

Vergaderjaar 2016–2017

33 542

Wijziging van het Wetboek van Strafvordering in verband met de regeling van het vastleggen en bewaren van kentekengegevens door de politie

C

MEMORIE VAN ANTWOORD

Ontvangen 8 maart 2017

1. Inleiding

Ik heb met belangstelling kennisgenomen van het voorlopig verslag van de vaste commissie voor Veiligheid en Justitie. Ik dank de leden van de verschillende fracties voor de door hen gestelde vragen die mij in de gelegenheid stellen op bepaalde onderdelen van het wetsvoorstel nader in te gaan. Dit betreft in het bijzonder de verhouding tot het internationale recht.

De leden van de **VVD**-fractie hadden met belangstelling kennisgenomen van het voorstel. Zij gaven aan dat zij in beginsel positief staan tegenover maatregelen die bijdragen aan de opsporing en vervolging van ernstige criminaliteit. De door deze leden gestelde vragen voorzie ik in het navolgende graag van een reactie.

Ook de leden van de **CDA**-fractie gaven aan met belangstelling kennis te hebben genomen van het wetsvoorstel. Zij hadden nog enkele vragen, die ik graag in deze memorie van antwoord beantwoord.

De leden van de **D66**-fractie hadden kennisgenomen van het voorstel. Zij merkten op dat het voorgestelde systeem voordelen voor de opsporing kan meebrengen, maar gaven aan nog wel zorgen en vragen te hebben ten aanzien van de proportionaliteit en de effectiviteit van de voorgestelde bepaling. Ik dank deze leden voor de door hen gestelde vragen en hoop deze zorgen met de beantwoording van hun vragen weg te kunnen nemen.

De leden van de **PvdA**-fractie hadden met belangstelling kennisgenomen van het wetsvoorstel. Zij gaven aan er goede nota van te hebben genomen dat de gegevens uitsluitend binnen vier weken geraadpleegd mogen worden voor de opsporing van een specifiek misdrijf en voor de aanhouding van voortvluchtige personen. Graag beantwoord ik de door deze leden gestelde vragen.

De leden van de **GroenLinks**-fractie merkten op met bezorgdheid te hebben kennisgenomen van het wetsvoorstel. Ik dank deze leden voor de door hen gestelde vragen, die mij de gelegenheid geven bepaalde onderdelen van het voorstel nader toe te lichten. Ik hoop hen door de beantwoording van de door hen gestelde vragen te kunnen overtuigen van de proportionaliteit en wenselijkheid van het voorstel.

De leden van de **ChristenUnie**-fractie gaven aan met belangstelling kennis te hebben genomen van het wetsvoorstel. Zij merkten op het belang te onderkennen van het benutten van alle informatie die door de overheid binnen de rechtsstatelijke kaders rechtmatig verkregen kan worden om plegers van (zwaardere) strafbare feiten én voortvluchtigen op te sporen. Tegelijkertijd, zo brachten zij naar voren, zien zij de risico's van een overheid die grootschalig ANPR-gegevens vastlegt. Met deze leden onderken ik het belang van een goede balans in de uitvoering ten aanzien van de doelbinding, de proportionaliteit en de wettelijke inkadering van de bevoegdheid in dit wetsvoorstel. Ik ben er van overtuigd dat met de voorgestelde wettelijke regeling is gekomen tot een evenwichtige regeling waarin een balans is gevonden tussen het belang van de opsporing bij de inzet van de voorgestelde bevoegdheid en het recht op bescherming van de persoonlijke levenssfeer. Graag beantwoord ik de door deze leden gestelde vragen.

2. Verhouding tot het internationale recht

De leden van de **VVD**-fractie vroegen of inzage kan worden gegeven in de algemene maatregel van bestuur (AMvB) bij dit wetsvoorstel. Een concept van de ontwerp-AMvB die op grond van het voorgestelde artikel 126jj Sv wordt opgesteld (hierna: het uitvoeringsbesluit) is recent in consultatie gegeven. Bijgevoegd treft u deze consultatieversie van het uitvoeringsbesluit aan.

Deze leden vroegen hoe wordt gewaarborgd dat de gegevens niet aan anderen worden verstrekt dan aan de in het wetsvoorstel genoemde officieren van justitie.

Het wetsvoorstel, zo beantwoord ik deze vraag, regelt dat alleen daartoe door de Minister van Veiligheid en Justitie geautoriseerde opsporingsambtenaren toegang hebben tot de database waarin deze gegevens zijn opgeslagen. In het uitvoeringsbesluit is vastgelegd dat de database zodanig wordt beveiligd dat ongeautoriseerde toegang (dus toegang door anderen dan de geautoriseerde opsporingsambtenaar) en pogingen daartoe worden gedetecteerd en dat tijdige interventie plaatsvindt. Dit gebeurt onder andere door persoonsgebonden authenticatie (artikel 10 van het uitvoeringsbesluit). Dat wil zeggen dat voor toegang tot de database altijd moet worden ingelogd met een aantal authenticatiegegevens en een unieke code. Alleen geautoriseerde opsporingsambtenaren krijgen een dergelijke unieke code. Wanneer wordt ingelogd in de database zal het systeem dit automatisch vastleggen, samen met de zoekvraag die wordt ingevoerd (artikel 9, vierde lid, van het uitvoeringsbesluit). Op deze wijze wordt voorkomen dat anderen toegang hebben tot het systeem. Voorts kan worden nagegaan welke geautoriseerde opsporingsambtenaar op welk moment heeft ingelogd. In de jaarlijkse privacy-audit (artikel 15 van het uitvoeringsbesluit) zal verslag worden gedaan van het aantal loggingen en de ingevoerde zoekvragen. De geautoriseerde opsporingsambtenaar mag het systeem alleen raadplegen na een bevel daartoe van de officier van justitie. Ook dit moet worden vastgelegd (artikel 8 van het uitvoeringsbesluit), zodat per zoekvraag controleerbaar is welk bevel daaraan ten grondslag ligt. Ook dit aspect zal in de jaarlijkse privacy-audit worden meegenomen.

Geautoriseerd, zo beantwoord ik een volgende vraag van deze leden, worden alleen opsporingsambtenaren die zijn belast met de taken of

werkzaamheden op het gebied van de coördinatie van het informatieproces ter ondersteuning van een goede uitvoering van de politietaak (artikel 6 van het uitvoeringsbesluit).

Deze leden vroegen verder hoe de geautomatiseerde verwijdering na vier weken plaatsvindt. Met de eerste nota van wijziging is in het wetsvoorstel expliciet vastgelegd dat de gegevens worden «vernietigd». «Vernietiging» van gegevens moet worden onderscheiden van «verwijdering» van gegevens. In dit laatste geval, mogen gegevens wel nog worden bewaard, maar niet meer voor (operationele doeleinden) worden gebruikt. Bij «vernietiging» worden de gegevens gewist. In het uitvoeringsbesluit is vastgelegd dat de gegevens «automatisch» worden vernietigd. Het ANPR-systeem en daarbij behorende ICT-voorzieningen zullen hierop worden ingericht.

Met de leden van de **D66**- en de **PvdA**-fractie ben ik van mening dat er een goede balans moet worden gevonden tussen het belang van de opsporing van ernstige strafbare feiten en het recht op de bescherming van de persoonlijke levenssfeer.

ANPR-gegevens, zo merk ik op naar aanleiding van de vraag van deze leden, kunnen een belangrijke bijdrage leveren aan de opsporing van strafbare feiten en de aanhouding van voortvluchtige personen. Ook de onderzoekers van de DSP-groep – die in opdracht van het WODC een onderzoek hebben gedaan naar ANPR – concludeerden dat ANPR een meerwaarde kan hebben voor de opsporing. Zij baseerden zich daarbij onder andere op ervaringen in het buitenland en ervaringen bij pilots in Nederland. Zie hierover *Hits en hints. De mogelijke meerwaarde van ANPR voor de opsporing*, uitgevoerd door de DSP-groep in opdracht van het WODC (bijlage bij *Kamerstukken II 2011/12, 31 051, nr. 10*). Graag geef ik een aantal voorbeelden van mogelijk gebruik van ANPR-gegevens, die duidelijk maken welke rol de gegevens kunnen spelen.

In de eerste plaats zouden ANPR-gegevens behulpzaam kunnen zijn bij het in beeld brengen van mogelijke verdachten. Een voorbeeld dat ook in eerdere stukken genoemd is, is het geval waarin bij een tankstation een zwaargewonde man had verklaard dat de plegers kort voor de overval in een ander voertuig achter hen reden. Met behulp van de ANPR-gegevens – die toen nog werden bewaard – kon worden achterhaald om welke voertuigen het kon gaan. Het opsporingsonderzoek kon op deze wijze worden gestart. Ook bij andere misdrijven waarbij voertuigen zijn betrokken of waarbij bekend is dat verdachten met een voertuig zijn weggevlucht, zoals bijvoorbeeld ramkraken, andere (gewelddadige) overvallen en ernstige misdrijven in het verkeer, zouden met behulp van ANPR-gegevens dat voertuig en daarmee mogelijke verdachten in beeld kunnen worden gebracht.

Daarnaast zouden ANPR-gegevens kunnen bijdragen aan het achterhalen van verblijfplaatsen van personen. Bij een ontvoering zouden ANPR-gegevens bijvoorbeeld een dergelijke bijdrage kunnen leveren. Indien het kenteken van het voertuig van de vermeende ontvoerder bekend is, zou met de opgeslagen ANPR-gegevens direct na de ontdekking van de ontvoering snel een beeld kunnen worden gevormd van de locaties waar het kenteken van betreffende voertuigen gedurende de daaraan voorafgaande periode door een camera is vastgelegd. Zo kan het gebied dat nader onderzocht moet worden, worden verkleind. Dat kan eraan bijdragen dat slachtoffers (eerder) gevonden worden. ANPR-gegevens kunnen ook behulpzaam zijn bij het achterhalen van verblijfplaatsen van verdachten en voortvluchtigen. Zo kan bijvoorbeeld worden nagegaan naar welke plaatsen het voertuig van de verdachten is gereden nadat het feit is gepleegd.

