Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2021–2022

35 447 Regels omtrent gegevensverwerking door samenwerkingsverbanden (Wet gegevensverwerking door samenwerkingsverbanden)

G

BRIEF VAN DE VOORZITTER VAN DE AUTORITEIT PERSOONSGEGEVENS

Aan de voorzitter van de vaste commissie voor Justitie en Veiligheid

Den Haag, 9 november 2021

Bij brief van 19 april 2021 van de Voorzitter van de vaste commissie voor Justitie en Veiligheid van de Eerste Kamer der Staten-Generaal is de Autoriteit Persoonsgegevens (AP) geraadpleegd over het gewijzigd voorstel voor de wet gegevensverwerking door samenwerkingsverbanden (WGS, hierna: het voorstel).

De Eerste Kamer vraagt het oordeel van de AP op het wetsvoorstel zoals dat voorligt in de Eerste Kamer,[1] mede gelet op het feit dat het voorstel op meerdere punten is geamendeerd door de Tweede Kamer. Meer specifiek wenst de Eerste Kamer antwoord op de volgende vragen:
A. Is voldoende afgebakend wie toegang tot de systemen heeft?
B. Kan misbruik van persoonsgegevens voldoende worden tegengegaan?

Gelet op het belang van het onderwerp maakt de AP in dit geval graag gebruik van de gelegenheid een derde maal een oordeel te geven en wel over de beoogde eindtekst.

Hoofdlijn advies

Het voorkomen en bestrijden van ernstige en ondermijnende criminaliteit is dermate belangrijk dat ook voor de AP vaststaat dat hiervoor ingrijpende inbreuken op het grondrecht op bescherming van persoonsgegevens noodzakelijk kunnen zijn. Niettemin heeft de AP in 2019 kritisch geadviseerd over zowel een eerste conceptwetsvoorstel voor de WGS als over een aangepast concept.[2]

[1] Gewijzigd voorstel van wet van 17 december 2020.
[2] Advies van de AP van 4 januari 2019 en aanvullend advies van de AP van 19 april 2019 over een aangepast concept.

kst-35447-G
ISSN 0921 - 7371
's-Gravenhage 2021

Het huidige voorstel is op een aantal punten verbeterd ten opzichte van dat concept. In de eerste plaats omdat enkele samenwerkingsverbanden nu uitdrukkelijk in de wet worden geregeld. Daarnaast is de mogelijkheid van aanwijzing van nieuwe samenwerkingsverbanden bij algemene maatregel van bestuur (amvb) meer in de wet omlijnd en is een aantal waarborgen toegevoegd, waaronder een rechtmatigheidscommissie.[3]

Algemene notie: uitholling van beginselen

Verdere aanpassingen zijn echter nog dringend noodzakelijk om uitholling van beginselen (met name de onschuldpresumptie, doelbindingsbeginsel, transparantiebeginsel en het beginsel van dataminimalisatie) en daarmee Kafkaëske toestanden voor grote aantallen mensen, te voorkomen.

Niet voldoen aan evenredigheidstoets

Het voorstel leidt tot een ernstige beperking van het grondrecht op bescherming van persoonsgegevens omdat het gaat om zeer veel (vaak bijzondere en «gevoelige») persoonsgegevens met vele verwerkingen die belangrijke gevolgen kunnen hebben voor betrokkenen. Voor het doel van het voorkomen en bestrijden van bepaalde ernstige criminaliteit kunnen vergaande beperkingen van het grondrecht gerechtvaardigd zijn. Dat neemt niet weg dat het voorstel op onderdelen in strijd komt met de eisen die voortvloeien uit het grondrecht van bescherming van persoonsgegevens. Verschillende bepalingen gaan namelijk verder dan strikt noodzakelijk en/of bevatten onvoldoende duidelijke en nauwkeurige regels en/of onvoldoende procedurele en materiële waarborgen.

De noodzakelijke aanpassingen zien vooral op:
- de noodzaak van de samenwerkingsverbanden FEC, RIEC's en iCOV beter motiveren in het licht van bestaande en aangekondigde maatregelen, met name het plan van aanpak witwassen, en doublures in de doelstellingen van de verbanden, omdat inbreuken op het privéleven en het recht op bescherming van persoonsgegevens alleen gerechtvaardigd zijn als zij noodzakelijk zijn;
- schrappen van de subsidiaire doelstellingen van het iCOV van het innen van overheidsvorderingen die oninbaar dreigen te worden en het uitoefenen van toezicht op een goede werking van de markt omdat het belang van deze doelen niet dragend is gemotiveerd en zodoende niet in balans is met de vergaande inbreuk op het grondrecht van betrokkenen;
- preciseren van risico's met betrekking tot «andere ernstige vormen van criminaliteit» als doelstelling van het FEC omdat anders het risico bestaat dat dit verband ook wordt gebruikt voor het opsporen en bestrijden van minder ernstige vormen van criminaliteit waardoor de vereiste balans tussen het doel en de inbreuk zoek is;
- duidelijke regels over wanneer de verbanden in actie mogen komen omdat anders het risico bestaat dat iedere burger door de mangel van de samenwerkingsverbanden wordt gehaald hetgeen vergaande consequenties kan hebben voor betrokkene;
- duidelijke regeling in de wetgeving zelf over uitzonderingen op de rechten van betrokkenen en meer transparantie om te voorkomen dat betrokkene wordt geconfronteerd met een «black box»;

Daarnaast:
- schrappen van de mogelijkheid van aanwijzing van nieuwe samenwerkingsverbanden bij amvb omdat artikel 10 van de Grondwet meebrengt dat belangrijke regels over de bescherming van persoonsgege-

[3] Artikel 1.8, zesde lid, van het voorstel.

vens (zoals welke samenwerkingsverbanden, voor welke doelen en met welke (private) deelnemers) door de wetgever *zelf* dienen te worden vastgesteld en niet mag worden overgelaten aan de regering.

De AP onderschrijft dat het verwerken van persoonsgegevens door samenwerkingsverbanden ten behoeve van het beter bestrijden van bepaalde vormen van ernstige of ondermijnende criminaliteit noodzakelijk kan zijn. Voor zover dat het geval is, is het ook aangewezen dit adequaat en in belangrijke mate in de wet zelf te regelen. Het voorstel in zijn huidige vorm is daarvoor echter onvoldoende. Naar het zich laat aanzien beoogt het voorstel de (opsporings)praktijk op onderdelen veel ruimte te geven. Te ruime bepalingen keren zich echter juist tegen de belangen van die praktijk. Mocht de Eerste Kamer deze wet immers in deze vorm aannemen, dan worden onder andere politie en justitie geconfronteerd met de onzekerheid van wetgeving die op onderdelen kan leiden tot onrechtmatige inbreuken op grondrechten van mensen en dan niet mag worden toegepast. De AP adviseert de Eerste Kamer dan ook om het wetsvoorstel in zijn huidige vorm niet aan te nemen.

Strekking van het concept

Het gewijzigd wetsvoorstel strekt er primair toe de verwerking van persoonsgegevens door vier bestaande samenwerkingsverbanden (het Financieel Expertisecentrum (FEC), de Infobox Crimineel en Onverklaarbaar Vermogen (iCOV), de Regionale Informatie- en Expertisecentra (RIEC's) en de Zorg- en Veiligheidshuizen (ZVH's) van een adequate juridische basis te voorzien.[4] Dit brengt onder meer mee dat gegevens effectiever tussen alle deelnemers van een verband kunnen worden gedeeld ten behoeve van gezamenlijke analyse. Nu moet de noodzaak en grondslag voor verstrekking vaak per deelnemer worden vastgesteld.[5] Ook wordt met het voorstel een groot aantal wettelijke geheimhoudingsplichten doorbroken.

Daarnaast geeft het voorstel de mogelijkheid om een samenwerkingsverband bij algemene maatregel van bestuur te regelen als bij amvb de doeleinden worden omschreven die passen binnen het raamwerk van hoofdstuk 3 van het voorstel. Aan drie van de vier samenwerkingsverbanden kunnen naast overheidsinstanties ook private partijen participeren en zodoende is publiek private samenwerking mogelijk.[6] Voorts bevat het voorstel in aanvulling op de AVG ook een aantal waarborgen voor de bescherming van persoonsgegevens die door deze samenwerkingsverbanden worden verwerkt.

Inhoudsopgave advies

[4] Kamerstukken II 2019/20 35 447, nr. 3, blz. 1.

[5] Kamerstukken II 2020/21, 35 447, nr. 6, blz. 12–13. De huidige verstrekking tussen deelnemers aan samenwerkingsverbanden vindt met name plaats op basis van bilaterale grondslagen in sectorale wetgeving. Het convenant iCOV (Stb. 2019, 11352) benadrukt dat een verstrekking alleen kan plaatsvinden als dat wettelijk is toegestaan.

[6] Uitgezonderd is de iCOV.

Advies

1. Algemene notie: uitholling van beginselen

In haar adviezen over een eerder (aangepast) concept voor een voorstel voor de WGS wees de AP op de substantiële risico's voor uitholling van bestuursrechtelijke en strafrechtelijke uitgangspunten. In reactie hierop stelt het kabinet in de memorie van toelichting:

«De stelling van de AP dat de WGS tot een ernstige verwatering van de rechtstatelijke uitgangspunten zal leiden die voor de verschillende rechtsgebieden gelden, wordt niet onderschreven. (...). De WGS laat een rechtsstatelijk uitgangspunt als de onschuldpresumptie volledig in stand: zij doet in geen enkel opzicht afbreuk aan *de wettelijke waarborgen die gelden vanaf het moment waarop een verdenking ontstaat*.»[7] (curs, AP).

Naar het oordeel van de AP brengt ook het voorliggende voorstel een substantiële uitholling van (rechtstatelijke) beginselen mee.

a. Onschuldpresumptie

Volgens de Europese richtlijn 2016/343 werkt de onschuldpresumptie[8] vanaf het moment dat iemand wordt verdacht een strafbaar feit te hebben begaan.[9] Het beginsel brengt onder meer mee dat verdachten voor onschuldig worden gehouden totdat hun schuld in rechte is komen vast te staan en dat de bewijslast voor de vaststelling van de schuld van de verdachte op de vervolgende instantie rust.

In de literatuur wordt echter gesteld dat door «mass surveillance programmes» deze onschuldpresumptie *de facto* geweld wordt aangegaan, bijvoorbeeld omdat een verdachte door een gebrek aan

[7] Kamerstukken II 2019/20, 35 447, nr. 3, blz. 40 e.v.
[8] Vgl. voor de onschuldpresumptie, artikel 48 van het Handvest van de grondrechten van de EU en artikel 6, tweede lid, EVRM.
[9] Richtlijn 2016/343 van 9 maart 2016.

transparantie geen inzicht heeft over hetgeen de overheid over hem of haar weet.[10]

Ook wordt in de literatuur wel een bredere uitleg aan de onschuldpresumptie gegeven in de zin dat de onschuldpresumptie de verhouding tussen de Staat en het individu regardeert:

«This requires the former to meet some threshold of suspicion before exercising any powers on the individual (including surveillance).»[11]

In deze zin stelt prof. Marianne Hirsch Ballin:

«the threshold of «reasonable suspicion» is to be considered as the acknowledgement that the Presumption of innocence is respected in cases of State interventions with the lives of the individuals».[12]

Volgens het voorstel zijn de samenwerkingsverbanden bevoegd om analyses te verrichten aan de hand van persoonsgegevens die voor andere doelen zijn verzameld, zonder dat er een duidelijke en objectieve verdenkingsvoorwaarde bestaat en zonder dat betrokkene daarvan precies op de hoogte is. In feite bestaat het risico dat heimelijk de doopceel van zo ongeveer elke burger wordt gelicht. Een duidelijk criterium van een objectieve verdenking leidt het oordeel van de AP tot de eerbiediging van de onschuldpresumptie in deze uitleg en maakt het verschil met «mass surveillance».[13]

Eerder wees de AP daarom op een alternatief: het invoeren van een mechanisme dat vergelijkbaar is met de melding ongebruikelijke transacties (zie over dat systeem nader punt 3.2.a).[14] In reactie hierop stelt het kabinet dat het lastig is om hieraan inspiratie te ontlenen, omdat bij de WGS risicomeldingen – anders dan bij de melding ongebruikelijke transacties – niet het startpunt, maar het *product* van de gegevensverwerking moeten zijn.

Naar het oordeel van de AP brengt de onschuldpresumptie *in de hiervoor weergegeven opvatting* juist mee dat een *duidelijk en objectief startpunt op basis van voldoende aanwijzingen* wordt vereist om persoonsgegevens binnen het verband te brengen omdat anders in beginsel iedere burger het risico loopt zonder goede grond door de mangel van de samenwerkingsverbanden te worden gehaald (zie nader punt 3.2.c). Dit klemt temeer nu – anders dan in het systeem van melding van ongebruikelijke transacties – politie en justitie al deelnemen aan de voorgestelde samenwerkingsverbanden en zodoende reeds bekend raken met allerlei informatie over burgers.

---

[10] Vgl. bijv. Unwitting subjects of surveillance and the presumption of innocence, Jonida Milaj, Jeanne Pia Mifsud Bonnici, Computer law and security review 2014, 419–428 en de daar aangehaalde literatuur.

[11] Jonida Milaj, Jeanne Pia Mifsud Bonnici, blz. 422.

[12] Marianne Hirsch Ballin, An inside view of Dutch counterterrorism strategy: countering terrorism through criminal law and the presumption of innocence, 2008.

[13] Vgl. de prejudiciële beslissing van het Hof van Justitie EU waarin het Hof stelt dat -aangaande de rechtsgrondslag van noodzakelijk voor het vervullen van een taak van algemeen belang- voor het plaatsen van een persoon op een zwarte lijst van mogelijke fraudeurs *«voldoende aanwijzingen»* moeten bestaan dat een persoon terecht op de lijst staat omdat plaatsing op de lijst verschillende rechten, waaronder de onschuldpresumptie, kan schaden (Hof van Justitie EU van 27 september 2017, zaak C-73/16).

