Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

35 958

Regels ten behoeve van de verwerking van persoonsgegevens in het kader van de coördinatie en analyse in verband met terrorismebestrijding en bescherming van de nationale veiligheid door het versterken van de weerbaarheid van de samenleving (Wet verwerking persoonsgegevens coördinatie en analyse terrorismebestrijding en nationale veiligheid)

Nr. 12

NOTA VAN WIJZIGING

Ontvangen 20 september 2023

Het voorstel van wet wordt als volgt gewijzigd:

A

Het opschrift komt te luiden: **Regels inzake de coördinatie ten aanzien van terrorismebestrijding en de bescherming van de nationale veiligheid ten behoeve van het verhogen van de weerbaarheid tegen dreigingen en risico's (Wet coördinatie terrorismebestrijding en nationale veiligheid)**

B

In de considerans wordt «regels te stellen ten aanzien van de verwerking van gegevens, waaronder persoonsgegevens, ten behoeve van de coördinatie en analyse in het kader van het verhogen van de weerbaarheid ten aanzien van terrorismebestrijding en bescherming van de nationale veiligheid, door het versterken van de weerbaarheid van de samenleving en daarbij de nodige waarborgen op te nemen voor de bescherming van de persoonlijke levenssfeer» vervangen door «een wettelijke grondslag te bieden voor de coördinatie ten aanzien van terrorismebestrijding en de bescherming van de nationale veiligheid ten behoeve van het verhogen van de weerbaarheid tegen dreigingen en risico's en daarbij de nodige waarborgen op te nemen voor de bescherming van de persoonlijke levenssfeer».

C

Artikel 2 komt te luiden:

kst-35958-12
ISSN 0921 - 7371
's-Gravenhage 2023

Artikel 2. Coördinatietaak

1. Onverminderd de taken en bevoegdheden van betrokken overheidsorganisaties op grond van de op hen toepasselijke wetgeving, coördineert Onze Minister de samenhang en effectiviteit van het beleid en de door overheidsorganisaties te nemen maatregelen in het kader van terrorismebestrijding en de bescherming van de nationale veiligheid, met het oog op het verhogen van de weerbaarheid tegen dreigingen en risico's, het beschermen van de nationale veiligheidsbelangen en het voorkomen van maatschappelijke ontwrichting.

2. De in het eerste lid bedoelde taak ziet op:

a. het bevorderen van de samenwerking tussen betrokken overheidsorganisaties en maatschappelijke organisaties;

b. het bevorderen van de informatiedeling tussen betrokken overheidsorganisaties voor zover dit noodzakelijk is met het oog op het treffen van maatregelen naar aanleiding van een concrete gebeurtenis;

c. het bevorderen van de samenhang en effectiviteit van het in het eerste lid bedoelde beleid en het evalueren van dit beleid, met name naar aanleiding van de concrete toepassing van het beleid en genomen maatregelen in de praktijk en, indien de evaluatie daartoe aanleiding geeft, het op basis daarvan in samenwerking met betrokken overheidsorganisaties ontwikkelen van voorstellen voor verbetering.

3. In verband met de taak, bedoeld in het eerste lid, kan Onze Minister trends en fenomenen signaleren, analyseren en duiden. In dat kader wordt geen onderzoek gedaan gericht op personen, of organisaties.

D

Artikel 3 komt te luiden:

Artikel 3. Gegevensverwerking

1. Onze Minister kan, voor zover dit noodzakelijk is voor de uitvoering van de in artikel 2 bedoelde taak, gegevens, waaronder persoonsgegevens, verwerken:

a. afkomstig uit publiek toegankelijke bronnen;

b. ontvangen op grond van artikel 6.

2. Bij het gebruik van de in het eerste lid, onderdeel a, bedoelde bronnen wordt, indien dit onlinebronnen zijn, geen gebruik gemaakt van technische hulpmiddelen die op basis van profilering persoonsgegevens verzamelen, analyseren en combineren.

3. Bij algemene maatregel van bestuur worden regels gesteld met betrekking tot te nemen technische, personele en organisatorische maatregelen, waaronder regels over functiescheiding, autorisatie voor het gebruik van bepaalde systemen, opslag en beveiliging.

4. Persoonsgegevens afkomstig uit publiek toegankelijke onlinebronnen, met uitzondering van bronnen die onder het toepassingsbereik van artikel 85 van de Algemene verordening gegevensbescherming en artikel 43 van de Uitvoeringswet Algemene verordening gegevensbescherming vallen, worden binnen een jaar na opslaan vernietigd of gepseudonimiseerd, tenzij dit vanwege het doeleinde van de verwerking niet mogelijk is. De resterende persoonsgegevens worden uiterlijk binnen vijf jaar na opslaan vernietigd, met dien verstande dat uitsluitend met het oog op de afhandeling van een inzageverzoek of een procedure in rechte deze gegevens langer bewaard kunnen worden, voor zover dat voor deze doeleinden noodzakelijk is.

5. In afwijking van het vierde lid kan de bewaartermijn van persoonsgegevens na advies van de in artikel 4 bedoelde functionaris voor gegevensbescherming telkens met vijf jaar worden verlengd, indien deze verlenging noodzakelijk is voor het signaleren, analyseren en duiden van

een trend of fenomeen als bedoeld in artikel 2, derde lid en deze verlenging geringe gevolgen heeft voor de bescherming van de persoonlijke levenssfeer van betrokkene.

6. Persoonsgegevens die voorkomen in gegevens verwerkt op grond van het eerste lid, onderdeel b, worden vernietigd zodra zij niet langer noodzakelijk zijn voor de uitvoering van de in artikel 2 bedoelde taak, doch uiterlijk vijf jaar na de laatste verwerking.

