Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

34 889

Wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen

Nr. 6

NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 30 april 2018

I ALGEMEEN

1. Inleiding

Met veel belangstelling heb ik kennis genomen van de inbreng van de leden van de fracties van uw Kamer inzake het voorstel tot wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen (hierna ook: het wetsvoorstel). Het is van groot belang dat binnen de Europese Unie een eenduidig juridisch kader gaat gelden voor de verwerking van persoonsgegevens door de opsporings- en vervolgingsinstanties. De criminaliteit draagt in toenemende mate een grensoverschrijdend karakter. Deze ontwikkeling noopt tot verdere intensivering van de gegevensuitwisseling tussen de bevoegde autoriteiten in de lidstaten. Een eenduidig kader voor de verwerking van persoonsgegevens vormt hiervoor een belangrijke voorwaarde, de lidstaten kunnen er dan op vertrouwen dat de doorgegeven persoonsgegevens zorgvuldig worden verwerkt. De richtlijn (EU) 2016/680 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (richtlijn gegevensbescherming opsporing en vervolging) vormt onderdeel van het EU-pakket op het gebied van de bescherming van persoonsgegevens. Dit pakket omvat tevens de verordening (EU) 2016/679 van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene verordening gegevensbescherming, hierna ook: AVG). De richtlijn gegevensbescherming opsporing en vervolging moet zijn geïmplementeerd uiterlijk op 6 mei 2018 (artikel 63, tweede lid,

kst-34889-6
ISSN 0921 - 7371
's-Gravenhage 2018

RI). Mede namens mijn ambtgenoot van Defensie beantwoord ik de door de leden van de fracties van uw Kamer gestelde vragen als volgt.

De leden van de VVD hebben melding gemaakt van lichte frustratie over het feit dat dit wetsvoorstel minder dan drie maanden voor de deadline naar de Kamer is gestuurd. De frustratie van de leden van deze fractie op dit punt kan ik begrijpen. De termijn voor de implementatie van de richtlijn is twee jaar. Deze termijn is echter aan de korte kant voor de afronding van de implementatie. Dit omvat het inventariseren van de precieze gevolgen van het onderhandelingsresultaat voor de nationale wetgeving op het gebied van de bescherming van persoonsgegevens, het in overleg met de betrokken uitvoeringsinstanties voorbereiden van een wetsvoorstel ter implementatie – inclusief het in kaart brengen van de gevolgen van het wetsvoorstel voor de werklasten van die instanties –, het opstellen van een wetsvoorstel waarmee de verschillende nationale wetten worden gewijzigd en het in procedure brengen daarvan. Wat betreft de inventarisatie van de gevolgen van het onderhandelingsresultaat moet erop worden gewezen dat de richtlijn voorziet in een aantal nieuwe verplichtingen voor de verwerkingsverantwoordelijke. Dit betreft bijvoorbeeld de verplichting tot melding van datalekken, de informatieplichten jegens de betrokkene, de beveiliging van de gegevens, de automatische vastlegging van gegevens over de gegevensverwerkingen (logging) en het aanwijzen van een functionaris voor gegevensbescherming. Wat betreft het overleg met de betrokken uitvoeringsinstanties moet worden vastgesteld dat de richtlijn consequenties heeft voor een groot aantal gegevensverwerkingen op het gebied van opsporing en vervolging. Dit betreft niet alleen de verwerking van persoonsgegevens door politie en openbaar ministerie, maar ook de verwerking door de Koninklijke marechaussee (Kmar), de bijzondere opsporingsdiensten, de buitengewoon opsporingsambtenaren, het Centraal Justitieel Incassobureau, de dienst Justis van het Ministerie van Justitie en Veiligheid en de strafkamers van de gerechten. Met deze instanties is intensief overleg gevoerd over de implicaties van de richtlijn op de gegevensverwerking, en de afgrenzing tussen de richtlijn en de Algemene verordening gegevensbescherming (AVG). Tijdens deze periode vond er ook periodiek overleg plaats met de Commissie en de andere lidstaten in een zogenaamde «expertgroup» om de implementatie af te stemmen. Dit alles heeft ertoe geleid dat het traject ter implementatie van de richtlijn langer heeft geduurd dan wenselijk. Ik hoop echter dat de leden van de fractie van de VVD en van de overige fracties desondanks bereid zijn dit wetsvoorstel met enige voortvarendheid te behandelen zodat de overschrijding van de implementatiedatum zoveel mogelijk kan worden voorkomen.

De leden van de CDA-fractie hebben met belangstelling kennis genomen van onderhavig wetsvoorstel. Gezien de gevoelige natuur van de gegevens waarmee gewerkt wordt, achten de leden van deze fractie achten het van belang dat er voor voldoende bescherming op het gebied van de verwerking van deze gegevens wordt gezorgd. Op verschillende vlakken zorgt de richtlijn daarvoor. Wel hebben de leden van deze fractie nog enkele vragen.
Zo hebben de leden van de CDA-fractie opgemerkt dat de datum van inwerkingtreding van de richtlijn op 6 mei aanstaande is gesteld en gevraagd of deze datum naar verwachting gehaald zal worden. De leden van deze fractie hebben tevens gevraagd welk tijdpad de regering hiervoor voor ogen heeft, wat de gevolgen zijn van het niet halen van dat datum van inwerkingtreding, en welke verklaring eraan ten grondslag ligt dat de wet ter implementatie van richtlijn 2016/680 pas wordt behandeld na de behandeling van de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

De AVG treedt op 25 mei in werking, de regels van de verordening zijn dan onherroepelijk van toepassing. Op 13 maart is het wetsvoorstel Uitvoeringswet Algemene verordening gegevensbescherming (34 851) door uw Kamer aangenomen. Hierboven ben ik, naar aanleiding van een opmerking van de leden van de VVD-fractie, reeds ingegaan op de vertraging rond de implementatie van de richtlijn gegevensbescherming opsporing en vervolging. Deze richtlijn moet uiterlijk op 6 mei 2018 zijn geïmplementeerd. Als een richtlijn niet tijdig wordt geïmplementeerd kan de Commissie een zogenaamde infractieprocedure starten bij het Hof van Justitie van de Europese Unie. Teneinde het risico op een infractieprocedure te minimaliseren is het van groot belang dat de richtlijn wordt geïmplementeerd, voor 6 mei 2018 of anders zo spoedig mogelijk na die datum. De Commissie is op de hoogte gehouden van de voortgang van de implementatie, door middel van periodieke rapportages in de eerder vermelde «expertgroup». Ik realiseer mij dat de implementatiedatum van de richtlijn niet goed haalbaar is maar streef er naar het wetsvoorstel bij voorkeur tegelijkertijd met, en anders zo kort mogelijk na, de AVG in werking te laten treden. De verordening en de richtlijn hangen inhoudelijk namelijk nauw met elkaar samen omdat zij, voor wat betreft het toepassingsgebied, elkaar wederzijds uitsluiten. Om te voorkomen dat overlap ontstaat tussen de regels op het gebied van de bescherming van persoonsgegevens die gelden voor de opsporingsinstanties enerzijds en andere overheidsinstellingen en bedrijven anderzijds, of dat andersom juist witte vlekken ontstaan in de toepasselijke regelgeving, is het wenselijk dat het wetsvoorstel ter implementatie van de richtlijn zoveel mogelijk tegelijkertijd in werking treedt als de Uitvoeringswet AVG. Ik zou het dan ook erg op prijs stellen indien uw Kamer dit wetsvoorstel met prioriteit zou willen behandelen. Uiteraard zal ik van mijn kant ook al het mogelijke doen om u hierbij van dienst te zijn.

De leden van de D66-fractie hebben met interesse kennisgenomen van voorliggend wetsvoorstel. Voor een doeltreffende politiële en justitiële samenwerking in strafzaken is het van belang dat een consequente en ook hoge mate van bescherming van persoonsgegevens van natuurlijke personen wordt gewaarborgd en dat de verwerking van persoonsgegevens bij de bevoegde autoriteiten wordt vergemakkelijkt. Deze leden van deze fractie hebben daarover nog een aantal vragen, evenals over de uitvoeringsgevolgen van de richtlijn.

De leden van de fractie van de SP hebben kennisgenomen van voorliggend wetsvoorstel en hebben hierover enkele vragen.

2. De Europeesrechtelijke achtergrond van de richtlijn

2.1 De verhouding tot de Algemene verordening gegevensbescherming

De leden van de fractie van het CDA hebben erop gewezen dat de verordening gegevensbescherming en de richtlijn elkaar wederzijds uitsluiten. Er is echter wel sprake van enige mate van materiële overlap. De leden van deze fractie hebben gevraagd waarom er bij de totstandkoming niet is gekozen om de overlap op te nemen in de verordening gegevensbescherming, en of dit niet tot een duidelijker geheel had geleid. De leden van de fractie van het CDA hebben verder gelezen dat de richtlijn en de verordening gegevensbescherming veel onderwerpen regelen, maar niet op identieke wijze. Hierbij lijkt nu de situatie te ontstaan dat er twee regimes komen te gelden voor organisaties die zowel onder de verordening gegevensbescherming als de richtlijn vallen. De leden van deze fractie meenden dat door de keuze voor een verordening en richtlijn die elkaar wederzijds uitsluiten confrontatie met verschillende regimes niet te voorkomen is, en hebben gevraagd in hoeverre organisaties

hierover worden voorgelicht. Zij hebben tevens gevraagd of de regering kan aangeven waarom dit niet tot veel extra administratie zal leiden.

De richtlijn gegevensbescherming opsporing en vervolging is van toepassing op de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen met inbegrip van de bescherming tegen en de voorkoming van gevaren van de openbare veiligheid. De AVG is van toepassing op de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. De leden van de fractie van het CDA hebben terecht opgemerkt dat, voor wat betreft het toepassingsbereik, de richtlijn en de verordening elkaar wederzijds uitsluiten: waar de richtlijn geldt is de verordening niet van toepassing en andersom. Weliswaar zijn de regels van de richtlijn en de AVG op een aantal punten identiek of min of meer gelijk, dat neemt niet weg dat ofwel de richtlijn ofwel de AVG van toepassing is. Op dat punt is er geen sprake van overlap. Er is wel sprake van overlap op het gebied van de inhoud van de normen; hiervoor is echter bewust gekozen om de toepassing van meer algemene regels op het gebied van gegevensbescherming eenvormig toe te passen. Dit vereenvoudigt tevens de uitvoering voor de instanties die taken uitvoeren zowel op het gebied van de richtlijn als van de AVG. Het lijkt dan ook niet waarschijnlijk dat het opnemen van de overlap in de verordening gegevensbescherming tot een duidelijker geheel zou hebben geleid.

Doelbinding is een belangrijk principe bij gegevensbescherming. De keuze voor de toepasselijke regeling hangt af van het antwoord op de vraag voor welk doel het persoonsgegeven wordt verwerkt. De AVG en de richtlijn sluiten elkaar wederzijds uit. Gaat het om de gegevensverwerking door bevoegde autoriteiten met het oog op de uitvoering van de politietaak en de vervolging van strafbare feiten, dan is de richtlijn van toepassing, gaat het om de gegevensverwerking voor andere doelen dan is de AVG in beginsel van toepassing (de AVG is niet van toepassing op de verwerking van persoonsgegevens in het kader van activiteiten die buiten de werkingssfeer van het Unierecht vallen, door de lidstaten bij de uitvoering van activiteiten die binnen de werkingssfeer van titel V, hoofdstuk 2, VEU vallen en door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit). Met dit onderscheid in het toepassingsgebied wordt overigens nauw aangesloten bij het huidige Europeesrechtelijke kader voor de verwerking van persoonsgegevens, zoals dat is uitgewerkt in de huidige Privacyrichtlijn (Pb L 281/31) en het Kaderbesluit dataprotectie (Pb L350/60). Ook in de huidige situatie hebben instanties bij de uitvoering van hun taken te maken met verschillende regimes. Zo verwerkt bijvoorbeeld het openbaar ministerie gegevens ten behoeve van de vervolging van strafbare feiten onder het regime van de Wet justitiële en strafvorderlijke gegevens (Wjsg); de verwerking van gegevens ten behoeve van de uitvoering van de Wet bijzondere opnemingen in psychiatrische ziekenhuizen (BOPZ) valt daarentegen onder de reikwijdte van de Wet bescherming persoonsgegevens (Wbp). Op grond van het huidige Europeesrechtelijke kader voor gegevensbescherming zijn de uitvoeringsinstanties reeds bekend met de toepassing van verschillende privacyregimes voor verschillende taken.

