het bestrijden van bijvoorbeeld sociale verzekeringsfraude, belasting- en premiefraude en misbruik van inkomensafhankelijke regelingen mogen samenwerkingsverbanden gezamenlijk gegevens verwerken op grond van artikel 64 Wet structuur uitvoeringsorganisatie werk en inkomen (Wet SUWI). In artikel 5a.1, onder 3 besluit SUWI is bepaald dat een of meer van de volgende gegevenscategorieën verwerkt mogen worden: arbeidsgegevens, gegevens inzake bestuursrechtelijke maatregelen en sancties, fiscale gegevens, gegevens roerende en onroerende goederen, gegevens over uitsluitingsgronden van bijstand of uitkeringen, handelsgegevens, huisvestingsgegevens, identificerende gegevens, inburgeringsgegevens, nalevingsgegevens, onderwijsgegevens, pensioengegevens, re-integratiegegevens, schuldenlastgegevens, uitkerings-, toeslagen- en subsidiegegevens, vergunningen en ontheffingen, zorgverzekeringsgegevens.

[10] Artikel 9, lid 1 AVG: Verwerking van persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid zijn verboden.

[11] Zie artikel 9, lid 2, onder g AVG en artikel 24 tot en met 30 UAVG (Uitvoeringswet bij de AVG).

[12] WGS Mvt, p. 12.

[13] Artikel 6, lid 1, onder c AVG.

waarvoor ze verworven zijn en niet voor andere doelen.[14] Dit beginsel biedt individuen de zekerheid dat de persoonsgegevens die ze delen met een instantie, bijvoorbeeld om belastingaangifte te doen of om een uitkering aan te vragen, niet zomaar verwerkt kunnen worden voor andere doelen. Door de doelbindingsvereiste los te laten biedt de WGS alle ruimte voor een of meerdere deelnemers aan een samenwerkingsverband om dit principe structureel te doorbreken. Dit is een risico waar ook de Werkgroep Verkenning Kaderwet op wees in zijn advies.[15]

Doelbinding wordt op nog een tweede manier losgelaten. Resultaten van de gezamenlijke gegevensverwerking mogen ook *verstrekt* worden aan deelnemende bestuursorganen voor nog eens andere doeleinden dan waarvoor ze verwerkt. Dat maakt het voorstel zo mogelijk nog minder voorzienbaar. Bovendien maakt het de weg vrij voor mogelijk oneigenlijk gebruik, en zelfs misbruik, als bestuursorganen gegevens verwerken op basis van hun wettelijke bevoegdheid en ze die gegevens vervolgens gebruiken voor andere, ver daarvan verwijderde doeleinden.

- *De informatieplicht wordt uitgehold*

De conceptwet neemt ook een andere belangrijke waarborg van het gegevensbeschermingsrecht grotendeels weg, namelijk de informatieplicht.[16] Een goed uitgevoerde informatieplicht kan bijdragen aan de voorzienbaarheid van de omstandigheden waaronder via een overheidsmaatregel inbreuk gemaakt mag worden op de persoonlijke levenssfeer en in het verlengde daarvan op andere rechten. Maar in de conceptwet is de informatieplicht de uitzondering op de regel geworden.

De conceptwet spreekt over een informatieplicht indien risicomeldingen verwerkt worden in een register. Op aanvraag worden individuen dan geïnformeerd. Indien gegevens systematisch verwerkt worden op grond van artikel 6, lid 3 van de WGS, waaronder door profilering, moet op een voor het publiek toegankelijke wijze informatie gegeven worden over de toepassing en het doel van de verwerkingswijze. Ook moet het publiek nuttige informatie krijgen over de onderliggende logica, de eventuele toepassing van kunstmatige intelligentie bij deze verwerking en de getroffen maatregelen om de kwaliteit van de verwerking te waarborgen. Dit is een belangrijke waarborg voor controle en verantwoording. Deze informatieverstrekking kan echter achterwege blijven als een deelnemende partij daar om zwaarwegende redenen bezwaar tegen heeft.[17] Dat zo'n partij bezwaar heeft, is niet ondenkbaar. Denk bijvoorbeeld aan bedrijven die hun bedrijfsbelangen willen beschermen.