[14] Advies AP van 4 januari 2019, blz. 8.

b. Afwijking van doelbindingsbeginsel

De AP stelde over een eerder concept dat het leidt tot verwatering van de scheidingen tussen rechtsgebieden en afwijking van het doelbindingsbeginsel. Het kabinet stelt dat de AP eraan voorbij lijkt te gaan dat de scheiding tussen de verschillende rechtsgebieden nu al niet absoluut is:

«Er zijn immers nu al talrijke bepalingen die het mogelijk maken om persoonsgegevens uit het ene rechtsgebied te benutten binnen een ander rechtsgebied (bijvoorbeeld het Besluit politiegegevens en de Uitvoeringsregeling Awr).» Dat een instantie die zelf niet bevoegd is bepaalde gegevens te verzamelen, die gegevens op grond van de WGS kan verkrijgen van een andere deelnemer die wel bevoegd is die gegevens te verzamelen, is *als constructie* niet uitzonderlijk. Zij is niet wezenlijk anders dan andere, al bestaande legitieme constructies waarin instanties bepaalde gegevens mogen doorverstrekken aan andere instanties. Het principe van doelbinding is geen absoluut beginsel.» (curs, AP).

Het is juist dat in bestaande sectorale wetgeving is geregeld dat gegevens uit één rechtsgebied naar een ander kunnen gaan en dat de AVG uitzondering op het doelbindingsbeginsel mogelijk maakt. Artikel 6, vierde lid, aanhef, AVG bepaalt – kort samengevat – dat de verwerking voor een ander, onverenigbaar, doel mag als dat een basis heeft in het lidstatelijk recht (dus de WGS).[15] Het lidstatelijk recht moet dan wel één van de belangen van artikel 23, eerste lid, AVG beschermen, zoals het voorkomen, het onderzoek, het opsporen en vervolgen van strafbare feiten.[16] Volgens het kabinet voldoet het voorstel hieraan.

De mogelijkheid van artikel 6, vierde lid, AVG neemt echter niet weg dat uitzonderingen op het doelbindingsbeginsel *slechts beperkt toelaatbaar* zijn, zoals ook door de wetgever herhaaldelijk is bevestigd.[17] De achtergrond hiervan is dat de burger er in beginsel van uit kan gaan dat persoonsgegevens die voor een bepaald doel zijn verleend, vervolgens niet voor een geheel ander doel worden gebruikt. Een en ander kan leiden tot een «chilling effect», zoals ook de rechtbank in de SyRI-uitspraak aangaf: Zonder vertrouwen in voldoende privacybescherming zullen burgers minder snel gegevens willen verstrekken of zal daarvoor minder draagvlak bestaan.[18]

---

[15] Artikel 6, vierde lid, AVG, luidt, voor zover relevant: Wanneer de verwerking voor een ander doel dan dat waarvoor de persoonsgegevens zijn verzameld *niet* berust op toestemming van de betrokkene of op een Unierechtelijke bepaling *of een lidstaatrechtelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van de in artikel 23, lid 1, bedoelde doelstellingen* houdt de verwerkingsverantwoordelijke bij de beoordeling van de vraag of de verwerking voor een ander doel verenigbaar is met het doel waarvoor de persoonsgegevens aanvankelijk zijn verzameld onder meer rekening met (...).

[16] Artikel 23, eerste lid bepaalt: De reikwijdte van de verplichtingen en rechten als bedoeld in de artikelen 12 tot en met 22 en artikel 34, alsmede in artikel 5 kan, voor zover de bepalingen van die artikelen overeenstemmen met de rechten en verplichtingen als bedoeld in de artikelen 12 tot en met 20, worden beperkt door middel van Unierechtelijke of lidstaatrechtelijke bepalingen die op de verwerkingsverantwoordelijke of de verwerker van toepassing zijn, op voorwaarde dat *die beperking de wezenlijke inhoud van de grondrechten en fundamentele vrijheden onverlet laat en in een democratische samenleving een noodzakelijke en evenredige maatregel* is ter waarborging van onder meer:
a) de nationale veiligheid (...).
Het tweede lid bepaalt dat de in het eerste lid bedoelde wettelijke maatregelen met name specifieke bepalingen bevatten met betrekking tot, in voorkomend geval, onder meer de doeleinden van verwerking, de categorieën van gegevens en waarborgen.

[17] Kamerstukken II 2017/18, 34 851, nr. 3, p. 37.

[18] In dezelfde zin rechtbank Den Haag (ECLI:NL:RBDHA:2020:865) in het vonnis over de Syri-wetgeving, onder 6.5.

c. Doorbreking van geheimhoudingsplichten

Bovendien is in bestaande wetgeving vaak sprake van een geheimhoudingsplicht voor overheidsinstanties zodat burgers en bedrijven ervan uit kunnen gaan dat verstrekte gegevens veilig zijn. Het voorstel gaat een stap verder dan de genoemde afwijkingen van het doelbindingsbeginsel door een hele reeks van geheimhoudingsplichten in sectorale wetgeving te doorbreken.[19]

Juist de *potentieel geweldige omvang* waarin het wetsvoorstel verwerking door bestaande en nieuwe samenwerkingsverbanden legitimeert van persoonsgegevens die voor andere doeleneinden zijn verzameld, bovendien zonder duidelijke drempel voor activering van een verband, maakt dat het voorstel op gespannen voet staat met genoemde uitleg van de onschuldpresumptie en het doelbindingsbeginsel. Bovendien worden veel geheimhoudingsplichten doorbroken. Daarbij speelt ook dat politie en justitie al deelnemer zijn aan de verbanden die in de wet worden geregeld. Een en ander kan de verhouding tussen overheid en burger wezenlijk wijzigen.

d. Weinig transparantie en weinig effectieve rechtsbescherming

Daarbij komt dat er feitelijk weinig transparantie bestaat en ook de rechtsbescherming *feitelijk* beperkt is.[20] Zo is het voor een individuele burger onmogelijk om te verifiëren welke gegevens er over hem of haar worden uitgewisseld, waar deze informatie terechtkomt en welke gevolgen dat kan hebben voor die persoon.[21] Dat maakt het onder meer moeilijk om af te dwingen dat onjuiste data in de informatieketen worden gecontroleerd en gecorrigeerd.[22]

De verplichting om betrokkenen te informeren over hen betreffende verwerkingen van persoonsgegevens zou namelijk niet van toepassing zijn indien de uitzonderingen op grond van artikel 13 of 14 AVG opgaan of op grond van de algemene uitzonderingsbepaling van artikel 23 AVG, uitgewerkt in artikel 41 Uitvoeringswet AVG. De toelichting stelt dat:

»de algemene uitzonderingsbepaling van artikel 23 AVG jo. artikel 41 Uitvoeringswet AVG van toepassing kan zijn.»[23]

Volgens artikel 41 Uitvoeringswet AVG kan *de verwerkingsverantwoordelijke* de verplichtingen en rechten, bedoeld in de artikelen 12 tot en met 21 en artikel 34 van de AVG buiten toepassing laten voor zover zulks

---

[19] Hoofdstuk 4 van het voorstel.

[20] Er zijn wel mogelijkheden om verweer te voeren: de betrokkene kan een weigering om te voldoen aan een inzageverzoek in de zin van artikel 15 AVG voorleggen aan de rechter.

[21] Vgl. ook het advies van de Raad voor het openbaar bestuur uit mei 2021, «Sturen of gestuurd worden». De Raad signaleert drie uitdagingen voor het waarborgen van de legitimiteit van sturen met data:
1. Partijen die sturen met data weten steeds meer over burgers, maar omgekeerd weten burgers steeds minder over partijen die sturen met data: de transparantie-paradox;
2. De dilemma's, afwegingen en subjectieve waardenoordelen in het proces van sturen met data verdwijnen in een *black box*;
3. Door het toepassen van data buiten de context waarvoor deze zijn verzameld, (semi-) automatische analyse en besluitvorming, en gebrek aan reflectie, kunnen goedbedoelde maatregelen ontsporen en is bijsturing vaak te lauw of te laat. De Raad vindt dat het openbaar bestuur de legitimiteit van sturen met data kan waarborgen door publieke verantwoording over sturen met data beter te organiseren.

[22] Vgl. het op verzoek van de Eerste Kamer uitgebrachte advies van het College van de rechten van de mens over het voorliggend voorstel van 24 juni 2021 (Kamerstukken I 2020/21, I 35 447, D).

[23] Kamerstukken II 2019/20, 35 447, nr. 3, blz. 18.

noodzakelijk en evenredig is ter waarborging van bijv. het belang van de nationale veiligheid. Aldus wordt, met een beroep op artikel 41 van de UAVG, in wezen aan de verwerkingsverantwoordelijke gelaten om in individuele gevallen uit de AVG voortvloeiende rechten en verplichtingen te beperken.[24]

Eerder gaf de AP al aan dat bepaald onzeker is of de huidige opzet van artikel 41 van de UAVG tegemoetkomt aan de eisen die artikel 23 van de AVG aan het mogen beperken van rechten van betrokkenen stelt.[25] De AVG maakt beperkingen van de rechten alleen mogelijk door middel van algemene, aan toepassing van de beperking voorafgaande, Unierechtelijke of lidstaatrechtelijke wettelijke bepalingen «die op de verwerkingsverantwoordelijke van toepassing zijn».[26] Het tweede lid van artikel 23 AVG eist ook dat de wetgeving bepaalde aspecten regelt, terwijl artikel 41, tweede lid, UAVG deze aspecten juist integraal overlaat aan de verwerkingsverantwoordelijke in het individuele geval. Ook uit rechtspraak van het Hof van Justitie EU[27] en uit de recent aangenomen «Guideline 10/2020 on restrictions under Article 23 GDPR» volgt zonneklaar dat op Europees niveau de opvatting is dat specificatie *in wetgeving* aangewezen is.[28] Temeer nu het hier om beperking van belangrijke rechten van betrokkene gaat komt ook des te meer belang toe aan de eis dat wetgeving duidelijk, nauwkeurig en in de toepassing voorspelbaar moet zijn.[29]

De AP adviseert dan ook met klem om, als beperkingen inderdaad nodig kunnen zijn, in deze regelgeving uit te werken welke rechten van betrokkenen in welke omstandigheden in welke zin mogen worden beperkt, daarbij aandacht te schenken aan de aspecten, bedoeld in artikel 23 AVG en het geheel in de toelichting te verantwoorden en niet te verwijzen naar artikel 41 Uitvoeringswet AVG.[30]

Daarnaast hebben verschillende adviesorganen erop gewezen dat in het voorstel rechtsbescherming ontbreekt, bijvoorbeeld tegen onterechte verdachtmaking als gevolg van fouten en vooroordelen in algoritmen. In reactie hierop stelt het kabinet dat betrokkenen in beginsel hun recht van bezwaar kunnen uitoefenen wanneer persoonsgegevens worden verwerkt op grond van artikel 6, eerste lid, onderdeel e (taak van algemeen belang) of f (gerechtvaardigde belangen):

«Wat betreft de risico's van fouten en vooroordelen in algoritmen geldt dat deze geadresseerd zullen moeten worden, wil de gegevensverwerking in het samenwerkingsverband juridisch aanvaardbaar zijn. De deelnemers zullen zorgvuldig te werk moeten gaan, onder meer door te zorgen dat de

---

[24] Vgl. uitvoeriger, het advies van de AP over de Verzamelwet Uitvoeringswet AVG van 11 november 2020, punt 3. Op dit advies is nog geen reactie.

[25] Punt 3 van het advies over het concept voor een wetsvoorstel Verzamelwet gegevensbescherming (Inventarisatie eerste ervaringen UAVG) van 11 november 2020 met kenmerk z2020-08972.

[26] Vgl. ook de brief van de AP van 19 januari 2018 aan de Voorzitter van de Tweede Kamer over het voorstel Uitvoeringwet AVG. en punt 3 van het advies over het concept voor een wetsvoorstel Verzamelwet gegevensbescherming (Inventarisatie eerste ervaringen UAVG) van 11 november 2020 met kenmerk z2020–08972.

[27] ECLI:EU:C:2020:791, La Quadrature du Net e.a., zie i.h.b. punt 209 en 210.

[28] https://edpb.europa.eu/system/files/2021-10/edpb_guidelines202010_on_art23_adopted_after_consultation_en.pdf. Zie i.h.b.: Punt. 9 «To be lawful, restrictions shall be provided for in a legislative measure», punt 16.: «The requiremet of a legislative measure entails that controllers can only rely on.a restriction provided for by Article 23 GDPR to the extent that this restriction has been specified in Union or Member state law.»

[29] Vaste jurisprudentie, zie ook overweging. 41 van de AVG.

[30] Vgl. het advies van 21 oktober 2021 over het concept voor een wetsvoorstel Uitvoeringswet verordening terroristische online-inhoud.

gegevens van voldoende kwaliteit zijn en dat zij beschikken over de nodige expertise om goede analyses uit te voeren en de uitkomsten op een passende en controleerbare wijze te duiden.»[31]

Deze oproep aan de deelnemers om zorgvuldigheid te betrachten miskent evenwel dat de wetgeving *zelf* zo veel mogelijk zorgvuldigheid bij de verwerking van persoonsgegevens moet *garanderen*. Goede bedoelingen en wettelijke waarborgen zijn immers niet hetzelfde. Daarnaast verdient opmerking dat als persoonsgegevens, zoals ook wordt voorgesteld, worden verstrekt op grond van artikel 6, eerste lid onderdeel c, (wettelijke verplichting), de uitoefening van het recht op bezwaar problematisch is (zie nader onder 3.2.e).

Voorafgaande algemene noties wijzen erop dat het voorstel kan leiden tot Kafkaëske toestanden voor grote aantallen mensen. Deze risico's kunnen goeddeels worden beperkt door:
– Een beperking van met name de doelen van de samenwerkingsverbanden (zie punt 3.2) en;
– Het schrappen van de mogelijkheid van nieuwe samenwerkingsverbanden bij amvb (zie punt 3.3).