Er is intensief overleg gevoerd met de betrokken instanties over de implicaties van de richtlijn op de gegevensverwerking, en de afgrenzing tussen de richtlijn en de AVG. Verschillende instanties hebben laten weten maatregelen te nemen om ervoor te zorgen dat medewerkers geïnformeerd zijn over de aanstaande wijzigingen. De politie zal deze richtlijn

implementeren via het verbeterprogramma naleving Wpg en informatiebeveiliging. Het openbaar ministerie heeft in 2017 een programma ingericht om zich voor te bereiden op de inwerkingtreding van de AVG en de richtlijn gegevensbescherming. Medewerkers van het openbaar ministerie zullen vanuit het programma worden geïnformeerd over de nieuwe wetgeving. De Minister van Defensie heeft bij de Koninklijke marechaussee extra privacyfunctionarissen aangesteld die tot taak hebben te adviseren over de inrichting van de toepasselijke IT-systemen en het werken met de privacy regimes. Degenen die met die gegevens werken, zullen worden opgeleid en getraind in het werken onder de verschillende regimes. Verder worden de IT-systemen zo ingericht dat de gegevens vanzelf in de juiste gegevensbakken worden opgenomen. Dit is voor het grootste deel nu al het geval.

De leden van de D66-fractie hebben geconstateerd dat de verplichtingen van de Richtlijn moeten worden omgezet in nationale wetgeving, terwijl de verplichtingen van de Verordening rechtstreeks werken. De leden van deze fractie onderschrijven het uitgangspunt dat zoveel mogelijk moet worden voorkomen dat de instanties binnen de strafrechtsketen worden geconfronteerd met verschillende verwerkingsregimes, met het oog op de uitvoerbaarheid van de regels voor de verwerking van de persoonsgegevens door de betreffende instanties, maar vragen zich toch af of de uitvoerbaarheid, in de gevallen waar geen recht gedaan kan worden aan dat uitgangspunt, niet in het geding komt. Zij zouden graag van de regering vernemen waar de knelpunten zitten in de uitvoering bij organisaties die aan zowel de Verordening, de nationale uitvoeringsbepalingen bij de Verordening en de Richtlijn moeten voldoen, en welke mogelijkheden hij ziet om in die gevallen tot een oplossing te komen.

Zoals hierboven, naar aanleiding van vragen van de leden van de CDA-fractie is opgemerkt, is de richtlijn – kort gezegd – van toepassing op de verwerking van persoonsgegevens ten behoeve van de uitvoering van de politietaak, de vervolging van strafbare feiten en de tenuitvoerlegging van straffen. Het was voor Nederland van bijzonder belang dat de uitvoering van de politietaak integraal onder de reikwijdte van de richtlijn zou worden gebracht, omdat de gegevensverwerking van de politie en de Kmar ten behoeve van de verschillende onderdelen van de politietaak – te weten de opsporing van strafbare feiten, de handhaving van de openbare orde en de hulpverlening – onderling nauw samenhangt. Uit de systematiek vloeit voort dat de instanties binnen de strafrechtsketen uitsluitend worden geconfronteerd met verschillende verwerkingsregimes voor zover zij taken uitvoeren die geen betrekking hebben op de uitvoering van de politietaak, als hierboven bedoeld, de vervolging van strafbare feiten of de tenuitvoerlegging van straffen. De gegevensverwerking vindt dan niet plaats ten behoeve van de strafrechtsketen, en valt dan onder het regime van de AVG. Dit is echter niet nieuw omdat ook thans, op grond van de EU-regelgeving, onderscheid wordt gemaakt tussen opsporing en vervolging enerzijds en andere taken anderzijds. Zoals eerder, naar aanleiding van vragen de leden van de fracties van de SP en het CDA, is opgemerkt leidt het van toepassing zijn van verschillende verwerkingsregimes als zodanig niet tot knelpunten. Wel is het van belang dat duidelijkheid bestaat over het regime dat in het concrete geval van toepassing is. Hierover is in het kader van de voorbereiding van het wetsvoorstel overleg gevoerd met de uitvoeringsinstanties. Ook heeft de wijziging van het regime voor de verwerking van persoonsgegevens ten behoeve van bepaalde taken ten dienste van de justitie (zoals de uitvoering van de vreemdelingentaak en het toezicht in het kader van aan de korpschef geattribueerde taken zoals die op grond van de Wet wapens en munitie en de Wet particuliere beveiligingsorganisaties en recherchebureaus) consequenties voor de beschikbaarheid van politiegegevens voor een

goede uitvoering van deze taken. De Wpg gaat namelijk uit van een systeem van «free flow of information» binnen de organisaties die onder de reikwijdte van de wet vallen (politie, de Kmar en de bijzondere opsporingsdiensten). Dit wil zeggen dat de verwerkingsverantwoordelijke politiegegevens ter beschikking stelt aan personen die door hemzelf dan wel door een andere verwerkingsverantwoordelijke zijn geautoriseerd voor de verwerking van politiegegevens, voor zover zij deze gegevens nodig hebben voor een goede uitvoering van hun taak (art. 15, eerste lid, Wpg). Omdat de verwerking van persoonsgegevens voor dit doel niet langer onder het regime van de Wpg valt, zijn aanvullend wettelijke maatregelen wenselijk om een goede toegang tot de politiegegevens ten behoeve van de uitvoering van deze taken te verzekeren. Daarom is in het wetsvoorstel een grondslag opgenomen voor de aanpassing van het Besluit politiegegevens, zodat wordt voorzien in de mogelijkheid van rechtstreekse toegang van de korpschef en de Minister van Defensie tot de betreffende politiegegevens, voor zover noodzakelijk voor het uitvoeren van die taken. Dit betreft een wijziging van artikel 23 van de Wet politiegegevens (Artikel I, onderdeel Y).

De leden van de SP-fractie hebben opgemerkt dat instanties die onder het toepassingsgebied van de richtlijn vallen, zoals de politie en de Koninklijke marechaussee (Kmar), niet alleen te maken krijgen met de nationale regelgeving ter implementatie van de richtlijn maar ook met zowel de bepalingen van de AVG en de Uitvoeringswet AVG, voor zover dit taken betreft die geen betrekking hebben op het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. De leden van deze fractie hebben gevraagd of voor deze leden concreet kan worden gemaakt in welke gevallen welke regelingen prevaleren voor welke instanties. Zij hebben tevens gevraagd of de regering denkt dat het voor de instanties zelf straks nog wel voldoende duidelijk is naar welk stuk regelgeving zij moeten kijken om aan de wet te voldoen.

Hierboven is, naar aanleiding van vragen van de leden van de CDA-fractie, reeds opgemerkt dat de keuze voor de toepasselijke regeling afhangt van het doel waarvoor het persoonsgegeven wordt verwerkt. Gaat het om de gegevensverwerking door bevoegde autoriteiten met het oog op de uitvoering van de politietaak en de vervolging van strafbare feiten, dan is de richtlijn van toepassing; gaat het om de gegevensverwerking voor andere doelen dan is de AVG in beginsel van toepassing. De Koninklijke marechaussee is belast met de uitvoering van de politietaak, als bedoeld in de artikel 4 Politiewet 2012. Op grond van de Politiewet 2012 valt onder de politietaak ook de uitvoering van de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken (vreemdelingentaak), waaronder begrepen de bediening van de daartoe door Onze Minister voor Immigratie en Asiel aangewezen doorlaatposten ter uitvoering van de Vreemdelingenwet (grensbewakingstaak). In de huidige situatie valt de verwerking van persoonsgegevens ten behoeve van de uitvoering van deze taken onder de reikwijdte van de Wpg. Dat gaat veranderen. De vreemdelingentaak en de grensbewakingstaak hebben geen betrekking op de uitvoering van de taken van de richtlijn, zodat de gegevensverwerking voor deze taken onder de AVG komt te vallen.
Voor de politie verandert het regime voor de verwerking van gegevens ten behoeve van bepaalde taken ten dienste van de justitie (zoals de uitvoering van de vreemdelingentaak en het toezicht in het kader van aan de korpschef geattribueerde taken zoals bijvoorbeeld in de Wet wapens en munitie en de Wet particuliere beveiligingsorganisaties en recherchebureaus). De verwerking van persoonsgegevens ten behoeve van de uitvoering van deze taken valt thans onder de Wpg. In de nieuwe situatie

zal deze gegevensverwerking worden beheerst door de AVG. Zoals hierboven is opgemerkt, is met de betrokken instanties intensief overleg gevoerd over de implicaties van de richtlijn op de gegevensverwerking, en de afgrenzing tussen de richtlijn en de AVG. Degenen die met die gegevens werken, zullen worden opgeleid en getraind in het werken met de verschillende regimes.

De leden van de SP-fractie hebben uit het voorliggende wetsvoorstel opgemaakt dat bijvoorbeeld bij het CJIB zowel de richtlijn als de AVG van toepassing kunnen zijn. De leden van deze fractie hebben gevraagd dat werkbaar is, en of dat niet tot problemen of onduidelijkheden leidt. De leden van deze fractie hebben tevens gevraagd of kan worden aangegeven wat in deze dan de verschillen tussen de AVG en de richtlijn zijn, en waar de bestaande Wpg en de Wjsg uitgebreidere waarborgen bieden dan de richtlijn.
De leden van de SP-fractie hebben voorts gevraagd of die waarborgen worden gehandhaafd en zo nee, waarom niet. Tenslotte hebben deze leden gewezen op het meerjarig verbeterplan, dat in 2016 tot stand is gekomen om de privacy bij de politie beter te waarborgen, en gevraagd hoe het hiermee staat, of dit wetsvoorstel de privacy waarborgen bij de politie verbetert en zo ja, op welke manier.

Het Centraal Justitieel Incasso Bureau (CJIB) is een agentschap dat ressorteert onder het Ministerie van Justitie en Veiligheid en dat onder andere is belast met het innen en incasseren van sancties die zijn opgelegd op basis van de Wet administratiefrechtelijke handhaving verkeersvoorschriften (Wahv) en de ondersteuning van het openbaar ministerie bij de tenuitvoerlegging van strafrechtelijke beslissingen. Daarnaast voert het CJIB in opdracht van bestuursorganen taken uit ter inning en incassering van opgelegde bestuurlijke boetes. Bij de uitvoering van deze taken verwerkt het CJIB persoonsgegevens zowel ten behoeve van de doelen van de richtlijn als ten behoeve van andere doelen, zoals bijvoorbeeld de administratiefrechtelijke afhandeling van verkeersvoorschriften en het innen en incasseren van bestuurlijke boetes. De gegevensverwerking rond de strafrechtelijke afdoening valt onder de reikwijdte van de richtlijn, de gegevensverwerking rond de administratiefrechtelijke afdoening valt onder de reikwijdte van de AVG. Zoals eerder, naar aanleiding van vragen van de leden van andere fracties is opgemerkt, leidt het van toepassing zijn van verschillende verwerkingsregimes als zodanig niet tot knelpunten. Wel is het van belang dat duidelijkheid bestaat over het regime dat in het concrete geval van toepassing is. Hierover is overleg gevoerd met het CJIB en is in de memorie van toelichting helderheid geboden (Kamerstukken II 2017/18, 34 889, nr. 3, blz. 12 en blz. 100/101).