Als derde voorbeeld kan worden genoemd de bijdrage die ANPR-gegevens zouden kunnen leveren aan het in kaart brengen van

medeverdachten. Met de ANPR-gegevens kan bijvoorbeeld worden nagegaan welke andere voertuigen steeds in de buurt van het voertuig van de verdachte waren (konvooi-analyse). Voorgaande toepassingen, waarbij na ontdekking van het strafbare feit wordt teruggezocht naar kentekengegevens, zijn onmogelijk indien ANPR-gegevens niet enige tijd zouden mogen worden opgeslagen.

Dit belang dat ANPR-gegevens kunnen hebben voor de opsporing moet worden afgewogen tegen het recht van burgers op bescherming van hun persoonlijke levenssfeer. Deze afweging heeft er toe geleid dat het wetsvoorstel het mogelijk maakt om ANPR-gegevens te bewaren, maar wel slechts onder een aantal strikte voorwaarden en waarborgen. Zo is sprake van een beperkte bewaartermijn van vier weken, is raadpleging slechts mogelijk voor twee in de wet opgenomen doelen (opsporing ernstige strafbare feiten en aanhouding voortvluchtigen) en is de toegang tot de gegevens beperkt en aan voorwaarden verbonden. Ik kom op deze aspecten hieronder naar aanleiding van vragen van de leden van de GroenLinks-fractie nog uitgebreid terug.

Ik meen dat hiermee een met voldoende waarborgen omklede en evenwichtige regeling wordt voorgesteld, die zowel recht doet aan het recht op bescherming van de persoonlijke levenssfeer van burgers als het belang van de opsporing en het belang van burgers bij het oplossen van ernstige strafbare feiten.

De leden van de D66-fractie wezen erop dat het College bescherming persoonsgegevens (hierna: het Cbp (thans de Autoriteit Persoonsgegevens)) en de Afdeling advisering van de Raad van State in hun adviezen bij het wetsvoorstel hadden aangegeven verschillende aspecten in de memorie van toelichting onvoldoende gemotiveerd te vinden. Naar aanleiding van die adviezen is de memorie van toelichting op die aspecten aangevuld. Daarnaast zijn naar aanleiding van die adviezen aanvullende waarborgen in het wetsvoorstel opgenomen. Zo is naar aanleiding van het advies van het Cbp de categorie misdrijven waarvoor de gegevens mogen worden geraadpleegd beperkt tot voorlopige hechtenisfeiten en bepaalde Wegenverkeerswetfeiten. Naar aanleiding van het advies van de Afdeling advisering van de Raad van State is deze categorie verder beperkt tot voorlopige hechtenisfeiten. Ook was naar aanleiding van het advies van het Cbp toegezegd de toegang tot de gegevens in het uitvoeringsbesluit te beperken tot daartoe door de Minister van Veiligheid en Justitie geautoriseerde opsporingsambtenaren (zie blz. 21 van de memorie van toelichting). Mede naar aanleiding van de (schriftelijke) inbreng van de leden van de Tweede Kamer is deze beperking van de toegang tot de gegevens met de eerste nota van wijziging in de wet zelf verankerd (*Kamerstukken II 2013/14, 33 542, nr. 7*).

Op het aspect dat zowel door de leden van de D66 en de PvdA-fractie is genoemd dat bij de vastlegging van de gegevens nog niet duidelijk is of en in hoeverre zij uiteindelijk van belang zijn voor het opsporen van een strafbaar feit (vastlegging «no hits»), ga ik graag hieronder in, bij de beantwoording van vragen van de leden van de GroenLinks-fractie over uitspraken van Europees Hof voor de Rechten van de Mens (hierna: EHRM) en het Hof van Justitie van de Europese Unie (hierna: HvJEU).

De leden van de PvdA-fractie vroegen in hoeverre er naast vaste camera's ook mobiele camera's zullen worden ingezet en onder welke omstandigheden. Ook stelden zij de vraag of daarmee een risico ontstaat voor een landelijk dekkend netwerk.

Ik kan deze leden bevestigen dat ook mobiele ANPR-camera's kunnen worden ingezet. Dat kunnen camera's in voertuigen zijn, maar ook «losse» camera's op een standaard die bijvoorbeeld (tijdelijk) langs de weg worden geplaatst. Voor de toepassing van dit wetsvoorstel zal het met name om deze laatste categorie mobiele camera's gaan. Op 1 januari 2017 zijn er ongeveer 400 vaste en 200 mobiele camera's in gebruik (voor de

huidige toepassingsmogelijkheden van ANPR). Van belang is dat dat niet betekent dat er ook op 600 locaties een ANPR-camera is geplaatst: per locatie zijn in veel gevallen meerdere (vaste) camera's nodig. In 2017 zullen nog meer vaste camera's worden aangesloten. Dit zal er toe leiden dat per 1 oktober 2017 op ongeveer op 180 locaties vaste ANPR-camera's worden ingezet voor de huidige toepassingen van ANPR, over het algemeen op snelwegen en rond knooppunten. Van een landelijk dekkend netwerk is dan ook geen sprake. In het uitvoeringsbesluit (artikel 3) zijn bovendien criteria opgenomen voor de plaatsing van ANPR-camera's; vastgelegd is dat ANPR-camera's alleen op bepaalde (risico)locaties kunnen worden ingezet. Ook is vastgelegd dat het verdere netwerk van camera's die worden ingezet voor de doelen van dit wetsvoorstel moet worden betrokken bij de beslissing over de proportionaliteit van de inzet van de camera's. Er zal dus altijd een keuze moeten worden gemaakt ten aanzien van de locaties waar ANPR een toegevoegde waarde heeft. Daarbij wordt onder meer uitgegaan van de eisen van proportionaliteit en subsidiariteit. Na inwerkingtreding van het wetsvoorstel zal jaarlijks een cameraplan worden opgesteld. In dit plan worden alle ANPR-camera's opgenomen die worden ingezet voor de doelen van dit wetsvoorstel. Het cameraplan wordt steeds openbaar gemaakt in de Staatscourant. Technisch is het inmiddels mogelijk om ook gezichten van bestuurders en passagiers zichtbaar vast te leggen door de voorruit heen, zo beantwoord ik een volgende vraag van deze leden. In andere landen wordt van deze technische mogelijkheid gebruikgemaakt om bijvoorbeeld bij snelheids-overtredingen vast te kunnen stellen wie de bestuurder van het voertuig was. Het vastleggen van gezichten is evenwel geen doel van Nederlandse ANPR-camera's. De in Nederland gebruikte ANPR-camera's van de politie zijn ook niet gericht op gezichtsherkenning en zijn daarop technisch niet afgesteld. De opstelling van de camera's is ook zodanig dat deze niet op gezichten, maar op het kenteken is gericht. Op het overgrote deel van de foto's zal dus ook geen (herkenbaar) gezicht te zien zijn. Dit is in overeenstemming met het wetsvoorstel, waarin wordt bepaald dat de «foto van het voertuig» kan worden vastgelegd. Daaruit kan reeds worden afgeleid dat het doel niet is het vastleggen van gezichten van bestuurders en passagiers. In lijn daarmee is in het uitvoeringsbesluit (artikel 5) vastgelegd dat camera's zo worden afgesteld dat op de beelden geen gezichten te herkennen zijn. Het is evenwel niet geheel uit te sluiten dat daarop toch gezichten zijn te herkennen, maar die worden niet verstrekt aan de opsporingsambtenaren die zijn betrokken bij het onderzoek. Van belang is dat de foto van het voertuig na vastlegging door de software wordt omgezet in een voor de computer herkenbaar kenteken. Bij deze omzetting wordt de foto dus niet bekeken door een opsporingsambtenaar. Verder wordt door de geautoriseerde opsporingsambtenaar gecontroleerd of op een foto die voldoet aan een zoekvraag op grond van het voorgestelde artikel 126j Sv gezichten herkenbaar voorkomen. Als dat onverhoopt het geval is, dan zal hij deze gezichten alsnog onherkenbaar maken voordat hij de foto verstrekt aan het opsporingsteam (artikel 5, vierde lid, van het uitvoeringsbesluit). Ook in die gevallen nemen opsporingsambtenaren belast met het onderzoek dus geen kennis van de gezichten.

De leden van de **GroenLinks**-fractie vroegen naar de verenigbaarheid van het wetsvoorstel met de uitspraak S & Marper (EHRM (Grote Kamer) 4 december 2008, appl.nrs. 30 576/04 en 30 566/04).

In antwoord op deze vraag stel ik voorop dat de door deze leden genoemde uitspraak betrekking heeft op vingerafdrukken en DNA-gegevens, gegevens die van een andere aard zijn dan ANPR-gegevens. Vingerafdrukken en DNA-gegevens kunnen direct worden teruggevoerd op een bepaalde persoon en kunnen specifieke individuen koppelen aan bepaalde plaatsen. Bovendien kan in het bijzonder van DNA-gegevens nog veel meer informatie over een bepaalde

persoon worden afgeleid. Op basis van ANPR-gegevens kan veelal slechts geconstateerd worden of een bepaald voertuig op een bepaald tijdstip op een bepaalde plaats is geweest. Dit betekent dat er eigenlijk altijd meer onderzoek nodig is om te kunnen vaststellen wie de bestuurder van het voertuig was en of deze persoon betrokken was bij het strafbare feit. Het vastleggen van vingerafdrukken en DNA-gegevens vormt een inbreuk op artikel 8, eerste lid, van het EVRM, waarin het recht op bescherming van de persoonlijke levenssfeer is vastgelegd. Een dergelijke inbreuk kan gerechtvaardigd zijn wanneer het bewaren van de desbetreffende gegevens bij wet is voorzien, een legitiem doel dient en noodzakelijk is in een democratische samenleving. Een en ander betekent onder meer dat een regeling proportioneel moet zijn. Dat gold volgens het EHRM niet voor de in het S & Marper-arrest centraal staande, vroegere bewaarregeling voor DNA-gegevens en vingerafdrukken van Engeland en Wales. Die regeling voorzag in het ongelimiteerd (permanent) bewaren van vingerafdrukken en DNA-gegevens van iedere vrijgesproken persoon, voor elk strafbaar feit, terwijl deze gegevens ongelimiteerd voor de opsporing in andere strafzaken konden worden gebruikt. Voor het gebruik van de DNA-gegevens en vingerafdrukken in andere strafzaken was de regeling zelfs primair bedoeld. Het EHRM stelde vast dat Engeland, Wales en Noord-Ierland de enige rechtsstelsels binnen de Raad van Europa zijn waarin vingerafdrukken en DNA-materiaal van personen van welke leeftijd dan ook en verdacht van welk strafbaar feit dan ook, voor onbepaalde tijd werden opgeslagen (r.o. 110). De perceptie dat de betrokken personen niet werden behandeld als onschuldige personen werd naar het oordeel van het EHRM vergroot door het feit dat hun data voor onbepaalde tijd werden bewaard op dezelfde wijze als de data van veroordeelde personen (r.o. 122). Daarbij overwoog het EHRM dat het opslaan van data van onschuldige personen in het bijzonder schadelijk kon zijn voor minderjarigen zoals S (r.o. 124).