In de conceptwet zijn enkele waarborgen opgenomen om de belangen van betrokkenen te beschermen,[18] voornamelijk in de vorm van eisen waaraan de AMvB's moeten voldoen. Maar de 'nadere voorwaarden en beperkingen' die volgens artikel 8, lid 1 van de WGS gesteld kunnen worden aan alle verwerkingen van gegevens, worden niet toegelicht. Aan de minimumvereisten die het EHRM stelt in geval van heimelijke surveillance wordt dan in ieder geval niet tegemoet gekomen. Juist deze (extra) waarborgen kunnen ook de rechten van betrokkenen wier gegevens heimelijk worden verwerkt door samenwerkingsverbanden sterker beschermen tegen het risico op willekeur en misbruik.

Per AMvB zal een betere beoordeling gemaakt kunnen worden van de voorzienbaarheid van de gevolgen voor individuen van dat specifieke samenwerkingsverband. Maar de WGS zelf moet ook voorzienbaar zijn. Daarvan is geen sprake. Een burger kan niet weten voor welk doel de gegevens die hij of zij heeft

---

[14] Artikel 5, lid 1, onder b AVG.
[15] Werkgroep verkenning kaderwet gegevensuitwisseling, 2014, p. 30.
[16] Zie artikel 13 en 14 AVG. Zo moeten de betrokkenen wier persoonsgegevens verwerkt worden geïnformeerd worden over de identiteit van de verwerkende partij, het doel van de gegevensverwerking, de rechtsgrond daarvoor en over welke categorieën persoonsgegevens gebruikt worden. En om een transparante en behoorlijke gegevensverwerking te waarborgen moet ook informatie gegeven worden over o.a. hoe lang de gegevens bewaard mogen worden, dat de betrokkene het recht heeft op inzage, rectificatie, gegevenswissing en 'beperking', dat hij of zij een klacht kan indienen bij de toezichthouder en van welke bronnen de gegevens afkomstig zijn. Indien er sprake is van geautomatiseerde besluitvorming moet de betrokkene ook daarover worden geïnformeerd, inclusief nuttige informatie over de onderliggende logica, het belang en de verwachten gevolgen voor de betrokkene. Als persoonsgegevens verwerkt gaan worden voor een ander doel dan waarvoor ze verkregen zijn, dan moet de betrokkene daar ook over geïnformeerd worden en wel voorafgaand aan die verdere verwerking.
[17] Artikel 8, lid 4 WGS.
[18] De AVG biedt de mogelijkheid om onder strikte voorwaarden de gegevensverstrekking in een samenwerkingsverband uit te zonderen van de informatieplicht, mits er sprake is van passende maatregelen om de belangen van betrokkenen te beschermen. Zie artikel 14, lid 5, onder c en artikel 23, lid 1 AVG.

gedeeld met een bestuursorgaan of private partij in de toekomst verwerkt gaan worden door een samenwerkingsverband dat opereert onder de WGS.

2. De 'dringende maatschappelijke behoefte' is onvoldoende onderbouwd

De noodzakelijkheidseis uit artikel 8 van de EVRM betekent niet alleen dat de concrete inzet van een maatregel of bevoegdheid noodzakelijk moet zijn, maar ook dat de introductie van de maatregel of bevoegdheid *an sich* noodzakelijk moet zijn in een democratische samenleving. Alleen al het bestaan van wetgeving op basis waarvan (persoons)gegevens kunnen worden verwerkt kan een inbreuk op het recht op privacy zijn.[19]

De conceptwet beoogt de wettelijke grondslag te creëren voor gezamenlijke gegevensverwerking door samenwerkingsverbanden op het terrein van vier brede doelcriteria. Dit zijn, samengevat, het tegengaan van fraude met overheidsgeld, handhaving van openbare orde en veiligheid, toezichthouden op naleving van wetten en het voorkomen, opsporen en vervolgen van strafbare feiten.

Uiteraard is het van belang dat maatschappelijke vraagstukken zoals grootschalige fraude, witwaspraktijken of ondermijnende criminaliteit effectief kunnen worden aangepakt. Maar in de toelichting op de conceptwet ontbreekt nu een overtuigende motivatie dat sprake is van een dringende maatschappelijke behoefte aan het creëren van een bevoegdheid voor gezamenlijke gegevensverwerking door allerlei verschillende soorten samenwerkingsverbanden. Weliswaar noemt het kabinet als reden dat publieke en private partijen in de praktijk knelpunten ervaren bij het uitwisselen en verwerken van gegevens wanneer zij met elkaar samenwerken. Onder meer de geheimhoudingsverplichtingen voor verschillende publieke en private actoren en de beperkingen in het huidige wettelijke kader om gegevens te mogen verwerken door samenwerkingsverbanden zitten hen daarbij in de weg.[20] Maar deze wettelijke grenzen zijn er niet voor niets: zij zijn waarborgen tegen onrechtmatige inbreuken op de eerbiediging van de persoonlijke levenssfeer en bescherming van persoonsgegevens, en in het verlengde daarvan tegen inbreuken op andere mensenrechten. Het omzeilen van dergelijke waarborgen door het creëren van een nieuwe wettelijke basis voor gegevensverwerking zal het werk van betrokken partijen ontegenzeggelijk gemakkelijker en efficiënter maken. Maar daarmee is nog geen dringende noodzaak voor het verruimen van het wettelijk kader aangetoond. Sterker nog: misbruik en willekeur ligt dan op de loer.