De regels van de richtlijn opsporing en vervolging en de AVG zijn deels gelijk, in het bijzonder voor wat betreft de verplichtingen van de verwerkingsverantwoordelijke. Bepaalde verplichtingen van de verwerkingsverantwoordelijke zijn opgenomen in zowel de richtlijn als de AVG, waarbij de uitwerking vanwege het specifieke toepassingsgebied van deze rechtsinstrumenten op onderdelen in meer of mindere mate afwijkt. Voorbeelden zijn de melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit en aan de betrokkene (artikelen 30 en 31 RI en 33 en 34 Avg), het treffen van passende technische en organisatorische maatregelen ter bescherming en beveiliging van de gegevens (artikelen 24, 25 en 32, Avg en 19, 20 en 29 RI), het opstellen van een gegevensbeschermingseffectbeoordeling (artikelen 35 Avg en 27 RI), het bijhouden van verwerkingsactiviteiten in een register (artikelen 30 Avg en 24 RI), de informatieverstrekking aan de betrokkene (artikelen 13 en 14 Avg en 13 RI) en de kennisgeving van rectificatie (artikelen 19 Avg en 16,

zesde lid, RI). Anders dan de richtlijn gegevensbescherming opsporing en vervolging bevat de AVG geen verplichting tot geautomatiseerde vastlegging van gegevens over de gegevensverwerking (logging). Een belangrijk onderscheid betreft de bevoegdheden van de toezichthoudende autoriteit. De AVG voorziet in verstrekkende bevoegdheden voor de toezichthoudende autoriteit, zowel op het gebied van de corrigerende maatregelen als op het gebied van de sanctionering (artikel 58 Avg). De corrigerende maatregelen omvatten het gelasten tot het in overeenstemming brengen van verwerkingen met de verordening en een tijdelijke of definitieve verwerkingsbeperking, waaronder een verwerkingsverbod. Er kunnen administratieve geldboeten worden opgelegd tot 10 of 20 miljoen euro (artikel 83, vierde en vijfde lid, Avg). De richtlijn laat de lidstaten op dit terrein meer ruimte voor eigen afwegingen. Voor wat betreft de corrigerende maatregelen dient te worden voorzien in effectieve bevoegdheden voor de toezichthoudende autoriteit (artikel 47, tweede lid, RI). De vastgestelde straffen dienen doeltreffend, evenredig en afschrikkend te zijn (artikel 57 RI).

De huidige Wpg en Wjsg bieden uitgebreidere waarborgen dan de richtlijn, onder meer op het punt van de bewaartermijnen en de verstrekking van persoonsgegevens aan derden, met het oog op buiten de strafrechtspleging gelegen doelen. Voor wat betreft de Wpg kan aanvullend worden gewezen op de regeling van de privacy audits (artikel 33 Wpg), voor wat betreft de Wjsg op de regeling van het aantekenen van verzet tegen de verwerking (artikelen 26, 39q en 50, eerste lid, Wjsg). De richtlijn verplicht de lidstaten te voorzien in passende termijnen voor het wissen van persoonsgegevens of voor een periodieke evaluatie van de noodzaak van de opslag van persoonsgegevens (artikel 5 RI). De Wpg en de Wjsg bevatten uitgebreide bepalingen over de verwerkingstermijnen en de vernietiging of archivering van de gegevens na afloop van die termijnen. Hiervoor kan worden verwezen naar de artikelen 8, zesde lid, 9, vierde lid, 10, zesde lid, 12, zesde lid en 14 van de Wpg, en 4, 6, 39d en 41 van de Wjsg. Verder bepaalt de richtlijn dat persoonsgegevens die zijn verzameld met het oog op de doelen van de richtlijn, kunnen worden verwerkt voor andere doeleinden als dit krachtens het Unierecht of het lidstatelijke recht is toegestaan. De AVG is dan op die verdere verwerking van toepassing, tenzij de verwerking geschiedt in het kader van een activiteit die buiten de werkingssfeer van het Unierecht valt (artikel 9, eerste lid, RI). De Wpg en de Wjsg bevatten uitgebreide regelingen voor de verstrekking van persoonsgegevens aan derden. Hiervoor kan worden verwezen naar de artikelen 18 tot en met 20 van de Wpg en 8 tot en met 14, 39f en 42 van de Wjsg. De regels rond de bewaartermijnen en de verstrekking van persoonsgegevens aan derden worden uiteraard gehandhaafd, de Autoriteit persoonsgegevens is belast met het uitoefenen van toezicht op de naleving van de wettelijke voorschriften (artikelen 25 Wpg en 27, 39r en 51Wjsg).

De Minister van Justitie en Veiligheid heeft uw Kamer bij brief van 20 december 2017[1] geïnformeerd over de stand van zaken rond het verbeterprogramma. De maatregelen die zijn opgenomen in het verbeterplan hebben ten doel uitvoering van de voorgeschreven privacy waarborgen te verbeteren. In bovengenoemde brief is aangegeven dat de politie een aantal maatregelen in gang heeft gezet. Zo werkt de politie aan een geautomatiseerde oplossing voor het proces van verstrekken en intrekken van autorisaties voor politiesystemen bij (ver)plaatsing of uitdiensttreding. Deze functie wordt al voor een aantal applicaties toegepast. Het Politiedienstencentrum (PDC) implementeert het kader «Privacy & Security by Design» waardoor reeds in de ontwerpfase van

[1] Kamerstukken II, 2017 -2018, 29 628 nr. 754, bijlage 1.

applicaties weloverwogen keuzes worden gemaakt met betrekking tot de bescherming van persoonsgegevens. Ook investeert de politie in het verhogen van het kennisniveau over de mogelijkheden van het gebruik van informatie, waaronder het delen van informatie met derden. In 2018 zal een nieuwe externe audit plaatsvinden naar de naleving van de Wpg door de politie.

3. Het toepassingsgebied van de richtlijn gegevensbescherming opsporing en vervolging en doelbinding

De leden van de VVD-fractie hebben opgemerkt dat de richtlijn en het onderliggende wetsvoorstel zien op de bescherming van de verwerking van persoonsgegevens met het oog op, kort gezegd, de opsporing en vervolging van strafbare feiten, en gevraagd of de regering exact kan aangeven wanneer de richtlijn van toepassing is. De leden van deze fractie hebben tevens gevraagd om bevestiging dat de verwerking van persoonsgegevens bij politietaken ten dienste van justitie niet onder het toepassingsbereik van deze richtlijn valt, omdat dan de AVG van toepassing is, en of dit in de praktijk problemen kan opleveren omdat onhelder is welk juridisch regime precies van toepassing is.

Het doel van de verwerking is bepalend voor het toepasselijke verwerkingsregime. Gaat het – kort gegzegd – om de gegevensverwerking door bevoegde autoriteiten met het oog op de uitvoering van de politietaak en de vervolging van strafbare feiten, dan is de richtlijn van toepassing, gaat het om de gegevensverwerking voor andere doelen dan is de AVG in beginsel van toepassing. De taken ten dienste van de justitie worden genoemd in artikel 1, eerste lid, onder i, van de Politiewet 2012. Bepaalde taken ten dienste van de justitie hebben betrekking op de uitvoering van de taken van de richtlijn. Het betreft onder andere de betekening van gerechtelijke mededelingen in strafzaken, het vervoer van rechtens van hun vrijheid beroofde personen en de dienst bij de gerechten. De verwerking van persoonsgegevens voor deze taken valt dan ook onder het toepassingsbereik van de richtlijn. Andere taken ten dienste van de justitie, zoals de uitvoering van de vreemdelingentaak alsmede de aan de korpschef opgedragen uitvoering van de Wet wapens en munitie, de Wet particuliere beveiligingsorganisaties en recherchebureaus, de Wet natuurbescherming en de Wet explosieven voor civiel gebruik, hebben echter geen betrekking op de uitvoering van de taken van de richtlijn. De verwerking van persoonsgegevens voor deze taken valt dus inderdaad onder het toepassingsbereik van de AVG. Dit behoeft in de praktijk geen problemen op te leveren omdat het toepasselijke juridische regime helder is. Hierboven is, naar aanleiding van de vraag van de leden van de fractie van D66, aangegeven dat de wijziging van het regime voor de verwerking van persoonsgegevens ten behoeve van de taken ten dienste van de justitie wel consequenties heeft voor de beschikbaarheid van politiegegevens voor een goede uitvoering van deze taken. De Wpg gaat uit van een systeem van «free flow of information» binnen de organisaties die onder de reikwijdte van de wet vallen. Omdat de verwerking van persoonsgegevens voor dit doel niet langer onder het regime van de Wpg valt, zijn aanvullend wettelijke maatregelen wenselijk om een goede toegang tot de politiegegevens ten behoeve van de uitvoering van de betreffende taken ten dienste van de justitie te verzekeren. Daarom is in het wetsvoorstel voorzien in de mogelijkheid van rechtstreekse toegang van de korpschef en de Minister van Defensie tot de betreffende politiegegevens, voor zover noodzakelijk voor het uitvoeren van die taken.

De leden van de CDA-fractie hebben in de memorie van toelichting gelezen dat verwerking van persoonsgegevens met het oog op doeleinden als inzet bestuurlijke, bestuursrechtelijke en privaatrechtelijke

bevoegdheden niet onder de reikwijdte van de richtlijn vallen, en gevraagd hoe zich dit verhoudt tot gebieden van opsporing waar er ingezet wordt op een integrale aanpak, zoals bij de bestrijding van georganiseerde criminaliteit. De leden van deze fractie hebben tevens gevraagd onder welke regime de verwerking van bestuurlijke, privaatrechtelijke en fiscale gegevens valt, die uiteindelijk dienen ter opsporing en vervolging. Zij hebben voorts gevraagd of dit kan veranderen naar gelang het doel van de verwerking verandert, en welke gevolgen het voor de opsporing en vervolging heeft indien de gegevens verwerkt worden onder het verkeerde regime.