Het geheel van deze kenmerken van de regeling, die ieder afzonderlijk al ruim waren, bracht het EHRM tot het oordeel dat de regeling niet proportioneel was, en dat de inbreuk die met het bewaren van de gegevens op het recht op eerbiediging van de persoonlijke levenssfeer wordt gemaakt, niet kon worden gerechtvaardigd (r.o. 119 en 125).

De hier voorgestelde ANPR-regeling wijkt op al de hiervoor genoemde punten in belangrijke mate af van de regeling die centraal stond in de S & Marper uitspraak van het EHRM. Allereerst mogen de ANPR-gegevens niet voor onbepaalde tijd worden bewaard; er geldt een (zeer korte) bewaartermijn van vier weken. De gegevens worden afzonderlijk van de overige politiegegevens bewaard en de toegang is voorbehouden aan speciaal daartoe geautoriseerde opsporingsambtenaren op bevel van de officier van justitie. Bovendien mogen de gegevens van onschuldige burgers niet (ongelimiteerd) worden gebruikt en zeker niet voor ieder strafbaar feit: de gegevens mogen uitsluitend in het kader van een concreet strafrechtelijk onderzoek op basis van een concrete zoekvraag worden geraadpleegd voor de twee in de wet opgesomde doelen (de opsporing van een voorlopige hechtenisfeit en de aanhouding van een voortvluchtige). Ik meen dan ook dat deze regeling ruimschoots binnen de grenzen van het EVRM blijft.

Deze leden wezen op de uitspraken Digital Rights (HvJEU 8 april 2016, C-293/12 en C-594/12) en Tele2 (HvJEU 21 december 2016, C-203/15 en C-698/15) van het HvJEU. Zij stelden over deze uitspraken verschillende vragen, die ik graag in onderlinge samenhang als volgt beantwoord. In beide genoemde uitspraken heeft het HvJEU zich kritisch uitgelaten over een algemene bewaarplicht voor telecommunicatiegegevens (verkeers- en locatiegegevens). Het Hof overwoog dat het bewaren van dergelijke telecommunicatiegegevens een ernstige aantasting vormt van het recht op bescherming van de persoonlijke levenssfeer – vastgelegd in

de artikelen 7 en 8 van het Handvest van de grondrechten van de EU –, omdat uit de gegevens zeer precieze conclusies kunnen worden getrokken over het privéleven van de personen van wie de gegevens zijn bewaard, zoals hun dagelijkse gewoonten, hun permanente of tijdelijke verblijfplaats, hun dagelijkse of andere verplaatsingen, de activiteiten die zij uitoefenen, hun sociale relaties en de sociale kringen waarin zij verkeren. Dit betekent dat, om een dergelijke inbreuk te rechtvaardigen, moet zijn voldaan aan de vereisten van een wettelijke grondslag, een legitiem doel en noodzakelijkheid (evenredigheid). Het HvJEU oordeelt in de uitspraken dat met het bewaren van de telecommunicatiegegevens een doel van algemeen belang wordt nagestreefd, te weten de bestrijding van criminaliteit (Digital Rights, r.o. 44). Ook ten aanzien van ANPR-gegevens geldt dat zij worden bewaard met het oog op het opsporen van ernstige strafbare feiten. Daarmee wordt ook in dit wetsvoorstel voldaan aan de eis dat sprake moet zijn van een legitiem doel.

De richtlijn die centraal stond in de Digital Rights-uitspraak werd evenwel niettemin onverbindend verklaard, omdat de regeling die daarin was opgenomen alles afwegende niet voldeed aan de eis van evenredigheid (proportionaliteit).

In de Tele2-uitspraak stond centraal de vraag in hoeverre een algemene (ongedifferentieerde) bewaarplicht voor telecommunicatiegegevens verenigbaar is met het Handvest van de grondrechten en welke waarborgen daarbij zouden moeten gelden.

Voordat ik inga op de overwegingen in de beide uitspraken, merk ik graag het volgende op. Het onderhavige wetsvoorstel vloeit niet voort uit Europese regelgeving, waardoor het Handvest van de grondrechten van de EU in beginsel daarop niet van toepassing is. Dat neemt evenwel niet weg dat, zoals ook de Afdeling advisering van de Raad van State in de voorlichting over de Digital Rights-uitspraak heeft opgemerkt (zie de bijlage bij *Kamerstukken II 2014/16*, 33 542, nr. 16), bij het bewaren van ANPR-gegevens rekening moet worden gehouden met het EVRM. Artikel 8 EVRM voorziet in een soortgelijke bescherming van het privéleven als het Handvest van de grondrechten van de EU, waardoor niet uitgesloten is dat daarvoor soortgelijke overwegingen gelden.

Met de leden van de fracties van D66, PvdA, GroenLinks en VVD kan worden vastgesteld dat dit wetsvoorstel en de regeling van de telecommunicatiegegevens gemeen hebben dat gegevens van onverdachte burgers worden opgeslagen. Daarmee is evenwel niet gezegd dat de overwegingen en voorwaarden in die uitspraken onverkort van toepassing zijn op ANPR-gegevens. De algemene bewaarregeling van telecommunicatiegegevens verschilt namelijk op belangrijke onderdelen van de hier voorgestelde bewaarregeling van ANPR-gegevens. Naast de aard van de gegevens (die langs de openbare weg worden verzameld) is het belangrijkste verschil dat van een ongedifferentieerde bewaarregeling geen sprake is; er is sprake van een geografische afbakening van de gebieden waarin ANPR-gegevens worden vastgelegd. Belangrijke verschillen zijn verder de duur van bewaartermijn, de kenbaarheid van de vastlegging en de beperkte toegang tot de gegevens. Wanneer naar de overwegingen van het HvJEU in de beide uitspraken over deze aspecten wordt gekeken dan meen ik dat de voorgestelde regeling zonder meer binnen de grenzen blijft die daaraan op grond van het recht op bescherming van de persoonlijke levenssfeer moeten worden gesteld. Ik licht dat toe.

Aard van de gegevens, verzameling langs de openbare weg

Essentieel is dat ANPR-gegevens van een andere aard zijn dan telecommunicatiegegevens. Daardoor moet de inbreuk die met de vastlegging en raadpleging daarvan op het recht op bescherming van de persoonlijke levenssfeer wordt gemaakt ook anders worden gewaardeerd. Met

telecommunicatiegegevens kan een meer omvattend beeld worden verkregen over gedragingen van burgers. Zoals hierboven reeds aan de orde kwam, kunnen deze gegevens volgens het HvJEU zeer nauwkeurige aanwijzingen verschaffen over het privéleven van degenen wier gegevens worden bewaard, zoals de gewoonten in het dagelijkse leven, uitgeoefende activiteiten, sociale relaties en sociale milieus. Op basis van onderhavig wetsvoorstel kan evenwel slechts een zeer beperkte set gegevens (het kentekennummer, een foto van het voertuig, de locatie van het waarnemen en het tijdstip van het passeren van de camera) worden bewaard. Met deze gegevens kan weliswaar inzicht worden verkregen in de locaties van een voertuig op bepaalde data of tijdstippen, maar er wordt geen direct inzicht verkregen in de aard of de duur van communicatie tussen personen evenals de aspecten die daarmee samenhangen zoals de sociale relaties tussen personen.

Daar komt bij dat kentekengegevens langs de openbare weg worden verzameld. De bestuurders van voertuigen kunnen weten en verwachten dat hun voertuig op de openbare weg aan de hand van het kenteken door de politie kan worden geregistreerd met het oog op de handhaving van wet- en regelgeving. Mede in het licht van het beginsel van de «reasonable expectation of privacy» van de betrokkene, waar ook de leden van de fractie van de ChristenUnie-fractie op wezen, dient het verzamelen en bewaren van kentekengegevens dan ook als een minder vergaande inbreuk op het recht op bescherming van de persoonlijke levenssfeer te worden beschouwd dan het verzamelen en bewaren van gegevens die betrekking hebben op vertrouwelijke communicatie (vgl. EHRM 2 september 2010, appl.nr. 35623/05 (Uzun), r.o. 66 en EHRM 28 januari 2003, appl.nr. 44647/98 (Peck)).

Reeds vanwege de andere aard van de gegevens kan niet worden gezegd dat de vereisten uit de uitspraken van het HvJEU (onverkort en in dezelfde mate) van toepassing zijn op de regeling voorgesteld in dit wetsvoorstel. Dat neemt niet weg dat wanneer naar de overwegingen uit de uitspraken wordt gekeken, kan worden geconstateerd dat in de hier voorgestelde regeling in de waarborgen die door het HvJEU worden genoemd, is voorzien.

Geografische afbakening

Bij de beoordeling en waardering van de evenredigheid van de bewaring van telecommunicatiegegevens stelt het HvJEU vast dat in het geval van een nationale regeling voor de algemene en ongedifferentieerde bewaring van alle verkeers- en locatie(telecommunicatie)gegevens, de bewaring van die gegevens de regel is terwijl de richtlijn 2002/58 eist dat deze bewaring de uitzondering vormt (r.o. 104). Daarbij lijkt het HvJEU in zowel de Digital Rights- als de Tele2-uitspraak veel gewicht toe te kennen aan het feit dat de gegevens van alle personen worden bewaard en de bewaring niet wordt beperkt tot gegevens die betrekking hebben op een bepaalde periode en/of een bepaald geografisch gebied en/of een kring van personen (algemene en ongedifferentieerde bewaarregeling) (Digital Rights, r.o. 59, Tele2, r.o. 103–106). Volgens het HvJEU zou kunnen worden gekozen voor een geografische afbakening aan de hand van een geografisch criterium wanneer de bevoegde nationale autoriteiten op basis van objectieve elementen van mening zijn dat in een of meer geografische gebieden een hoog risico bestaat dat daar misdrijven van een bepaalde ernst («serious crime») worden gepleegd (Tele2, r.o. 111).