2. Het juridisch toetsingskader

a. AVG en Richtlijn gegevensbescherming opsporing en vervolging[32]

Op de verwerking van persoonsgegevens binnen samenwerkingsverbanden is de AVG van toepassing.[33] Volgens artikel 1 beschermt de AVG de grondrechten en de fundamentele vrijheden van natuurlijke personen en met name hun recht op bescherming van persoonsgegevens.[34] De verstrekking van politiegegevens en van justitiële en strafvorderlijke gegevens door opsporingsambtenaren en officieren van justitie aan een samenwerkingsverband valt onder de reikwijdte van de richtlijn gegevensbescherming opsporing en vervolging.[35]

De AVG biedt een rechtsgrond voor verwerking van persoonsgegevens, als deze voortvloeit uit een wettelijke verplichting of noodzakelijk is voor de vervulling van een taak van algemeen belang en deze taak is vastgesteld bij lidstatelijk recht. De rechtsgrond voor deze verwerking moet worden vastgesteld bij Unierecht of lidstatelijk recht dat op de verwerkingsverantwoordelijke van toepassing is. Het doel van de verwerking wordt in die rechtsgrond vastgesteld of is met betrekking tot de bedoelde verwerking noodzakelijk voor de vervulling van een taak van algemeen belang of voor de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend. Het Unierecht of het lidstatelijke recht moet *beantwoorden aan een doelstelling van algemeen belang* en *moet evenredig* zijn met het nagestreefde gerechtvaardigde doel.[36]

Daarnaast eist artikel 5 AVG (doelbindingsbeginsel) dat sprake is van een welbepaald, uitdrukkelijk omschreven en gerechtvaardigd doel.

---

[31] Voor zover het gebruik van big data uitmondt in een besluit als bedoeld in de Awb, kan de betrokkene de big-data-analyse in ieder geval in dat verband aan de orde stellen.
[32] Richtlijn 2016/680 van 27 april 2016. De richtlijn is in Nederland omgezet in de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens.
[33] Artikel 2 AVG en Kamerstukken II 2019/20, 35 447, nr. 3, blz. 33.
[34] Artikel 1, tweede lid, AVG.
[35] Kamerstukken II 2019/20, 35 447, nr. 3, blz. 34.
[36] Artikel 6, derde lid, AVG.

b. Handvest van de grondrechten EU[37]

Artikel 7 van het Handvest waarborgt het recht op bescherming van het privéleven. Artikel 8 van het Handvest bepaalt dat persoonsgegevens eerlijk en voor welbepaalde doeleinden moeten worden verwerkt, en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Artikel 8 van het Handvest en artikel 16 van het VWEU bepalen dat eenieder in de Europese Unie recht heeft op bescherming van zijn persoonsgegevens.

Beperkingen op de uitoefening van de in het Handvest erkende rechten en vrijheden moeten bij wet worden gesteld en de wezenlijke inhoud van die rechten en vrijheden eerbiedigen.[38] Met inachtneming van het evenredigheidsbeginsel kunnen slechts beperkingen worden gesteld, indien zij noodzakelijk zijn en daadwerkelijk beantwoorden aan door de Unie erkende doelstellingen van algemeen belang of aan de eisen van de bescherming van de rechten en vrijheden van anderen (artikel 52 van het Handvest). Het evenredigheidsbeginsel vereist volgens vaste rechtspraak van het Hof van Justitie EU dat handelingen van de instellingen van de Unie *geschikt* zijn om de door de betrokken regeling nagestreefde legitieme doelstellingen te verwezenlijken en *niet verder gaan dan wat daarvoor geschikt en noodzakelijk* is.[39] De betrokken regeling die de inmenging bevat, voldoet slechts aan het evenredigheidsbeginsel indien zij *duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de betrokken maatregel* bevat die minimale eisen opleggen, zodat degenen van wie de gegevens zijn doorgegeven over voldoende garanties beschikken dat hun persoonsgegevens *doeltreffend worden beschermd tegen het risico van misbruik.*[40] Zij moet in het bijzonder aangeven in welke omstandigheden en onder welke procedurele en materiële voorwaarden een maatregel die voorziet in de verwerking van dergelijke gegevens kan worden genomen, en aldus waarborgen dat de inmenging tot het *strikt noodzakelijke* wordt beperkt.[41]

Relevant in dit verband zijn met name *de reikwijdte van de maatregel* en *de aard van de gegevens.*[42] Ook kijkt het Hof naar de *waarborgen waarmee de maatregel was omkleed*, zoals de mate waarin de betrokken persoon controle op de gegevensverwerking heeft kunnen uitoefenen en de aanwezigheid van effectief onafhankelijk toezicht. Bij de proportionali-

---

[37] Ook artikel 8 van het Europees Verdrag voor de rechten van de mens (EVRM) bevat het recht van een ieder op respect voor zijn privéleven, familie- en gezinsleven, woning en correspondentie. In het Handvest van de grondrechten is een artikel opgenomen dat ervoor moet zorgen dat bepalingen die in het Handvest corresponderen met het EVRM, op dezelfde manier door de rechters in Straatsburg (EHRM) en Luxemburg (Hof van Justitie) worden uitgelegd (vgl. artikel 52 en 53 van het Handvest).

[38] Het Hof van Justitie EU neemt een inbreuk op de wezenlijke inhoud van het recht niet snel aan (vgl. bijv. HvJ EU PNR overeenkomst Canada – EU, punt 150 en 151).

[39] Vgl. de arresten Afton Chemical, C 343/09, EU:C:2010:419, punt 45; Volker und Markus Schecke en Eifert, EU:C:2010:662, punt 74; Nelson e.a., C 581/10 en C 629/10, EU:C:2012:657, punt 71; Sky Österreich, C 283/11, EU:C:2013:28, punt 50, en Schaible, C 101/12, EU:C:2013:661, punt 29). Vgl. ook Schwarz, C 291/12, punt 54 en 55.

[40] Vgl. bijv. het advies van het Hof van Justitie EU van 26 juli 2017 (overeenkomst tussen Canada en EU PNR-gegevens), punt 140, met de verwijzingen.

[41] Vgl. bijv. het advies van het Hof van Justitie EU van 26 juli 2017 (overeenkomst tussen Canada en EU PNR-gegevens), punt 141.

[42] Vgl. de arresten van 8 april 2014, Digital Rights Ireland e.a., C-293/12 en C-594/12, EU:C:2014:238, punten 54 en 55, en 21 december 2016, Tele2 Sverige en Watson e.a., C-203/15 en C-698/15, EU:C:2016:970, punten 109 en 117; zie in die zin eveneens arrest EHRM, 4 december 2008, S. en Marper tegen Verenigd Koninkrijk, CE:ECHR:2008:1204JUD003056204, punt 103).

teitstoets is cruciaal of de beperkingen van het grondrecht en het doel dat ermee wordt beoogd voldoende met elkaar in balans zijn.[43]

c. Artikel 10 Grondwet

De Grondwet geeft in artikel 10, eerste lid, eenieder, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer. De Grondwet geeft aan de wetgever een belangrijke verantwoordelijkheid: deze moet beoordelen of de beperking van fundamentele rechten van burgers blijft binnen de grenzen die de Grondwet stelt en daarbij voldoet aan eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. Aan deze verantwoordelijkheid wordt geen recht gedaan als de concrete invulling vrijwel geheel wordt overgelaten aan de amvb. De hoofdelementen die in algemene zin in ieder geval in de formele wet moeten worden neergelegd zijn de reikwijdte en de structurele elementen van een regeling.[44]

3. Toetsing

Anders dan het eerdere concept voor een kaderwet, regelt het huidige voorstel enkele samenwerkingsverbanden uitdrukkelijk in de wet zodat de uiteindelijk beoogde bepalingen nu ook exact bekend zijn. Dat maakt bij deze gelegenheid ook de preciezere juridische toets mogelijk die anders pas bij de amvb's aan de orde was geweest.

3.1. Ernst van de inbreuk

Het is klip en klaar dat de verwerkingen door samenwerkingsverbanden vaak een ernstige inbreuk op het privéleven[45] van betrokkene en de bescherming van zijn of haar persoonsgegevens opleveren. Voor wat betreft de RIEC's gaat het met name om het burgerservice-nummer «gegevens over de verblijfstatus», «gegevens over de woonsituatie», «financiële gegevens», «fiscale gegevens», «voertuiggegevens», «kadastrale gegevens», «gegevens betreffende zakelijke relaties met anderen», «gegevens over seksueel gedrag of geaardheid», politiegegevens en justitiële gegevens, «gegevens over vergunning- en subsidieaanvragen, hierop genomen besluiten en juridische procedures», «gegevens inzake toezicht en handhaving alsmede getroffen bestuurlijke maatregelen.« Eigenlijk is er nauwelijks een gegeven te bedenken dat er niet onder valt.[46] Het gaat daarbij bovendien niet alleen om de gegevens van de betrokkene zelf, maar ook van mensen in een directe kring van de betrokkene. Bovendien kan de analyse door een samenwerkingsverband vergaande consequenties voor betrokkene hebben. Volgens de toelichting is bijvoorbeeld beoogd dat indien een verband tot doel heeft fraudebestrijding, verstrekking aan een private partij plaats heeft voor het doel van het verband. «In dat geval is het onthouden van een hypotheek aan

---

[43] Vgl. L.M. Verheij en H.R. Kranenborg, De Algemene Verordening Gegevensbescherming in Europees en Nederlands perspectief, met name par. 2.4.5.

[44] Vgl. de Afdeling advisering in het (eerste) advies over het voorstel voor de WGS (Kamerstukken II 2019/20, 35 447, nr. 4).

[45] Het door artikel 7 van het Handvest gewaarborgde recht op bescherming van het privéleven ziet op alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (zie in die in arresten van 9 november 2010, Volker und Markus Schecke en Eifert, C-92/09 en C-93/09, EU:C:2010:662, punt 52; 24 november 2011, Asociación Nacional de Establecimientos Financieros de Crédito, C-468/10 en C-469/10, EU:C:2011:777, punt 42, en 17 oktober 2013, Schwarz, C-291/12, EU:C:2013:670, punt 26).

[46] Vgl. de uitspraak van de rechtbank Den Haag in de zaak SyRI (ECLI:NL:RBDHA:2020:865): «De opsomming van gegevens is weliswaar bedoeld om de gegevensverwerking in te perken (beginsel van dataminimalisatie), maar is in feite zo ruim dat er nauwelijks een persoonsgegeven te bedenken is dat niet voor verwerking in aanmerking komt.» Vgl. ook V. Gantchev, SyRI en zijn rechtsopvolger de WGS: Oude wijn in nieuwe zakken, TRA, 2021/32.

«bijvoorbeeld, een hypotheekfraudeur» een goede uitkomst».[47] Vraag daarbij is of en hoe is vastgesteld dat sprake is van een «hypotheekfraudeur» indien betrokkene niet onherroepelijk is veroordeeld. Als het gaat om een verband met als doel de behandeling van complexe casuïstiek met het oog op het voorkomen van ernstige overlast, kan het verband ertoe leiden dat voor betrokkene eerder een vorm van verplichte GGZ wordt voorbereid.

Bovendien bevat het voorstel – anders dan nu – in beginsel een verplichting tot verstrekking van persoonsgegevens voor deelnemers aan een samenwerkingsverband. Daarbij bevat het voorstel doorbreking van veel specifieke geheimhoudingsplichten[48] en kunnen naast de wettelijke deelnemers andere publieke en private instanties deelnemen.[49] Dit kan volgens het kabinet ook «cross sectorale informatiedeling» tussen publieke en private partijen omvatten, hetgeen voor betrokkene en zijn of haar naasten grote gevolgen kan hebben.[50]

Ten slotte worden de gegevens maximaal vijf jaar bewaard. Een en ander maakt dat sprake is van een ernstige inbreuk op het recht op bescherming van persoonsgegevens.

3.2. Noodzaak wettelijke regeling van de vier bestaande samenwerkingsverbanden

Het evenredigheidsbeginsel brengt mee dat uitzonderingen op de bescherming van de persoonsgegevens en de beperkingen ervan binnen de grenzen van het strikt noodzakelijke blijven.[51] De betrokken regeling die de inmenging bevat, voldoet slechts aan dit vereiste indien zij *duidelijke en nauwkeurige regels over de reikwijdte en de toepassing van de betrokken maatregel* bevat die minimale eisen opleggen, zodat degenen van wie de gegevens zijn doorgegeven over voldoende garanties beschikken dat hun persoonsgegevens *doeltreffend worden beschermd tegen het risico van misbruik.*

a. Gerechtvaardigde doelen

Het Handvest en de AVG eisen een gerechtvaardigd doel voor het verwerken van persoonsgegevens. Bij de gezamenlijke gegevensverwerking door het viertal samenwerkingsverbanden dat het voorstel regelt gaat het om de integrale aanpak van risico's van respectievelijk: inbreuken op de integriteit van het financiële stelsel, van witwas- of fraudeconstructies, van georganiseerde criminaliteit, en van complexe problemen rond personen op het vlak van zorg en veiligheid.[52]

---

[47] Kamerstukken II 2019/20 35 447, nr. 3, blz. 54.

[48] Artikel 1.5 en hoofdstuk 4 van het voorstel.

[49] Aan het FEC kunnen private partijen participeren; aan de RIEC's kunnen private partijen deelnemen bij of krachtens amvb en ook voor de ZVH is deelname van private partijen noodzakelijk (Kamerstukken II 2020/21, 35 447, nr. 6, blz. 56): «Wat zodoende onder de voorgestelde wet zou kunnen, is publiek-private samenwerking binnen het FEC of binnen de Zorg- en Veiligheidshuizen, of – via een toekomstige amvb – een samenwerkingsverband tussen politie, OM en bedrijven ter bestrijding van ernstige vormen van criminaliteit. Dit zijn vormen van *cross-sectorale informatie*-deling tussen publieke en private partijen.»

[50] Vgl. Kamerstukken II 2018/19, 17 050, nr. 576. Cross-sectorale gegevensdeling tussen private partijen is reeds mogelijk, met een vergunning van de Autoriteit persoonsgegevens. De Autoriteit persoonsgegevens kan een dergelijke vergunning verlenen, indien de verwerking noodzakelijk is met het oog op een zwaarwegend belang van derden en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van betrokkenen niet onevenredig wordt geschaad (artikel 33, vijfde lid, Uitvoeringswet AVG).

