Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

33 542 Wijziging van het Wetboek van Strafvordering in verband met de regeling van het vastleggen en bewaren van kentekengegevens door de politie

Nr. 43

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 6 april 2018

De vaste commissie voor Justitie en Veiligheid heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Justitie en Veiligheid over de brief van 9 januari 2018 over het ontwerpbesluit tot vaststelling van nadere regels voor het vastleggen en bewaren van kentekengegevens op grond van artikel 126jj van het Wetboek van Strafvordering door de politie (Kamerstuk 33 542, nr. 42).

De vragen en opmerkingen zijn op 12 februari 2018 aan de Minister van Justitie en Veiligheid voorgelegd. Bij brief van 5 april 2018 zijn de vragen beantwoord.

De voorzitter van de commissie,
Van Meenen

De griffier van de commissie,
Hessing-Puts

kst-33542-43
ISSN 0921 - 7371
's-Gravenhage 2018

I. Vragen en opmerkingen vanuit de fracties

1. Inleiding

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van dit ontwerpbesluit. Zij hebben hierover nog een enkele vraag.

De leden van de D66 fractie hebben kennisgenomen van het ontwerpbesluit. Zij hebben nog enkele vragen en opmerkingen.

De leden van de GroenLinks-fractie hebben met belangstelling kennisgenomen van het ontwerpbesluit. Zij waarderen het dat voorzien is in een groot aantal privacybeschermende voorschriften. Zo is het onherkenbaar maken van inzittenden van passerende voertuigen, niet-openbare plaatsen of van personen in de regeling verankerd en is geregeld dat opgeslagen beelden vier weken na vastlegging automatisch worden vernietigd. Tegelijkertijd vragen deze leden of voldoende rekenschap is afgelegd over het feit dat nu de kentekenregistratieplicht en de daaruit voortkomende gegevensverzamelingen binnenkort worden aangewend waarvoor het stelsel aanvankelijk niet is bedoeld. Voornoemde leden missen ook een degelijke inschatting van de effectiviteit van deze vorm van het vastleggen en bewaren van kentekengegevens. Dat maakt het op dit moment lastig een goede proportionaliteitsafweging te maken tussen de privacy-impact van deze maatregel en de opsporing van strafbare feiten. De aan het woord zijnde leden vragen de Minister hierin te voorzien.

De leden van de SP-fractie hebben destijds tegen het wetsvoorstel gestemd dat er toe strekte het mogelijk te maken Automatic Numberplate Recognition-gegevens (ANPR-gegevens) vier weken lang te bewaren en ook te kunnen gebruiken voor opsporingsdoelen. De wet is uitgebreid behandeld en de behandeling heeft behoorlijk wat jaren in beslag genomen. De wet is inmiddels helaas aangenomen en nu ligt een algemene maatregel van bestuur (AMvB) voor met regels die betrekking hebben op de uitvoering de wet. Over deze AMvB hebben voornoemde leden enkele vragen.

2. De reikwijdte van dit besluit

De leden van de CDA-fractie lezen in de nota van toelichting dat op ANPR-gegevens die door andere instanties worden verzameld de wetgeving die geldt voor de gegevensverwerking door die instanties van toepassing is. Deze leden constateren dat er ook gebruik gemaakt wordt van het ANPR-systeem ten behoeve van de integraal optredende overheid, bijvoorbeeld in het kader van integrale verkeerscontroles. Kan de Minister toelichten of dit besluit ook nog in een aparte regeling voorziet bij integraal georganiseerd overheidsoptreden? Kunnen bijvoorbeeld door de politie verzamelde gegevens, dus politiegegevens, die gebruikt worden ten behoeve van de selectie van hit/no hit op basis van ANPR ook gebruikt en gedeeld worden door en met andere overheden? Of kan informatie van andere overheden toegevoegd worden aan de ANPR-informatie op basis waarvan de politie optreedt? Algemener gesteld: op basis van welke criteria en regelgeving wordt in het kader van ANPR informatie tussen (keten)partners gedeeld?

3. Toelichting op de bepalingen

De leden van de CDA-fractie constateren dat vanaf medio mei 2018 de Algemene Verordening Gegevensbescherming (AVG) van toepassing is. Op grond van dit besluit zullen gegevens van burgers/verdachten worden

opgeslagen. Deze leden vragen of de AVG nog van invloed is op het proces of de wijze waarop deze gegevens worden opgeslagen.