Anders dan de hiervoor bedoelde regeling ten aanzien van telecommunicatiegegevens, is de hier voorgestelde regeling niet gebaseerd op een Europese richtlijn die voorziet in een verbod op de verwerking van bepaalde gevoelige persoonsgegevens waarbij een uitzondering op dat verbod slechts onder strikte voorwaarden mogelijk is. Bovendien, en dit is een van de belangrijkste verschillen tussen de in de uitspraken centraal

staande bewaarregelingen en de regeling in dit wetsvoorstel, is in dit wetsvoorstel wel in een geografische afbakening voorzien. In het cameraplan wordt vastgelegd op welke locaties camera's worden geplaatst en ingezet voor de vastlegging van ANPR-gegevens op grond van dit wetsvoorstel. Alleen camera's opgenomen in het cameraplan mogen worden gebruikt. De ANPR-camera's mogen voor de toepassing op grond van artikel 126jj Sv uitsluitend worden geplaatst op locaties die aan bepaalde criteria voldoen. Die criteria worden opgenomen in het uitvoeringsbesluit (artikel 3). Deze criteria zijn:

- of sprake is van een locatie met een bepaald risico (zoals bijvoorbeeld een vliegveld);
- of sprake is van een locatie met een intensieve verkeersstroom of een bepaalde functie;
- of sprake is van een locatie waarvan bekend is dat bepaalde strafbare feiten op dergelijke locaties worden gepleegd.

Kort samengevat worden ANPR-camera's slechts ingezet op voor de opsporing mogelijk relevante locaties. Bij de beslissing tot plaatsing en gebruik van ANPR-camera's zal bovendien het verdere netwerk van camera's dat voor deze toepassing wordt ingezet, worden betrokken. Dit wordt eveneens in het uitvoeringsbesluit vastgelegd. Anders dan bij de regeling van de telecommunicatiegegevens die in de uitspraken van het HvJEU centraal stonden, is er dus geen sprake van een ongedifferentieerde bewaring van alle ANPR-gegevens van alle voertuigen op alle wegen in Nederland: er gelden wel degelijk objectieve criteria aan de hand waarvan wordt bepaald op welke locaties ANPR-gegevens worden vastgelegd ten behoeve van de opsporing. Er zal dus altijd een keuze moeten worden gemaakt ten aanzien van de locaties waar ANPR een toegevoegde waarde heeft. Daarbij wordt onder meer uitgegaan van de eisen van proportionaliteit en subsidiariteit. De locaties waar de camera's zijn en worden geplaatst, worden opgenomen in het cameraplan. Het cameraplan wordt jaarlijks herzien. Dit betekent dat jaarlijks wordt herbeoordeeld of de reeds aangewezen locaties nog steeds aan de gestelde criteria voldoen en of aanwijzing van nieuwe locaties – uiteraard eveneens met toepassing van deze criteria – gewenst en noodzakelijk is.

Lengte bewaartermijn

In de Digital Rights-uitspraak leek de lengte van de bewaartermijn een belangrijke rol te spelen bij de vraag of de regeling proportioneel was. In die uitspraak ging het om een bewaartermijn van ten minste zes maanden en ten hoogste twee jaar (r.o. 64). In dit wetsvoorstel is gekozen voor de veel kortere bewaartermijn van vier weken.

Kenbaarheid

Het HvJEU lijkt bij de beoordeling van de regeling van belang te vinden dat onschuldige burgers niet worden ingelicht over het bewaren en gebruiken van hun gegevens, waardoor zij het gevoel zouden kunnen hebben dat zij voortdurend in de gaten worden gehouden (Digital Rights, r.o. 37, Tele2, r.o. 100). Allereerst kan tegen deze achtergrond ten aanzien van het gebruik van ANPR-gegevens worden gewezen op de «reasonable expectation of privacy». Het feit dat de gegevens worden vastgelegd langs de openbare weg, maakt reeds dat de verwachting van de burgers over in hoeverre zij (of hun voertuigen) worden waargenomen, anders is dan bij (verkeers)gegevens over vertrouwelijke communicatie. Daar komt bij dat in het voorgestelde artikel 126jj Sv is bepaald dat de aanwezigheid van de ANPR-camera «op duidelijke wijze kenbaar» moet zijn gemaakt (zie het voorgestelde artikel 126jj Sv, eerste lid, tweede volzin, Sv). Dit betekent dat alle camera's die worden ingezet op grond van artikel 126jj Sv moeten zijn opgenomen in het cameraplan. Dat cameraplan wordt

jaarlijks in de Staatscourant gepubliceerd en is dus voor eenieder raadpleegbaar. Tot slot kan ten aanzien van dit punt worden gewezen op de rechten die degene om wiens gegevens het gaat heeft op grond van de Wet politiegegevens (WPG) tot kennisneming van gegevens die hemzelf betreffen (artikelen 25 en 26 WPG). Omdat ANPR-gegevens politiegegevens zijn, zijn die bepalingen van de WPG van toepassing.

Toegang tot de gegevens

Uit beide uitspraken kan worden afgeleid dat de toegang tot (raadpleging van) gegevens moet worden beperkt, door zowel materiële als procedurele voorwaarden (Digital Rights, r.o. 61–62, Tele2, r.o. 115 e.v.). Aan beide voorwaarden is in dit wetsvoorstel voldaan.

Allereerst is er sprake van een strikte doelbinding (materiële voorwaarde). Het HvJEU hecht waarde aan een objectief criterium voor de toegang tot gegevens en noemt als voorbeeld «serious crime». In onderhavig wetsvoorstel is sprake van een dergelijk objectief criterium. De gegevens mogen alleen voor twee in dit wetsvoorstel opgenomen doelen worden geraadpleegd: de opsporing van misdrijven waarvoor voorlopige hechtenis is toegelaten en de aanhouding van een voortvluchtige. Door aan te sluiten bij het criterium of voor een bepaald misdrijf voorlopige hechtenis is toegelaten, is sprake van een objectief criterium aan de hand waarvan kan worden bepaald of sprake is van een voldoende zwaarwegend misdrijf. Ik kom op dit punt hieronder nog terug. Door voor de voortvluchtige te verwijzen naar artikel 564 Sv is ook voor die grond voorzien in een heldere en objectieve afbakening.

Daarnaast wordt de toegang tot de gegevens procedureel beperkt. Allereerst hebben alleen daartoe door de Minister van Veiligheid en Justitie geautoriseerde opsporingsambtenaren toegang tot de bewaarde gegevens. Naar aanleiding van de Digital Rights-uitspraak is bovendien bepaald dat zij de gegevens slechts mogen raadplegen na een bevel daartoe van de officier van justitie. Voordat de officier van justitie zijn bevel geeft, moet hij zich rekenschap geven van de proportionaliteit en de subsidiariteit van de zoekvraag. Dit betekent dat de omvang van de zoekvraag moet zijn afgestemd op het doel van de bevraging. Meer concreet betekent dit dat het geografische gebied en/of de periode in tijd waarover kentekens worden gezocht in evenwicht moeten zijn met de feiten en omstandigheden die tot die zoekvraag aanleiding geven. In het bevel moet de officier van justitie rekenschap geven van deze afweging. Door deze eisen die aan het bevel worden gesteld in het voorgestelde artikel 126jj Sv, vierde lid, worden ook toezicht en controle achteraf door de rechter in de strafzaak mogelijk.

Beveiliging

Tot slot wordt in beide uitspraken aangegeven dat er passende en organisatorische maatregelen moeten zijn getroffen om de gegevens doeltreffend te beschermen (Digital Rights, r.o. 66–68, Tele2, r.o. 122). In het uitvoeringsbesluit ANPR zullen regels worden opgenomen over de beveiliging van het systeem waarin de ANPR-gegevens worden bewaard. Er zijn voorschriften opgenomen over automatische logging en vernietiging van gegevens, detectie van en beveiliging tegen ongeautoriseerde toegang en het onderhoud van het systeem (paragraaf 3 van het uitvoeringsbesluit). Via jaarlijkse privacy-audits wordt de naleving van de wettelijke voorschriften gemonitord (artikel 15). De Autoriteit Persoonsgegevens houdt toezicht op de verwerking van de gegevens.

De leden van de GroenLinks-fractie vroegen naar de verhouding tussen «serious crime» zoals het HvJEU die noemt in de bovengenoemde

uitspraken en de voorlopige hechtenisfeiten die in dit wetsvoorstel worden genoemd.

In Europese richtlijnen wordt een onderscheid gemaakt tussen verschillende strafbare feiten. Er zijn «offences» (overtredingen), «crimes» (misdrijven) en «serious crimes» (misdrijven van een bepaalde ernst). Soms worden ook andere afbakeningen gebruikt. In welke gevallen sprake is van «serious crime» wordt over het algemeen overgelaten aan de nationale wetgever. Ook het HvJEU geeft weliswaar enkele voorbeelden van «serious crime» maar definieert dit begrip verder niet. Misdrijven waarvoor voorlopige hechtenis is toegelaten, kunnen worden aangemerkt als «serious crime». Het gaat immers om misdrijven die in verband met hun ernst moeten worden onderscheiden van andere misdrijven, waardoor daarvoor voorlopige hechtenis kan worden opgelegd en de inzet van bepaalde zwaardere (bijzondere) opsporingsbevoegdheden mogelijk is.

In antwoord op de vraag van deze leden waarom er niet voor een voorafgaande machtiging door de rechter-commissaris is gekozen wijs ik in de eerste plaats op de ernst van de inbreuk op de persoonlijke levenssfeer: die inbreuk is, zoals hierboven reeds aan de orde kwam, bij het bewaren van ANPR-gegevens minder vergaand dan bij het bewaren van telecommunicatiegegevens. De keuze voor de officier van justitie als autoriteit die over de raadpleging beslist, past in dat licht beter binnen het huidige wettelijke stelsel. Het vereiste van een bevel van de officier van justitie geldt op basis van de huidige wetgeving voor de inzet van andere bijzondere opsporingsbevoegdheden, zoals de stelselmatige observatie, de stelselmatige inwinning van informatie en de infiltratie. Het gaat hier om bevoegdheden die een verdergaande inbreuk op de persoonlijke levenssfeer van de betrokken personen vormt dan het bewaren van ANPR-gegevens en de toegang daartoe in een concreet geval.