[51] Vgl. bijv. het advies van het Hof van Justitie EU van 26 juli 2017 (overeenkomst tussen Canada en EU PNR-gegevens), punt 140, met de verwijzingen.

[52] Kamerstukken II 2019/20, 35 447, nr. 3, blz. 35.

Aan te nemen valt dat deze doelen – *in abstracto* – vallen binnen de doeleinden waarvoor het Handvest beperkingen op het recht op bescherming van persoonsgegevens toelaat. Zo acht het Hof van Justitie EU het bestrijden van ernstige (financieel-economische) criminaliteit een doel van algemeen belang. Hiervoor kunnen zelfs zware inbreuken gerechtvaardigd zijn.[53]

Volgens het kabinet gaat het steeds om bij de doelen om zwaarwegende algemene belangen. Maar het «zwaarwegend algemeen belang» vereist een belangenafweging tussen het belang dat gediend wordt met de gezamenlijke verwerking van persoonsgegevens en het belang van de persoonlijke levenssfeer van degenen op wie de persoonsgegevens betrekking hebben.[54] Daarbij moet worden getoetst aan de beginselen van proportionaliteit en subsidiariteit. Als het belang dat wordt gediend met de inbreuk zwaarwegend is, is – gelet op het proportionaliteitsbeginsel – kan een zwaardere inbreuk op het recht op bescherming van persoonsgegevens gerechtvaardigd zijn.

(i) iCOV
In dit verband valt op het doel van de iCOV van het «in kaart brengen van onverklaarbaar of crimineel vermogen». Elk onderzoek door de iCOV naar een onverklaarbaar vermogensbestanddeel van elke burger lijkt aldus door de nieuwe wet gelegitimeerd. Maar het zal met het oog op de proportionaliteit en evenredigheid moeten gaan om aanwijzingen van een mogelijk substantieel vermogensbestanddeel, van een bepaalde hoogte of bepaald misdrijf, anders kan er snel een disbalans bestaan tussen het doel en de inbreuk op het recht op bescherming van persoonsgegevens.

De iCOV kent daarnaast nog andere, subsidiaire, doelen, namelijk het innen van overheidsvorderingen die oninbaar dreigen te worden en het uitoefenen van toezicht op een goede werking van de markt.[55] Deze doelen vallen volgens het kabinet onder het zwaarwegend belang van het voorkomen van wanordelijkheden en strafbare feiten in de zin van het Europees recht. Ten aanzien van deze doelen is echter op geen wijze aannemelijk gemaakt waarom deze van zodanig zwaarwegend algemeen belang zouden zijn – waarom er een zodanig ernstig probleem bestaat dat niet adequaat door de huidige mogelijkheden kan worden opgelost – dat de voorgestelde wettelijke regeling noodzakelijk is. Bovendien zijn ook deze doelen op geen enkele wijze beperkt (zie hierna, onderdeel b).

(ii) FEC, RIEC's en iCOV
Met het voorstel wordt de huidige praktijk van vier bestaande samenwerkingsverbanden grotendeels gecodificeerd: het FEC, de RIEC's, de Infobox crimineel en onverklaarbaar vermogen en de Zorg- en Veiligheidshuizen.[56] De eerste drie van deze vier verbanden strekken met name tot het voorkomen en opsporen van financieel-economische criminaliteit, andere ernstige criminaliteit en georganiseerde criminaliteit. Zoals in het

---

[53] Zie Hvj EU PNR-overeenkomst Canada-EU, punt 149.
[54] Vgl. Kamerstukken II 2019/20, 35 447, nr. 3, blz. 8.
[55] «Het doel van iCOV dient subsidiair, voor zover het doel van iCOV is gericht op het uitoefenen van toezicht op de goede werking van de markt, het belang van het «handhaven van het economisch welzijn van het land» als bedoeld in artikel 8, tweede lid, EVRM. Dit belang is gediend met gezamenlijke gegevensverwerking door de Belastingdienst (waarvan de missie een financieel gezond Nederland inhoudt), door DNB (dat gericht is op een stabiel financieel stelsel) en door ACM (dat als missie heeft om bij te dragen aan een gezonde economie door markten goed te laten werken).»
[56] In de Nota naar aanleiding van het verslag is door het kabinet gesteld: «Hetgeen nu in het wetsvoorstel wordt geregeld, is voor een belangrijk deel een codificatie van de bestaande praktijk.» (Kamerstukken II 2020/21, 35 447, nr. 6, blz. 5).

jaarverslag 2020 van de RIEC's wordt opgemerkt bevat elke casus ook wel een aspect van witwassen.

De vraag is waarom de eerste drie verbanden eigenlijk nodig zijn indien een adequate uitvoering wordt gegeven aan de Wet ter voorkoming van witwassen en financiering van terrorisme (WWFT).

De nationale regelgeving inzake het voorkomen en bestrijden van witwassen in de WWFT is in belangrijke mate een implementatie van de gewijzigde vierde Europese anti-witwasrichtlijn. Als «poortwachters» van het financiële stelsel zijn WWFT-instellingen, zoals banken, verplicht om cliënten en hun transacties te onderzoeken op witwasrisico's. Bij het cliëntenonderzoek vergaren WWFT-instellingen informatie over de cliënt zodat zij in staat zijn de risico's op witwassen te beoordelen. «Ongebruikelijke transacties» van cliënten moeten de WWFT-instellingen vervolgens melden aan de Financiële Inlichtingen Eenheid (FIE). Door analyse van de gemelde ongebruikelijke transacties tracht de FIE transacties en geldstromen bloot te leggen die te relateren zijn aan witwassen, financieren van terrorisme of onderliggende misdrijven. Nadat die transacties «verdacht» zijn verklaard door de FIE worden deze ter beschikking gesteld aan diverse handhavings- en opsporingsdiensten. Een en ander betekent dat bij een adequate toepassing van dit wettelijke stelsel er welbeschouwd al geen noodzaak bestaat voor de drie genoemde verbanden.

Bovendien heeft het kabinet een plan van aanpak witwassen opgesteld. Het plan bestaat uit drie pijlers: het verhogen van barrières voor witwassen, het versterken van de effectiviteit van «poortwachters» zoals banken, en het toezicht op de naleving vergroten alsmede de opsporing en vervolging versterken.[57] Onderdeel van dat plan is ook het wetsvoorstel plan van aanpak witwassen dat volgens het kabinet wetsvoorstel plan van voor het eind van dit jaar zal worden ingediend bij de Tweede Kamer en ertoe strekt om de poortwachtersfunctie van banken te versterken.[58] Inmiddels hebben veel poortwachters hun capaciteit sterk uitgebreid.

Daarnaast wijst de AP op de titel van het verkennend onderzoek in het Wetboek van Strafvordering, onderdeel van de Wet bijzondere opsporingsbevoegdheden (Wet BOB).[59] Dat onderzoek biedt mogelijk een bruikbaar kader om, voorafgaand aan de opsporing, onderzoek te doen op basis van *aanwijzingen* dat binnen verzamelingen van personen misdrijven worden beraamd of gepleegd waarvoor voorlopige hechtenis is toegelaten die gezien hun aard of samenhang met andere misdrijven die binnen die verzamelingen van personen worden beraamd of gepleegd, een ernstige inbreuk op de rechtsorde opleveren.[60] Niet het vermelden van een concreet misdrijf, maar deze aanwijzingen vormen de aanleiding voor dit onderzoek. Hierbij kan het noodzakelijk zijn om

---

[57] Brief van 30 juni 2019.

[58] In het consultatievoorstel plan van aanpak witwassen uit 2019 worden de volgende maatregelen voorgesteld: a. Een verplichting voor WWFF-instellingen om in geval van een verhoogd risico op witwassen navraag te doen bij vorige financiële dienstverleners van de cliënt naar gebleken integriteitsrisico's en daartoe persoonsgegevens te verstrekken. b. Een grondslag om de bestaande plicht tot het monitoren van transacties van cliënten door WWFT-instellingen te kunnen uitbesteden aan een derde partij. c. Een grondslag voor WWFT-instellingen om transacties van cliënten te kunnen delen met andere WWFT-instellingen.

[59] Artikel 126gg Sv.

[60] Indien dit noodzakelijk is voor de uitvoering van het onderzoek kan de officier van justitie bepalen dat artikel 5, eerste lid, aanhef en onder b, van de AVG met betrekking tot het onderzoek niet van toepassing is op daarbij nader aan te geven openbare registers die bij wet zijn ingesteld (artikel 126gg, tweede lid, Sv). Deze bepaling is overigens problematisch omdat de wet zelf – zo nodig – moet voorzien in verwerking van persoonsgegevens voor een ander doel (artikel 6, vierde lid, AVG en artikel 3, derde en vierde lid, van de Wet politiegegevens).

onderzoek te doen naar een hele sector, waarbij wordt gedacht aan vervlechting van criminele en legale activiteiten als grootschalige investeringen van drugsgeld in onroerend goed.[61] De aanwijzingen moeten voortvloeien uit feiten en omstandigheden en dienen zo concreet mogelijk te zijn dat valt uit te maken dat sprake is van misdrijven die voldoen aan de criteria. Uit de evaluatie van de Wet BOB blijkt dat een verkennend onderzoek slechts incidenteel wordt ingesteld.

In het licht van deze Europese en nationale bestaande en aankomende (wettelijke) maatregelen om witwassen (beter) aan te pakken is de vraag waarom de voorgestelde samenwerkingsverbanden voor zover die in het teken staan van het voorkomen en bestrijden van witwassen nodig zijn en waarom niet kan worden volstaan met het stelsel van, met name de WWFT.

Voorts wijst de AP erop dat de doelen van de vier samenwerkingsverbanden elkaar deels overlappen: Zowel het FEC, de RIEC'S en de iCOV hebben het bestrijden van fraude- en witwasconstructies tot onderwerp. In het jaarverslag 2020 van de RIEC's is bijv. gesteld dat evenals in voorgaande jaren witwassen en financiële malversaties binnen RIEC-verband de meest voorkomende thema's zijn omdat in iedere casus wel een element hiervan voorkomt. Dat roept de vraag op opname van de vier verbanden met deels dezelfde doelen en deels dezelfde deelnemers in de wet zodoende allemaal nodig is en of niet kan worden volstaan met minder. Dat is lijn met het beginsel van dataminimalisatie in de AVG.

(iii) Zorg- en Veiligheidshuizen
De samenwerking in het Zorg- en Veiligheidshuis heeft tot doel een bijdrage te leveren aan het voorkomen, verminderen en bestrijden van criminaliteit en ernstige overlast en het bieden van passende zorg, in situaties waarin sprake is van complexe (zorg)problematiek die zonder interventie leidt of kan leiden tot onveilige situaties voor personen of binnen een gebied.[62]
Daarbij verdient opmerking dat door de recente Wet verplichte geestelijke gezondheidszorg (GGZ) de mogelijkheden om gegevens te delen zijn verruimd. Bovendien wijst de AP op het consultatievoorstel voor de Wet aanpak meervoudige problematiek sociaal domein. Dit voorstel verankert een duidelijke taak voor gemeenten om te komen tot een integrale en gecoördineerde aanpak voor meervoudige problematiek.
Ten slotte valt op dat in de toelichting niet voor alle samenwerkingsverbanden is vermeld waarom deze *geschikt* zijn om bij te dragen aan de gestelde doelen, hetgeen uit een oogpunt van Europese recht cruciaal is. Ten aanzien van bijv. de RIEC's volgen uit het jaarverslag 2020 aanwijzingen dat zij inderdaad tot bepaalde resultaten hebben geleid, maar dit is niet voor alle te regelen samenwerkingsverbanden vermeld.

De AP adviseert om de voorgestelde doelen van de iCOV van het innen van overheidsvorderingen en het uitoefenen van toezicht op de markt uit het voorstel te schrappen. Ook overigens is de AP van oordeel dat in het kader van de noodzaak van het voorstel de bestaande en toekomstige (wettelijke) mogelijkheden in het kader van het plan van aanpak witwassen en verder aangekondigde praktische maatregelen, onvoldoende zijn belicht. Tevens adviseert de AP om de geschiktheid en effectiviteit van alle te regelen verbanden om de nagestreefde doelen te bereiken, empirisch te onderbouwen.

---

[61] Aldus Kamerstukken II 1996/1997, 25 403, nr. 3, blz. 49.
[62] Kamerstukken II 2019/20, 35 447, nr. 3, blz. 104.

b. Welbepaalde doelen

Naast gerechtvaardigde doelen eisen het Handvest en artikel 5 AVG ook welbepaalde en uitdrukkelijke doelen voor het verwerken van persoonsgegevens. De mate waarin de nationale regels «nauwkeurig» of «welbepaald» zijn, is tevens cruciaal voor de verdere bescherming omdat de doelomschrijving essentieel is voor de effectieve toepassing van de andere privacy-rechtelijke waarborgen, zoals de noodzaaktoets.

Het doel van het FEC is – kort samengevat – een versterking van de integriteit van het financiële stelsel. In het voorstel is sprake van risico's met betrekking tot *financieel-economische* criminaliteit en *andere ernstige vormen van criminaliteit* of van terrorismefinanciering (artikel 2.2, tweede lid).