Zoals eerder, naar aanleiding van vragen van de leden van verschillende fracties, is opgemerkt is het doel van de verwerking bepalend voor het toepasselijke verwerkingsregime. Gaat het om de gegevensverwerking met het oog op de uitvoering van de politietaak en de vervolging van strafbare feiten door de bevoegde autoriteiten, dan is de richtlijn van toepassing; gaat het om de gegevensverwerking voor andere doelen dan is de AVG in beginsel van toepassing. De persoonsgegevens die onder het regime van de richtlijn worden verwerkt, kunnen verder worden verwerkt voor andere doelen als dit krachtens het Unierecht of het lidstatelijke recht is toegestaan. De AVG is dan op die verdere verwerking van toepassing, tenzij de verwerking geschiedt in het kader van een activiteit die buiten de werkingssfeer van het Unierecht valt (artikel 9, eerste lid, RI). De Wpg bevat een uitgebreide regeling voor de verstrekking van politiegegevens aan andere overheidsinstanties. Dit kan aan de orde zijn bij de integrale aanpak van criminaliteit. De Wpg biedt verschillende mogelijkheden tot verstrekking van politiegegevens aan derden. In alle gevallen geldt het vereiste van een zwaarwegend algemeen belang. Gaat het om structurele verstrekking op landelijk niveau dan is regeling in de wet of het Besluit politiegegevens aangewezen (artikel 18 Wpg). In het Besluit politiegegevens zijn de personen en instanties aangewezen aan wie politiegegevens kunnen worden verstrekt. Dit betreft bijvoorbeeld ook de verstrekking aan de vertegenwoordigers van de deelnemende bestuursorganen aan een Regionaal Informatie- en Expertisecentrum (RIEC), voor zover het betreft politiegegevens die relevant zijn voor het geïntegreerd handhavend optreden bij de bestrijding van georganiseerde criminaliteit (artikel 4:3, zevende lid, Bpg). Gaat het om verstrekking op regionaal of lokaal niveau dan biedt de Wpg aanvullend de mogelijkheid tot verstrekking in incidentele gevallen dan wel in het kader van samenwerkingsverbanden, met het oog op de doelen die nauw samenhangen met de uitvoering van de politietaak (artikelen 19 en 20 Wpg). De AVG biedt de mogelijkheid tot de verstrekking van persoonsgegevens aan andere overheidsorganen met het oog op de verdere verwerking van die gegevens voor andere doelen dan waarvoor deze zijn verzameld. Daarbij wordt onderscheid gemaakt tussen verenigbare en niet verenigbare doelen. Als er sprake is van verenigbare verwerking, is er geen andere afzonderlijke rechtsgrond vereist dan die op grond waarvan de verzameling van persoonsgegevens werd toegestaan. Als er sprake is van niet-verenigbare verwerking is de verdere verwerking slechts toegestaan op grond van een Unierechtelijke of lidstaatrechtelijke bepaling die in een democratische samenleving een noodzakelijke en evenredige maatregel vormt ter waarborging van een belangrijke doelstelling van algemeen belang, als bedoeld in artikel 23, eerste lid, Avg. Als persoonsgegevens, die worden verwerkt voor bestuurlijke, privaatrechtelijke en fiscale doelen, verder worden verwerkt ten behoeve van de doelen van de richtlijn (opsporing en vervolging van strafbare feiten) valt de verdere verwerking onder het toepassingsbereik van de richtlijn. De verdere verwerking valt dan onder het regime van de Wpg of de Wjsg. Het toepasselijke verwerkingsregime is dus inderdaad afhankelijk van het doel van de verwerking. Als de persoonsgegevens onder het verkeerde regime worden verwerkt

dan behoeft dat niet bij voorbaat nadelig te zijn voor de betrokkene. De normen van de richtlijn en de AVG zijn inhoudelijk deels gelijk, dit is hierboven naar aanleiding van een vraag van de leden van de SP-fractie over de verschillen tussen de AVG en de richtlijn (paragraaf 2.1), nader toegelicht. In geval er sprake zou zijn van nadeel voor de betrokkene vanwege de verwerking onder het verkeerde regime dan staan de betrokkene verschillende mogelijkheden open voor rechtsbescherming. Dit omvat de mogelijkheid tot het indienen van een verzoek om bemiddeling of advies dan wel een klacht bij de Autoriteit persoonsgegevens (AP) of het instellen van beroep bij de bestuursrechter. Overigens is de Autoriteit persoonsgegevens belast met het toezicht op de naleving van het bij of krachtens de wet bepaalde, de AP beschikt over de nodige bevoegdheden om daaraan invulling te geven.

De leden van de CDA-fractie hebben gevraagd of de regering kan aangeven, indachtig de Ondermijningswetgeving die nog moet verschijnen, of de richtlijn gegevensbescherming invloed zal hebben op de informatie-uitwisseling tussen verschillende instanties nu deze uitwisseling van groot belang is voor de bestrijding van ondermijnende criminaliteit. Onder verwijzing naar het delen van politie-informatie in een concrete zaak met een instantie als Veilig Thuis dan wel andere ketenpartners, hebben de leden van deze fractie gevraagd of deze mogelijkheden worden verruimd of juist beperkt. De leden van deze fractie hebben voorts gevraagd of ik aan de hand van een concrete casus kan schetsen hoe dit in de praktijk gaat lopen, en hoe dit gaat plaatsvinden op het vlak van ondermijning. Zij hebben tenslotte gevraagd deze nieuwe wetgeving voldoende juridische ruimte biedt om aan de in de praktijk geformuleerde behoefte aan informatiedeling te voldoen, en in welk opzicht de Ondermijningswet hier in de praktijk op aan zal kunnen sluiten.

Zoals hierboven, naar aanleiding van vragen van de leden van de fracties van de SP en het CDA, aan de orde is gekomen kunnen op grond van de richtlijn gegevensbescherming opsporing en vervolging de persoonsgegevens, die zijn verzameld met het oog op de doelen van die richtlijn, verder worden verwerkt voor andere doeleinden als dit krachtens het Unierecht of het lidstatelijke recht is toegestaan. De Wpg en de Wjsg bevatten uitgebreide regelingen voor de verstrekking van persoonsgegevens aan derden. Deze regelingen blijven onveranderd, ook voor wat betreft het delen van politie informatie in een concrete zaak met een instantie als Veilig Thuis dan wel andere ketenpartners. Het is dan ook niet waarschijnlijk dat de richtlijn invloed zal hebben op de informatie-uitwisseling tussen verschillende instanties.

Zoals hierboven is opgemerkt, blijft de regeling van de Wpg voor de verstrekking van persoonsgegevens aan andere ketenpartners onveranderd. De huidige regeling voorziet in de mogelijkheid van verstrekking van politiegegevens aan andere personen of instanties met het oog op een zwaarwegend algemeen belang, ter uitvoering van de bij of krachtens algemene maatregel van bestuur aan te geven taak of in incidentele gevallen of in het kader van samenwerkingsverbanden indien het doel van de verstrekking verenigbaar is met de politietaak. De wet biedt de mogelijkheid van verstrekking zowel in incidentele gevallen als in het kader van samenwerkingsverbanden en biedt de nodige ruimte om aan de in de praktijk geformuleerde behoefte aan informatiedeling te voldoen. De betrokken partijen zijn uiteraard gehouden om daarbij de regels van de Europese Unie op het gebied van de bescherming van persoonsgegevens na te leven. Dat geldt vanzelfsprekend ook voor de ondermijningswetgeving die ter uitvoering van het Regeerakkoord 2017–2021 bij brief van 16 februari jl. aan uw Kamer is aangekondigd. Daarbij zij erop gewezen

dat op de in deze brief genoemde informatie-uitwisseling binnen gemeenten niet de Wpg maar de AVG van toepassing is.

3.1 De gevolgen van het toepassingsbereik van de richtlijn voor de Wpg, de Wjsg en andere wetten die betrekking hebben op de verwerking van persoonsgegevens ten behoeve van opsporing en vervolging.

3.1.1 De wet justitiële en strafvorderlijke gegevens
De leden van de fractie van het CDA hebben gelezen dat de richtlijn het toepassingsbereik van de Wjsg verruimt tot de verwerking van tenuitvoerleggingsgegevens. Het gaat hier om persoonsgegevens en gegevens van rechtspersonen die betrekking hebben op de tenuitvoerlegging van straffen en maatregelen. De leden van deze fractie hebben gevraagd wie verantwoordelijk is voor geldige verwerking van deze gegevens, en of deze organisatie voldoende wordt geïnformeerd over de ophanden zijnde inwerkingtreding van de richtlijn.

Artikel 553 van het Wetboek van Strafvordering bepaalt dat de tenuitvoerlegging van rechterlijke beslissingen geschiedt door het openbaar ministerie dan wel op voordracht van deze door de Minister van Justitie en Veiligheid. Voor de tenuitvoerlegging van vrijheidsbenemende sancties is de Minister van Justitie en Veiligheid op grond van de zogeheten Beginselenwetten direct verantwoordelijk. Op het moment dat de Wet herziening tenuitvoerlegging strafrechtelijke beslissingen (Stb. 2017, 82) in werking treedt zal niet meer artikel 553 Sv maar artikel 6:1:1 Sv gelden, waarin is bepaald dat de tenuitvoerlegging van rechterlijke beslissingen en strafbeschikkingen geschiedt door de Minister van Justitie en Veiligheid; waarbij voor de goede orde wordt opgemerkt dat het openbaar ministerie ook bij deze nieuwe verantwoordelijkheidsverdeling nog taken in de fase van de tenuitvoerlegging houdt, zoals bijvoorbeeld het stellen van voorwaarden bij een voorwaardelijke invrijheidsstelling en het houden van toezicht op de naleving van voorwaarden. Voor het antwoord op de vraag van de leden van deze fractie betekent dit dat zowel het College van procureurs-generaal als de Minister van Justitie en Veiligheid verwerkingsverantwoordelijke voor de tenuitvoerleggingsgegevens kunnen zijn, onder de huidige en onder de toekomstige wetgeving. In het wetsvoorstel is hiermee rekening gehouden bij het aanwijzen van de verwerkingsverantwoordelijke voor tenuitvoerleggingsgegevens (Artikel II, onderdeel A; wijziging van artikel 1, onderdeel k, onder 3° Wjsg). Het openbaar ministerie is nauw betrokken bij de voorbereiding van het wetsvoorstel en in dat kader geïnformeerd over de inwerkingtreding van de richtlijn. Dit geldt ook voor de uitvoeringsdiensten van het Ministerie van Justitie en Veiligheid die – namens openbaar ministerie dan wel Minister – de feitelijke tenuitvoerlegging van opgelegde straffen verzorgen, zoals de Dienst Justitiële Inrichtingen en het Centraal Justitieel Incassobureau, waaronder het Administratie- en Informatiecentrum Executie (AICE).

3.1.2 Andere wetten die betrekking hebben op de verwerking van persoonsgegevens voor opsporing en vervolging
De leden van de VVD-fractie vreesden dat te strenge regels het moeilijk maken voor de opsporingsdiensten om criminaliteit te bestrijden en wilden dat het mogelijk is om op een snelle en niet bureaucratische wijze informatie uit te wisselen tussen overheidsdiensten in het kader van criminaliteitsbestrijding. De leden van deze fractie hebben gevraagd of de regering kan uitleggen of de uitwisseling van gegevens makkelijker of moeilijker wordt in het kader van criminaliteitsbestrijding, en of daarvan voorbeelden zijn te geven. Zij hebben tenslotte gevraagd of er aanpassingen van het wetsvoorstel mogelijk zijn die het uitwisselen van

gegevens in het kader van criminaliteitsbestrijding vergemakkelijken, en zo ja, welke, en of de regering bereid is die aanpassingen door te voeren.

Zoals hierboven, naar aanleiding van vragen van de leden van de fracties van het CDA, reeds aan de orde is gekomen bevatten de Wpg en de Wjsg uitgebreide regelingen voor de verstrekking van persoonsgegevens aan derden. Deze regelingen wordt ongewijzigd gehandhaafd, zodat de mogelijkheden tot uitwisseling van gegevens in het kader van criminaliteitsbestrijding onveranderd blijven en makkelijker noch moeilijker worden. Voor de beantwoording van de vraag over aanpassingen van het wetsvoorstel die het uitwisselen van gegevens in het kader van criminaliteitsbestrijding vergemakkelijken verwijs ik kortheidshalve naar de beantwoording van een soortgelijke vraag van de leden van deze fractie. Nu de richtlijn geen specifieke regels stelt over de verstrekking van gegevens aan derden zou een dergelijke aanpassing ook niet voortvloeien uit de implementatie van die richtlijn, zodat sprake zou zijn van een «nationale kop». Wel kan in dit verband worden opgemerkt dat thans een conceptwetsvoorstel voor een Wet gegevensverwerking door samenwerkingsverbanden in voorbereiding is. Dit wetsvoorstel vloeit voort uit een brief van de Minister van Veiligheid en Justitie van 14 december 2014 aan de Tweede Kamer over de aanpak van fraude (Kamerstukken II 2014/15, 32 761, nr. 79). Het conceptvoorstel voor een Wet gegevensverwerking door samenwerkingsverbanden (WGS) heeft tot doel de mogelijkheden tot het uitwisselen van persoonsgegevens binnen samenwerkingsverbanden te verbeteren met het oog op het behartigen van bepaalde doelen van algemeen belang, bijvoorbeeld het beter bestrijden van fraude. Een voorbeeld is een samenwerkingsverband van gemeenten, de politie, het openbaar ministerie en de Belastingdienst waarin zij de inzet van hun bestuurlijke, strafrechtelijke c.q. fiscale taken en bevoegdheden op elkaar afstemmen om tot de meest effectieve aanpak van bijvoorbeeld ondermijnende criminaliteit in de vorm van witwassen of hennepteelt te komen. Een samenwerkingsverband moet bij algemene maatregel van bestuur onder de werking van de WGS worden gebracht, anders is de WGS niet van toepassing. De WGS heeft dus niet tot doel een exclusief regime voor gegevensverwerking door samenwerkingsverbanden te creëren. Deze wet zal dan ook geen implicaties hebben voor de talloze bestaande samenwerkingsverbanden die binnen de grenzen van het huidige recht voldoende wettelijke mogelijkheden zien om op de voor hen noodzakelijke wijze persoonsgegevens te verwerken. Naar verwachting zal het conceptwetsvoorstel dit voorjaar in consultatie kunnen worden gegeven.