In het systeem van het Wetboek van Strafvordering is de machtiging van de rechter-commissaris voorbehouden aan ingrijpende bevoegdheden waarvan de toepassing gepaard gaat met aan vergaande inbreuken op de persoonlijke levenssfeer. Het gaat dan bijvoorbeeld om het aftappen van telecommunicatie (artikel 126m Sv) en het direct af luisteren (artikel 126l Sv). Ook de bewaring van telecommunicatiegegevens die in de uitspraken van het HvJEU centraal stond, heeft betrekking op (verkeers)gegevens rond vertrouwelijke communicatie. Bij ANPR gaat het niet om dergelijke vertrouwelijke communicatie, maar om gegevens die slechts een zeer beperkt beeld kunnen geven van iemands privéleven en daarmee een geringe inbreuk op het recht op bescherming van de persoonlijke levenssfeer oplevert. Ik ben dan ook van mening dat kan worden volstaan met een bevel door de officier van justitie.

Deze leden stelden voorts enkele vragen over de gevolgen van de Tele2-uitspraak voor het bewaren van telecommunicatiegegevens en het wetsvoorstel daarover (zie *Kamerstukken II 2015/16, 34 537, nr. 2*). De consequenties van de Tele2-uitspraak voor wetsvoorstel 34 537 moeten nader worden onderzocht. Hiervoor wordt overleg gevoerd met de opsporingsinstanties en het openbaar ministerie. Het arrest is niet alleen van groot belang voor Nederland maar ook voor de andere lidstaten van de Europese Unie. Over de wijze waarop opvolging kan worden gegeven aan het arrest zal dan ook tevens overleg moeten worden gevoerd met de andere lidstaten. Zodra ik meer inzicht heb in de precieze consequenties van het arrest voor het wetsvoorstel 34 537 en de positie van de andere lidstaten, zal Uw Kamer daarover in het kader van de behandeling van dat wetsvoorstel worden geïnformeerd.

Deze leden vroegen welke alternatieve opsporingsmethoden ter beschikking staan. In algemene zin kan op voorhand niet worden aangegeven welke opsporingsbevoegdheden wel en welke geen rol zullen spelen in een concreet opsporingsonderzoek. Bij ieder strafbaar feit wordt, afhankelijk van de omstandigheden van het geval, bezien welke opspo-

ringsbevoegdheden en -methoden een bijdrage kunnen leveren aan de opsporing van dat strafbare feit. Bij strafbare feiten waarbij verplaatsingen met gemotoriseerde voertuigen geen rol spelen, of waarbij de inzet van andere bevoegdheden voldoende bewijsmateriaal oplevert, zal de ANPR-bevoegdheid niet snel in beeld komen. Bij andere strafbare feiten kunnen ANPR-gegevens een indicatie geven over de aanwezigheid van een voertuig met een bepaald kenteken op of rond een bepaalde locatie. Dit kan bijdragen aan het bewijs of richting geven aan het onderzoek. Een voorbeeld kan dit verduidelijken. Wanneer er in de buurt van een ANPR-camera een overval is gepleegd, kunnen – al dan niet in combinatie met getuigenverklaringen – voertuigen in beeld worden gebracht waarmee de verdachten zijn gevluht en/of de vluchtroute van het voertuig kan worden nagegaan. Zo kunnen mogelijke verdachten en hun verblijfplaatsen in beeld komen. Afhankelijk van de omstandigheden van het geval is het goed denkbaar dat er geen alternatief is voor de bevoegdheid zoals hier voorgesteld. In gevallen waarin er bijvoorbeeld geen getuigen zijn die het kentekennummer van het voertuig hebben genoteerd, is ANPR vaak de enige manier waarop de betrokken voertuigen in beeld kunnen worden gebracht. Met de hier voorgestelde bevoegdheid kan dan in kaart worden gebracht welke voertuigen rond het tijdstip van het plegen van het misdrijf aanwezig waren rond de plaatsdelict.

Deze leden vroegen of het wetsvoorstel is getoetst aan richtlijn 2016/680/EU over de bescherming van persoonsgegevens die worden verwerkt voor politieke en strafvorderlijke doeleinden. In antwoord op deze vraag verduidelijk ik graag het volgende. De ANPR-gegevens die op grond van dit wetsvoorstel worden bewaard zijn politiegegevens. Op die ANPR-gegevens is de Wet politiegegevens (WPG) van toepassing voor zover met het voorgestelde artikel 126jj Sv niet van die wet niet wordt afgeweken. Inmiddels is een wetsvoorstel ter implementatie van de genoemde richtlijn in procedure. Dat wetsvoorstel is voor advies voorgelegd aan de Autoriteit Persoonsgegevens. De daar voorgestelde wijzigingen van de WPG zullen ook van toepassing zijn op de verzamelde ANPR-gegevens.

Deze leden stelden een vraag over de inzage in de ANPR-gegevens. Deze inzage is geregeld in de artikelen 25 e.v. van de WPG. Op grond van artikel 25 WPG kan een betrokkene een verzoek tot kennisneming tot de verantwoordelijke (de korpschef) richten over (ANPR-)gegevens die op hem betrekking hebben. Een verzoek tot kennisneming wordt in beginsel toegewezen, met dien verstande dat er een aantal wettelijke gronden tot weigering zijn (zie artikel 27 WPG): de kennisneming kan worden onthouden indien die onthouding noodzakelijk is voor de goede uitvoering van de politietoek, de bescherming van de rechten van de betrokkene, de bescherming van de rechten en vrijheden van derden of de veiligheid van de staat. Een besluit over een dergelijk verzoek is een besluit in de zin van de Awb (artikel 29, eerste lid, WPG). Dat betekent dat de betrokkene tegen een eventuele afwijzing van zijn verzoek kan opkomen bij de bestuursrechter. Ook kan de betrokkene zich voor bemiddeling en advies wenden tot de Autoriteit Persoonsgegevens (artikel 29, tweede lid, WPG).

Op grond van de artikelen 25 e.v. WPG, zo beantwoord ik een volgende vraag van deze leden, kan de betrokkene eveneens kennisnemen van informatie over het gebruik van de gegevens. De bepalingen in richtlijn 2016/680/EU over het informeren van de betrokkene zullen worden geïmplementeerd door een wijziging van de WPG. Zoals gezegd is die wet ook van toepassing op de ANPR-gegevens.

De leden van de **ChristenUnie**-fractie gaven aan dat voor hen zwaar weegt dat bestuurders zich in de publieke ruimte begeven en daarmee dus geen absoluut recht op privacy kunnen inroepen.

Desgevraagd kan ik deze leden bevestigen dat het feit dat de kentekengegevens langs de openbare weg worden verzameld met zich meebrengt dat de «reasonable expectation of privacy» van personen anders moet worden gewogen.

In de zaak Peck tegen het Verenigd Koninkrijk van 28 januari 2003 (44647/98) overwoog het EHRM dat «the reasonable expectation of privacy» van een persoon van belang kan zijn bij de beoordeling in hoeverre het privéleven van een persoon wordt geraakt door maatregelen buiten de woning of een andere plaats waar hij mag verwachten onbevangen zichzelf te zijn. Het waarnemen van de activiteiten van een individu in een openbare ruimte door middel van optische apparatuur waarbij de beelden niet worden vastgelegd, vormt als zodanig geen inbreuk op het privéleven van de betrokkene. Het vastleggen en het systematische of permanente karakter van de vastlegging kunnen echter aanleiding geven tot een andere afweging, aldus het EHRM in de Peck-uitspraak.

In een uitspraak uit 2004 over cameratoezicht langs de openbare weg liet de Hoge Raad het oordeel van het gerechtshof in stand dat het feit dat, overigens gedurende een korte tijd, door middel van camera's gedragingen van de verdachte die zich in het openbaar afspeelden waren waargenomen geen aantasting vormde van de persoonlijke levenssfeer van de verdachte. Het oordeel dat die waarneming geen betrekking had op een situatie waarin de verdachte mocht verwachten onbevangen zichzelf te kunnen zijn getuigde niet van een onjuiste rechtsopvatting (HR 20 april 2004, LJN AL8449).

Uit deze uitspraken kan worden afgeleid dat het waarnemen van gedragingen op de openbare weg als zodanig geen inbreuk maakt op de persoonlijke levenssfeer van personen, zoals deze leden ook al aangaven. Dit ligt anders als de waargenomen gegevens op systematische wijze worden vastgelegd en bewaard. Dat kan een inbreuk vormen op het in artikel 8 EVRM vastgelegde recht op bescherming van de persoonlijke levenssfeer. In dergelijke gevallen kan evenwel nog steeds worden gesteld dat deze inbreuk bij het vastleggen van (kenteken)gegevens langs de openbare weg – in verband met de «reasonable expectation of privacy» – minder groot is dan wanneer bijvoorbeeld de inhoud van telefoongesprekken wordt vastgelegd (vgl. EHRM 2 december 2010, appl.nr. 35623/05 (Uzun), r.o. 66). Dat is relevant voor de beantwoording van de vraag of de inbreuk gerechtvaardigd is op grond van het tweede lid van artikel 8 EVRM, waarin onder andere het vereiste van proportionaliteit is vastgelegd. Ik ben daarop hierboven reeds nader ingegaan, in antwoord op vragen van de leden van de GroenLinks-fractie naar de S & Marper-uitspraak en de uitspraken van het HvJEU. Graag verwijs ik deze leden daarnaar.

3. Bewaarwijze gegevens

De leden van de **VVD**-fractie vroegen waarom voor de bewaartermijn aansluiting is gezocht bij de bewaartermijn die geldt voor het bewaren van beelden van gemeentelijke toezichtcamera's.