7. Onze Minister is de verwerkingsverantwoordelijke voor de verwerking van persoonsgegevens op grond van deze wet.

E

Artikel 4 komt te luiden:

Artikel 4. Functionaris gegevensbescherming

Onze Minister benoemt een functionaris voor gegevensbescherming die in het bijzonder is belast met de taken, bedoeld in artikel 37 van de Algemene verordening gegevensbescherming, ten aanzien van de verwerking van persoonsgegevens op grond van deze wet.

F

Artikel 5 wordt als volgt gewijzigd:

1. In het eerste lid wordt «4, derde lid» vervangen door «3, eerste lid».

2. In het eerste en tweede lid, wordt «de verwerkingsverantwoordelijke» vervangen door «Onze Minister».

G

Na artikel 5 wordt een artikel ingevoegd luidende:

Artikel 5a. Toetsing en rapportage

Onze Minister laat de wijze waarop uitvoering wordt gegeven aan zijn in artikel 2 bedoelde taak toetsen. Een rapportage van de resultaten van deze toetsing wordt aan de Staten-Generaal gezonden.

H

In artikel 6 wordt «artikel 3, eerste lid, onderdeel a, bedoelde taken» vervangen door «artikel 2 bedoelde taak».

I

Artikel 7 komt te luiden:

Artikel 7. Gegevensverstrekking door Onze Minister

1. Onze Minister kan ten behoeve van de in artikel 2 bedoelde taak, gegevens, waaronder persoonsgegevens, verstrekken aan:

a. de in artikel 6, aanhef en onderdelen a tot en met e, bedoelde verwerkingsverantwoordelijken;

b. de politie in verband met haar taken op grond van artikel 3 van de Politiewet 2012;

c. de Koninklijke Marechaussee in verband met haar taken op grond van artikel 4 van de Politiewet 2012;

d. het openbaar ministerie in verband met zijn taken op grond van artikel 124 van de Wet op de rechterlijke organisatie;

e. de diensten, genoemd in artikel 1, onderdeel a, van de Wet op de inlichtingen- en veiligheidsdiensten 2017, in verband met de uitvoering van de taken op grond van die wet;

f. Onze Minister die het aangaat, voor zover de verstrekking noodzakelijk is in verband met de bij of krachtens de wet aan hem opgedragen taken.

2. Onze Minister verstrekt persoonsgegevens gepseudonimiseerd, tenzij dit vanwege de doeleinden van de verwerking niet mogelijk is. Persoonsgegevens worden voor openbaarmaking geanonimiseerd, tenzij dit vanwege de doeleinden van de verwerking niet mogelijk is.

3. Onverminderd artikel 2, derde lid, ziet een verstrekking als bedoeld in het eerste lid niet op een duiding van de uitingen van een persoon waardoor die persoon in verband wordt gebracht met een trend of fenomeen.

J

In artikel 8, eerste en tweede lid, wordt «taken» vervangen door «taak».

K

In artikel 11 wordt «Wet verwerking persoonsgegevens coördinatie en analyse terrorismebestrijding en nationale veiligheid» vervangen door «Wet coördinatie terrorismebestrijding en nationale veiligheid».

TOELICHTING

Op 2 juni 2022 vond het debat plaats over de werkwijze van de NCTV (nationaal coördinator terrorismebestrijding en veiligheid). Tijdens dit debat heb ik toegezegd naar aanleiding van de zorgen die door de Kamer zijn geuit op een zorgvuldige wijze te kijken naar een wijziging van het wetsvoorstel. Daarnaast zijn gedurende het debat een aantal moties aangenomen[1], waaronder de motie van het lid van der Plas[2] waarin de Kamer het kabinet oproept om te onderzoeken op welke wijze de functies die de NCTV binnen de nationale crisisstructuur vervult verder losgekoppeld kunnen worden van de analysefuncties waar de NCTV zich mee bezighoudt. Daarbij is toegezegd de uitvoering van deze motie te betrekken bij de behandeling van het wetsvoorstel. Inmiddels is ter uitvoering van de betreffende motie een rapportage met aanbevelingen afgerond en aangeboden aan de Tweede Kamer middels brief van 16 februari 2023.[3] Daarbij is tevens aangegeven dat nu het wetsvoorstel niet ziet op de nationale crisisstructuur de opvolging van de in brief opgenomen aanbevelingen verder buiten het traject van dit wetsvoorstel ter hand wordt genomen.

De periode na het debat heb ik de verschillende mogelijkheden onderzocht waarop aanpassing van het wetsvoorstel mogelijk is en wat dit zou betekenen. In bijgaande nota van wijziging is het resultaat hiervan opgenomen. De voorgestelde wijzigingen zien op de volgende uitgangspunten:

– terug naar de kerntaak van de NCTV, namelijk coördineren;

– versterken van de controle op het naleven van de regels opgenomen in het wetsvoorstel.

---

[1] Motie van het lid van der Werf c.s. van 2 juni 2022 (Kamerstukken II, 2021/22, 32 761, nr. 227); Motie van het lid Sylvana Simons van 2 juni 2022 (Kamerstukken II, 2021/22, 32 761, nr. 234); Motie van het lid van der Plas van 2 juni 2022 (Kamerstukken II, 2021/22, 32 761, nr. 238.).

[2] Motie van het lid van der Plas van 2 juni 2022 (Kamerstukken II 2021/22, 32 761, nr. 237).

[3] Kamerstukken II 2022/23, 30 821, nr. 177.

Met de voorgestelde wijzigingen wordt een toekomstbestendig kader gecreëerd dat zowel recht doet aan het belang van het werk van de NCTV, als aan de controleerbaarheid van de werkzaamheden van de NCTV in de toekomst en de bescherming van persoonsgegevens in overeenstemming met de Algemene verordening gegevensbescherming (AVG). Daarnaast is van de gelegenheid gebruik gemaakt om enkele technische en redactionele verbeteringen aan te brengen.