4. De consequenties van de Richtlijn gegevensbescherming opsporing en vervolging voor de wetgeving op het gebied van de bescherming van persoonsgegevens

De leden van de D66-fractie constateerden dat grootschalige gegevensverwerking (bigdata) kennelijk in toenemende mate van belang is door onder andere het gebruik van systemen als het Criminaliteits Anticipatie Systeem (CAS) door de politie en dat daar risico's voor de persoonlijke levenssfeer van betrokkenen aan zitten. De aan het woord zijnde leden zagen in ieder geval drie risico's, betrekking hebbend op het ontstaan van een completer beeld van personen door koppeling van gegevens, het ruimer inzetten van gegevens dan alleen in het kader van opsporing en het terecht komen van gegevens in andere strafdossiers voordat het vonnis dat het bewijs onrechtmatig oordeelt, onherroepelijk is. De leden van deze fractie zouden graag vernemen of, en zo ja hoe, de regering in dit voorstel tot uitvoering van de Richtlijn rekening heeft gehouden met deze ontwikkelingen van grootschalige gegevensverwerkingen en de daarbij behorende (voornoemde) risico's voor inbreuken op de persoonlijke levenssfeer van betrokkenen.

De waarborgen uit de richtlijn zijn techniekonafhankelijk en bieden daarmee ook bescherming bij het gebruik van nieuwe technische toepassingen waarmee op grote schaal persoonsgegevens kunnen worden verwerkt. Het betreft hier waarborgen ten aanzien van geautomatiseerde individuele besluitvorming (artikel 11 RI), «privacy by design» (artikel 20 RI), gegevensbeschermingseffectbeoordeling (artikel 27 RI), het voorafgaand consulteren van de toezichthoudende autoriteit (artikel 28 RI) en de beveiliging van gegevens (artikel 29 RI). Met het wetsvoorstel worden deze waarborgen in de Wpg en de Wjsg opgenomen. In aanvulling daarop stelt de huidige Wpg grenzen aan de grootschalige verwerking van persoonsgegevens. Naar aanleiding van het uitgangspunt van die wet, dat politiegegevens uitsluitend worden verwerkt voor welomschreven en gerechtvaardigde doelen, worden binnen de politietaak bepaalde doelen onderscheiden waarvoor politiegegevens mogen worden verwerkt. De leden van de fractie van D66 hebben gewezen op het risico van het ontstaan van een completer beeld van personen door koppeling van verschillende gegevens zonder aanvullende waarborgen dan zonder die koppeling mogelijk is. In reactie hierop kan worden opgemerkt dat de Wpg waarborgen biedt ter voorkoming van het verkrijgen van een completer beeld van personen door het koppelen van verschillende gegevens. Er gelden namelijk specifieke regels voor het geautomatiseerd vergelijken en in combinatie zoeken van politiegegevens (artikel 11 Wpg). Deze regels voorzien in de mogelijkheid de politiegegevens die worden verwerkt met het oog op een bepaald doel binnen de politietaak, geautomatiseerd te vergelijken met politiegegevens die worden verwerkt voor een ander doel, teneinde vast te stellen of verbanden bestaan tussen de betreffende gegevens. Het verdere gebruik van de gerelateerde gegevens is gekoppeld aan instemming van een daartoe bevoegde functionaris. Alleen de daartoe geautoriseerde ambtenaren van politie kunnen worden belast met de gegevensvergelijking. Indien dit noodzakelijk is ten behoeve van een bepaald onderzoek of een bepaald doel binnen de politietaak kunnen alle beschikbare politiegegevens, inclusief de gegevens van onverdachte personen, in combinatie met elkaar worden verwerkt. Deze zoekmogelijkheid dient op grond van de wet te worden voorbehouden aan een beperkte kring van politieambtenaren die de vereiste deskundigheid en ervaring bezitten. Bovendien is voor het gebruik van deze mogelijkheid een opdracht van het bevoegde gezag vereist. Dit is de officier van justitie of de burgemeester, afhankelijk van het doel van de verwerking. De leden van deze fractie hebben ten tweede gewezen op de mogelijkheid om gegevens, verkregen door de inzet van bijzondere opsporingsbevoegdheden, ruimer in te kunnen zetten dan alleen in het kader van opsporing. In reactie hierop kan worden opgemerkt dat het Wetboek van Strafvordering specifieke regels geeft voor het verdere gebruik van gegevens, die zijn verkregen met behulp van bepaalde bijzondere opsporingsbevoegdheden waarmee informatie wordt verzameld met betrekking tot personen die betrokken zijn bij de communicatie van de persoon tegen wie het opsporingsonderzoek is gericht. Aldus kunnen telefoongesprekken met familieleden, die geheel buiten de criminele activiteiten staan van de persoon tegen wie het onderzoek is gericht, worden afgetapt en opgenomen. De officier van justitie kan echter bepalen dat gegevens die zijn verkregen door stelselmatige observatie met behulp van een technisch hulpmiddel dat signalen registreert, het opnemen van vertrouwelijke communicatie, het opnemen van telecommunicatie of het vorderen van gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker, kunnen worden gebruikt voor een ander strafrechtelijk onderzoek of de verwerking met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij ernstige misdrijven (artikel 126dd Sv). Dit kan aan de orde zijn als deze gesprekken inzicht geven in de betrokkenheid van personen bij andere strafbare

feiten. Deze regeling beperkt niet alleen het verdere gebruik van de verkregen gegevens tot bepaalde doelen maar vereist daarvoor tevens de voorafgaande instemming van de officier van justitie. De leden van deze fractie hebben ten derde gewezen op het dilemma van het groter wordende risico met het gebruik van big data toepassingen dat bewijs in andere strafdossiers terecht kan komen voordat een vonnis, dat het oordeel bevat dat het bewijs onrechtmatig verkregen is, onherroepelijk is geworden, omdat de Wjsg in tegenstelling tot de Wpg geen zelfstandig rechtmatigheidscriterium bevat. Naar aanleiding hiervan kan worden opgemerkt dat het wetsvoorstel juist voorziet in de opneming van een zelfstandig rechtmatigheidscriterium in de Wjsg. Dit betreft artikel II, onderdelen B en AC, van het wetsvoorstel (artikel 3, derde lid en 39c Wjsg). Afgezien daarvan moet worden opgemerkt dat het leerstuk van het onrechtmatig bewijs een strafvorderlijk leerstuk is, dat ook strafvorderlijk kan worden gesanctioneerd. Als de rechter in een strafzaak vaststelt dat het bewijs onrechtmatig is verkregen, dan is het aan de rechter om de gevolgen hiervan te bepalen. Dit kan leiden tot strafvermindering, het buiten beschouwing laten van bewijsmateriaal of zelfs het niet-ontvankelijk verklaren van de officier van justitie. Als dit bewijs ook in andere strafzaken terecht is gekomen dan is het oordeel daarover eveneens aan de rechter, en ligt het in de rede te verwachten dat dit oordeel gelijkluidend zal zijn. Het toezicht op de naleving van het rechtmatigheidscriterium van de Wpg en de Wjsg is in handen van de Autoriteit persoonsgegevens. Het niet naleven van dit voorschrift kan leiden tot de sancties die in deze wetten zijn voorzien.

De leden van de D66-fractie hebben verder geconstateerd dat sinds 2016 in de Verenigde Staten de Judicial Redress Act geldt, waardoor burgers van de Europese Unie rechtsmiddelen ten dienste staan waaronder het neerleggen van een klacht bij de Amerikaanse autoriteiten in geval van onrechtmatige gegevensverwerking. Onder verwijzing naar de geschiedenis inzake de verhouding tussen de Europese Unie en de Verenigde Staten ten aanzien van gegevensuitwisseling zouden de leden van deze fractie graag vernemen of er eventuele knelpunten zijn ten aanzien van het geboden beschermingsniveau van de betrokkene in dit wetsvoorstel en het beschermingsniveau van de Judicial Redress Act.

Op grond van de Judicial Redress Act kunnen burgers van de Europese Unie evenals Amerikaanse burgers op grond van de US Privacy Act toegang krijgen tot een onafhankelijke rechter in de Verenigde Staten. Op grond van eerstgenoemde wet kunnen burgers van de Europese Unie, en dus ook die van Nederland, een beroep doen op een Amerikaanse rechter ten aanzien van bepaalde schendingen van de bescherming van hun persoonsgegevens, met name wanneer autoriteiten toegang of rectificatie van gegevens hebben geweigerd of de gegevens van een Europese ingezetene op onrechtmatige wijze hebben ontsloten. Een belangrijke voorwaarde voor de verstrekking van persoonsgegevens aan derde landen is dat het betrokken derde land of internationale orgaan een «adequate level of protection» voor de voorgenomen gegevensverwerking waarborgt (in de Nederlandse teksten vertaald als een passend niveau van gegevensbescherming of een toereikend niveau van gegevensbescherming). Deze voorwaarde is niet alleen terug te vinden in het huidige Kaderbesluit dataprotectie (artikel 13, eerste lid, onderdeel d, Kb dataprotectie) en de Privacyrichtlijn (artikel 25, eerste lid, Privacyrichtlijn) maar ook in de richtlijn gegevensbescherming opsporing en vervolging (artikel 36, eerste lid, RI) en de AVG (artikel 45, eerste lid, Avg). In vergelijking met de huidige Privacyrichtlijn en het Kaderbesluit gegevensbescherming is het systeem aangescherpt, in die zin dat de Commissie exclusief is belast met de beoordeling van de vraag of het niveau van gegevensbescherming adequaat is. Het juridische kader voor

de verstrekking van gegevens aan derde landen van de richtlijn is opgenomen in dit wetsvoorstel (Artikel I, onderdeel S; artikel 17a Wpg).

De Judicial Redress Act vormt een essentieel onderdeel van de rechtsbescherming van Europese burgers bij de uitwisseling van gegevens tussen de bevoegde autoriteiten in de Europese Unie en de Verenigde Staten, en vormt tevens een belangrijk element voor de beoordeling van het niveau van gegevensbescherming in de Verenigde Staten. Met het systeem voor de verstrekking van persoonsgegevens aan derde landen in de richtlijn gegevensbescherming opsporing en vervolging wordt voortgebouwd op het bestaande criterium van het passend of toereikend niveau van gegevensbescherming, dat voor de Amerikaanse autoriteiten destijds aanleiding heeft gegeven tot de vaststelling van de Judicial Redress Act. Voor zover de regering bekend is er dan ook geen sprake van knelpunten ten aanzien van het geboden beschermingsniveau in dit wetsvoorstel en het beschermingsniveau van de Judicial Redress Act.