Zoals deze leden terecht opmerken bestaat er een aantal verschillen tussen het bewaren van gegevens van gemeentelijke toezichtcamera's op grond van artikel 151c van de Gemeentewet en het bewaren van ANPR-gegevens. Deze leden wezen daarbij bijvoorbeeld op het verschil dat gemeentelijke camerabeelden worden vastgelegd in verband met de openbare orde, terwijl ANPR-gegevens worden vastgelegd in verband met de opsporing van ernstige strafbare feiten.

Er zijn evenwel ook overeenkomsten. Zo kunnen in beide gevallen gegevens worden vastgelegd zonder dat daarvoor vooraf een concrete aanleiding is. Ook betreft het in beide gevallen de plaatsing van camera's van de op bepaalde locaties waar dit naar de mening van de verantwoor-

delijken aangewezen is. Op grond van deze gemeenschappelijke kenmerken is ertoe besloten in dit wetsvoorstel ook voor de bewaartermijn aansluiting te zoeken bij de wettelijke regeling voor gemeentelijke toezichtcamera's.

Overigens geldt dat voor zover binnen de bewaartermijn van vier weken blijkt dat de ANPR-gegevens relevant zijn voor de opsporing van een bepaald strafbaar feit, zij verder mogen worden verwerkt voor dat doel. In die gevallen geldt de verwerkingstermijn op grond van de WPG: de gegevens kunnen dan worden bewaard gedurende een jaar met het oog op de uitvoering van de dagelijkse politietaak (artikel 8 WPG) of zo lang als dat noodzakelijk is voor het onderzoek naar de schending van de rechtsorde in een bepaald geval (artikel 9 WPG).

Voor het antwoord op de vraag van de leden van deze fractie hoe dit wetsvoorstel zich verhoudt tot de Tele2-uitspraak van het HvJEU verwijs ik hen graag naar mijn antwoord in paragraaf 2 van deze memorie op een soortgelijke vraag van de leden van de GroenLinks-fractie.

De leden van de **PvdA**-fractie vroegen onder welke omstandigheden de ANPR-gegevens langer dan vier weken mogen worden bewaard. Zij vroegen of die mogelijkheid alleen geldt voor buitenlandse kentekengegevens. Ik begrijp deze laatste vraag zo dat zij verband houdt met artikel 1a van het wetsvoorstel. Graag verhelder ik dat die bepaling geen betrekking heeft op kentekengegevens die worden vastgelegd op grond van het voorgestelde artikel 126jj Sv. Artikel 1a betreft een wijziging van artikel 4 van de Wet administratiefrechtelijke handhaving verkeersvoorschriften. Het gaat in die bepaling om kentekengegevens die zijn vastgelegd in verband met de overtreding van de Wegenverkeerswet 1994, de Wet aansprakelijkheidsverzekeringen motorrijtuigen, de Provinciewet of de Gemeentewet. Gedacht kan worden aan de kentekengegevens van een voertuig dat is «geflitst» vanwege een snelheidsovertreding. De bepaling is ingevoegd bij amendement. Het oorspronkelijke amendement zag alleen op buitenlandse kentekens. In de laatste versie van het amendement is dit evenwel gewijzigd naar *alle* kentekens (zie *Kamerstukken II 2015/16*, 33 542, nr. 37). Het amendement maakt het mogelijk dat in gevallen waarin geen adres bekend is, de termijn voor bekendmaking van de beschikking (geldboete) wordt verlengd van vier maanden naar acht maanden.

Zoals gezegd geldt de bepaling die wordt ingevoegd in de Wet administratiefrechtelijke handhaving verkeersvoorschriften niet voor gegevens die worden bewaard op grond van het voorgestelde artikel 126jj Sv. Voor laatstgenoemde gegevens geldt dat zij automatisch worden vernietigd na vier weken. Indien binnen vier weken een zoekvraag wordt gedaan mogen de ANPR-gegevens die aan die zoekvraag voldoen verder worden verwerkt overeenkomstig de artikelen 8 en 9 WPG. Die gegevens mogen dan worden bewaard gedurende een jaar (artikel 8 WPG) of zolang als dat noodzakelijk is voor dat onderzoek (artikel 9 WPG).

Deze leden vroegen welke functionarissen toegang hebben tot de ANPR-gegevens. In het voorgestelde artikel 126jj, derde lid, Sv is vastgelegd dat alleen de daartoe door de Minister van Veiligheid en Justitie geautoriseerde opsporingsambtenaren toegang hebben tot de ANPR-gegevens die worden bewaard op grond van artikel 126jj Sv. Voor de vraag welke opsporingsambtenaren zullen worden geautoriseerd, verwijs ik deze leden graag naar mijn in paragraaf 2 gegeven antwoord op een gelijklopende vraag van de leden van de VVD-fractie. Zoals ik daar heb aangegeven gaat het uitsluitend om opsporingsambtenaren die zijn belast met de taken of werkzaamheden op het gebied van de coördinatie van het informatieproces ter ondersteuning van een goede uitvoering van de politietaak (zie artikel 6 van het uitvoeringsbesluit).

In antwoord op de vraag over de toegang tot de ANPR-gegevens van de inlichtingen- en veiligheidsdiensten en buitenlandse autoriteiten, stel ik

graag voorop dat noch de inlichtingen- en veiligheidsdiensten noch buitenlandse autoriteiten zelf rechtstreeks toegang hebben tot de ANPR-gegevens die op grond van het voorgestelde artikel 126jj Sv worden bewaard. Die toegang blijft uitsluitend voorbehouden aan de (Nederlandse) geautoriseerde opsporingsambtenaren. Wel kunnen deze diensten en autoriteiten een verzoek tot verstrekking van de ANPR-gegevens doen.

Voor de inlichtingen- en veiligheidsdiensten geldt dat zij op grond van artikel 17 van de WIV 2002 aan ieder bestuursorgaan, dus ook de politie, een verzoek kunnen doen tot verstrekking van gegevens. In de WPG is voorzien in een «spiegelbepaling», waarin een grondslag voor de verstrekking van de gegevens aan de inlichtingen- en veiligheidsdiensten is opgenomen (artikel 17, eerste lid, WPG). In het voorgestelde artikel 126jj, vijfde lid, Sv is deze spiegelbepaling van toepassing verklaard op ANPR-gegevens. De ANPR-gegevens kunnen op grond van die bepaling aan de inlichtingen- en veiligheidsdiensten worden verstrekt voor zover dat voortvloeit uit de Wet op de inlichtingen- en veiligheidsdiensten 2002.

Ook de bepalingen over de verstrekking aan de openbare lichamen Bonaire, Sint Eustatius en Saba en aan buitenlandse autoriteiten (artikelen 17 en 17a BPG) zijn van toepassing op de ANPR-gegevens. De regels over de verstrekking aan die autoriteiten worden bij algemene maatregel van bestuur (het Besluit politiegegevens (BPG)) nader uitgewerkt. In het uitvoeringsbesluit wordt voorzien in afwijkende regels voor de verstrekking aan deze autoriteiten van ANPR-gegevens die op grond van dit wetsvoorstel worden bewaard. Daarmee wordt gewaarborgd dat de ANPR-gegevens uitsluitend aan buitenlandse autoriteiten kunnen worden verstrekt onder dezelfde omstandigheden als die waaronder de Nederlandse politie daarvan gebruik kan maken. Dat wil onder andere zeggen dat de gegevens alleen kunnen worden verstrekt in het kader van een concreet strafrechtelijk onderzoek naar een strafbaar feit wanneer er sprake is van een voldoende concrete zoekvraag. De officier van justitie moet toestemming geven voor de verstrekking van de gegevens. Bij de verstrekking zullen als voorwaarden worden gesteld dat de ANPR-gegevens door de ontvangende autoriteiten niet zullen worden gebruikt voor andere doelen dan waarvoor zij verstrekt zijn, dat de gegevens na de verwezenlijking van die doeleinden worden vernietigd en dat de gegevens niet worden doorverstrekt. Hiermee wordt gewaarborgd dat na de verstrekking aan het buitenland de doelbinding van toepassing blijft (vgl. de artikelen 13 en 14 van het conceptuitvoeringsbesluit).

De leden van de **ChristenUnie**-fractie vroegen onder welke omstandigheden een bewaartermijn langer dan vier weken zal strijden met de eis van proportionaliteit. Zij vroegen voorts of een termijn van vier weken toereikend is om het beoogde effect te bereiken.

Zoals in paragraaf 2 van deze memorie aan de orde kwam, is de bewaartermijn één van de aspecten die meeweegt bij de vraag of een bewaarregeling proportioneel is. Op voorhand kan geen algemene grens worden aangegeven ten aanzien van de lengte van de bewaartermijn. Of een bewaartermijn proportioneel is, is mede afhankelijk van de aard van de gegevens, het doel waarvoor de gegevens worden bewaard en de overige waarborgen die in de regeling zijn opgenomen.

Louter bezien vanuit het belang van de opsporing bij de ANPR-gegevens kan worden gesteld dat de bewaartermijn zo lang mogelijk zou moeten zijn. Het is immers altijd mogelijk dat pas na lange tijd blijkt dat een ANPR-gegeven relevant is voor de opheldering van een strafbaar feit. Dit belang moet evenwel worden afgewogen tegen het belang dat burgers hebben bij de bescherming van hun persoonlijke levenssfeer. Ik ben van mening dat met een bewaartermijn van vier weken een redelijk evenwicht is gevonden tussen deze belangen.

Ten aanzien van de situatie in het Verenigd Koninkrijk, waar deze leden naar verwezen, kan worden opgemerkt dat daar sprake is van een getrappt systeem. Blijkens het rapport van de DSP-groep mogen de gegevens gedurende de eerste maand worden geraadpleegd voor alle misdrijven. Na afloop van die periode mogen de gegevens alleen nog maar worden geraadpleegd voor de opsporing van bepaalde ernstige misdrijven. Overigens heb ik inmiddels via contacten bij het Home Office vernomen dat de bewaartermijn in het Verenigd Koninkrijk enige tijd geleden is verkort van vijf jaar naar twee jaar. Het debat over de meest optimale opslagtermijn is daar nog gaande, waarbij goed wordt gekeken naar de proportionaliteit en noodzakelijkheid van een langdurige opslag.