Cameraplan (artikel 2)

De leden van de D66-fractie vragen de Minister nader toe te lichten wat de reden is dat voor mobiele camera's niet van tevoren kan worden vastgelegd op welke locaties zij worden geplaatst. Kan in ieder geval de regio of gemeente worden vastgelegd waar deze camera's ingezet worden? Om hoeveel camera's, vast of mobiel, gaat het in totaal? Wordt achteraf ook getoetst hoe vaak mobiele camera's zijn ingezet? Worden gegevens over het gebruik en de plaatsing van camera's achteraf openbaar gemaakt? Zo nee, waarom niet?

Criteria voor plaatsing en inzet (artikel 3)

De leden van de D66-fractie vragen de Minister nader toe te lichten hoe de afweging aangaande de proportionaliteit en subsidiariteit van het plaatsen van camera's gemaakt wordt. Kan de Minister hiervoor concrete voorbeelden geven? Bijvoorbeeld van een geval waarin het plaatsen van camera's niet past binnen randvoorwaarden van proportionaliteit en subsidiariteit? Hoe verhoudt dit zich tot de opmerking in de nota van toelichting dat er geen concreet vermoeden hoeft te zijn van een concreet te verwachten individueel strafbaar feit voor de plaatsing en inzet van camera's? Betekent dit niet dat overal in Nederland en zonder enige aanleiding camera's geplaatst kunnen worden? Op basis waarvan wordt deze afweging gemaakt? Hoe kan een locatie waarvan geen concreet vermoeden bestaat van een te verwachten strafbaar feit een voor de opsporing relevante locatie zijn? Hoe kan het plaatsen van camera's op een locatie waarvan geen concreet vermoeden bestaat van een te verwachten strafbaar feit door de toetsing op de randvoorwaarden van proportionaliteit en subsidiariteit komen?

Geen woningen of gezichten (artikel 5)

De leden van de D66-fractie vragen of de Minister nader kan toelichten waarom een bewaartermijn van vier weken noodzakelijk is. Hoe vaak wordt de uitzondering gebruikt om met toestemming van de officier van justitie af te wijken van de bepaling dat personen onherkenbaar moeten worden gemaakt? Kan de Minister een overzicht geven van alle instanties die direct toegang hebben tot de gegevens?

Raadpleging (artikel 7)

De leden van de SP-fractie merken op dat de verzoekende opsporingsambtenaar een geautomatiseerde aanvraag indient bij de officier van justitie om bepaalde gegevens te mogen terugzoeken. De officier van justitie beslist dan. Als hij positief beslist, geeft hij vervolgens het bevel aan de geautoriseerde opsporingsambtenaar. Waarom is toch voor deze constructie gekozen en niet om het afgeven van het bevel te beleggen bij de rechter-commissaris? Zeker ook gezien het advies van het Hof van Justitie van de Europese Unie in de zaak Digital Rights Ireland en Seitlinger e.a. (C-293/12) dat eerder eiste dat er toestemming moet zijn van een rechterlijke of onafhankelijke instantie. De officier van justitie is immers betrokken bij de zaak zelf en gezien het geautomatiseerde karakter van deze handeling lijkt het er op dat er niet echt een zorgvuldige objectieve beoordeling zal plaatsvinden bij elke aanvraag. Graag ontvangen deze leden een reactie op dit punt.

Centrale opslag (artikel 9)

De leden van de SP-fractie vragen de Minister ook te verduidelijken wanneer gegevens vernietigd worden als zij gebruikt worden bij een onderzoek. Deze leden lezen dat gegevens die aan het buitenland verstrekt worden vernietigd worden zodra de doeleinden waarvoor zij verstrekt zijn verwezenlijkt is. Is ditzelfde het geval voor de Nederlandse situatie? Geldt dit ook voor de situatie wanneer de gegevens door de Nederlandse inlichtingendiensten zijn opgevraagd? Zo ja, hoe wordt dan gecontroleerd of en wanneer de inlichtingendiensten de informatie hebben vernietigd?