Het eerste uitgangspunt aan de hand waarvan wijzigingen zijn doorgevoerd is een uitvloeisel van een herbezinning op de kerntaak van de NCTV. Zoals aan bod kwam in paragraaf 2.1 van de memorie van toelichting bij het wetsvoorstel, is de toenmalige NCtb opgericht om te coördineren en zo versnippering en het gebrek aan regie op het terrein van terrorismebestrijding, en later ook de nationale veiligheid, tegen te gaan. Daarbij werd een gemeenschappelijk beleidskader en een centrale organisatie wezenlijk gevonden. Met de voorgestelde wijzigingen wordt vastgelegd dat coördineren de primaire taak van de NCTV is. Het analyseren van trends en fenomenen die van belang zijn voor terrorismebestrijding en nationale veiligheid kan dan ook geen op zichzelf staand doel zijn. De analysetaak keert dan ook niet terug als zelfstandige taak in het wetsvoorstel, met dien verstande dat het uiteraard wel van belang blijft om op basis van afdoende kennis te coördineren. De NCTV maakt daartoe geïntegreerde analyses vanuit breed maatschappelijk oogpunt op basis van inlichtingen, analyses en informatie van ketenpartners (zoals AIVD, politie, wetenschap en overige ministeries), aangevuld met eigen expertise. Daar hoort niet bij dat analyses worden verstrekt aan organisaties naar aanleiding van een vraag of bepaalde uitingen van een persoon passen binnen een bepaalde trend of een bepaald fenomeen. Daar hoort ook niet bij dat personen ten gevolge van een dergelijke analyse in verband kunnen worden gebracht met een trend of fenomeen. In de memorie van toelichting bij het wetsvoorstel werd dit aangeduid als de zogenoemde «korte analyses». Deze mogelijkheid wordt met deze nota van wijziging expliciet uitgesloten (artikel I, nieuw artikel 7, derde lid). Dit ligt feitelijk in het verlengde van de reeds in het wetsvoorstel opgenomen bepaling dat er geen onderzoek wordt gedaan gericht op personen.

Concreet betekent dit het volgende.

Voor een goede uitvoering van de coördinatietaak en de doelstellingen die daarmee worden nagestreefd blijft het noodzakelijk om over een bepaald kennisniveau te beschikken. Het verhogen van de weerbaarheid tegen terroristische dreigingen en risico's en andere dreigingen en risico's voor de nationale veiligheid vereist kennis van trends en fenomenen die hierop van invloed zijn. En met de ontwikkeling van de maatschappij naar een wereld waar trends en fenomenen zich mede ontwikkelen in discussies die zich grotendeels hebben verplaatst naar het digitale domein, geldt dat het raadplegen van publieke bronnen waar deze discussies worden gevoerd noodzakelijk is. Tevens geldt ten algemene dat veel informatie online te vinden is en zodra deze informatie persoonsgegevens bevat kan er al snel sprake zijn van een verwerking in de zin van de AVG.[4] Zonder kennis van wat er speelt is de NCTV niet goed in staat de coördinerende rol goed te vervullen en de juiste overheidsorganisaties te betrekken en bijeen te brengen.

---

[4] Ingevolge artikel 4, onderdeel 2, van de AVG is verwerking «*een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;*»

Voor de werkwijze van de NCTV betekent de aanpassing in de taak zoals die is opgenomen in het wetsvoorstel verschillende dingen, al naar gelang de specifieke situatie die het betreft.

Daarbij dient te worden benadrukt dat er veel verschillende situaties aan de hand kunnen zijn die verschillende werkzaamheden en handelen vergen.

Een aanleiding om over te gaan tot coördinatie kan bijvoorbeeld gevormd worden door een concrete gebeurtenis of een concreet incident. Afhankelijk van de situatie kunnen direct coördinerende werkzaamheden opgestart worden, maar kan het ook noodzakelijk zijn om eerst een beoordeling te maken van de vraag of en zo ja in welke mate coördinatie vereist is. Het kan zijn dat daarbij bepaalde basisinformatie uitgezocht dient te worden, maar nog geen sprake is van analysewerkzaamheden ten aanzien van trends en fenomenen. In andere gevallen kan het wel noodzakelijk zijn om analysewerkzaamheden te verrichten doordat een inschatting gemaakt dient te worden van de gevolgen van die gebeurtenis op een bepaalde trend of fenomeen, waarvoor het nodig kan zijn om publiek toegankelijke onlinebronnen, waaronder social media, te raadplegen zodat een inschatting gemaakt kan worden van de aard en het effect van het incident of de gebeurtenis op een bepaalde trend of fenomeen. Op basis van deze inschatting worden vervolgens indien noodzakelijk coördinerende werkzaamheden opgestart, bijvoorbeeld omdat sprake is van een nog niet onderkend fenomeen. Deze coördinatie kan dan inhouden dat ketenpartners, bijvoorbeeld gemeenten, bijeengebracht worden en waar nodig een aanpassing van het beleid plaats vindt. Een andere aanleiding kan gevormd worden door berichtgeving in de media of vragen vanuit de politiek over een bepaalde situatie. In deze gevallen is er sprake van een noodzaak tot het kunnen maken van een actuele en korte inschatting van een bepaalde situatie met het oog op het kunnen beoordelen van de noodzaak van coördineren en de mate waarin wordt gecoördineerd. In alle gevallen geldt dat het vergaren van informatie voor coördinatiewerkzaamheden zich niet kan uitstrekken tot het doen van onderzoek gericht op personen of organisaties.