Deze begrippen zijn niet «wel bepaald». Illustratief in dit verband is overweging 61 en 62 en 65 van of van Justitie in de zaak Digital Rights Ireland waar het Europese Hof van Justitie viel over de evenredigheid en proportionaliteit van de Europese richtlijn die toegang tot locatiegegevens mogelijk maakte met het oog op het aanpakken van «ernstige criminaliteit». Het Hof vernietigde deze Europese richtlijn en stelde:

«Bovendien bevat richtlijn 2006/24 geen materiële en procedurele voorwaarden betreffende de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan. Artikel 4 van deze richtlijn, dat de toegang van deze autoriteiten tot de bewaarde gegevens regelt, *bepaalt niet uitdrukkelijk* dat deze toegang en het latere gebruik van de betrokken gegevens strikt gebonden zijn aan het doel, *nauwkeurig afgebakende zware criminaliteit* te voorkomen, op te sporen of strafrechtelijk te vervolgen, maar bepaalt enkel dat elke lidstaat de procedure en de te vervullen voorwaarden vaststelt voor toegang tot de bewaarde gegevens overeenkomstig de vereisten inzake noodzakelijkheid en evenredigheid.»[63]

Deze opmerking ziet weliswaar op de toegang tot opgeslagen verkeersgegevens die strikt gebonden moet zijn aan het doel «nauwkeurig afgebakende criminaliteit» te voorkomen of bestrijden. Een en ander geldt naar het oordeel van de AP echter ook voor de verwerking van persoonsgegevens door samenwerkingsverbanden ten behoeve van «andere ernstige vormen van criminaliteit».[64] Om tegemoet te komen aan deze Europese eisen, zou in beginsel kunnen worden uitgegaan van een bepaalde aard van delicten met bepaalde maximale gevangenisstraffen van, bijvoorbeeld, zes jaar of meer, met, zo nodig, enige uitzonderingen daarop.

Onverminderd het hiervoor onder 3.2.a opgemerkte over het schrappen van de subsidiaire doelen van de iCOV geldt een en ander nog sterker voor het doel van de iCOV van het «het uitoefenen van toezicht op een goede werking van de markt.» (artikel 2.10).

---

[63] Vgl. ook punt 65 van het advies.

[64] De AP wijst er bijvoorbeeld op dat het begrip «ernstig misdrijf» in de Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven ter implementatie van artikel 3 van richtlijn 2016/681 in de begripsbepaling is omschreven als een strafbaar feit als bedoeld in bijlage 2 van deze wet, waarop naar wettelijke omschrijving een gevangenisstraf van drie jaar of meer is gesteld. Volgens artikel 13 van de WWFT heeft de Financiële Inlichtingen Eenheid tot taak het voorkomen en opsporen van witwassen en onderliggende basisdelicten en het financieren van terrorisme.

Illustratief is de volgende overweging uit het bindend advies[65] van het Hof van Justitie EU over de PNR-overeenkomst tussen de EU en Canada, waarin een enigszins vergelijkbare bepaling was opgenomen. De overeenkomst moest het mogelijk maken dat zogenaamde Passender Name Record (PNR) gegevens aan de Canadese autoriteiten worden doorgegeven met het oog op het gebruik, de bewaring en in voorkomend geval de latere doorgifte van gegevens, teneinde terrorisme en andere grensoverschrijdende criminaliteit te bestrijden.[66] Canada betreft een «derde land» in de zin van de AVG. Voor het doorgeven van persoonsgegevens naar landen buiten de Europese Unie stelt de AVG dat dit alleen mag als het door de AVG geboden beschermingsniveau niet wordt ondermijnd.[67] Deze uitspraak is relevant omdat hetgeen geldt voor derde landen, niet minder kan zijn dan de privacy-waarborgen die gelden voor lidstaten. Wat de noodzaak van de inmengingen betreft, bepaalt het Hof dat verschillende bepalingen van de overeenkomst verder gaan dan strikt noodzakelijk is en geen duidelijke en nauwkeurige regels bevatten:

«Op grond van artikel 3, lid 5, onder a) en b), van deze overeenkomst mag Canada, «per geval te beoordelen», PNR-gegevens tevens verwerken *«met het oog op de uitoefening door de overheid van toezicht* of verantwoordingsplicht», respectievelijk «teneinde te voldoen aan een gerechtelijke dagvaarding of een gerechtelijk bevel».
De bewoordingen van de gevallen waarin Canada krachtens artikel 3, lid 5, onder a) en b), van de voorgenomen overeenkomst PNR-gegevens mag behandelen zijn daarentegen zo vaag en algemeen dat zij *niet aan de gestelde vereisten van duidelijkheid en nauwkeurigheid* voldoen.[68]

Weliswaar ziet de iCOV op uitoefening van toezicht *op een goede werking van markt*, maar dat neemt niet weg dat sprake is van een weinig duidelijke en nauwkeurige bepaling.

Gelet op het voorgaande adviseert de AP om de wettelijke doelen van de samenwerkingsverbanden aan te scherpen.

c. Het startpunt van een signaal

Zoals vermeld eist het recht duidelijke en precieze regels en criteria in de wetgeving die inbreuk maakt op grondrechten. In dat verband is ook het startpunt voor een samenwerkingsverband om te worden geactiveerd naar het oordeel van de AP vaag.[69] Weliswaar bevat het voorstel een

---

[65] Een lidstaat, het Europees Parlement, de Raad of de Commissie kan op grond van artikel 218, lid 11 EU-Werkingsverdrag het advies inwinnen van het EU-Hof over de verenigbaarheid van een voorgenomen verdrag met de Verdragen of over de bevoegdheid om dit verdrag te sluiten. Indien het EU-Hof afwijzend adviseert, kan het voorgenomen verdrag niet in werking treden, tenzij na voorafgaande wijziging daarvan of na herziening van de EU-Verdragen.

[66] Daartoe voorziet het verdrag onder meer in een bewaartermijn van vijf jaar voor deze gegevens, in vereisten op het gebied van de beveiliging en de integriteit van de PNR-gegevens, in een onmiddellijke afscherming van gevoelige gegevens, in een recht om toegang tot de gegevens te krijgen, ze te laten verbeteren en ze te laten wissen, en in de mogelijkheid om administratieve en gerechtelijke rechtsmiddelen aan te wenden.

[67] De AVG was nog niet van toepassing ten tijde van het uitbrengen van het advies van het Hof van Justitie EU, maar de voorloper daarvan, de richtlijn 95/46, wel. Dat doet niet af aan de materiële overwegingen evenzeer gelden onder het regime van de AVG. Artikel 44 AVG bepaalt dat de Commissie kan besluiten dat een derde land een passend niveau van gegevensbescherming kent (adequaatheidsbesluit van de Commissie), of er kunnen aanvullende passende waarborgen worden geboden bij de doorgifte van gegevens (artikel 45 en 46 AVG). De voorgenomen overeenkomst strekt er dus toe een soort «adequaatheidsbesluit» in de zin van artikel 25, lid 6, van richtlijn 95/46 in het leven te roepen (overweging 31 van het advies).

[68] HvJ EU PNR, punt 181.

[69] Opmerking verdient dat het voorstel volgens het kabinet gaat over verdere verwerking, niet over de initiële vergaring (Kamerstukken II 2020/21, 35 447, nr. 6, blz. 52).

omschrijving in artikel 1 van een «signaal», namelijk: een melding van een of meer deelnemers in een samenwerkingsverband dat bepaalde gedragingen of situaties betreffende natuurlijke personen, rechtspersonen of fenomenen aanleiding kunnen zijn om ten behoeve van het doel van het samenwerkingsverband gezamenlijk gegevens te verwerken.[70]

Erg concreet is dit echter niet, en het wordt ook niet toegelicht aan de hand van duidelijke praktijkvoorbeelden. Wanneer is er «aanleiding»? Met name als het gaat om een signaal over het *voorkomen* van nieuwe criminaliteit lijkt dit erg vaag. Bovendien is een signaal erg zwak (en zodoende snel aanwezig) als het wordt afgezet tegen het resultaat van het samenwerkingsverband. Dat is namelijk omschreven als «een *eerste* vermoeden dat sprake is van onrechtmatige activiteiten waarop het verband zich richt». Blijkbaar is voor «aanleiding» minder nodig dan een «eerste vermoeden van een onrechtmatigheid. Ten slotte is niet duidelijk dat steeds een objectieve aanwijzing wordt vereist. Als de AP het goed ziet, wordt voor de iCOV zelfs helemaal geen signaal vereist om persoonsgegevens gezamenlijk te verwerken; wel is in het voorstel bepaald dat een rapportage van de iCOV alleen op verzoek van een deelnemer kan worden gedaan.[71]

Dat neemt niet weg dat een duidelijke regel naar het oordeel van het Hof van Justitie EU cruciaal is omdat hiermee misbruik van persoonsgegevens kan worden voorkomen. En, zoals eerder omschreven, vormt de eis van duidelijke en objectieve aanwijzingen naar het oordeel van de AP in feite ook de garantie voor het waarborgen van de onschuldpresumptie in ruime zin en het verschil met «mass surveillance» maatregelen.

In dit verband wijst de AP op artikel 7 van de recente Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven. Volgens deze implementatiewet verwerkt de Passagiersinformatie-eenheid (Pi-NL) de ontvangen passagiersgegevens met het oog op het beoordelen van de passagiers voorafgaand aan hun geplande aankomst in of geplande vertrek uit Nederland om te bepalen welke personen vanwege mogelijke betrokkenheid bij een terroristisch of ernstig misdrijf moeten worden onderworpen aan een nader onderzoek door een bevoegde instantie. In artikel 6, eerste lid, onderdeel c, wordt bepaald dat de Pi-NL bevoegd is passagiersgegevens te analyseren voor het opstellen van nieuwe of het bijstellen van bestaande criteria die worden gebruikt bij de beoordelingen die worden verricht om te bepalen welke personen betrokken zouden kunnen zijn bij een terroristisch of ernstig misdrijf. In artikel 7 worden voor het opstellen van de risico-criteria nadere regels gegeven. In artikel 7 van die wet is ten aanzien van de criteria die de Pi-NL

---

[70] Voor de *RIECS* bevat het voorstel enige voorschriften over type, aantal en gewicht van een signaal (artikel 2.23, tweede en derde lid). Bij amvb kunnen nadere regels worden gegeven over de criteria (artikel 2.23, negende lid). Voor het *FEC* geldt dat indien een deelnemer signalen heeft inzake bedreigingen of risico's van inbreuken op de integriteit van de financiële sector als bedoeld in artikel 2.2 kunnen deelnemers daarover overleggen. De criteria voor een signaal (aard, de eisen van kwaliteit en betrouwbaarheid waaraan het signaal moet voldoen)om te worden voorgedragen voor een signalenoverleg worden voor het FEC en voor het FEC bij amvb bepaald (artikel 2.6, tweede lid). Voor de *Zorg- en Veiligheidshuizen* geldt dat een deelnemer een casus voor overleg kan aanmelden bij een Zorg- en Veiligheidshuis naar aanleiding van «gedragingen van een betrokkene of een situatie waarin een betrokkene verkeert, die verband houden met het doel, bedoeld in artikel 2.25, en daartoe gegevens verwerken.»

[71] Wel voorziet artikel 2.14 in een delegatiegrondslag dat bij of krachtens algemene maatregel van bestuur regels worden gesteld over de wijze waarop indicatoren als bedoeld in artikel 2.13 worden vastgesteld.

gebruikt, bepaald wie ze vaststelt en aan welke eisen zij moeten voldoen, zoals doelgericht, evenredig en specifiek.[72]
Hoewel het voorliggende voorstel niet strekt tot implementatie van een Europese richtlijn, geeft het wel aan dat in de Richtlijn over een aanpalend terrein nadrukkelijk aandacht is voor de eisen aan de criteria om passagiers nader te onderzoeken.

Gelet op het voorgaande adviseert de AP om in de wet een duidelijk en objectief signaal op basis van voldoende aanwijzingen als startpunt neer te leggen voor alle samenwerkingsverbanden en tevens duidelijke voorbeelden te bespreken.

d. De categorieën van gegevens

Het recht eist ook dat zo veel mogelijk duidelijk is om welke gegevens het gaat. In het advies over de PNR-overeenkomst achtte het Hof bijv. «alle beschikbare contactgegevens» en «alle beschikbare betalingsfacturatie» niet precies genoeg.[73]

Gelet hierop is de vraag of de verstrekking van «financiële gegevens» of «gegevens betreffende zakelijke relaties» (artikel 2.22, eerste lid) in het kader van de RIEC's voldoende precies zal zijn. Daarbij verdient echter aantekening dat in het licht van de doelstelling van de RIEC's en dit samenwerkingsverband, namelijk het bestrijden van georganiseerde criminaliteit, het juist zal gaan om het verkrijgen van een zo compleet mogelijk financieel plaatje. Niet goed valt in te zien hoe dit doel kan worden bereikt met de verstrekking van slechts bepaalde, nader aangeduide, financiële gegevens.

Lastiger is artikel 2.30, eerste lid, dat betrekking heeft op gegevens genoemd die deelnemers in het kader van een Zorg -en Veiligheidshuis verstrekken: gegevens betreffende relaties met gezinsleden en andere directe sociale contacten. De aard van die gegevens is vervolgens in het wetsvoorstel wel nader afgebakend. Maar opmerkelijk is dat ook ten aanzien van deze derden weer gegevens betreffende gezinsleden en directe contacten kunnen worden verstrekt. Weliswaar dient de verstrekking steeds noodzakelijk te zijn, maar dit geeft ruimte om gegevens van personen die bovendien in een ver verband staan met de betrokkene, te verstrekken aan het verband en te betrekken in de analyse.

Gelet op het voorgaande adviseert de AP om – zo veel als mogelijk in het licht van de doelstelling van de verbanden – de categorieën van persoonsgegevens nader in de wet te beperken.

---

[72] Artikel 7 van de PNR-wet strekt tot uitvoering van artikel 6, vierde lid, van de Richtlijn 2016/681 en luidt: 1. De criteria, bedoeld in artikel 6, eerste lid, onderdeel c, worden door de Passagiersinformatie-eenheid in overeenstemming met de betrokken bevoegde instanties vastgesteld en regelmatig getoetst. 2. De criteria zijn doelgericht, evenredig en specifiek voor het misdrijf waarbij de mogelijke betrokkenheid van een persoon overeenkomstig de criteria kan worden bepaald. 3. De criteria zijn niet gebaseerd op godsdienst of levensovertuiging, ras of etnische afkomst, politieke gezindheid, gezondheid, seksuele leven of geaardheid of lidmaatschap van een vakvereniging van betrokkenen. 4. Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld over a.de wijze waarop de criteria worden opgesteld en bijgesteld; en b.de eisen waaraan de criteria en de toepassing ervan moeten voldoen.