3. Sterkere waarborgen voor het recht op non-discriminatie nodig

Het gelijkheidsbeginsel en het verbod op discriminatie kunnen in het geding komen bij gezamenlijke gegevensverwerking door samenwerkingsverbanden en de daaruit voortvloeiende bestuursbesluiten en andere interventies. De Wetenschappelijke Raad voor het Regeringsbeleid schreef ook dat niet alleen het proces van gegevensverwerking, maar ook de uitkomsten daarvan - in de vorm van beslissingen over een individu - raken aan de rechten van burgers.[21] Het gelijkheidsbeginsel is verankerd in artikel 1 van de Grondwet en houdt in dat alle mensen gelijk behandeld moeten worden voor de wet. In het verlengde hiervan ligt het verbod op discriminatie. Deze gelijkheidsrechten zijn ook in internationale mensenrechtenstandaarden verankerd,[22] waaronder in verdragen over specifieke vormen van discriminatie.[23] Volgens internationale mensenrechtenstandaarden hebben overheden de plicht en bedrijven de verantwoordelijkheid om proactief discriminatie te voorkomen.[24] Zowel publieke als private actoren moeten risico's op discriminatie voorkomen en aanpakken in het ontwerp, de verdere ontwikkeling en het gebruik van algoritmes en andere analysemethodes.[25] Het is een tekortkoming dat

---

[19] EHRM (Grote Kamer) 4 december 2015, nr. 47143/06, *Zakharov/Rusland*, r.o. 168-171; EHRM 29 juni 2006, nr. 54934/00 *Weber en Saravia/Duitsland*, r.o. 78; HvJEU (Grote Kamer) 8 april 2014, gevoegde zaken C-293/12 en C-594/12, *Digital Rights Ireland*, r.o. 32.

[20] Conceptwetsvoorstel gegevensverwerking door samenwerkingsverbanden (WGS), internetconsultatieversie, Memorie van Toelichting, p. 5.

[21] *Big data in een vrije en veilige samenleving*, Wetenschappelijke Raad voor het Regeringsbeleid (WRR), Amsterdam University Press, Den Haag/Amsterdam, 2016, p. 121.

[22] Artikel 20 en 21 van het Handvest, artikel 14 van de EVRM, artikel 26 van het Internationaal Verdrag inzake burgerrechten en politieke rechten.

[23] Zie onder andere het Verdrag tot uitbanning van alle vormen van rassendiscriminatie (CERD) en het Verdrag tot uitbanning van alle vormen van discriminatie tegen vrouwen.

[24] Zie *The UN Guiding Principles on Business & Human Rights* (UNGPs) en ondersteunende documenten.

[25] Zie *The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems*.

de conceptwet niet ingaat op de gevolgen voor het recht op non-discriminatie en op de voorzorgsmaatregelen die samenwerkingsverbanden moeten nemen om dit recht te waarborgen.

In artikel 6 lid 3 van de conceptwet staat dat, mits bij AMvB bepaald, samenwerkingsverbanden gegevens systematisch mogen verwerken. Daaronder valt het combineren, structureren, profileren en analyseren van gegevens met als doel om daaruit 'noodzakelijke informatie af te leiden en vast te leggen'. Uit de toelichting blijkt dat daarmee het blootleggen van patronen of het opstellen van groepsprofielen wordt beoogd. Aan de hand daarvan kunnen lijsten worden opgesteld van personen, organisaties of bedrijven die met het oog op het doel van een samenwerkingsverband een verhoogd risico laten zien.[26] Denk bijvoorbeeld aan een lijst van personen met een verhoogd risico op het plegen van fraude.