Een andere reden om over te gaan tot analysewerkzaamheden met het oog op het kunnen uitvoeren van de coördinatietaak is de noodzaak om op basis van kennis van trends en fenomenen te kunnen coördineren. Daarbij geldt dat er tevens sprake is van een wisselwerking. Fenomeenkennis ontstaat ook door kennis opgedaan bij de coördinatie naar aanleiding van gebeurtenissen en incidenten. Op het terrein van de nationale veiligheid zijn meerdere spelers met ieder een eigen rol, vanuit de eigen taken en bevoegdheden. Uiteraard geldt hier dat een belangrijke rol is weggelegd voor de inlichtingen- en veiligheidsdiensten maar bijvoorbeeld ook de politie. De AIVD heeft een bijzondere rol omdat deze dienst een taak heeft ten aanzien van het doen van onderzoek gericht op personen en organisaties. Bij de NCTV komt als coördinator veel informatie samen en wordt de samenwerking en een samenhangend beleid bevorderd. Daarbij geldt dat vanuit de NCTV ook wordt gekeken naar vroegtijdige signalering van nieuwe ontwikkelingen met het oog op het ontwikkelen van preventief beleid. Hierbij geldt dat er sprake is van nauwe samenwerking en afstemming. Dit proces is dynamisch omdat trends en fenomenen ook samenhangen met actuele gebeurtenissen en incidenten.

Het voorgaande zal in de werkprocessen verankerd worden zodat er steeds beslismomenten zijn over de noodzaak tot bepaalde type werkzaamheden en de voortzetting daarvan.

Daarmee wordt ook recht gedaan aan de beginselen van proportionaliteit en subsidiariteit doordat de noodzaak op verschillende momenten opnieuw wordt bezien. Maar die proportionaliteit en subsidiariteit komen ook op andere manieren terug, namelijk bij de wijze waarop vervolgens om wordt gegaan met de persoonsgegevens die nog wel kunnen worden verwerkt.

Daarbij kan onderscheid worden gemaakt tussen het opslaan van gegevens in de systemen van de NCTV («inkomend») en het verstrekken van gegevens door de NCTV aan andere organisaties («uitgaand»).

In het wetsvoorstel was reeds geregeld dat er beschermingsmaatregelen worden getroffen voor persoonsgegevens die worden opgeslagen in de systemen van de NCTV, doordat bij algemene maatregel van bestuur regels worden gesteld met betrekking tot te nemen technische, personele en organisatorische maatregelen, waaronder regels over functiescheiding, autorisatie voor het gebruik van bepaalde systemen, opslag en beveiliging (met de nota van wijziging verplaatst van artikel 4, vierde lid, naar artikel 3, derde lid). Daarnaast wordt met de nota van wijziging een aantal waarborgen verder verduidelijkt en ingeperkt aan de hand van een «trechtermodel», zodat verzekerd is dat persoonsgegevens niet langer bewaard worden dan noodzakelijk. Daarbij is van belang dat onder het begrip «publieke toegankelijke onlinebronnen» meerdere type bronnen zijn te onderscheiden. Krantenartikelen en wetenschappelijke artikelen zijn namelijk ook publiek toegankelijke (online) bronnen. Deze bronnen worden uitgesloten van de opgenomen vernietigingsplicht ten aanzien van persoonsgegevens. Naast het feit dat dit type gegevens eenvoudig opnieuw «vergaard» zou kunnen worden, is het vernietigen van krantenberichten en dergelijke disproportioneel voor het doel dat daarmee gediend wordt. Voor het bepalen van de reikwijdte van deze categorie wordt aangesloten bij artikel 85 van de Algemene verordening gegevensbescherming (AVG) en artikel 43 van de Uitvoeringswet Algemene verordening gegevensbescherming die zien op «journalistieke doeleinden en ten behoeve van uitsluitend academische, artistieke of literaire uitdrukkingsvormen». Voor alle andere persoonsgegevens die afkomstig zijn van publiek toegankelijke onlinebronnen geldt vervolgens dat binnen een jaar een schifting heeft plaatsgevonden, waarbij persoonsgegevens ofwel worden vernietigd, ofwel gepseudonimiseerd, ofwel behouden als geen van beide mogelijk is (artikel 3, vierde lid).

In dit kader is het van belang om eerst een aantal begrippen te verduidelijken. Bij persoonsgegevens in de zin van de AVG gaat het niet alleen om gegevens aan de hand waarvan een persoon rechtstreeks geïdentificeerd kan worden (een «geïdentificeerde» persoon). Ook gegevens aan de hand waarvan iemand indirect geïdentificeerd kan worden kunnen persoonsgegevens zijn (een «identificeerbare» persoon).[5] Met name die laatste categorie kan in de praktijk moeilijker af te bakenen zijn. Het anonimiseren en pseudonimiseren van persoonsgegevens vormen belangrijke beschermings- en beveiligingsmaatregelen. Pseudonimiseren betekent dat persoonsgegevens door het gebruik van aanvullende gegevens aan een natuurlijke persoon kunnen worden gekoppeld, waardoor deze persoon identificeerbaar is. Om te kunnen bepalen of een

[5] De AVG definieert persoonsgegevens in artikel 4, onder 1, als « alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene»); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online-identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;»

persoon identificeerbaar is dient rekening te worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij worden gebruikt door de verwerkingsverantwoordelijke of door een andere persoon om de natuurlijke persoon direct of indirect te identificeren. Of er sprake is van «middelen waarvan redelijkerwijs valt te verwachten dat zij zullen worden gebruikt» moet rekening worden gehouden met alle objectieve factoren. Het gaat bijvoorbeeld om de kosten van en de tijd benodigd voor identificatie, met inachtneming van de beschikbare technologie op het tijdstip van verwerking en de technologische ontwikkelingen. De AVG is niet van toepassing op anonieme gegevens, dat wil zeggen persoonsgegevens die zodanig anoniem zijn gemaakt dat de betrokkene niet meer identificeerbaar is.[6] Bij gegevens die verstrekt worden aan andere partijen geldt daarbij dat het van belang is de positie van de ontvanger te betrekken. Met andere woorden, is de ontvanger in staat met «redelijke middelen» een persoon te (her)identificeren.[7]

Deze definiëring maakt ook dat voor de vraag of er sprake is van anonimisering of pseudonimisering relevant is welke middelen redelijkerwijs ingezet kunnen worden om een persoon te (her)identificeren en door wie.