[73] Punten 158 en 159 van het advies van het Hof van Justitie EU over de PNR-overeenkomst tussen EU en Canada. Anderzijds verdient opmerking dat in artikel 20, tweede lid, onderdeel c, van de PNR-wet «alle betalingsinformatie» wordt genoemd ter uitwerking van Richtlijn 2016/681.

e. Verstrekkingsplicht

Uitgangspunt voor verstrekking van persoonsgegevens die noodzakelijk zijn voor het doel van het verband, aan het samenwerkingsverband in het voorstel is «ja, tenzij zich zwaarwegende redenen daartegen verzetten» (artikel 1.5, eerste lid).[74] Het kabinet benadrukt daarmee dat de samenwerking niet vrijblijvend kan zijn.

Uit een oogpunt van het beginsel van subsidiariteit lijkt een verstrekkingsbevoegdheid minder vergaand dan een verplichting.[75] De grondslag van een *wettelijke verplichting* brengt verder mee dat voor betrokkene geen bezwaar mogelijk is. De verwerkingsgrondslag van een publieke taak (e-grondslag) past ook naar het oordeel van de AP beter dan de wettelijke verplichting (c-grondslag), omdat het meestal bestuursorganen zijn die persoonsgegevens verstrekken aan het samenwerkingsverband.

Gelet op het voorgaande adviseert de AP om de grondslag te wijzigen in een bevoegdheid.

f. Geautomatiseerde gegevensanalyse

De diverse activiteiten die de samenwerkingsverbanden verrichten met het oog op de respectievelijke wettelijke doelen zijn deels in de wet zelf neergelegde en bij amvb kunnen aanvullende activiteiten worden aangewezen.[76] Het gaat bij de activiteiten bijvoorbeeld om signalenoverleg of casusoverleg. Het voorstel bevat voor de iCOV expliciet de mogelijkheid van geautomatiseerde gegevensanalyse omdat de iCOV dit instrument nu al gebruikt; voor het FEC en de RIEC's is voorzien in een grondslag voor geautomatiseerde gegevensanalyse. Met geautomatiseerde gegevensanalyse wordt in het voorstel gedoeld op verwerkingsprocessen waarbij bijvoorbeeld wiskundige en statistische procedures worden gehanteerd. In geen geval zal er sprake zijn van geautomatiseerde besluitvorming door het samenwerkingsverband als bedoeld in artikel 22 AVG.[77]

In het eerdergenoemde bindend advies van het Hof van Justitie EU over de doorgifte van persoonsgegevens van luchtreizigers van de Unie naar Canada stelt het Hof dat de noodzaak om over dergelijke waarborgen te beschikken groter is wanneer de persoonsgegevens geautomatiseerd worden verwerkt en dat de mate waarin de geautomatiseerde verwerking van de PNR-gegevens een inmenging oplevert in de rechten die in de artikelen 7 en 8 zijn verankerd, hoofdzakelijk afhangt van de vooraf

---

[74] Artikel 1.5, eerste lid: Elke deelnemer verstrekt de bij of krachtens deze wet aangewezen categorieën van gegevens aan het samenwerkingsverband, voor zover dat noodzakelijk is voor het doel van het samenwerkingsverband, tenzij naar het oordeel van de deelnemer zwaarwegende redenen zich daartegen verzetten. Deze verplichting tot verstrekking is mede van toepassing indien een specifieke geheimhoudingsbepaling van toepassing is die het toelaat dat een ander wettelijk voorschrift daarop een uitzondering maakt. Er is geen schending van het beginsel van dataminimalisatie (artikel 5 AVG) omdat het steeds gaat om verstrekking van gegevens *noodzakelijk* voor het doel van het samenwerkingsverband.

[75] Vgl. nader het advies van de AP inzake toegang tot gegevens voor poortwachters bij het voorkomen van witwassen van 16 december 2019, blz. 13 (z2019-21482).

[76] Het gaat dan bijvoorbeeld om de mogelijkheid van profilering voor de RIEC's (artikel 2.18, tweede lid). Profilering is elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

[77] Kamerstukken II 2019/20, 35 447, nr. 3. blz. 52.

vastgestelde modellen en criteria en de databases waarop dit type van gegevensverwerking is gebaseerd.[78]

Hierbij sluit artikel 1.9 aan, dat bijzondere waarborgen voor geautomatiseerde gegevensanalyse bevat.
Maar juist gelet op de omstandigheid dat de mate van inmenging op het recht op bescherming van persoonsgegevens bij geautomatiseerde verwerking grotendeels afhangt van de modellen, criteria en de databases, waarop dit type van gegevensverwerking is gebaseerd, valt op dat hierop niet is ingegaan.[79] Artikel 1.9, derde lid, verplicht bovendien tot transparantie over de gehanteerde patronen en indicatoren of andere onderliggende logica. In de toelichting op dit artikel wordt ook onderkend dat dit een belangrijke waarborg is, waarbij is verwezen naar de SyRI-uitspraak van de rechtbank.[80]

Gelet op het voorgaande en het gestelde onder 3.2.c adviseert de AP om, zo veel als mogelijk is, inzicht te verschaffen in de modellen, criteria en databases die worden gehanteerd bij geautomatiseerde gegevensanalyse.

g. Bewaren

Volgens artikel 1.8, zevende lid, worden persoonsgegevens die door het samenwerkingsverband gezamenlijk worden verwerkt, vernietigd of geanonimiseerd zodra zij niet langer noodzakelijk zijn voor het doel van het samenwerkingsverband, en worden in ieder geval uiterlijk vijf jaar na de datum van eerste verwerking verwijderd uit de systemen van het samenwerkingsverband of geanonimiseerd, tenzij een wettelijk voorschrift daaraan in de weg staat of de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering. In bijzondere gevallen en voor zover dat noodzakelijk is voor het doel van het samenwerkingsverband kunnen persoonsgegevens die worden bewaard, in opdracht van de deelnemers, na verkregen instemming van de deelnemer die de betreffende persoonsgegevens heeft verstrekt, ter beschikking worden gesteld voor hernieuwde verwerking.

Over deze bepaling heeft de AP de volgende opmerkingen.

In de eerste plaats is onduidelijk wanneer persoonsgegevens niet langer noodzakelijk zijn voor het doel van het samenwerkingsverband en «verwijderd worden uit het systeem of geanonimiseerd.» Wanneer een verwerking door een samenwerkingsverband geen sturingsinformatie heeft opgeleverd, kan het voor het verband toch «handig» zijn om de persoonsgegevens nog te bewaren om eventueel later te kunnen gebruiken.

In dit verband verwijst de AP naar het bindend advies van het Hof over de PNR overeenkomst over de doorgifte en verwerking van gegevens uit het Passenger Name Record (PNR-overeenkomst). De PNR gegevens worden in beginsel 5 jaar bewaard. Het Hof stelt over de bewaring van de PNR-gegevens ten aanzien van reizigers die zijn gecontroleerd en ten aanzien waarvan geen risico is vastgesteld dat er, zodra zij vertrokken zijn, tussen hun PNR-gegevens en de doelstelling van de voorgenomen

---

[78] Advies Hof PNR-overeenkomst, punt 172.

[79] Vgl. in breder verband, het advies van de Raad voor openbaar bestuur, Sturen of gestuurd worden? De Raad vindt dat het openbaar bestuur de legitimiteit van sturen met data kan waarborgen door publieke verantwoording over sturen met data beter te organiseren.

[80] Vgl. voorts voor wat betreft de mogelijke regeling van profilering door de RIEC's op de conclusie ECLI:NL:PHR:2021:618 17 juni 2021 waarin naar voren komt dat profilering specifieke wettelijke eisen vergt en de noodzaak om te onderscheiden tussen harde en zachte informatie.

overeenkomst geen verband lijkt te bestaan te bestaan dat de *bewaring* van deze gegevens rechtvaardigt.

Mede gelet hierop hecht de AP eraan te onderstrepen dat indien de analyse en bewerkingen door het samenwerkingsverband geen aanwijzingen voor risico's met het oog op de doelen van het verband of sturingsinformatie hebben opgeleverd, er in beginsel geen grond is voor het samenwerkingsverband om de persoonsgegevens te bewaren. De AP adviseert uitdrukkelijk te bepalen dat in dat geval de persoonsgegevens worden gewist en adviseert tevens in te gaan op een intern adequaat controlemechanisme terzake.

Op de tweede plaats is de uitzonderingsmogelijkheid in de tweede volzin die erin voorziet om in «bijzondere gevallen» een hernieuwde verwerking toe te passen, ruim en onduidelijk. In de toelichting wordt hierop ook niet nader ingegaan, zodat een rechtvaardiging ontbreekt. Naar het oordeel van de AP zal het hier uitsluitend kunnen gaan om gevallen waarin sprake is van «nova», dus nieuwe feiten of omstandigheden. Met het oog op het voorkomen van misbruik, adviseert de AP om de clausule over bijzondere gevallen nader te preciseren en te motiveren.

h. Verstrekking resultaten aan derden

Daarnaast dient het *gebruik* van bewaarde gegevens door deelnemers en derden volgens het Hof in zijn advies over de PNR-overeenkomst te worden gebaseerd op *objectieve criteria* en moet het worden onderworpen aan *voorafgaande controle door een rechterlijke instantie of onafhankelijke bestuurlijke autoriteit.*[81] Volgens het voorstel wordt aan de deelnemers sturingsinformatie verschaft en *kan* dit ook aan derden plaatsvinden onder de voorwaarden in artikel 1.7, tweede lid.[82]

Als waarborg is opgenomen dat elk samenwerkingsverband een rechtmatigheidsadviescommissie[83] dient in te stellen die toetst of verstrekking van resultaten aan *derden* is toegestaan.[84] Een rechtmatigheidsadviescommissie bestaat doorgaans uit privacy-experts en compliance deskundigen en beoordeelt in ieder geval de rechtmatige verwerking van persoonsgegevens in het samenwerkingsverband, aldus de toelichting.[85] De inrichting van deze commissie en de gehanteerde

---

[81] Het Hof stelt: «Het gebruik van de aldus opgeslagen PNR-gegevens moet worden gebaseerd op objectieve criteria ter bepaling van de omstandigheden waarin en de voorwaarden waarop de in de voorgenomen overeenkomst bedoelde Canadese autoriteiten toegang kunnen krijgen tot deze gegevens met het oog op het gebruik ervan. Tevens moet dit gebruik – behalve in naar behoren gerechtvaardigde dringende gevallen – worden onderworpen aan een voorafgaande controle door hetzij een rechterlijke instantie, hetzij een onafhankelijke bestuurlijke entiteit, waarvan de beslissing houdende toelating van het gebruik wordt gegeven naar aanleiding van een gemotiveerd verzoek dat de voornoemde autoriteiten met name in het kader van een procedure ter voorkoming, opsporing of vervolging van strafbare feiten hebben ingediend.»

[82] Artikel 1.7, tweede lid: Tenzij een deelnemer daartegen bezwaar heeft, kunnen de resultaten van de verwerking binnen het samenwerkingsverband aan een *derde* worden verstrekt, voor zover de verstrekking bij of krachtens deze wet van een grondslag is voorzien, de verstrekking door de rechtmatigheidsadviescommissie, bedoeld in artikel 1.8, zesde lid, op rechtmatigheid is getoetst en de verstrekking noodzakelijk is voor:
a. de vervulling van een publiekrechtelijke taak die aan de derde is opgedragen, wanneer deze taak verenigbaar is met het doel van het samenwerkingsverband, of
b. de behartiging van de gerechtvaardigde belangen of uitvoering van wettelijke verplichtingen van een private derde, wanneer deze belangen of verplichtingen verenigbaar zijn met het doel van het samenwerkingsverband.

[83] Artikel 1.8, zesde lid.

[84] Artikel 1.7, tweede lid.

[85] Kamerstukken II 2019/20, 35 447, nr. 3, blz. 72.

werkwijze hoeven volgens de toelichting niet in de wet geregeld, maar kan bij amvb.[86]

Naar het oordeel van de AP staat daarmee niet vast dat deze commissie voldoende «onafhankelijk» is in de zin van genoemde rechtspraak van het Hof van Justitie EU; bovendien is slechts sprake van een advies.

In dat verband wijst de AP ook op de recente Wet gebruik van passagiersgegevens voor de bestrijding van terroristische en ernstige misdrijven.[87] In die wet is -ter implementatie van artikel 12 van de richtlijn 2016/681- de bewaartermijn van de passagiersgegevens en het gebruik van gegevens door andere bevoegde autoriteiten met nadere waarborgen omgeven. Naarmate de bewaring langer is dan zes maanden, gelden zwaardere waarborgen voor het gebruik. Het gaat om de eis dat passagiersgegevens na zes maanden dienen te worden gedepersonaliseerd en de eis dat mededeling aan andere autoriteiten na zes maanden alleen mogelijk is na toestemming van de officier van justitie en kennisgeving aan de functionaris gegevensbescherming. Dit geeft aan dat het Europees recht zwaardere voorwaarden stelt aan het gebruik van passagiersgegevens naarmate de bewaring langer duurt. Eenzelfde idee zou ook bij het voorliggende voorstel passend zijn.

De AP adviseert om te voorzien in de waarborg van een voorafgaande toets door een onafhankelijke bestuurlijke autoriteit bij gebruik door derden van door het samenwerkingsverband bewaarde persoonsgegevens.

Een en ander klemt te meer nu volgens het kabinet het voorstel ook «cross sectorale gegevensdeling» tussen private en publieke partijen omvat.[88] Op grond van de Uitvoeringswet AVG is het delen van persoonsgegevens van strafrechtelijke aard ten behoeve van derden afhankelijk van een vergunning van de AP.[89] Daarbij is vereist dat bij de uitvoering wordt voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van betrokkene niet onevenredig wordt aangetast. De AP staat zeer kritisch tegenover cross sectorale gegevensdeling tussen private partijen. Volgens de recente handreiking van de AP is uitgangspunt dat het cross-sectoraal delen tussen private partijen van gegevens op een zwarte lijst niet is toegestaan.[90] Dit omdat de gegevens in meerdere sectoren terecht kunnen komen en daarmee grote gevolgen kunnen hebben voor de betrokkene.