Er ontstaat een probleem als via profilering ongerechtvaardigd onderscheid gemaakt wordt op grond van verboden persoons- of groepskenmerken (zoals godsdienst, ras, geslacht, nationaliteit of seksuele geaardheid). De gedachte is vaak dat technologie neutraal is en dat alleen mensen vooroordelen hebben. Maar zo eenvoudig is het niet. Zowel een algoritme als de gegevens waarop een algoritme wordt toegepast kunnen gekleurd zijn, een *bias* bevatten. *Biases* en verhuld gebruik van bepaalde kenmerken zijn belangrijke oorzaken voor ongerechtvaardigd onderscheid. Profielen kunnen worden opgesteld op basis van kenmerken als etniciteit, religie en seksuele gerichtheid. Dit kan zowel direct als via proxy's; indicatoren die neutraal lijken, maar die wel degelijk iets zeggen over bijvoorbeeld etniciteit of religie. Als de overheid of een bedrijf op basis van dit soort profielen besluiten neemt, kan iemand daardoor bijvoorbeeld worden uitgesloten van bepaalde sociale voorzieningen of verzekeringen. Hij of zij kan ook, zonder daar zelf weet van te hebben, ingedeeld worden in een bepaalde risicogroep, waardoor diens handelen onder een vergrootglas van de autoriteiten komt te liggen.

Denk bijvoorbeeld aan de persoonsgerichte aanpak van terrorisme, radicalisering en (gewelddadig) extremisme.[27] Onderzoek duidt erop dat daarbij kenbare, objectieve en eenduidige beoordelingscriteria ontbreken en er brede en door elkaar gebruikte begrippen als 'radicalisering' en 'extremisme' worden gehanteerd.[28] Daardoor bestaat het risico dat individuen op basis van hun religieuze uitingen gesignaleerd worden als 'risicovol', zonder dat daarvoor een objectieve en redelijke rechtvaardiging bestaat. Zij worden zodoende onevenredig onderwerp van casusoverleggen, data-analyses, en daaruit voortvloeiende overheidsinterventies die kunnen leiden tot mensenrechteninbreuken, ook al hebben ze geen strafbare feiten gepleegd of waren ze dat van plan.[29]

Voor samenwerkingsverbanden die geautomatiseerde profilering mogen toepassen zou het risico op discriminatie en de getroffen maatregelen om dat te voorkomen meegewogen moeten worden in de proportionaliteitstoets. Ook verdient het aanbeveling dat er een onafhankelijke kwaliteitstoets van de gehanteerde analysemethodes plaatsvindt. De toelichting op het conceptwetsvoorstel stelt dat afhankelijk van het samenwerkingsverband en het type data-analyse de te gebruiken algoritmes getest moeten worden.[30] Er wordt echter geen verdere uitleg gegeven over hoe dit georganiseerd en ingevuld moet worden. Gezien de aanzienlijke mensenrechtenrisico's mag een uitgebreidere toelichting verwacht worden. Hoe wordt voorkomen dat de algoritmes en andere analysemethodes onbedoeld discrimineren of andere negatieve rechtsgevolgen hebben?

Vanuit het oogpunt van verantwoording en transparantie is het belangrijk dat openbaar wordt gemaakt wanneer welke algoritmes en andere analysemethodes worden gebruikt. Daarbij moet duidelijk en

---

[26] WGS MvT, p. 13, 15.
[27] *Convenant persoonsgerichte aanpak voorkoming radicalisering en extremisme*, Staatscourant 2017, 413214, 20 juli 2017.
[28] Dit beeld komt naar voren uit een reeks van interviews die Amnesty International Nederland afnam in de periode december 2016 - juli 2017 met professionals die betrokken zijn bij de persoonsgerichte aanpak en een analyse van officiële beleidsdocumenten. Zie ook *De Nederlandse Jongerenwerker over de Wirwar van het Signaleren van Radicalisering versus Extremisme op Lokaal Niveau*, Q.A.M. Eijkman en A. de Weert, Kenniscentrum Sociale Innovatie, Utrecht: Hogeschool Utrecht, 2017.
[29] Uit onderzoek naar de Britse contra-extremisme 'Prevent' blijkt dat dit risico van discriminatoire signalering en doorverwijzing van moslims zeer reëel is bij dergelijke inschattingen van vaag en breed geformuleerde risico's als 'terrorisme', 'extremisme'. Zie: *Eroding Trust. The UK's PREVENT Counter-Extremism Strategy in Health and Education*, Open Society Justice Initiative (OSJI), Open Society Foundations, 2016; Zie ook *Preventing Education? Human Rights and UK Counterterrorism Policy in Schools*, Rights Watch (UK), juli 2016.
[30] WGS MvT, p. 18.