In antwoord op de vraag van deze leden hoe de bewaartermijn van vier weken zich verhoudt tot de toepasselijkheid van artikel 8 WPG merk ik graag op dat de ANPR-gegevens die op grond van het voorgestelde artikel 126jj Sv worden vastgelegd apart van de overige politiegegevens worden bewaard. Na vier weken worden zij automatisch vernietigd. Binnen die vier weken kan – als aan de voorwaarden van dit wetsvoorstel is voldaan – in het kader van een concreet strafrechtelijk onderzoek het ANPR-systeem worden bevroegd. De gegevens die aan die zoekvraag voldoen (de «hits») mogen verder worden verwerkt op grond van de artikelen 8 en 9 WPG. Dit betekent dat zij overeenkomstig die artikelen mogen worden bewaard en verwerkt en dat de bewaartermijnen van die artikelen van toepassing zijn op de verwerking van die gegevens. Het gaat dan bijvoorbeeld om het kenteken van het voertuig van de verdachte, dat op de plaats-delict door een camera is vastgelegd rond het tijdstip waarop het strafbare feit is gepleegd. Dat kenteken mag dan worden bewaard zolang dat noodzakelijk is voor het onderzoek naar dat strafbare feit (artikel 9 WPG).

4. Kentekenfraude

De leden van de **D66**-fractie wilden weten hoe het ANPR-systeem inspeelt op het risico dat gebruik wordt gemaakt van gestolen kentekenplaten. De leden van de **ChristenUnie**-fractie vroegen hoe vaak kentekenfraude voorkomt en vroegen of criminelen hierdoor het ANPR-systeem kunnen omzeilen. Graag beantwoord ik deze vragen in onderlinge samenhang als volgt.

In antwoord op deze vragen stel ik graag voorop dat de toepassing van ANPR juist een zeer effectief middel kan zijn bij het opsporen van gestolen voertuigen of het gebruik van gestolen kentekenplaten.

Ook in de huidige situatie maken criminelen gebruik van gestolen voertuigen of gestolen kentekens om de opsporing te bemoeilijken. In de jaren 2015 en 2016 is 18.395 keer aangifte gedaan van diefstal van een kenteken. In het eerder al genoemde WODC-rapport is aangegeven dat er tot nu toe geen aanwijzingen zijn voor een toename van valse of onherkenbare kentekenplaten als reactie op ANPR. Van belang is ook dat personen in Nederland, anders dan bijvoorbeeld in het Verenigd Koninkrijk, geen kentekenplaat kunnen bestellen zonder een eigendomsbewijs te overleggen. Ook zijn nieuwe kentekenplaten die zijn aangevraagd ter vervanging van bijvoorbeeld gestolen kentekenplaten herkenbaar aan de duplicaatcode (het kleinere, extra cijfer dat daarop is geplaatst). Kentekenplaten waarvoor vervanging bij de RDW is aangevraagd kunnen op een referentielijst worden opgenomen met de vermelding dat de originele kentekenplaten gestolen of vermist zijn. Daarnaast sluit het gebruik van een vervalst kenteken niet uit dat dit kenteken op andere locaties wordt waargenomen, zodat een verband kan worden gelegd met strafbare feiten die in de omgeving van die locaties zijn gepleegd. Doordat ook een foto van het voertuig wordt opgenomen,

kan in voorkomende gevallen worden vastgesteld of het gaat om een voertuig met gestolen of valse nummerplaten. De leden van de ChristenUnie-fractie vroegen in dit verband naar de waarborgen die gelden bij de bewaring van blanco kentekens. Ter bestrijding van fraude met blanco kentekens zijn binnen het systeem Gecontroleerde Afgifte en Inname Kentekenplaten (GAIK) maatregelen van kracht die bewerkstelligen dat blanco kentekens goed beveiligd zijn. Daarop wordt toezicht gehouden door de RDW. Bij een overtreding wordt een sanctie opgelegd. Alleen erkende bedrijven mogen betrokken zijn bij het productie- en afgifteproces. De locatie van blanco kentekens moet altijd vastgelegd zijn. Eventuele diefstal moet altijd gemeld worden. Daarmee zijn voor de omgang met blanco kentekenplaten strenge maatregelen in werking. Een en ander heeft erin geresulteerd dat het aantal gestolen blanco kentekens is gedaald van 2.439 in 2015 naar 773 in 2016.

Het is mogelijk, zo beantwoord ik een volgende vraag van deze leden, dat de RFID-chip in de toekomst beter te beveiligen is tegen misbruik dan een (blanco) kentekenplaat. Dit hangt af van verschillende factoren. Er is nog geen beslissing genomen over het gebruik van RFID-chips (zie ook *Handelingen II* 2014/15, 2790, 2791, 2795). Er is thans nog veel onduidelijk over de (on)mogelijkheden rond het gebruiken van RFID-chips in kentekens. Op dit moment kan dan ook niet worden voorzien of deze techniek in de toekomst een bruikbaar en verantwoord alternatief zal vormen.

5. Horizonbepaling en evaluatie

De leden van de **VVD**-fractie vroegen hoe ervoor gezorgd wordt dat de evaluatie binnen drie jaar kan worden afgerond en de voorhang tijdig in het parlement behandeld zal zijn.

Met deze leden ben ik van mening dat het van belang is dat de evaluatie tijdig wordt gestart en afgerond opdat er voldoende ruimte is voor de voorhangprocedure.

Daarom ben ik op dit moment al in overleg met het WODC over de aanpak van de evaluatie. Met het WODC zal een planning worden gemaakt voor dit onderzoek zodat het tijdig kan worden opgeleverd.

Mocht de wet over drie jaar vervallen, zo beantwoord ik een volgende vraag van deze leden, dan heeft dat geen consequenties voor strafzaken waarin ANPR-gegevens worden gebruikt die op grond van het voorgestelde artikel 126jj Sv zijn vastgelegd. Immers, op het moment van vastlegging zijn deze gegevens op een wettelijke grondslag rechtmatig verkregen. Iets anders is dat geen ANPR-gegevens meer op grond van de voorgestelde bevoegdheid mogen worden vastgelegd en bewaard vanaf het moment dat de wettelijke bepaling vervalt. Het is dus niet meer mogelijk om in een lopende of nieuwe strafzaak alsnog de database te bevragen nadat de bepaling zou zijn komen te vervallen.

De leden van de **CDA**-fractie vroegen hoe er feitelijk voor gezorgd gaat worden dat de wet in de praktijk correct wordt uitgevoerd.

Met deze leden onderschrijf ik het belang van strikte naleving van de privacy-waarborgen en adequaat toezicht. Daartoe is in het systeem een aantal waarborgen ingebouwd die ervoor zorgen dat voorschriften in acht worden genomen. Zo kan alleen de geautoriseerde opsporingsambtenaar inloggen in het systeem, omdat alleen deze ambtenaar beschikt over een aantal authenticatiegegevens en een unieke code. Ik ben daarop in paragraaf 2 reeds ingegaan in antwoord op een vraag van de leden van de VVD-fractie.

Daarnaast legt het systeem een aantal gegevens automatisch vast. Zo zal het systeem als wordt ingelogd vastleggen dat wordt ingelogd, evenals de ingevoerde zoekvraag. Niet bevoegde raadpleging, oneigenlijk gebruik of

misbruik, kunnen op deze wijze worden gedetecteerd. In het conceptuivoeringsbesluit zijn voorschriften over deze «logging» vastgelegd (zie de artikelen 8 en 10).

Jaarlijks zal er een (privacy-)audit worden uitgevoerd, waarin het gebruik van de ANPR-gegevens en de naleving van de voorschriften zal worden getoetst. In de evaluatie zal ook, mede op basis van de resultaten van deze jaarlijkse audits, worden ingegaan op de privacyaspecten van dit wetsvoorstel. De evaluatie zal tijdig aan Uw Kamer worden gezonden, zodat zij kan worden betrokken bij de besluitvorming in het kader van de voorhangprocedure van het verlengingsbesluit.

Tot slot kan er nog op worden gewezen dat de Autoriteit Persoonsgegevens toezicht houdt op de verwerking van persoonsgegevens, en dus ook op de verwerking van ANPR-gegevens op grond van dit wetsvoorstel.

De leden van de **D66**-fractie gaven aan de horizonbepaling als een belangrijke waarborg te zien. Zij vroegen evenwel of dit ook een teken is dat wordt getwijfeld aan de effectiviteit van dit wetsvoorstel. De leden van de **PvdA**-fractie vroegen of de periode opgenomen in de horizonbepaling (drie jaar) moet worden gezien als een in beginsel eindige periode of als een experimenteerperiode. Graag beantwoord ik deze vragen als volgt. Eerdere versies van dit wetsvoorstel zijn opgesteld onder het kabinet Rutte I. In het regeerakkoord van dat kabinet was opgenomen dat voorgenomen maatregelen inzake opslag, koppeling en verwerking van persoonsgegevens zoveel mogelijk worden voorzien van een horizonbepaling en dat deze maatregelen bij de voorbereiding nadrukkelijk moeten worden getoetst op effectiviteit («Vrijheid en verantwoordelijkheid», Regeerakkoord VVD-CDA, blz. 42). In het regeerakkoord van het huidige kabinet is vastgelegd dat bij de bouw van systemen en het aanleggen van databestanden bescherming van persoonsgegevens uitgangspunt is. Inbreuken door de overheid zijn voorzien van een horizonbepaling en worden geëvalueerd («Bruggen slaan», Regeerakkoord VVD-PVDA, blz. 28).

Om deze afspraken gestand te doen bevat het wetsvoorstel een horizonbepaling. Daarmee is dus geenszins beoogd tot uitdrukking te brengen dat wordt getwijfeld aan de effectiviteit van het wetsvoorstel. De ervaringen in het buitenland en de eerdere ervaringen in Nederland met het gebruik van ANPR-gegevens in pilots, laten zien dat die gegevens een belangrijke bijdrage aan de opsporing van ernstige strafbare feiten kunnen leveren. Zie hierover ook *Hits en hints. De mogelijke meerwaarde van ANPR voor de opsporing*, uitgevoerd door de DSP-groep in opdracht van het WODC (bijlage bij *Kamerstukken II 2011/12, 31 051, nr. 10*). In paragraaf 2 van deze memorie heb ik in aanvulling daarop nog een aantal voorbeelden gegeven van de mogelijke meerwaarde van ANPR. De meerwaarde van de evaluatie is vooral gelegen in de verscherpte controle op de effectiviteit van de regeling ten aanzien van zowel het belang voor de opsporing als de waarborgen om de persoonlijke levenssfeer te beschermen.