Beveiligingseisen (artikel 10, 11 en 12)

De leden van de D66-fractie lezen dat de toegang tot het centrale opslagsysteem op deugdelijke wijze is beveiligd, onder meer door middel van persoonsgebonden authenticatie. Welke eisen worden er gesteld aan de persoonsgebonden authenticatie? Worden er maatregelen als 2factor-authentication toegepast? Worden de gegevens versleuteld opgeslagen? Zo ja, welke eisen worden er aan de versleuteling gesteld? Zo nee, waarom niet?

Jaarlijkse audit (artikel 15)

De leden van de GroenLinks-fractie stellen het op prijs dat er een jaarlijkse privacy-audit wordt uitgevoerd over de uitvoering van de bij of krachtens artikel 126jj gegeven regels. Zij vragen of deze audits ook naar de Kamer kunnen worden gestuurd. Daarnaast vragen deze leden wie deze audits zal/zullen uitvoeren. Wat is de rol van de Autoriteit Persoonsgegevens hierin?

II. Reactie van de Minister van Justitie en Veiligheid

1. Inleiding

De leden van de CDA-fractie gaven aan met belangstelling kennis te hebben genomen van het ontwerpbesluit. Zij hadden hierover nog enkele vragen, die ik graag beantwoord.

De leden van de D66-fractie hadden kennisgenomen van het ontwerpbesluit. Graag beantwoord ik de vragen en opmerkingen die deze leden nog hadden.

De leden van de GroenLinks-fractie gaven aan met belangstelling kennis te hebben genomen van het ontwerpbesluit. Ik dank deze leden voor de waardering die zij uitspraken voor het grote aantal privacybeschermende voorschriften dat is opgenomen in dit ontwerpbesluit. Zij wezen op de verankering van het onherkenbaar maken van inzittenden van passerende voertuigen, niet openbare plaatsen en personen en de automatische vernietiging na vier werken.
Deze leden vroegen, althans zo begrijp ik hun vraag, of de gegevens die op grond van artikel 126jj Sv worden opgeslagen, op termijn voor andere doelen zullen worden gebruikt dan waarvoor zij worden opgeslagen. Graag stel ik deze leden op dit punt gerust. Reeds op het niveau van de wet is vastgelegd dat deze gegevens niet voor andere doelen mogen worden geraadpleegd dan de in artikel 126jj Sv genoemde doelen. Met de tweede nota van wijziging (Kamerstuk 33 542, nr. 20) is in het derde lid van artikel 126jj Sv het woord «uitsluitend» ingevoegd om deze strikte doelbinding te benadrukken. In het ontwerpbesluit is in aanvulling daarop vastgelegd dat ook als de gegevens aan buitenlandse autoriteiten worden verstrekt, niet kan worden afgeweken van deze doelbinding (zie artikel 13,