Voor persoonsgegevens die voorkomen in gegevens die afkomstig zijn van publiek toegankelijke onlinebronnen, met uitzondering van de hierboven genoemde categorie van kort gezegd kranten en boeken die worden opgeslagen met het oog op het kunnen analyseren, signaleren en duiden van trends en fenomenen geldt dat binnen een jaar:
– Persoonsgegevens worden vernietigd, of indien dit niet mogelijk is;
– Persoonsgegevens worden gepseudonimiseerd, of indien niet mogelijk is:
– Persoonsgegevens langer worden bewaard.

Voor wat betreft pseudonimisering geldt dat dit betekent dat de personen die toegang hebben tot deze gegevens niet over de aanvullende gegevens kunnen beschikken die voor identificatie van personen vereist is. Deze pseudonimisering biedt met name bescherming tegen bijvoorbeeld datalekken. Binnen de organisatie zijn immers de aanvullende gegevens beschikbaar om pseudonimisering ongedaan te maken. Dat neemt niet weg dat dit een belangrijke beschermingsmaatregel is doordat derden niet over deze gegevens beschikken.

Het onderdeel «niet mogelijk» in bovengenoemd stroomschema ziet op twee aspecten, namelijk zowel de noodzaak tot behoud van de betreffende persoonsgegevens gelet op het doel waarvoor deze zijn opgeslagen, als de vraag indien de betreffende persoonsgegevens behouden dienen te blijven in welke vorm dat nodig en mogelijk is. Zoals hierboven al bod kwam, kan het onmogelijk zijn om persoonsgegevens te pseudonimiseren omdat aan de hand van aanvullende gegevens identificatie alsnog mogelijk is en deze aanvullende gegevens redelijkerwijs ingezet kunnen worden door een persoon. Als deze aanvullende gegevens namelijk zien op zeer openbare informatie, dan is de vraag of pseudonimisering wel mogelijk is. Niettemin kan het weghalen van direct identificerende persoonsgegevens ook dan meerwaarde hebben. Ter illustratie: het pseudonimiseren van een zeer bekend persoon kan onmogelijk zijn omdat

---

[6] Zie onder meer overweging 26 van de AVG en advies 4/2007 van Groep gegevensbescherming artikel 29, over het begrip persoonsgegeven, goedgekeurd 20 juni 2007, 01248/07/NL, WP 136.

[7] Arrest van het Gerecht van 26 april 2023, in de zaak T-557/20, Gemeenschappelijke Afwikkelingsraad (GAR) tegen Europese toezichthouder voor gegevensbescherming (EDPS) en arrest van het Hof van Justitie van de EU van 19 oktober 2016 in de zaak C-582/14, Patrick Breyer tegen Bundesrepublik Deutschland.

uit de context onmiddellijk zal blijken om wie het gaat. Als pseudonimisering echter alleen door andere personen binnen de organisatie ongedaan kan worden gemaakt, maar niet door derden of door de personen die toegang hebben tot de gepseudonimiseerde persoonsgegevens, dan is pseudonimisering wel mogelijk.

Binnen uiterlijk vijf jaar dienen alle resterende persoonsgegevens afkomstig van social media vernietigd te zijn (artikel 3, vierde lid). Hiervoor gelden twee uitzonderingen. Voor de eerste categorie geldt dat deze gegevens wel beschikbaar blijven voor de coördinatietaak, maar dat deze gegevens van dusdanige publieke aard zijn, dat de gevolgen voor de bescherming van de persoonlijke levenssfeer gering zijn, terwijl deze gegevens nog wel van belang zijn voor een trend of fenomeen. Voor deze categorie geldt dat na advies van de functionaris voor gegevensbescherming, die hierna aan bod komt, de bewaartermijn telkens met vijf jaar kan worden verlengd (artikel 3, vijfde lid). Een voorbeeld betreft het manifest van Anders Breivik. Dit manifest is van publieke aard waardoor de gevolgen voor de persoonlijke levenssfeer van deze betrokkene van het langer bewaren van zijn persoonsgegevens beperkt zijn. Vanwege de impact van de gebeurtenissen rondom Anders Breivik kan het manifest echter wel voor langere duur van belang zijn voor het analyseren van een trend of fenomeen. Voor de tweede categorie binnen de uitgezonderde categorie geldt dat de gegevens niet voor de coördinatietaak beschikbaar blijven, maar voor andere doeleinden langer bewaard moeten blijven, namelijk het kunnen afhandelen van inzageverzoeken van betrokkenen of rechtszaken die daarmee samenhangen (artikel 3, vierde lid). Indien bijvoorbeeld een procedure bij een rechtbank aanhangig is waarbij persoonsgegevens betrokken zijn die onder de vernietigingsplicht vallen, worden deze vernietigd in de systemen die worden gebruikt voor de coördinatietaak. Het dossier voor de rechtszaak bevat deze gegevens nog wel om de rechtszaak te kunnen afhandelen.

Ten aanzien van de verstrekking van gegevens door de NCTV (uitgaande processen) geldt dat het wetsvoorstel een gesloten systeem bevat. Een verstrekking van gegevens waarin persoonsgegevens zijn opgenomen is alleen mogelijk aan de in artikel 7 opgenomen partijen.