5. Het advies van de Autoriteit persoonsgegevens

Naar aanleiding van het advies van de Autoriteit persoonsgegevens hebben de leden van de CDA-fractie gevraagd of de politie en het openbaar ministerie gevraagd is te adviseren over onderhavig wetsvoorstel, en of de regering gezien de invloed van onderhavig wetsvoorstel op het werk van politie en het openbaar ministerie hiertoe bereid is.
De leden van deze fractie hebben in de memorie van toelichting gelezen dat de grensbewakingstaak en de vreemdelingentaken onder verschillende privacyregimes gaan vallen terwijl zij onderling in de praktijk een hoge mate van vervlechting kennen. In de Wpg worden de vreemdelingentaken en de daarmee samenhangende grensbewakingstaak uitgezonderd waardoor de verwerking van persoonsgegevens onder de AVG komt te vallen. De leden van deze fractie hebben gevraagd of deze gegevens daarmee van een mindere mate van bescherming worden voorzien. De leden van deze fractie hebben voorts gevraagd of de regering wil ingaan op het bezwaar van de Autoriteit persoonsgegevens rondom het toepasselijke regime voor de vreemdelingensignalering in het Schengen Informatiesysteem. De regering geeft aan dat er wordt aangesloten op de systematiek van EU-regelgeving, maar deze leden hebben zich afgevraagd of dit in de praktijk niet alsnog tot uitvoerings- en handhavingsproblematiek kan leiden.

Het is niet gebruikelijk dat een wetsvoorstel ter implementatie van dwingende Europese regelgeving in consultatie wordt gegeven, omdat bij implementatieregelgeving de termijn voor implementatie strikt is. Bovendien worden nationale keuzes zoveel mogelijk vermeden zodat er weinig ruimte is voor de te consulteren organen om te reageren op onderwerpen waarop keuzes kunnen worden gemaakt. Ingevolge Titel 1.2 van de Algemene wet bestuursrecht gelden voor regelingen ter implementatie van bindende EU-rechtshandelingen in beginsel dan ook geen advies-, overleg-, inspraak-, en voorpublicatieverplichtingen. In gevallen waarin het horen van adviescolleges en andere instanties over nationale regelgeving niet wettelijk is voorgeschreven, ligt het in de rede dat de raadpleging in de fase van de voorbereiding van bindende EU-rechtshandelingen in de plaats treedt van het horen over de uiteindelijke implementatieregeling (artikel 9.16 Ar).
In plaats van consultatie over het wetsvoorstel is ervoor gekozen het openbaar ministerie en de politie, alsmede de andere betrokken instanties, reeds te betrekken bij de onderhandelingen over de toenmalige ontwerprichtlijn in Brussel, zodat daarmee rekening kon worden gehouden bij de inbreng van de Nederlandse delegatie. Tevens zijn deze

instanties nauw betrokken bij de voorbereiding van het wetsvoorstel. In het licht van de tijdsdruk rond de implementatie en de betrokkenheid van de politie en het openbaar ministerie bij de onderhandelingen en de voorbereiding van dit wetsvoorstel zie ik geen aanleiding deze instanties te vragen te adviseren over het wetsvoorstel.

De huidige Wpg is van toepassing op de verwerking van politiegegevens in het kader van de uitvoering van de politietaak. De uitvoering van de politietaak betreft de taken, bedoeld in de artikelen 3 en 4, eerste lid, van de Politiewet 2012. Dit omvat de uitvoering van de bij of krachtens de Vreemdelingenwet 2000 opgedragen taken, ook bekend als de vreemdelingentaken, en de bediening van de daartoe door Onze Minister voor Immigratie en Asiel aangewezen doorlaatposten, ook bekend als de grensbewakingstaak (artikel 4, eerste lid, onderdeel f, PW 2012). Deze taken behoren weliswaar tot de politietaak, als bedoeld in de artikelen 3 en 4, eerste lid, van de Politiewet 2012, maar hebben geen betrekking op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, zodat de verwerking van persoonsgegevens voor deze doelen buiten de reikwijdte valt van de richtlijn gegevensbescherming opsporing en vervolging. Naar aanleiding daarvan wordt in het wetsvoorstel voorgesteld artikel 4, eerste lid, onderdeel f, van de Politiewet 2012 uit te zonderen van de reikwijdte van de Wpg. De grensbewakingstaak en de vreemdelingentaken behoren dus wel tot de politietaak maar vallen niet onder het regime van de richtlijn. Deze taken vallen beide onder de reikwijdte van de AVG, en gaan dus niet onder verschillende privacyregimes vallen. Dit neemt niet weg dat als de uitvoering van de grensbewakingstaak of de vreemdelingentaken aanleiding geeft tot de opsporing en vervolging van strafbare feiten, inclusief de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, de verwerking van persoonsgegevens voor dat doel wel onder de reikwijdte van de richtlijn valt. De Wpg is dan van toepassing. Dit betekent niet dat de gegevens daarmee van een mindere mate van bescherming worden voorzien. De AVG bevat uitgebreide waarborgen voor een zorgvuldige gegevensverwerking, daarvoor kan worden verwezen naar het voorstel voor de Uitvoeringswet AVG en de toelichting daarop (Kamerstukken 34 851). Deze persoonsgegevens worden op een wijze beschermd, die passend is voor de verwerking van persoonsgegevens van personen die niet is gerelateerd aan de opsporing en vervolging van strafbare feiten of een ander doel van de richtlijn. Dit leidt er toe dat betrokkene meer invloed kan uitoefenen op de verwerking van zijn persoonsgegevens, door gebruikmaking van de rechten die hem op basis van de AVG ter beschikking staan.

Zoals reeds eerder, naar aanleiding van andere vragen van de fracties is opgemerkt, is het doel van de verwerking van persoonsgegevens leidend voor het toepasselijke verwerkingsregime. Gaat het om de gegevensverwerking door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid, dan is de richtlijn gegevensbescherming opsporing en vervolging van toepassing. Gaat het om de gegevensverwerking ten behoeve van andere doeleinden, dan is de AVG in beginsel van toepassing. Hiermee wordt aangesloten bij de bestaande systematiek rond EU-rechtsinstrumenten. Gaat het om EU-regelgeving op het gebied van asiel en migratie, dan werd voor de toepassing van regels op het gebied van de verwerking van persoonsgegevens tot nu toe verwezen naar, of aangesloten bij, de huidige Privacyrichtlijn van 1995. Gaat het om EU-regelgeving op het gebied van de opsporing en vervolging van strafbare feiten, dan werd voor de

toepassing van regels op het gebied van de verwerking van persoonsgegevens tot nu toe verwezen naar, of aangesloten bij, het huidige Kaderbesluit dataprotectie. Dit betreft een op zichzelf heldere systematiek, die eveneens van toepassing is op de gegevensverwerking in het Schengen Informatiesysteem (SIS). De verwerking van persoonsgegevens in het SIS met het oog op weigering van toegang tot of verblijf op het grondgebied van de lidstaten is thans geregeld in een verordening. De verwerking van persoonsgegevens met het oog op de politiële en justitiële samenwerking in strafzaken is thans geregeld in een raadsbesluit. De verordening en het besluit bevatten afzonderlijke regels voor gegevensbescherming (respectievelijk hoofdstukken VI en XII). In de voorstellen van de Commissie voor nieuwe verordeningen voor het SIS worden de verschillende gegevensbeschermingsregimes voor de verschillende doeleinden van het SIS gehandhaafd. De eerdergenoemde verordening wordt vervangen door een nieuwe verordening. In deze verordening worden de voorwaarden en procedures vastgesteld voor het opnemen en verwerken van signaleringen in verband met onderdanen van derde landen in het SIS en voor het uitwisselen van aanvullende informatie en extra gegevens met het oog op weigering van toegang tot en verblijf op het grondgebied van de lidstaten. Het eerdergenoemde raadsbesluit wordt eveneens vervangen door een verordening. Voor deze ontwerpverordeningen geldt dat wanneer de bevoegde autoriteiten in het kader van deze verordeningen persoonsgegevens verwerken, de AVG van toepassing is tenzij de nationale bepalingen tot omzetting van de richtlijn gegevensbescherming opsporing en vervolging van toepassing zijn. De nationale bepalingen tot omzetting van de richtlijn gegevensbescherming opsporing en vervolging zijn van toepassing op de verwerking van gegevens door bevoegde nationale autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van bedreigingen van de openbare veiligheid (artikelen 46, tweede en derde lid, Vo COM 882 en 64, tweede en derde lid, Vo COM 883). Ook hierbij geldt dat als het doel van de gegevensverwerking is gericht op asiel en migratie, de AVG van toepassing is op de gegevensverwerking voor dat doel. Als de gegevens worden geraadpleegd voor opsporing en vervolging, dan valt de verdere verwerking van de gegevens onder het regime van de richtlijn gegevensbescherming opsporing en vervolging, en daarmee onder het toepassingsbereik van de Wpg of Wjsg.

De leden van de SP-fractie hebben gevraagd welke extra taken de Autoriteit Persoonsgegevens er door de implementatie van deze richtlijn bijkrijgt. De leden van deze fractie hebben tevens gevraagd of de regering de mening van de AP, dat naleving van de thans geldende normen op problemen stuit en dat daarom de keuze voor minimumimplementatie niet bevorderlijk is voor tussentijdse naleving, deelt en zo ja, wat zij hier aan gaat doen. De leden van deze fractie hebben verder gevraagd of de regering puntsgewijs kan reageren op elk van de punten van de AP uit haar adviesbrief ten aanzien van dit wetsvoorstel, waarop zij baseert dat de richtlijn is gebaseerd op een onjuiste opvatting over de grondslag en reikwijdte van de richtlijn en hierdoor niet voldoet aan de vereiste nauwgezette omzetting van de Richtlijn in nationaal recht.

Op grond van de Wpg en de Wjsg is de Autoriteit persoonsgegevens belast met het toezicht op de verwerking van persoonsgegevens overeenkomstig het bij en krachtens deze wetten bepaalde (artikelen 35, eerste lid, Wpg en 27, eerste lid, Wjsg). Deze taak omvat tevens het geven van advies over wetsvoorstellen en ontwerpen van algemene maatregelen van bestuur die geheel of voor een belangrijk deel betrekking hebben op de verwerking van persoonsgegevens (artikelen 35, tweede lid, Wpg en 27, tweede lid, Wjsg). De richtlijn bevat een uitgebreide regeling

van de taken van de AP (artikel 46, eerste lid, RI). Deze taken zijn opgenomen in de Wpg en de Wjsg. De extra taken betreffen het beter bekend maken van het publiek met de regels, waarborgen en rechten rond de verwerking van persoonsgegevens, het beter bekend maken van de verwerkingsverantwoordelijken en de verwerkers met hun verplichtingen uit hoofde van het bij of krachtens de wet bepaalde, het desgevraagd verstrekken van informatie aan iedere betrokkene over de uitvoering van zijn rechten uit hoofde van het bij of krachtens de wet bepaalde, het behandelen van klachten van betrokkenen, het naar aanleiding van een klacht controleren van de rechtmatigheid van de verwerking en het informeren van de betrokkene daarover, het samenwerken met de toezichthoudende autoriteiten in andere lidstaten, het verrichten van onderzoeken naar de naleving van het bij of krachtens deze wet bepaalde, het volgen van de relevante ontwikkelingen rond de bescherming van persoonsgegevens, het verstrekken van advies naar aanleiding van een voorafgaande raadpleging en het leveren van een bijdrage aan het Europees Comité voor gegevensbescherming dat met de AVG is ingesteld (artikel 35b, eerste lid, onderdelen c. tot en met l., Wpg en 27, derde lid, Wjsg). Naar aanleiding hiervan kan nog worden opgemerkt dat van het toezicht van de AP is uitgezonderd het toezicht op de verwerking van persoonsgegevens door gerechten in het kader van hun gerechtelijke taken. Zoals in de memorie van toelichting bij de Uitvoeringswet Avg is aangegeven, is het aan de rechterlijke instanties zelf om hierin te voorzien (Kamerstukken II 2017/18, 34 851, nr. 3, blz. 24). Met het oog op de ratio van de bescherming van de onafhankelijkheid van de rechtspraak ligt het daarbij voor de hand de termen «rechterlijke taken» en «gerechtelijke taken» ruimer uit te leggen dan in de memorie van toelichting bij het wetsvoorstel is aangegeven (Kamerstukken II 2017/18, 34 889, nr. 3, blz. 98) en daaronder te verstaan «alle gerechtelijke activiteiten in het kader van rechtszaken».