toegankelijk worden uitgelegd hoe de uitkomsten tot stand komen. Dit is deels geregeld in de concept-WGS,[31] maar wordt niet verder toegelicht. Ook moet worden vastgelegd welke acties worden ondernomen om discriminatie of een andere negatieve impact op mensenrechten te identificeren, documenteren en mitigeren. Regelmatige *impact assessments* en herstelmaatregelen voor onbedoelde discriminatoire *biases* in *tools* en data. Ook is het van belang dat een onafhankelijke beoordeling van en toezicht op de (uit)werking van algoritmes en andere analysemethodes mogelijk is.[32]

4. Procedurele rechten staan onder druk

Het recht op toegang tot een effectief rechtsmiddel en het recht op toegang tot de rechter kunnen in het huidige conceptwetsvoorstel onder druk komen te staan. Zoals hiervoor toegelicht creëert het conceptwetsvoorstel een grondslag voor geautomatiseerde profilering en kunnen zo risicoprofielen worden opgesteld. Analysemethodes die daarvoor gebruikt worden zijn over het algemeen zeer ondoorzichtig en ingewikkeld voor een leek.

Hierdoor zal het voor veel individuen onduidelijk zijn hoe een resultaat en een daaruit voortvloeiend besluit tot stand zijn gekomen. Soms zal het simpelweg niet zichtbaar zijn of er sprake is van een benadeling in een concrete situatie. Hierdoor is het lastig voor een betrokkene om actie te ondernemen tegen een besluit en daaruit voorkomende interventies en maatregelen die inbreuk maken op de mensenrechten, zoals het recht om niet gediscrimineerd te worden.

Amnesty International maakt zich zorgen dat het recht op een effectief rechtsmiddel en de toegang tot de rechter, zoals vastgelegd in artikel 13 en 6 van de EVRM, in het geding zijn als gevolg van het gebruik van ondoorgrondelijke, niet-kenbare data-analyses in samenwerkingsverbanden, zoals beoogd in de concept-WGS.

Het recht op een effectieve rechtsbescherming staat op nog een andere manier onder druk. De Afdeling Advies van de Raad van State publiceerde onlangs een ongevraagd advies over de effecten van digitalisering op de rechtstatelijke verhoudingen. Daarin beschrijft de Afdeling onder andere de problemen die zich kunnen voordoen bij het gebruik van ketens bij overheidsbesluiten. De controle, verantwoordelijkheid en verantwoording zijn bij ketenbeslissingen problematisch. Individuen hebben amper zicht op hoe informatienetwerken van de overheid lopen, welke persoonsgegevens zich in de verschillende netwerken bevinden en welke bestuursorganen daar gebruik van maken. De rechten die het gegevensbeschermingsrecht burgers toekent,[33] bieden in dat geval geen of weinig effectieve rechtsbescherming.[34]

Tenslotte bestaan er risico's voor het recht op een eerlijk proces. Wanneer een individu een besluit (publiek, dan wel privaat) wil aanvechten dat (deels) gebaseerd is op of voorbereid door algoritmes of andere niet-transparante analysemethodes, kan het recht op een open, eerlijke en evenwichtige procedure onder druk komen te staan. Er moet immers sprake zijn van een *equality of arms*, terwijl juist in deze situatie een ongelijke informatiepositie van de procespartijen zeer goed denkbaar is. Wanneer gebruik is gemaakt van zogenoemde zelflerende algoritmes is de toets hoe een besluit tot stand is gekomen nagenoeg onmogelijk. De Afdeling Bestuursrechtspraak van de Raad van State oordeelde in een zaak waarin besluitvorming gebaseerd was op big data-analyse dat door zo'n besluit een ongelijkwaardige procespositie van partijen kan ontstaan.

---

[31] Artikel 8, lid 4 WGS.

[32] Zie *The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems* voor een uitgebreidere beschrijving van *human rights due diligence*; Het *AI Now Institute* heeft een praktisch raamwerk ontwikkeld voor *algorithmic impact assessments*. In New York is eerder dit jaar een task force gestart die het stadsbestuur moet adviseren over te volgen procedures voor het beoordelen van algoritmes die door het lokale bestuur gebruikt worden. Dergelijke initiatieven kunnen bij de ontwikkeling van een onafhankelijke kwaliteitstoets behulpzaam zijn.