Daarnaast geldt dat het afhankelijk is van de concrete situatie of en zo ja op welke wijze deze verstrekking mogelijk is. De opgenomen hoofdregel is dat persoonsgegevens gepseudonimiseerd worden verstrekt, tenzij dit vanwege het doeleinde van de verwerking niet mogelijk is. Bij openbaarmaking geldt anonimisering als hoofdregel. Bij bepaalde coördinerende werkzaamheden is het niet mogelijk om deze te verrichten zonder dat er persoonsgegevens worden verstrekt aan de betrokken ketenpartners en kan dit ook niet op gepseudonimiseerde wijze. In het geval van bijvoorbeeld noodzakelijke coördinerende werkzaamheden rond een terugkerende Syriëganger die vervolgd dient te worden, kan het verstrekken van bijvoorbeeld de naam waarschijnlijk onvermijdelijk zijn. Verder kan het pseudonimiseren van persoonsgegevens in bepaalde gevallen onmogelijk zijn omdat een persoon dusdanige bekendheid geniet dat altijd herleidbaar is om wie het gaat. Ook hier geldt dat het meestal om publieke personen zal gaan. Daarbij geldt overigens ook dat in die gevallen de verwachting is dat de bescherming die pseudonimiseren biedt niet nodig is. Het benoemen van een president van een land als onderdeel van een beschrijving van gebeurtenissen zal bijvoorbeeld geen schade berokkenen aan de betreffende president.

Een belangrijke waarborg ten aanzien van de verstrekking van analyses is zoals hierboven reeds opgemerkt dat expliciet wordt uitgesloten dat er een duiding plaatsvindt van uitingen van een persoon die juist door die

duiding worden geassocieerd met een bepaalde trend of een bepaald fenomeen dat een dreiging of risico vormt voor de nationale veiligheid (artikel 7, derde lid). Met uitingen wordt bedoeld alle vormen van gedragingen en uitspraken die wijzen op een bepaald gedachtegoed. De achterliggende gedachte is uit te sluiten dat een analyse van de NCTV er de oorzaak van is dat een persoon in verband wordt gebracht met een trend of fenomeen. Omgekeerd betekent dit dat er wel ruimte is om bepaalde publieke personen die reeds op andere wijze in verband zijn gebracht met een trend of fenomeen wel benoemd kunnen worden. Het «op andere wijze in verband gebracht» kan op verschillende manieren plaatsvinden. Van belang is in ieder geval dat er sprake is van een bepaalde algemene bekendheid in relatie tot de trend en het fenomeen. Dit kan zijn omdat het om een persoon gaat die zelf publiekelijk op de voorgrond treedt als vertegenwoordiger van een trend of fenomeen, zoals een leider van ISIS. Ook kan het gaan om een persoon die bekend is geworden vanwege een gebeurtenis die gelinkt is aan een trend of fenomeen, zoals bijvoorbeeld de gebeurtenissen rondom Anders Breivik. Wat niet mogelijk is, is dat in een analyse een persoon wordt genoemd en die persoon vervolgens door die analyse in verband wordt gebracht met bijvoorbeeld gewelddadig gedachtegoed. Het is geen taak van de NCTV om antwoord te geven op de vraag of een persoon als gevaar voor de nationale veiligheid kan worden beschouwd omdat het gedachtegoed van die persoon aangemerkt kan worden als passend binnen een trend of fenomeen zoals jihadisme.

Deze normering geldt naast de bepaling dat het kunnen opstellen van analyses van trends en fenomenen geen onderzoek kan worden gedaan gericht op personen en organisaties. Overigens geldt ten aanzien van publieke organisaties eveneens dat het niet doen van onderzoek gericht op organisaties niet wegneemt dat organisaties een rol kunnen spelen in een trend of fenomeen en dus voor kunnen komen in producten van de NCTV. Een voorbeeld betreft «Een perspectief op de transformatie van ISIS na de val van het «kalifaat»». De kennis van trends en fenomenen en eventuele analyses die daaruit volgen zullen echter altijd in het licht dienen te staan van de coördinerende taak.

Een belangrijk gevolg van het voorgaande is ook dat het daarmee niet langer mogelijk is dat overheidsorganisaties, zoals gemeenten, een beroep doen op de kennis van de NCTV bij de vraag of uitingen van een persoon die zich in die gemeente begeeft passen binnen een bepaalde trend of een bepaald fenomeen indien die persoon niet al onderwerp is geweest van bijvoorbeeld betrokkenheid bij een terroristische aanslag. Mocht de NCTV een dergelijk verzoek ontvangen, dan zal al naar gelang de concrete vraag die gesteld wordt, worden verwezen naar de AIVD of de politie, die uiteraard een eigen afweging maken of de gestelde vraag past binnen de aan hen toebedeelde taken en verantwoordelijkheden. Het ontvangen van meer algemene informatie over trends en fenomenen blijft overigens wel mogelijk.

Het tweede gehanteerde uitgangspunt is een versterking van «checks and balances», wat concreet betekent dat als een bepaalde taak wordt toegekend, er een tegenwicht georganiseerd dient te worden die in verhouding staat tot die taak. Met de bovengenoemde wijziging is er al sprake van een inperking, doordat de analysetaak als zelfstandige taak wegvalt en tevens de mogelijkheid tot het verstrekken van de zogenoemde «korte analyses» wordt geschrapt. Niettemin wordt voorzien in aanvullende waarborgen ter versterking van de controle op de werkzaamheden van de NCTV, naast de controlemechanismen die al in het wetsvoorstel zijn opgenomen zoals de verplichting tot het uitvoeren van een gegevensbeschermingsaudit.