Ik deel de mening van de Autoriteit persoonsgegevens dat de naleving van de thans geldende normen op problemen stuit. Mijn ambtsvoorganger heeft uw Kamer geïnformeerd over de uitkomsten van de externe audit naar de naleving van de Wpg door de politie en over het door de politie opgestelde verbeterplan. Ik verwijs kortheidshalve naar de eerdere brief hierover aan uw Kamer (Kamerstukken II 2015/16, 33 842, nrs. 3 en 4). Mijn ambtsvoorganger heeft in reactie op de evaluaties van de Wpg en de Wjsg geconstateerd dat beide wetten in onderling verband moeten worden herzien (Kamerstukken II 2014/15, 33 842, nr. 2). De zorg van de Autoriteit persoonsgegevens is dat de thans gehanteerde minimumimplementatie ertoe leidt dat de uitvoeringspraktijk op termijn tweemaal zal worden geconfronteerd met wijzigingen in het van toepassing zijnde wettelijk kader van gegevensbescherming. Ik merk op dat de korte implementatietermijn redelijkerwijs geen ruimte laat voor een andere keuze dan minimumimplementatie. Bovendien zal de politie ook na de herziening van de Wpg en Wjsg gebonden blijven aan de verplichtingen die voortvloeien uit de richtlijn gegevensbescherming opsporing en vervolging. De aangekondigde herziening zal moeten plaatsvinden binnen de kaders van deze richtlijn. De minimumimplementatie is dan ook geen argument voor de politie om niet tussentijds al te investeren in de naleving van de verplichtingen die voortvloeien uit de richtlijn.

Voor de beantwoording van de vraag over de omzetting van de richtlijn in nationaal recht verwijs ik naar de memorie van toelichting bij het wetsvoorstel, waarin reeds puntsgewijs is gereageerd op de punten van het advies van de Autoriteit persoonsgegevens ten aanzien van dit wetsvoorstel, inclusief het oordeel van de AP over de grondslag en de reikwijdte van de richtlijn en de omzetting van de richtlijn in nationaal recht (Kamerstukken II 2017/18, 34 998, nr. 3, paragraaf 8, punt l).

6. Uitvoeringsgevolgen van de richtlijn gegevensbescherming opsporing en vervolging

De leden van de D66-fractie hebben begrepen dat het effect van de uitvoering van de Richtlijn is dat de bevoegde autoriteiten met het oog op voorkoming, het onderzoek, de opsporing, de vervolging en de tenuitvoerlegging van strafbare feiten meer in overeenstemming met private bedrijven gaan handelen onder andere ten aanzien van het beveiligingsniveau van persoonsgegevens. De leden van deze fractie meenden dat deze verplichtingen ten aanzien van cyberveiligheid nogal een omslag is in de handels- en denkwijze van publieke organisaties, en zouden graag vernemen hoe de regering rekening houdt met de praktische uitvoerbaarheid van deze belangrijke omslag, mede vanuit het oogpunt van capaciteit en geldelijke middelen bij politie en justitie.

De Minister van Veiligheid en Justitie heeft in 2016 onderzoek laten doen naar de vraag of met het toen voorziene budget voor de materiële lasten, de vastgestelde voornemens ten aanzien van de sterkte, prestaties, dienstverlening, kwaliteit personeel, huisvesting en ICT ook daadwerkelijk en in het voorziene tempo gerealiseerd kunnen worden. Dit onderzoek vond plaats in het kader van de herijking van de realisatie van de nationale politie. De verbetering van de naleving van de Wpg en informatiebeveiliging zijn meegenomen in dit onderzoek.[2] In het rapport «Inzicht in de omvang van het personele en materiële budget nationale politie 2016–2020», dat op 22 maart 2016 aan de Tweede Kamer is aangeboden, is zichtbaar gemaakt dat het lastenniveau dat ontstaat door de afgesproken politiesterkte en het realiseren van de vastgestelde voornemens voor de politie hoger zijn dan de beschikbare omvang van het politiebudget. Het toenmalige kabinet heeft in reactie op dit onderzoek besloten extra middelen meerjarig aan de begroting 2017–20121 van de politie toe te voegen. De benodigde investeringen in de naleving van de Wpg en de informatiebeveiliging van de politie kunnen uit deze middelen worden bekostigd.

Het openbaar ministerie heeft bij de impactanalyse van het wetsvoorstel ten aanzien van de beveiliging aangegeven extra kosten te verwachten. Voor de invulling van de verplichtingen van de verwerkingsverantwoordelijke op het gebied van de beveiliging wordt rekening gehouden met de aard, reikwijdte, context en de doeleinden van de verwerking, alsmede met de risico's en vrijheden van de betrokkene. Op dit punt laat de richtlijn de verwerkingsverantwoordelijke dus een zekere marge voor afweging. In de impactanalyse wordt de aanname gedaan dat aanvullende beveiligingsmaatregelen moeten worden genomen, vanwege de scopeverbreding waarover de richtlijn gaat. In de sfeer van «firewalls», «internetsecurity» en «intruder-detection» zullen daarom extra maatregelen nodig zijn. De bestaande situatie voldoet reeds aan de Baseline Informatiebeveiliging Rijksdienst (BIR) en het Voorschrift Informatiebeveiliging Rijksdienst, Bijzondere Informatie (VIR-BI) voor gerubriceerde gegevens. De incidentele kosten voor extra risico dekkende maatregelen om de volledige scope te dekken van de omvang van de Richtlijn zijn door het openbaar ministerie geraamd op 0,5–1,5 miljoen euro en de structurele kosten van extra beveiliging op 0,5 miljoen euro.

De leden van de D66-fractie hebben verder gelezen dat in de memorie van toelichting nader is ingegaan op het punt van opleiding en scholing van degenen die belast zijn met gegevensverwerking. De regering heeft daarbij het meerjarig verbeterplan aangehaald waarbij kennis van de Wpg en informatiebeveiliging een standaard onderdeel is geworden van de

[2] Ik verwijs hiervoor naar pagina 15, 57 en 58 van de rapportage.

basisopleiding. De aan het woord zijnde leden hebben gevraagd of de regering de maatregelen uit het verbeterplan, de beperkte opleiding van personeel bij de Justitiële Informatiedienst (JustID) en de «awareness-campagnes» bij de Hoge Raad en JustID voldoende vind in het licht van voornoemde omslag in de denkwijze bij politie en justitie, en of er net als bij het meerjarig verbeterplan resultaten over de opleiding en «awarenesscampagnes» voornoemde instanties bekend zijn. Tot slot zouden de leden van de D66-fractie willen vernemen hoe in dit opleidings- en scholingsplan rekening is gehouden met de training van de functionarissen voor de gegevensbescherming die de bevoegde autoriteiten op grond van artikel 32 van de Richtlijn moeten aanstellen.

De Hoge Raad heeft beleid rondom datalekken en een meldingsprocedure datalekken vastgesteld en zal dit op korte termijn in de organisatie bekend maken. De beveiliging van de verwerkte persoonsgegevens is op orde. De in de richtlijn voorgeschreven benodigde logging van gegevens over de gegevensverwerking en andere benodigde systeemaanpassingen dienen in de periode tot 2023 te worden gerealiseerd. De daartoe benodigde middelen worden in die periode beschikbaar gesteld. Naar verwachting is het register van verwerkingsactiviteiten begin mei opgesteld. Binnen Justid hebben meerdere ambtenaren privacy opleidingen gevolgd en er worden diverse kennisbijeenkomsten bezocht om de kennis en kunde op een hoger en meer verspreid niveau te krijgen. De «awarenesscampagne» binnen Justid via het intranet en voorlichtingsbijeenkomsten hebben tot nu toe het gewenste effect zodat hiermee ook na de inwerkingtreding van het wetsvoorstel doorgegaan zal worden, ook na de implementatie van de richtlijn en de inwerkingtreding van de AVG. De politie en de Hoge Raad hebben inmiddels een functionaris voor gegevensbescherming aangesteld. Conform artikel 36, zesde lid van dit wetsvoorstel zullen aan de functionaris voor gegevensbescherming de middelen ter beschikking worden gesteld die nodig zijn voor het vervullen van de taken en voor het in standhouden van de deskundigheid. Justid valt onder de verantwoordelijkheid van de Minister van Justitie en Veiligheid en heeft daardoor als functionaris voor gegevensbescherming de betreffende functionaris van het departement. Wel wordt er binnen Justid een «privacy officer» aangesteld en hebben meerdere medewerkers de Certified Information Privacy Manager (CIPM) opleiding gevolgd waardoor de kennis en kunde ten aanzien van privacy ruim aanwezig is.

6.1 Financiële gevolgen

De leden van de SP-fractie hebben gevraagd of het extra geld dat nodig is voor de politie naar aanleiding van dit wetsvoorstel komt uit het in het regeerakkoord toegezegde bedrag van 267 miljoen euro of dat deze bedragen ergens anders vandaan komen.

De lasten die verbonden zijn aan de uitvoering van de richtlijn gegevensbescherming opsporing en vervolging worden door de politie meegenomen in de opstelling van de begroting van de politie. De middelen die de politie ontvangt uit het Regeerakkoord 2017–2021[3] worden hiervoor niet ingezet.

[3] «Vertrouwen in de toekomst», Regeerakkoord 2017–2021, VVD, CDA, D66 en Christen Unie.

II. ARTIKELSGEWIJS

Artikel 13 van de Richtlijn

De leden van de VVD-fractie hebben begrepen dat dit artikel betrekking heeft op de informatie die de verwerkingsverantwoordelijke moet verstrekken aan betrokkenen, maar dat de richtlijn de mogelijkheid geeft om deze informatieverplichting te beperken (zie artikel 13 lid 3). De leden van de deze fractie hebben zich afgevraagd of het niet nuttig kan zijn om de informatieverplichting verder te beperken in het belang van de opsporing en vervolging van strafbare feiten, of het bijvoorbeeld ook mogelijk zou zijn een uitzondering te maken op de verplichte informatieverstrekking voor personen ten aanzien van wie wordt vermoed dat zij slachtoffer kunnen worden van een strafbaar feit, bij getuigen en/of bij personen die voor een strafbaar feit zijn veroordeeld (meer precies, bij het voorgestelde artikel 6b onder b, c en d van de Wet politiegegevens), en wat de voor- en nadelen daarvan zouden zijn.