---

[86] Artikel 1.8, zesde lid.

[87] Wet van 5 juni 2019, houdende regels ter implementatie van richtlijn (EU) 2016/681 van het Europees Parlement en de Raad van 27 april 2016 over het gebruik van persoonsgegevens van passagiers (PNR-gegevens) voor het voorkomen, opsporen, onderzoeken en vervolgen van terroristische misdrijven en ernstige criminaliteit (PbEU 2016, L 119), Staatsblad 2019, 205.

[88] Kamerstukken II 2020/21 35 447, nr. 6, blz. 53.

[89] Artikel 33, vierde lid, Uitvoeringswet AVG. Vgl. ook Kamerstukken 2018/19, 17 050, nr. 576, blz. 5.e.v.

[90] Handreiking cross sectorale gegevensdeling tussen private partijen, AP 15 juli 2021. Er is sprake van een cross-sectorale zwarte lijst als private partijen een zwarte lijst willen gaan delen met andere private partijen buiten hun eigen sector. Voorbeelden van sectoren zijn: detailhandel, toerisme, horeca, logistieke sector, financiële sector, telecomsector, etc. Bij een cross-sectorale zwarte lijst vindt het delen niet enkel plaats in een sector, maar worden de gegevens in diverse sectoren gedeeld.

De AP adviseert in het licht van het voorgaande in te gaan op de noodzaak voor en specifieke waarborgen bij het cross sectoraal delen van gegevens tussen (private) derden, in het bijzonder wat betreft persoonsgegevens van strafrechtelijke aard.[91]

i. Sturingsinformatie als resultaat

Opvallend is dat het kabinet stelt dat de uitkomst van een analyse waaraan het OM of de opsporing deelneemt *geen* verdenking oplevert, maar alleen «sturingsinformatie».[92]

«Zij kunnen de uitkomst van een analyse meewegen bij de beslissing over het al dan niet starten van het strafrechtelijk onderzoek. Van een verandering van de voorschriften in het Wetboek van Strafvordering met betrekking tot het vorderen van gegevens is geen sprake. Wel geeft het wetsvoorstel een betere basis voor het verstrekken van informatieproducten aan OM en opsporingsdiensten uit een samenwerkingsverband waaraan zij deelnemen, in een fase waarin (nog) geen verdenking bestaat.»[93]

De AP heeft hierover drie opmerkingen. In de eerste plaats is onwaarschijnlijk dat de uitkomst van een analyse van de gegevens van verschillende deelnemers waaraan politie en justitie deelnemen, geen verdenking kan opleveren. Aan een op feiten of omstandigheden gebaseerd redelijk vermoeden van schuld aan enig strafbaar feit in de zin van artikel 27 van het Wetboek van Strafvordering (Sv) wordt in de strafrechtspraak vrij snel voldaan, zoals bijvoorbeeld een anonieme tip. Bovendien impliceert reeds de titel van «infobox *crimineel* en verklaarbaar vermogen» dat in voorkomende gevallen wel degelijk sprake zal zijn van een verdenking als uitkomst van de behandeling door het samenwerkingsverband. Gesteld is in de toelichting dat de rapportages van de iCOV inzichtelijk maken waar het *criminele* of fiscaal ontdoken vermogen wordt verborgen: «Ze tonen tevens *welke sleutelfiguren* zich hiermee bezighouden.»[94]

Op de tweede plaats lijkt sprake van een cirkelredenering in de zin dat het OM en andere opsporingsambtenaren sturingsinformatie kunnen krijgen, maar zij zitten al als deelnemer «aan tafel» bij het samenwerkingsverband.

Op de derde plaats is gesteld dat van «een verandering van de voorschriften in het Wetboek van Strafvordering met betrekking tot het vorderen van gegevens geen sprake is». Dat is echter kort door de bocht, omdat het belang van deze strafvorderlijke bevoegdheid door de nieuwe wet wel sterk afneemt. Zo bepaalde in 2011 de Rechtbank Utrecht dat als

---

[91] Vgl. ook artikel 10 AVG: Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen mogen op grond van artikel 6, lid 1, alleen worden verwerkt onder toezicht van de overheid of indien de verwerking is toegestaan bij Unierechtelijke of lidstaatrechtelijke bepalingen *die passende waarborgen* voor de rechten en vrijheden van de betrokkenen bieden. Omvattende registers van strafrechtelijke veroordelingen mogen alleen worden bijgehouden onder toezicht van de overheid.

[92] Sturingsinformatie is omschreven in het voorstel als: gegevens betreffende natuurlijke personen, rechtspersonen of fenomenen, inhoudende een eerste vermoeden dat sprake is van onrechtmatige activiteiten, of voornemens daartoe, op de bestrijding waarvan het samenwerkingsverband is gericht, met inbegrip van de onderliggende gegevens uit een risicoanalyse, ten behoeve van de uitvoering van publiekrechtelijke taken of uitoefening van publiekrechtelijke bevoegdheden (artikel 1.1).

[93] Kamerstukken II 2019/2020 35 447, nr. 3, blz. 53.

[94] Vgl. Kamerstukken II 2019/20 35 447, nr. 3, blz. 54: «Wat betreft het onthouden van een hypotheek wordt opgemerkt dat als het doel van het samenwerkingsverband fraudebestrijding is, het juist beoogd is dat verstrekking aan een (private) deelnemer mogelijk is voor het doel van dat samenwerkingsverband. In dat geval is het onthouden van een hypotheek aan bijv. een *hypotheekfraudeur* een goede uitkomst (curs, AP)».

sprake is van een samenwerkingsverband van verschillende opsporingsdiensten voor de aanpak van georganiseerde misdaad, waartoe een convenant was afgesloten, dat dit convenant onvoldoende waarborgen geeft om voor de gegevensuitwisseling artikel 126nd Sv opzij te zetten. Een vordering op grond van het Wetboek van Strafvordering blijft noodzakelijk, aldus de rechtbank.[95]
Voor toepassing van de strafvorderlijke bevoegdheden tot het vorderen van gegevens (Titel IVA, Negende afdeling) wordt steeds een verdenking van een misdrijf vereist. Als het gaat om bijzondere gegevens, gelden bovendien zwaardere voorwaarden. Na de inwerkingtreding van het wetsvoorstel lijkt zo'n vordering aan een samenwerkingsverband echter veelal niet nodig zijn omdat al in de fase voordat sprake is van een strafvorderlijke verdenking wegens een misdrijf de uitkomst van het samenwerkingsverband waaraan politie en justitie deelneemt, al aan politie en justitie wordt verstrekt. Daarmee is *de facto* sprake van een grote verruiming van de strafvorderlijke bevoegdheden tot het vorderen van gegevens omdat de uitkomst en gegevens uit het samenwerkingsverband zonder vordering van strafvorderlijke autoriteiten en zonder verdenking van een misdrijf aan de strafvorderlijke overheid worden verstrekt, sterker nog: de strafvorderlijke overheid zit steeds aan tafel.

De AP adviseert in te gaan op de verhouding van de verstrekking door het verband van de uitkomst aan politie en justitie tot de bevoegdheden tot het vorderen van gegevens in strafvordering, meer in het bijzonder op de genoemde drie punten.

j. Operationele conclusie punt 3.2

Gelet op het voorgaande adviseert de AP om meer zorgvuldige afwegingen te maken ten aanzien van nut en noodzaak van wettelijke regeling van bepaalde samenwerkingsverbanden. Dit geldt met name:
- de noodzaak van de verbanden die in het teken staan van het aanpakken witwassen, dragend motiveren in het licht van bestaande en aankomende (wettelijke) maatregelen ter bestrijding van witwassen;
- het preciseren van de wettelijke doelen van het FEC, van, met name, het voorkomen en bestrijden van «ernstige criminaliteit»;
- het schrappen van de voorgestelde doelen van de iCOV van het innen van dreigende overheidsvorderingen en het uitoefenen van toezicht op de markt;
- een duidelijk en objectief signaal op basis van voldoende aanwijzingen in de wet als startpunt voor alle samenwerkingsverbanden met duidelijke voorbeelden;
- de clausule over «bijzondere gevallen» waarin een hernieuwde verwerking kan plaatsvinden, preciseren en verduidelijken;
- te voorzien in de waarborg van een voorafgaande toets door een onafhankelijke bestuurlijke autoriteit bij gebruik door derden van door het samenwerkingsverband bewaarde persoonsgegevens;
- de verwerkingsgrondslag voor verstrekking aan de samenwerkingsverbanden wijzigen van een wettelijke verplichting in een publieke taak;
- inzicht verschaffen in de modellen, criteria en databases die zoal worden gehanteerd bij geautomatiseerde gegevensanalyse;
- de verhouding bezien tot de strafvorderlijke bevoegdheid tot het vorderen van gegevens.

[95] Rb. Utrecht 26 augustus 2011, ECLI:NL:RBUTR:2011:BR5923.

3.3. Aanwijzing nieuwe samenwerkingsverbanden bij amvb

Een wezenlijk punt van de AP bij de eerdere concepten was het ontbreken van betrokkenheid van de wetgever bij de samenwerkingsverbanden.[96] Hieraan is deels tegemoetgekomen door vier samenwerkingsverbanden in het wetsvoorstel zelf te regelen in plaats van bij amvb.

Volgens het huidige voorstel is aanwijzing van een samenwerkingsverband bij amvb uitsluitend mogelijk als bij amvb doeleinden worden omschreven die passen binnen het raamwerk van hoofdstuk 3:
a. het voorkomen en bestrijden van ernstige vormen van criminaliteit;
b. het voorkomen van grootschalig of systematisch onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen; of
c. het voorkomen van grootschalige of systematische ontduiking van wettelijke verplichtingen tot betaling van belastingen, retributies en rechten bij in- en uitvoer.

De motivering voor de mogelijkheid van aanwijzing van nieuwe samenwerkingsverbanden bij amvb is het bevorderen van flexibiliteit.[97] De vraag is echter of er een voldoende noodzaak bestaat voor deze flexibiliteit. In de eerste plaats worden thans vier verbanden in de wet opgenomen. Kennelijk bestaat er nu geen noodzaak om andere samenwerkingsverbanden in de wet op te nemen. Daarnaast wordt de wet na vijf jaar geëvalueerd en mogelijk aangepast. Bij deze stand van zaken adviseert de AP om eerst ervaring op te doen met de wettelijke verbanden en – zo nodig – na wetsevaluatie te komen tot aanpassing.

Daarnaast geldt ook hier (zie punt 3.2, onder b) dat de wettelijke doelen niet «welbepaald» in de zin van artikel 5 AVG en artikel 4 van de Richtlijn gegevensbescherming opsporing en vervolging zijn omschreven: wat is precies «het voorkomen en bestrijden van ernstige criminaliteit»[98] en «grootschalig of systematisch[99]»?

Bovendien veronderstelt artikel 10, derde lid, van de Grondwet dat de crux van de regeling die de bescherming van persoonsgegevens beperkt, in de wet zelf wordt opgenomen.[100] Daaronder valt naar het oordeel van de AP hier in elk geval de precieze doelstelling, de deelnemende partijen, waaronder met name ook private partijen, en de categorieën van bijzondere persoonsgegevens. Op cruciale onderdelen wordt nu juist de

---

[96] Aanvullend advies AP van 19 april 2019, blz. 4. Vgl. ook het advies van de Afdeling advisering.

[97] Kamerstukken II 2019/20, 35 447, nr. 3. blz. 1.

[98] Vgl. de Nota naar aanleiding van het verslag (Kamerstukken II 2020/21, 35 447, nr. 6, 129): «Onder «het voorkomen en bestrijden van ernstige vormen van criminaliteit» in de zin van artikel 3.1, onderdeel a, *moet in ieder geval* worden verstaan het voorkomen en bestrijden van «misdrijven die een ernstige inbreuk op de rechtsorde opleveren». Dergelijke formules komen voor in artikel 10 Wpg, diverse artikelen uit het Wetboek van Strafvordering en artikel 3.22 Telecommunicatiewet. Aangezien het in dit wetsvoorstel niet alleen gaat om misdrijven, maar ook om bestuurlijk beboetbare feiten, is gekozen voor de bredere term «criminaliteit» in plaats van «misdrijven». (...) Deze voorbeelden moeten omwille van de toekomstbestendigheid en flexibiliteit overigens *niet uitputtend* worden opgevat, maar zij geven een indicatie van de ernst van de criminaliteit in de zin van het voorgestelde artikel 3.1, onderdeel a, van het onderhavige wetsvoorstel.» (curs; AP).

[99] Vgl. de Nota naar aanleiding van het verslag (Kamerstukken II 2020/21 35 447, nr. 6, blz. 130): «De onderdelen b en c van artikel 3.1 dienen mutatis mutandis op dezelfde wijze als onderdeel a te worden gelezen voor wat betreft het vereiste grootschalige of systematische karakter van de in onderdelen b en c bedoelde vormen van onrechtmatig gebruik van overheidsgelden en overheidsvoorzieningen of van ontduiking van wettelijke verplichtingen tot betaling van belastingen, retributies en rechten bij in- en uitvoer.»

[100] Artikel 10, derde lid, van de Grondwet luidt: De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens. Vgl. het advies van de Afdeling advisering Raad van State (Kamerstukken II 2019/20, 35 447, nr. 4, blz. 26).

bevoegdheid tot regeling gelaten aan de regering, zij het met voor-[101] en nahangprocedure.[102] Daarmee ontbreekt echter de volle betrokkenheid van het parlement als medewetgever bij formele wetten en bovendien biedt een formele wet de burger meer rechtszekerheid dan een amvb, temeer nu het bij nieuwe samenwerkingsverbanden waarschijnlijk eveneens om ernstige inbreuken op het recht op bescherming van persoonsgegevens gaat. Het kan niet zo zijn dat voor meer beperkte inbreuken op het grondrecht een formele wet wordt vereist, waar ernstige inbreuken in beginsel worden vastgesteld door de regering.