Ten eerste zal het toezicht op de naleving van de AVG en de bepalingen in het wetsvoorstel die zien op de verwerking van persoonsgegevens worden versterkt door te voorzien in de benoeming van een functionaris voor gegevensbescherming (f-g), specifiek voor de toepassing van dit wetsvoorstel. De taken en positie van een f-g worden rechtstreeks geregeld door de AVG. Een f-g is een interne, onafhankelijke toezichthoudende functionaris. De AVG regelt rechtstreeks zijn taken en zijn onafhankelijke positie. Een f-g wordt aangewezen op grond van zijn professionele kwaliteiten en, in het bijzonder, zijn deskundigheid op het gebied van de wetgeving en de praktijk inzake gegevensbescherming en zijn vermogen om zijn taken onder de AVG te vervullen. Daarnaast werkt een f-g samen met de Autoriteit Persoonsgegevens (AP). Door te voorzien in de benoeming van een f-g specifiek ten aanzien van de verwerking van persoonsgegevens onder dit wetsvoorstel, wordt de zogenoemde «accountability» van de NCTV aanzienlijk versterkt. Ten tweede zal naast toezicht door de f-g en de AP op de naleving van regels inzake de verwerking van persoonsgegevens, de Inspectie Justitie en Veiligheid (IJenV) toe gaan zien op de naleving van de normen in het wetsvoorstel die niet zien op de verwerking van persoonsgegevens. De IJenV heeft als Rijksinspectie een goede kennis van de domeinen van JenV en vervult uit dien hoofde al een belangrijke rol in de controle op de uitvoering van de taken door het Ministerie, waaronder cybersecurity en nationale veiligheid.

Van belang is daarbij uiteraard dat de IJenV over afdoende capaciteit en expertise beschikt. Daarnaast geldt dat de IJenV de frequentie van controles moet kunnen aanpassen aan haar bevindingen. Met de IJenV vindt dan ook in het kader van de voorbereiding op de uitvoering afstemming plaats over de vraag wat de IJenV nodig heeft om zijn taak op een goede manier te kunnen uitvoeren zodat daar rekening mee gehouden kan worden. De huidige inschatting is dat de capaciteitsinzet ongeveer 2 fte bedraagt. Ter uitvoering van het wetsvoorstel wordt gewerkt aan een algemene maatregel van bestuur. Op het moment dat het ontwerp gereed is voor consulatie zal tevens de IJenV worden gevraagd een actuele inschatting te maken van de benodigde capaciteit bij gelegenheid van het verrichten van de uitvoeringstoets. Voor wat betreft de benodigde expertise geldt dat de IJenV reeds ervaring heeft in het domein nationale veiligheid, zoals cybersecurity, maar bijvoorbeeld ook ten aanzien van de nationale veiligheidsstrategie.

Daarnaast geldt dat het van belang is dat er tussen de IJenV en de AP onderling overleg kan plaatsvinden waar dat nodig is om hun werkzaamheden af te stemmen. Uiteraard is het aan de IJenV en de AP om hier in onderling overleg vorm aan te geven, bijvoorbeeld door het sluiten van een convenant. Als Minister is het van belang om de omstandigheden te creëren dat beide toezichthouders hun werk kunnen doen, maar uiteraard niet te treden in de eigen professionele afwegingen van deze organisaties waaronder het oordeel over de frequentie van het toezicht. Wellicht ten overvloede geldt tot slot dat zoals gebruikelijk de ontwerp-amvb aan de AP zal worden voorgelegd voor advies.

Met deze communicerende vaten wordt voorzien in optimale controle op de werkwijze van de NCTV, ook in de toekomst.

Voor de financiële kant geldt dat de kosten voor de f-g binnen de NCTV binnen het huidige financiële kader NCTV opgevangen zullen worden. Dat geldt ook voor de kosten die de IJenV zal moeten maken voor de uitvoering van de toezichts- en rapportageverplichting. Dit zal in totaal ongeveer 2 fte beslaan (€ 230.000). Er zijn geen verdere administratieve en uitvoeringslasten bij partijen buiten de NCTV aan verbonden.

Artikelsgewijs

A, B en K

Het opschrift, het «gelet op» in de considerans en de citeertitel worden aangepast aan de inperking van de taak opgenomen in het wetsvoorstel. Tevens wordt een vereenvoudiging doorgevoerd door deze kernachtiger te formuleren.

C

In het oorspronkelijke wetsvoorstel was in artikel 2 een reikwijdte bepaling opgenomen met daarin tevens de doelstellingen opgenomen van de taken. De taken zelf waren opgenomen in artikel 3. Ter vereenvoudiging van het wetsvoorstel zijn de artikelen 2 en 3 samengevoegd in een nieuw artikel 2, waarin zowel de taak als de doelstellingen die met de taak worden nagestreefd zijn opgenomen nu deze onlosmakelijk zijn verbonden. De analysetaak als zelfstandige taak is daarin geschrapt. Daarnaast zijn redactionele verbeteringen aangebracht.

In het voorgestelde eerste en tweede lid van artikel 2 is de coördinatietaak vastgelegd. In het eerste lid is het «beschermen van vitale belangen van de samenleving» vervangen door het meer actueel gehanteerde begrip «beschermen van nationale veiligheidsbelangen». Inhoudelijk is geen verschil beoogd. Daarnaast is verduidelijkt dat ook maatschappelijke organisaties een rol kunnen spelen in de samenwerking met overheidsorganisaties, bijvoorbeeld in de aanpak van extremisme en terrorisme (onderdeel a). In het tweede lid is tevens verduidelijkt dat het bewaken van de samenhang van beleid van belang is (onderdeel c).