Voor het antwoord op hun vraag naar de planning van de evaluatie van de wettelijke regeling, verwijs ik de leden van de PvdA-fractie graag naar mijn eerder gegeven antwoord op een gelijklopende vraag van de leden van de VVD-fractie. Zoals daar aangegeven ben ik hierover al met het WODC in gesprek. Voor de evaluatie zal gebruik kunnen worden gemaakt van de jaarlijkse (privacy-)audit. De uitkomsten van de evaluatie zullen aan Uw Kamer worden gezonden. Dat is vastgelegd in artikel II, derde lid, van het wetsvoorstel.

6. Overige

De leden van de **D66**-fractie vroegen naar de reactiecapaciteit van de politie. Deze «reactiecapaciteit» houdt verband met het direct optreden van de politie nadat een op een referentielijst opgenomen kenteken is gesignaleerd door een ANPR-camera (directe opvolging) of nadat door een camera een overtreding is vastgelegd (zoals bij roodlichtcamera's). Deze reactie op «hits» heeft betrekking op de huidige toepassingsmogelijkheden van ANPR. Die situatie moet worden onderscheiden van de toepassing op grond van dit wetsvoorstel. Hier gaat het om het achteraf, in het kader van een lopend onderzoek, raadplegen van eerder vastgelegde ANPR-gegevens. Aldus kunnen de ANPR-gegevens de politie, die al bezig was met het onderzoek, mogelijk verder op weg helpen. Mogelijk kan daarmee de inzet van andere opsporingsbevoegdheden worden voorkomen.

De leden van de **PvdA**-fractie wezen op de Europese jurisprudentie en op de technologische ontwikkelingen en vroegen in hoeverre het wetsvoorstel up-to-date en toekomstbestendig is.

Zoals deze leden aangaven is het wetsvoorstel verschillende keren aangepast. Met een tweede nota van wijziging is het voorstel aangepast naar aanleiding van de uitspraak van het HvJEU (*Kamerstukken II 2015/16, 33 542, nr. 20*). Ik meen dat het wetsvoorstel daarmee ruimschoots voldoet aan de eisen die aan de regeling worden gesteld in verband met het recht op bescherming van de persoonlijke levenssfeer. Ik ben hierop in paragraaf 2 reeds uitgebreid ingegaan.

Bij het opstellen van het wetsvoorstel is rekening gehouden met eventuele technologische ontwikkelingen. Zo spreekt het voorgestelde artikel 126jj Sv niet over «camera's», maar over een «technisch hulpmiddel». Dit laat ruimte om in de toekomst eventuele andere hulpmiddelen waarmee kentekengegevens kunnen worden vastgelegd, te gaan gebruiken. Omdat het van belang is dat een dergelijk technisch hulpmiddel aan bepaalde eisen voldoet in verband met de betrouwbaarheid en de kwaliteit van de vastgelegde gegevens, worden in het uitvoeringsbesluit daarover eisen gesteld, waaronder met welke foutmarges ANPR-camera's kentekens mogen herkennen en aflezen. In aanvulling daarop zullen bij ministeriële regeling technische eisen worden gesteld aan de apparatuur. Er wordt voor het niveau van een ministeriële regeling gekozen zodat snel kan worden ingespeeld op technologische ontwikkelingen.

Het is niet uitgesloten dat in de toekomst ook met andere technieken voertuigbewegingen (kunnen) worden vastgelegd. Voor de vastlegging, bewaring en raadpleging van die gegevens door de politie en de KMar zal ook in dergelijke gevallen een voldoende wettelijke grondslag nodig zijn. Dit wetsvoorstel voorziet in een dergelijke grondslag voor zover het gaat om de vastlegging op of aan de openbare weg door de politie en de KMar van het kenteken, de foto van het voertuig, de locatie van vastlegging en het tijdstip van vastlegging met behulp van een technisch hulpmiddel. Deze leden vroegen verder of ik naast de rechtszaken die in de memorie van toelichting zijn genoemd, nog andere rechtszaken kan noemen waarin doeltreffend gebruik gemaakt kon worden van bewaarde ANPR-gegevens. Helaas moet ik deze leden op dit punt teleurstellen, aangezien er geen voorbeelden van recente rechtszaken zijn waarin gebruik is gemaakt van de hier voorgestelde toepassing van ANPR. Nadat het (toenmalige) College bescherming persoonsgegevens begin 2010 oordeelde dat er geen wettelijke basis is voor het bewaren van alle «no hits», worden die gegevens namelijk niet meer standaard bewaard.

De leden van de **ChristenUnie**-fractie vroegen door welke andere instanties naast de politie ook kentekenregistratie plaatsvindt. Deze leden verwijzen naar een rapport van het WODC uit 2013.

Voordat ik op deze vraag inga, benadruk ik graag dat andere instanties géén gebruik mogen maken van de ANPR-gegevens die op grond van dit wetsvoorstel worden bewaard. In het voorgestelde artikel 126jj, vijfde lid, Sv is bepaald dat paragraaf 3 van de WPG – waarin de grondslag is opgenomen voor de verstrekking van politiegegevens aan andere instanties – niet van toepassing is op de ANPR-gegevens die op grond van dit wetsvoorstel worden bewaard. Er is alleen een uitzondering gemaakt voor de verstrekking aan de inlichtingen- en veiligheidsdiensten en buitenlandse autoriteiten. Ik ben daarop in paragraaf 3 van deze memorie in antwoord op een vraag van de leden van de PvdA-fractie ingegaan. Het genoemde WODC-rapport biedt een overzicht van de instanties die gebruikmaken van ANPR-gegevens. Naast de politie zijn in het rapport de volgende instanties genoemd: het openbaar ministerie, de Koninklijke marechaussee, de Douane, de Belastingdienst, Rijkswaterstaat, de Rijksdienst voor het Wegverkeer, het samenwerkingsverband Nationale Databank Wegverkeersgegevens, de Inspectie Leefomgeving en Transport, gemeenten, en de stichting I-Watch. Deze instanties maken ook nu nog gebruik van ANPR. Laatstgenoemde stichting is geen overheidsorgaan maar verricht wel taken voor de overheid.

Ten aanzien van de Belastingdienst heeft de Hoge Raad in drie recente uitspraken¹ gewezen op de noodzaak van een voldoende precieze wettelijke grondslag voor het verzamelen, vastleggen, bewaren, bewerken en gebruiken van ANPR-gegevens.

Binnen het domein van Veiligheid en Justitie wordt verder door het Centraal Justitieel Incasso Bureau (CJIB) gebruikgemaakt van ANPR. Daarnaast is mij bekend dat Schiphol samen met de KMar en de douane ANPR gebruikt en dat in het sociale domein ANPR kan worden toegepast, bijvoorbeeld bij de bestrijding van uitkeringsfraude. Het komt verder voor dat ANPR wordt gebruikt voor bijvoorbeeld de toegang tot parkeergelegenheid van de overheid. Dat is als zodanig geen overheidsactiviteit maar een beheersactiviteit.

Deze leden vroegen wat er gebeurt met de informatie van roodlichtcamera's en of die informatie gebruikt kan worden voor de opsporing van verdachten of voortvluchtigen.

Informatie van roodlichtcamera's, zo beantwoord ik deze vraag, wordt vastgelegd ter handhaving van de verkeersregels. Alleen de gegevens van overtreders worden vastgelegd, niet van de overige voertuigen die de camera passeren. De met roodlichtcamera's vastgelegde gegevens komen niet in de database met ANPR-gegevens die op grond van dit wetsvoorstel wordt aangelegd, omdat dit gescheiden systemen zijn. In de loop van 2017 zal aan een aantal flitspalen van het CJIB een vaste ANPR-camera worden toegevoegd. Beide functies worden dan op één locatie verenigd, maar het blijven gescheiden systemen. Gegevens die in het kader van de verkeershandhaving door roodlichtcamera's zijn vastgelegd kunnen in voorkomende gevallen wel worden verstrekt aan de politie ter opsporing van strafbare feiten.

Tot slot vroegen deze leden of ANPR-gegevens ook kunnen worden gebruikt voor de opsporing van gestolen voertuigen. Ook vroegen zij of het juist is dat dat in Amsterdam door het gemeentebestuur een proef is gedaan met het vastleggen van kentekens van stilstaande auto's met het oog op de controle van betaling van parkeergelden, en dat daarbij van tientallen vastgelegde kentekens is geconstateerd dat het gestolen voertuigen betreft.

Op dit moment wordt ANPR reeds gebruikt om gestolen voertuigen op te sporen. Gestolen voertuigen worden na aangifte automatisch op een

¹ Zie ECLI:NL:HR:2017:286, ECLI:NL:HR:2017:287 en ECLI:NL:HR:2017:288.

referentielijst geplaatst. Is de aangifte nog niet gedaan, maar is er wel melding gedaan bij de politie, dan wordt een gestolen voertuig op een zogenaamde spoedlijst geplaatst om zo snel mogelijk te kunnen acteren. Zodra het gestolen voertuig een ANPR-camera passeert, levert dat een «hit» op, waar de politie op kan reageren. Om de slagkracht in de signalering van gestolen voertuigen te verhogen heeft de dienst Parkeerbeheer van de gemeente Amsterdam met de politie Amsterdam een convenant gesloten. Op basis daarvan kan deze dienst met haar scanauto's – ingezet voor controle op betaling van parkeergelden – eveneens kentekens van gestolen voertuigen detecteren. Het betreft kentekens die voorkomen op een referentielijst van de RDW. De scanauto's van de dienst parkeerbeheer kunnen bij controle een hit opleveren die wordt doorgegeven aan de politie. Met de inwerkingtreding van dit wetsvoorstel kan bovendien, nadat aangifte is gedaan, worden nagegaan of het kenteken van het voertuig in de daaraan voorafgaande uren of dagen door een camera is vastgelegd. Dit kan bijdragen aan de opheldering van het misdrijf en de teruggave van het voertuig aan de rechtmatige eigenaar.

De Minister van Veiligheid en Justitie,
S.A. Blok