[33] Zie ook voetnoot 16.

[34] *Ongevraagd advies over de effecten van digitalisering voor de rechtstatelijke verhoudingen*, Raad van State, Staatscourant 2018, nr. 50999, §3.3.

5. Toezicht moet sterker geregeld worden

- *Sterker toezicht bij heimelijke gegevensverwerking*

Amnesty vraagt zich af in hoeverre bij de heimelijke verwerking van gegevens door samenwerkingsverbanden onder de WGS wordt voldaan aan de mensenrechtelijke eis van effectief en onafhankelijke toezicht. Individuen zijn bij zo'n heimelijke samenwerking niet op de hoogte van inperkingen van hun rechten en hebben in de praktijk dan ook geen mogelijkheid om de rechtmatigheid ervan te betwisten voor een rechter. Ook als resultaten van gegevensverwerkingen door samenwerkingsverbanden invloed hebben op de ontwikkeling van overheidsbeleid is het lastig om daar als samenleving zicht op de hebben en verantwoording voor af te dwingen.

In de context van heimelijke surveillance heeft het EHRM de voorwaarde gesteld dat sprake moet zijn van adequate en effectieve garanties tegen misbruik. Het garanderen van effectief en onafhankelijk toezicht is hiervoor een belangrijk middel. Op basis van artikel 13 van de EVRM dient het toezicht zich uit te strekken tot alle fases in de uitvoering van de bevoegdheid: voorafgaand aan de verzameling en verwerking van gegevens, tijdens en achteraf. In toenemende mate is er consensus onder Europese rechters dat rechterlijk toezicht de sterkste waarborg is.[35] Dit werpt de vraag op of een dergelijk uitgebreid toezichtstelsel ook niet vereist is voor de heimelijke gegevensverwerking in samenwerkingsverbanden.

- *Toezicht op private sector via human rights due diligence*

De private sector heeft de verantwoordelijkheid om mensenrechten te respecteren en de overheid heeft de plicht om mensenrechtenschendingen door bedrijven te voorkomen en aan te pakken. Dit volgt uit de richtlijnen voor bedrijven op het gebied van mensenrechten die in VN-verband zijn vastgelegd in de *UN Guiding Principles on Business and Human Rights* (UNGPs).[36] Als onderdeel van het nemen van deze verantwoordelijkheid moeten bedrijven doorlopend proactief en reactief stappen zetten om ervoor te zorgen dat zij geen schendingen van mensenrechten veroorzaken of daaraan bijdragen. Dit proces wordt *human rights due diligence* genoemd en bestaat uit het identificeren, voorkomen en aanpakken van mensenrechtenschendingen. Transparantie is hierbij de sleutel. Het proces om risico's te identificeren moet openbaar gemaakt worden. Net als de geïdentificeerde risico's en de concrete stappen die gezet zijn om deze te voorkomen of te beperken.[37]

Amnesty is van mening dat private partijen waarmee gezamenlijk gegevens verwerkt worden onder de WGS zouden de UNGPs moeten onderschrijven en *human rights due diligence* uit moeten voeren, in elk geval met betrekking tot de analyse-*tools* die ze ontwikkelen en gebruiken.

Het voorgestelde wetsvoorstel schept een bevoegdheid tot zeer verregaande gegevensverwerking in samenwerkingsverbanden. Dit levert een inbreuk op voor het recht op de bescherming van de persoonlijke levenssfeer, en in het verlengde daarvan de rechten op non-discriminatie, een effectief rechtsmiddel en een eerlijk proces. Amnesty International meent dat het concept-WGS daarbij op verschillende punten het bestaande gegevensbeschermingsrecht dreigt te ondermijnen en onvoldoende waarborgen kent tegen misbruik en willekeur. Om aan de mensenrechtelijke eisen te voldoen zal dit conceptwetsvoorstel op verschillende punten verbeterd moeten worden.

---

[35] *Klass e.a./Duitsland*, r.o. 56; EHRM 18 mei 2010, nr. 26839/05, *Kennedy/Verenigd Koninkrijk*, r.o. 167; EHRM 22 februari 2013, nr. 39315/06, *Telegraaf e.a./Nederland*, r.o. 98; *Zakharov/Rusland*, r.o. 233; *Szabó en Vissy/Hongarije*, r.o. 77.

[36] Zie The UN Guiding Principles on Business & Human Rights (UNGPs) en ondersteunende documenten.

[37] Zie *The Toronto Declaration*, p. 7-11.