In het derde lid is tot slot uitdrukking gebracht dat met het oog op deze coördinatietaak analyses van trends en fenomenen opgesteld kunnen worden, met dien verstande dat dit – net als in het oorspronkelijke wetsvoorstel – geen bevoegdheid inhoudt tot het doen van onderzoek gericht op personen of organisaties.

D

Het voorstelde artikel 3 betreft een technisch en redactioneel aangepaste versie van het in het oorspronkelijke wetsvoorstel opgenomen artikel 4 over gegevensverwerking. De volgende leden keren niet terug. Het oorspronkelijke eerste lid (waarin werd vastgelegd dat de verwerking van (persoons)gegevens alleen mogelijk was onder de voorwaarden opgenomen in het artikel) en het oorspronkelijke onderdeel c van het derde lid (verwerking van gegevens ontvangen van andere dan in artikel 6 bedoelde overheidsorganisaties) keren beide niet terug in het artikel omdat dit reeds volgt uit andere bepalingen in het wetsvoorstel. Het spreekt voor zich dat verwerking alleen mogelijk is voor zover dit toegestaan is door het wetsvoorstel en de AVG. Het onderdeel «ontvangen van andere dan de in artikel 6 bedoelde overheidsorganisaties» volgt feitelijk al uit onderdeel f van artikel 6 en is daarmee al in inbegrepen in artikel 3, eerste lid, onderdeel b (nieuw).

Artikel 3, eerste, tweede en derde lid, zijn inhoudelijk verder gelijk aan het oorspronkelijk in het wetsvoorstel opgenomen artikel 4, derde lid, onderdelen a en b, vierde en vijfde lid.

In artikel 3, vierde lid, is zoals toegelicht in het algemene deel vastgelegd dat binnen een jaar na het opslaan van persoonsgegevens afkomstig van social media (publiek toegankelijke onlinebronnen, met

uitzondering van krantenberichten en dergelijke) een schifting wordt gemaakt waarbij persoonsgegevens ofwel worden vernietigd, ofwel gepseudonimiseerd, ofwel behouden, waarna binnen uiterlijk vijf jaar in totaal de resterende persoonsgegevens worden vernietigd. Dit voor zover voor het doel van de afronding van een rechterlijke procedure of een inzageverzoek deze persoonsgegevens voor de duur van de afronding van die procedure voor dat doel behouden dienen te blijven.

In dit artikellid is een deel van de verplichting tot pseudonimiseren zoals oorspronkelijk opgenomen in artikel 4, eerste lid (oud) opgenomen, namelijk het deel dat betrekking heeft op het opslaan van persoonsgegevens. De plicht om als hoofdregel persoonsgegevens te pseudonimiseren die aan andere organisaties worden verstrekt is opgenomen in artikel 7, tweede lid.

In artikel 3, vijfde lid, is de in het algemeen deel toegelichte uitzondering op de vernietigingsplicht opgenomen voor berichtgeving waarvan het noodzakelijk is om deze voor het signaleren, analyseren en duiden van een trend of fenomeen langer te bewaren, terwijl de verlenging geringe gevolgen heeft voor de persoonlijke levenssfeer van de betrokken persoon.

In artikel 3, zesde lid, is de bewaartermijn opgenomen van persoonsgegevens die niet onder de voorgaande artikelleden vallen.

Nieuw is tot slot het zevende lid waarin wordt verduidelijkt dat de Minister van Justitie en Veiligheid de verwerkingsverantwoordelijke is voor dit wetvoorstel.

E

Het voorgestelde artikel 4 regelt de benoeming van een functionaris voor gegevensbescherming specifiek ter versterking van de controle op de naleving van de AVG bij de taakuitvoering op grond van bijgaand wetsvoorstel.

F, H en J

Deze wijzigingen betreffen technische aanpassingen.

G

In het voorgestelde artikel 5a is opgenomen dat Onze Minister de wijze waarop uitvoering wordt gegeven aan zijn taken, bedoeld in deze wet, laat toetsen, waarbij een rapportage van de resultaten van deze toetsing aan de Staten-Generaal wordt gezonden. Dit artikel ziet op de Inspectie Justitie en Veiligheid.

Op grond van artikel 60 van het Organisatiebesluit Ministerie van Justitie en Veiligheid is de Inspectie Justitie en Veiligheid (IJenV) als Rijksinspectie onder meer belast met het houden van toezicht op de uitvoering en de naleving van de wet- en regelgeving op het terrein van het ministerie en van wet- en regelgeving op andere daartoe bij of krachtens de wet aangewezen beleidsterreinen. Met de inwerkingtreding van bijgaand voorstel zal de IJenV gemachtigd zijn ten aanzien van de controle op de uitvoering en naleving van de hierin opgenomen taak. Met het voorgestelde artikel 5a wordt wettelijk vastgelegd dat deze controle plaatsvindt en er een rapportage aan de Staten-Generaal plaatsvindt.

I

Artikel I stelt het voorgestelde artikel 7 omwille van de leesbaarheid in zijn geheel opnieuw vast. Daarbij is ten eerste de verwijzing naar de taken die oorspronkelijk in de onderdelen a en b van artikel 3, eerste lid, waren opgenomen aangepast naar de taak in het voorgestelde artikel 2 (nieuw). Een tweede wijziging ziet op de toevoeging van een artikellid (derde lid) waarin expliciet is vastgelegd dat het wetsvoorstel geen grondslag biedt voor het verstrekken van gegevens met daarin een duiding van de uitingen van een persoon, waardóór die persoon in verband wordt gebracht met een trend of fenomeen.

In het tweede lid tot slot zijn de passages over pseudonimisering en anonimisering van persoonsgegevens die worden verstrekt samengebracht.

De Minister van Justitie en Veiligheid,
D. Yesilgöz-Zegerius