Gelet op het voorgaande adviseert de AP om de mogelijkheid van aanwijzing van samenwerkingsverbanden bij amvb uit het wetsvoorstel te schrappen.

3.4 Coördinerend functionaris voor gegevensbescherming

Voorgesteld is dat de deelnemers één van de functionarissen voor gegevensbescherming (fg) van de deelnemende overheidsinstanties of overheidsorganen aanwijzen als coördinerend functionaris voor gegevensbescherming voor het samenwerkingsverband (artikel 1.4, tweede lid). De coördinerend functionaris voor gegevensbescherming is een aanspreekpunt voor deelnemers naast de eigen functionaris voor gegevensbescherming die het eerste aanspreekpunt blijft voor bestuurders van de afzonderlijke deelnemers. Deze coördinerend functionaris voor gegevensbescherming heeft een coördinerende en faciliterende taak en moet samenwerken met de andere fg's van de deelnemers om te proberen tot consensus te komen, aldus de toelichting.[103]

Taken van de functionaris gegevensbescherming zijn met name het informeren en adviseren van de verwerkingsverantwoordelijke en verwerkers en toezien op de naleving van de AVG (artikel 39 AVG). De vraag is hoe deze rol van coördinerend functionaris zich verhoudt tot de onafhankelijkheid van de functionaris gegevensbescherming en de eis in artikel 38, zesde lid, van de AVG dat andere taken of plichten niet tot een belangenconflict leiden. De rol van coördinerend functionaris hoeft immers niet samen te vallen met de rol van functionaris van de «eigen» deelnemende organisatie.

Gelet op het voorgaande is de positie van de coördinerend functionaris gegevensbescherming onduidelijk en problematisch in het licht van de eis van onafhankelijkheid in de AVG.

3.5. Amendement delen van persoonsgegevens tussen verbanden

Een aantal door de Tweede Kamer aangenomen amendementen is uit een oogpunt van bescherming van persoonsgegevens te kenschetsen als positief, zoals de mogelijkheid van het parlement om de uitbreiding van

---

[101] In onder meer artikel 2.22, tweede lid, is een «voorhangprocedure» opgenomen voor aanvulling van de categorieën van gegevens. Bij een voorhangprocedure wordt het ontwerp voor een amvb voorgelegd aan beide Kamers van de Staten-Generaal, vóórdat dit ontwerp wordt aangeboden aan de Afdeling advisering van de Raad van State.

[102] Het voorgestelde hoofdstuk 3 regelt dat met een «nahangprocedure» nieuwe samenwerkingsverbanden onder de werking van de WGS kunnen worden gebracht. Deze nahangprocedure houdt in dat na publicatie van een vastgestelde amvb elk van beide Kamers van de Staten-Generaal een periode van vier weken krijgt waarin zij bij meerderheid van stemmen kan verzoeken om het in de amvb geregelde onderwerp bij wet te regelen. In dat geval wordt de amvb onverwijld ingetrokken en wordt een daartoe strekkend wetsvoorstel zo spoedig mogelijk ingediend (Vgl. Kamerstukken II 2020/21, 35 447, nr. 19).

[103] Kamerstukken II 2019/20, 35 447, nr. 3, blz. 66.

samenwerkingsverbanden vooraf goed te keuren[104] en het niet hanteren van algoritmes waarvan de uitkomsten niet navolgbaar of controleerbaar zijn.[105]

Ook is aangenomen het amendement van het lid Yesilgöz-Zegerius over het opnemen van een grondslag voor het delen van gegevens tussen samenwerkingsverbanden.[106] Het delen van gegevens uit het samenwerkingsverband met een ander samenwerkingsverband is volgens indiener niet zonder meer mogelijk. De indiener vindt dat hiervoor in deze wet een duidelijke grondslag moet worden geboden.

«Zo kan bijvoorbeeld een RIEC resultaten delen met Zorg- en Veiligheidshuizen wanneer criminele familieleden inwonen bij kinderen met jeugdzorgproblematiek ten einde de oorzaken beter te kunnen duiden en de kinderen beter te kunnen helpen.»

In de eerste plaats is de noodzaak van dit amendement niet duidelijk. Volgens de memorie van toelichting bij het eerdere voorstel biedt artikel 1.7, tweede lid, namelijk al de mogelijkheid om de resultaten van de verwerking aan een derde te verstrekken, waaronder ook de deelnemers van een ander samenwerkingsverband kunnen vallen.[107] Ervan uitgaande dat onder inwonende «criminele familieleden» worden verstaan inwonende familieleden die (onherroepelijk) zijn veroordeeld wegens bepaalde strafbare feiten, wijst de AP erop dat persoonsgegevens van natuurlijke personen uit de directe kring van betrokkene al binnen het voorstel vallen. Daaronder vallen namelijk ook justitiële en strafvorderlijke en tenuitvoerleggingsgegevens (artikel 2.30, eerste lid).

Wezenlijker is het in het licht van het beginsel van dataminimalisatie een vergaande stap om persoonsgegevens uit een samenwerkingsverband met een ander verband te delen,[108] temeer voor zover de doelen en werkwijzen van het verband aangaande de Zorg- en Veiligheidshuizen, zoals het kabinet zelf aangeeft, fundamenteel verschillen met de andere drie verbanden om een algemene regeling te treffen. Dat lijkt ook opnieuw een uitzondering op het doelbindingsbeginsel (zie punt 1).

Gelet op het voorgaande adviseert de AP de mogelijkheid om persoonsgegevens te delen tussen de ZVH en de andere drie verbanden te schrappen.

---

[104] Kamerstukken II 2019/20, 35 447, nr. 11.

[105] Kamerstukken II 2019/20, 35 447, nr. 13.

[106] Kamerstukken II 2019/20 35 447, nr. 14. Artikel 1.7, achtste lid: De resultaten van de verwerking binnen het samenwerkingsverband kunnen worden verstrekt aan een ander samenwerkingsverband als bedoeld in deze wet, voor zover de verstrekking noodzakelijk is voor het doel van het ontvangende samenwerkingsverband en uitsluitend voor zover de deelnemers die de betreffende persoonsgegevens aan het samenwerkingsverband hebben verstrekt, daarmee instemmen. Ter vaststelling of de betrokkene bekend is bij een ander samenwerkingsverband, kunnen de deelnemers van de beide samenwerkingsverbanden identificerende en contactgegevens alsmede het burgerservicenummer van die betrokkene uitwisselen.

[107] Kamerstukken II 2019/20, 35 447, nr. 3, blz. 56.

[108] Vgl. Kamerstukken II 2019/20, 35 447, nr. 3, blz. 61: «Dit wetsvoorstel regelt de gezamenlijke gegevensverwerking voor vier samenwerkingsverbanden. Het doel, de werkwijze, en de aard van de gegevens die aan de orde kunnen zijn bij de verschillende samenwerkingsverbanden is soms fundamenteel verschillend. Dit speelt met name bij de Zorg- en Veiligheidshuizen ten opzichte van de andere drie samenwerkingsverbanden die dit wetsvoorstel regelt. Om die reden bevat dit wetsvoorstel geen specifieke bepalingen die het mogelijk maken om gegevens uit te wisselen tussen de Zorg- en Veiligheidshuizen en de andere samenwerkingsverbanden. De doelen en werkwijzen van de samenwerkingsverbanden liggen daarvoor te ver uit elkaar om hiervoor een generieke regeling te treffen.»

4. Facultatieve en harmoniserende karakter

Het oorspronkelijke wetsvoorstel was vormgegeven als brede kaderwet. Naar aanleiding van het advies van de AP en de Afdeling advisering van de Raad van State bij het oorspronkelijke wetsvoorstel is het wetsvoorstel ingrijpend aangepast en zijn hoofdelementen van de gezamenlijke gegevensverwerking in het wetsvoorstel opgenomen voor de vier samenwerkingsverbanden.[109]

Een doelstelling van het voorstel is harmonisatie. Dat geldt voor de regeling van de vier verbanden en mogelijk de nieuwe verbanden in een amvb op basis van het voorstel. Maar in andere wetgeving kunnen en zullen andere samenwerkingsverbanden ontstaan. Het is volgens het kabinet niet mogelijk of nodig met name vanwege de verscheidenheid in verbanden om alle samenwerkingsverbanden te harmoniseren.[110]

Als de regeling voor aanwijzing bij amvb uit hoofdstuk 3 wordt geschrapt (zie punt 3), wordt de harmonisatiedoelstelling nog verder beperkt. Dan lijkt het passender om de noodzakelijke samenwerkingsverbanden in sectorale wetgeving op te nemen, zodat de wettelijke regeling zo precies mogelijk op de situatie kan worden afgestemd.

5. Reactie op specifieke vragen

De Eerste Kamer heeft twee specifieke vragen gesteld, die hieronder worden beantwoord.

a. Is voldoende afgebakend wie toegang tot de systemen heeft?

In het voorgestelde artikel 1.8, tweede lid, is voorzien in een aantal waarborgen voor toegang tot de systemen:

2. Uitsluitend door de deelnemers geautoriseerde personen hebben toegang tot de systemen waarin de deelnemers gezamenlijk persoonsgegevens verwerken. De deelnemers onderhouden een systeem van autorisaties dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Geautoriseerd worden slechts personen die zijn aangewezen ten behoeve van de inzet in het samenwerkingsverband en die zijn belast met:
   a. de uitvoering van de gegevensverwerking voor de doelen van het samenwerkingsverband,
   b. de toetsing op rechtmatigheid, of
   c. het onderhoud of de ondersteuning van de systemen.
3. Bij of krachtens algemene maatregel van bestuur kunnen regels worden gesteld omtrent de betrouwbaarheidsvereisten aan geautoriseerde personen als bedoeld in het tweede lid.

De controle op de naleving van de waarborgen, zoals vast te stellen bij amvb op basis van de artikelen 1.8 en 1.9, zal, voor zover het om informatiebeveiliging en – als onderdeel daarvan – het invoeren van een geaccrediteerd systeem van autorisaties gaat, moeten worden ingericht volgens de daarop betrekking hebbende richtlijnen van de Minister van Binnenlandse Zaken en Koninkrijksrelaties. Het gaat daarbij om de Baseline Informatiebeveiliging Overheid (BIO). De BIO bevat ook richtlijnen voor het uitvoeren van beveiligingsupdates en het laten uitvoeren van reguliere audits teneinde te controleren dat de systematiek van autorisaties actueel en veilig blijft. Deze borgen ook dat bijvoorbeeld

---

[109] Aanvullend advies van de AP van 19 april 2019 en Kamerstukken II 2019/20, 35 447, nr. 4, blz. 26.

[110] Kamerstukken II 2019/20, 35 447, nr. 3, blz. 33.

personen die toegang hadden tot de systemen, geen toegang meer zullen hebben nadat zij niet meer geautoriseerd zijn, aldus de toelichting.[111]

Opvallend is dat voor wat betreft de veiligheidshuizen deelnemers ook op incidentele basis *derden* toegang kunnen verlenen.[112] Bij of krachtens amvb kunnen nadere regels worden gesteld over incidentele deelname van derden aan het overleg. Voor deze derden is onduidelijk welke criteria voor toegang gelden. Het verdient aanbeveling om hierin uitdrukkelijk te voorzien.

De voorgestelde wettelijke regeling met de mogelijkheid om nadere regels te stellen lijkt overigens voldoende om de toegang tot de systemen adequaat te reguleren.

Natuurlijk komt het uiteindelijk aan op de toepassing in de praktijk door de deelnemers. In dit verband wijst de AP op, onder meer, de volgende kritische opmerkingen van de Inspectie Justitie en veiligheid over screening van medewerkers van partners van uit 2017:[113]

«De Inspectie constateert dat de wijze waarop thans de screening van bij het samenwerkingsverband betrokken personen geregeld is en uitgevoerd wordt, niet bijdraagt aan het vertrouwen om informatie met elkaar te delen.»

«Omdat het niet screenen van gemeenteambtenaren over het algemeen een zorgpunt is voor de partners, kan dit een mogelijke verklaring zijn voor het relatief beperkt betrekken van het bestuur in de (voorbereiding op een) geïntegreerde aanpak.»

Het is onduidelijk of en in hoeverre deze aandachtspunten inmiddels zijn verbeterd. Gelet op de datalek-rapportages bij de AP over gemeenten kan worden getwijfeld over het niveau van implementatie van de BIO.

b. Kan misbruik van persoonsgegevens voldoende worden tegengegaan?

De vraag is wat onder «misbruik» moet worden verstaan en wanneer dat «voldoende» wordt tegengegaan. In de rechtspraak van het Hof van Justitie EU wordt, zoals eerder vermeld, in het kader van het evenredigheidsbeginsel en de noodzaak gewezen op het risico van misbruik als een wettelijke regeling niet voldoende precies en duidelijk is. Omdat de Europese eisen daaromtrent onder punt 3.2. zijn behandeld, is deze vraag eigenlijk al beantwoord (3.2.j.). Kort samengevat bevat het voorstel onvoldoende waarborgen tegen het risico van misbruik omdat de inmengingen op het recht op bescherming van persoonsgegevens beter moeten worden afgebakend en op genoemde onderdelen preciezer in de wet moeten worden omschreven.

Autoriteit Persoonsgegevens,

Aleid Wolfsen
Voorzitter

---

[111] Kamerstukken II 2020/21, 35 447, nr. 6. blz. 63.

[112] Artikel 2.31, negende lid: Indien noodzakelijk voor het doel, bedoeld in artikel 2.25, kunnen de deelnemers, bedoeld in artikel 2.27, eerste lid, derden op incidentele basis laten deelnemen aan het overleg, bedoeld in het vijfde en zesde lid. Deze derden krijgen uitsluitend toegang tot de persoonsgegevens die in het Zorg- en Veiligheidshuis worden verwerkt voor zover dat noodzakelijk is voor het doel, bedoeld in artikel 2.25.

[113] Inspectie Veiligheid en Justitie 2017, De aanpak van ondermijning, blz. 23.