De richtlijn voorziet in een meer actieve informatieverplichting voor de verwerkingsverantwoordelijke, dat wil zeggen dat de betrokkene wordt geïnformeerd over de verwerking van persoonsgegevens zonder dat daaraan een verzoek van de betrokkene ten grondslag ligt. De richtlijn biedt de lidstaten de mogelijkheid de verstrekking van de informatie uit te stellen, te beperken of achterwege te laten als dat een noodzakelijke en evenredige maatregel is om bepaalde belangen te beschermen (artikel 13, derde lid, RI). Daarnaast biedt de richtlijn de lidstaten de mogelijkheid bepaalde verwerkingscategorien geheel of gedeeltelijk onder één van die belangen te brengen (artikel 13, vierde lid, RI).
In de memorie van toelichting is aangegeven dat van de mogelijkheid van artikel 13, derde lid, van de richtlijn geen gebruik is gemaakt omdat deze mogelijkheid een afweging in afzonderlijke gevallen veronderstelt en een dergelijke afweging niet goed verenigbaar is met de wijze van implementatie van de actieve informatieplicht voor specifieke gevallen (Kamerstukken II 2017/18, 34 889, nr. 3, blz. 78). In de Wjsg is deze mogelijkheid evenmin opgenomen. Naar aanleiding van de vraag van de leden van de VVD-fractie kan worden opgemerkt dat het in de praktijk inderdaad kan voorkomen dat de persoon over wie persoonsgegevens worden verwerkt, zoals een getuige of een slachtoffer, zodanige contacten onderhoudt met de verdachte dat het in het belang van het opsporingsonderzoek niet wenselijk is dat de getuige of het slachtoffer wordt geïnformeerd over de gegevensverwerking om te voorkomen dat de verdachte daarvan op de hoogte raakt. In een dergelijk geval dient de verwerkingsverantwoordelijke de mogelijkheid te hebben de informatieplicht jegens de getuige of het slachtoffer buiten toepassing te laten. Aldus is het wenselijk de door de richtlijn geboden mogelijkheid van het uitstellen, beperken of achterwege laten van de verstrekking van informatie om bepaalde belangen te beschermen, in de Wpg op te nemen. Ook voor de Wjsg is opneming van deze mogelijkheid wenselijk, omdat in alle fasen van het opsporingsonderzoek politiegegevens aan het openbaar ministerie kunnen worden verstrekt. Alsdan kan het eveneens van belang zijn de verstrekking van informatie aan de betrokkene, zoals een verdachte, getuige of slachtoffer, buiten toepassing te kunnen laten. Daarom zal bij nota van wijziging worden voorgesteld de Wpg en de Wjsg op dit punt aan te passen. Indien de ervaringen tijdens de implementatie daartoe aanleiding geven dan kan, binnen de kaders van de richtlijn, nadere aanpassing of bijstelling van de wettelijke regeling worden voorgesteld.

Artikel 15 van de richtlijn

De leden van de VVD-fractie hebben erop gelezen dat de richtlijn betrokkenen het recht geeft om uitsluitsel te krijgen of bepaalde persoonsgegevens worden verwerkt en, indien dat het geval is, om die persoonsgegevens in te zien. Artikel 15 van de richtlijn geeft lidstaten de mogelijkheid om dit inzagerecht te beperken. In de memorie van toelichting staat dat van deze mogelijkheid gebruik is gemaakt voor gegevens betreffende informanten, infiltranten en getuigenbescherming, maar in artikel 27, derde lid, van de Wet politiegegevens staat een verwijzing naar artikel 12 van de (huidige) Wet politiegegevens, die alleen maar verwijst naar informanten. De leden van deze fractie hebben gevraagd of infiltranten en gegevens betreffende getuigenbescherming dan ook onder de uitzondering vallen. Verder konden de leden van deze fractie zich voorstellen dat het raadzaam zou zijn om breder gebruik te maken van de ruimte die de richtlijn biedt om het inzagerecht te beperken, bijvoorbeeld door nog meer gegevens uit te zonderen van deze verplichting. Zij hebben gevraagd hoe de regering daar tegenover staat.

Het recht op inzage betreft een fundamenteel recht van de betrokkene. Als dat recht bij voorbaat wordt beperkt of zelfs uitgesloten dan vormt dit een ernstige aantasting van de rechten van burgers. De verplichting van de verwerkingsverantwoordelijke om inzage te geven in de persoonsgegevens die worden verwerkt, en daarmee rekenschap af te leggen over de gegevensverwerking en de juistheid van de verwerkte gegevens, vormt daarvan het spiegelbeeld. Zoals hierboven aan de orde is gekomen biedt de richtlijn de mogelijkheid om bepaalde verwerkingscategorieën geheel of gedeeltelijk uit te zonderen van het recht op inzage. De regering heeft aanleiding gezien om enkele verwerkingscategorieën uit te zonderen, omdat verstrekking van deze persoonsgegevens aan de betrokkene in zijn algemeenheid onwenselijk is in het licht van de belangen van opsporing en vervolging. Deze belangen prevaleren dus bij voorbaat boven het belang van de betrokkene op inzage. Mede gelet op de voorzieningen op basis van de richtlijn zie ik vooralsnog geen aanleiding tot verdere verruiming. Dit betekent niet dat in andere gevallen een verzoek om inzage moet worden gehonoreerd. Zoals in de beantwoording van de vorige vraag van de leden van deze fractie aan de orde is gekomen, is het recht op inzage geen absoluut recht. Een verzoek tot inzage kan worden afgewezen voor zover dit een noodzakelijke en evenredige maatregel is vanwege de in de wet neergelegde redenen, zoals de vermijding van nadelige gevolgen voor de opsporing en vervolging van strafbare feiten of de bescherming van de rechten en vrijheden van derden (artikelen 27 Wpg en 21 Wjsg). Deze weigeringsgronden gelden onverkort. Dit betekent dat, als er reden bestaat tot weigering van inzage, de gronden daarvoor in het afzonderlijke geval moeten worden aangevoerd en onderbouwd. Het is dan uiteindelijk aan de rechter om de rechtmatigheid van die beslissing te toetsen.

I. Wpg, artikel 4a en II. Wjsg, artikel 7

De leden van de D66-fractie hebben de regering gevraagd nader in te gaan op de keuze om de verplichting tot het opstellen van een risicobeperkingsplan (artikel 29, tweede lid, Richtlijn) bij algemene maatregel van bestuur te regelen. De aan het woord zijnde leden hebben begrepen dat de keuze is gebaseerd op het feit dat deze verplichting erg gedetailleerd is uitgewerkt, maar achtten deze keuze voorshands minder bevorderlijk voor het bewustzijn bij bevoegde autoriteiten ten aanzien van cyberveiligheid dan een keuze deze verplichting, al dan niet gedeeltelijk, op te nemen in de wet.

De implementatie van bindende EU-rechtshandelingen in het nationale recht vindt plaats door middel van het vaststellen van algemeen verbindende voorschriften. Dit kan zowel een wet in formele zin zijn als een algemene maatregel van bestuur. De richtlijn bevat uitgebreide verplichtingen op het gebied van de beveiliging van persoonsgegevens. Dit betreft technische en organisatorische maatregelen om te waarborgen dat de verwerking in overeenstemming met de richtlijn wordt verricht en de rechten van de betrokkene worden beschermd. De verplichtingen van de richtlijn zijn grotendeels opgenomen in de Wpg en de Wjsg. Dit betreft de verplichtingen tot gegevensbescherming door middel van beveiliging en ontwerp en door standaardinstellingen. Aanvullend zijn enkele verplichtingen uitgewerkt in het Besluit politiegegevens en het Besluit justitiële en strafvorderlijke gegevens. Hiervoor is gekozen vanwege het meer technische karakter van deze voorschriften. De naleving van deze wettelijke voorschriften in de dagelijkse praktijk zal worden verzekerd doordat deze worden opgenomen in instructies en werkvoorschriften voor het politiepersoneel dat in aanraking komt met persoonsgegevens. Het opnemen van de meer technische voorschriften in een algemene maatregel van bestuur zal dan ook geen enkel gevolg hebben voor de naleving van de verplichtingen door de verwerkingsverantwoordelijke, evenals het toezicht daarop door de AP.

I. Wpg, artikel 6c en II. Wjsg, artikel 7d

De leden van de D66-fractie hebben geconstateerd dat verwerkingsverantwoordelijken de mogelijkheid hebben een verwerker in te schakelen om namens de verwerkingsverantwoordelijke gegevens te verwerken. De leden van deze fractie hebben gevraagd of de regering kan toelichten of zij knelpunten voorziet nu de verwerkingsverantwoordelijke zich aan het verwerkingsregime van de Richtlijn moet houden en de verwerker aan het regime van de AVG.

De verwerkingsverantwoordelijke kan gebruik maken van de diensten van een verwerker. De verwerker verwerkt de persoonsgegevens dan namens de verantwoordelijke. Dit betekent dat de verwerker gehouden is het verwerkingsregime na te leven dat van toepassing is op de verwerkingsverantwoordelijke. In het geval van verwerking op basis van het regime van de richtlijn betreft dit de Wpg of de Wjsg. Op dit punt wijkt de situatie overigens niet af van die op basis van de huidige privacywetgeving voor politie en justitie, als gebruik wordt gemaakt van de diensten van een verwerker. Ik voorzie op dit punt dan ook geen knelpunten.

I. Wpg, artikel 35c en II. Wjsg, artikel 27

De leden van de D66-fractie waren van mening dat het expliciet opnemen van een (algemene) bevoegdheid voor de Autoriteit Persoonsgegevens voor het instellen van een tijdelijke of definitieve begrenzing van het verwerken van gegevens, waaronder een verwerkingsverbod (artikel 47, tweede lid, Richtlijn), voor de Autoriteit Persoonsgegevens van belang is voor een goede omzetting van de richtlijn in nationale regelgeving. De leden van deze fractie zagen wel enig risico van een dergelijk verwerkingsverbod voor de voortgang van een onderzoek, de opsporing, de vervolging van strafbare feiten of de tenuitvoerlegging van een straf, en hebben gevraagd of de regering nader kan toelichten waarom er voor is gekozen om een dergelijke (algemene) bevoegdheid niet expliciet in de wet op te nemen (artikel 35c Wpg en artikel 27 Wjsg).

De richtlijn verplicht de lidstaten niet om bepaalde bevoegdheden tot handhaving toe te delen aan de toezichthoudende instantie. De richtlijn voorziet in een verplichting voor de lidstaten bij wet erin te voorzien dat

elke toezichthoudende autoriteit effectieve bevoegdheden heeft tot het treffen van corrigerende maatregelen, zoals de verwerkingsverantwoordelijke of de verwerker te waarschuwen dat met de voorgenomen verwerkingen waarschijnlijk een inbreuk op de krachtens deze richtlijn vastgestelde bepalingen wordt gemaakt, te gelasten de verwerkingen, waar passend, op een nader bepaalde manier en binnen een nader bepaalde periode in overeenstemming te brengen met de richtlijn, met name door het rectificeren of wissen van gegevens of beperken van de verwerking, en het opleggen van een tijdelijke of definitieve begrenzing van het verwerken, waaronder een verwerkingsverbod (artikel 47, tweede lid, RI). De richtlijn volstaat met een verplichting voor de lidstaten te voorzien in effectieve bevoegdheden terzake zonder dat bepaalde bevoegdheden dwingend worden voorgeschreven, waarbij rekening gehouden kan worden met de specifieke nationale situatie. Op basis van de huidige privacywetgeving voor politie en justitie hebben de bevoegdheden van de AP bij het toezicht op de naleving voornamelijk betrekking op het uitoefenen van bestuursdwang en het opleggen van een bestuurlijke boete. In dit wetsvoorstel wordt voorgesteld de bevoegdheden van de AP bij het toezicht op de naleving te verruimen, onder meer door aanpassing van de regeling voor het opleggen van een bestuurlijke boete. Dit betreft zowel de gevallen waarin een dergelijke boete kan worden opgelegd als de maximale hoogte van die boete. Mede in het licht van de voorgestelde verruiming acht ik een algemene bevoegdheid tot het opleggen van een verwerkingsverbod minder passend voor de specifieke situatie van opsporing en vervolging, omdat dit met zich mee zou kunnen brengen dat de criminaliteitsbestrijding ernstig wordt belemmerd.

De Minister voor Rechtsbescherming,
S. Dekker