vierde lid, onder a, van het ontwerpbesluit). Daarnaast is in artikel 126jj, vijfde lid, Sv vastgelegd dat deze gegevens niet aan derden mogen worden verstrekt. Het gebruik van de gegevens voor andere doelen dan opgesomd in artikel 126jj Sv is dus – zonder een wetswijziging – niet mogelijk. Op de gegevensverstrekking aan de inlichtingen – en veiligheidsdiensten ga ik hieronder, in antwoord op een vraag van de leden van de D66-fractie, nog in. Graag verwijs ik deze leden naar die reactie.
Over de te verwachten resultaten die met dit wetsvoorstel behaald kunnen worden, zo beantwoord ik een volgende vraag van deze leden, is in het kader van de behandeling van dit wetsvoorstel in zowel de Tweede als de Eerste Kamer uitvoerig gesproken. Zoals daar aan de orde is gekomen, kan de bevoegdheid van artikel 126jj Sv een belangrijke bijdrage leveren aan de opsporing van ernstige strafbare feiten en de aanhouding van voortvluchtigen. De betekenis van de gegevens voor een concreet opsporingsonderzoek is bij voorbaat niet te specificeren omdat dit per opsporingsonderzoek zal verschillen. De betekenis kan variëren van het fungeren als sturingsinformatie waarmee richting kan worden gegeven aan het opsporingsonderzoek – bijvoorbeeld doordat bepaalde personen als verdachte in beeld komen – tot het gebruik als bewijsmateriaal in de strafzaak – bijvoorbeeld doordat een alibi van een verdachte wordt weerlegd. Doordat sprake is van een nieuwe bevoegdheid, is niet aan te geven in hoeveel strafzaken ANPR-gegevens een bijdrage zullen kunnen leveren. Wel kan worden aangegeven in welk soort zaken ANPR-gegevens mogelijk een rol zullen spelen. Het zal in alle gevallen gaan om delictscenario's waarbij voertuigen betrokken zijn. Daarbij kan in de eerste plaats worden gedacht aan strafbare feiten die betrekking hebben op voertuigen, zoals voertuigdiefstal. In tweede plaats kunnen ANPR-gegevens een rol spelen bij strafbare feiten waarbij voertuigen worden gebruikt ofwel om het strafbare feit te plegen ofwel als vluchtauto. Voorbeelden hiervan zijn plofkraken, (woning)inbraken, ontvoeringen, terroristische misdrijven en mobiel banditisme. Zowel de jaarlijkse privacy-audits – die ook steeds aan Uw Kamer zullen worden gezonden – als de wetsevaluatie zullen gegevens opleveren over het aantal gevallen waarin ANPR-gegevens zijn bevraagd en voor welk type zaken. Met betrekking tot de privacy-impact kan ook worden gewezen op de maatregelen die in dit besluit zijn opgenomen en die door deze leden ook benoemd zijn in hun inbreng. Deze bepalingen vormen een aanvulling op de strikte beperkingen die al in de wet zijn opgenomen ten aanzien van de toegang tot de gegevens. Ik meen dat daarmee een goede balans is gevonden tussen het belang van deze gegevens voor de opsporing en de bescherming van de persoonlijke levenssfeer van burgers.

De leden van de SP-fractie gaven aan destijds tegen het wetsvoorstel te hebben gestemd. Zij hadden nog enkele vragen over het ontwerpbesluit, die ik in het onderstaande graag beantwoord.

2. De reikwijdte van dit besluit

De leden van de CDA-fractie wezen op het gebruik dat wordt gemaakt van het ANPR-systeem ten behoeve van integrale acties waarbij verschillende overheidsorganen betrokken zijn, althans zo begrijp ik hun vraag. In antwoord op de vraag van deze leden stel ik voorop dat het bij integrale acties niet gaat om de toepassing van de bevoegdheid van artikel 126jj Sv maar om de inzet van ANPR op grond van artikel 3 van de Politiewet. Het gaat dan om het vergelijken van kentekens van passerende voertuigen met kentekens die op referentielijsten voorkomen – voor de politie bijvoorbeeld lijsten met gestolen voertuigen of lijsten met kentekens ten aanzien waarvan nog boetes openstaan. Er kan dan worden opgetreden als het kenteken van een passerend voertuig overeenkomt met een kenteken op de referentielijst. Deze «hits» mogen worden bewaard,

kentekens van andere passerende voertuigen niet. De «hits» worden verwerkt op grond van de artikelen 8 en 9 van de Wet politiegegevens (Wpg). Deze gegevens kunnen overeenkomstig de artikelen 16 tot en met 24 Wpg worden verstrekt aan andere personen of instanties. Deze bepalingen kennen een gedifferentieerd verstrekkingenregime, inhoudende dat verstrekkingen van gegevens aan derden in beginsel expliciet zijn geregeld in de Wet of het Besluit politiegegevens, evenals de doeleinden waarvoor verstrekt mag worden. Daarnaast kan de verantwoordelijke in overeenstemming met het bevoegde gezag beslissen tot de verstrekking van politiegegevens voor bepaalde doeleinden, die nauw samenhangen met de uitvoering van de politietaak. De beslissing tot verstrekking kan betrekking hebben op bijzondere gevallen (art. 19 Wpg) of op een samenwerkingsverband van de politie met personen of instanties (artikel 20 Wpg). De politie mag gegevens van andere overheidsinstanties ontvangen. Dit kan in de eerste plaats doordat de politie die gegevens van die instantie – overeenkomstig de bepalingen uit het Wetboek van Strafvordering – in het kader van een concreet opsporingsonderzoek vordert. Daarnaast mag de politiegegevens ontvangen van andere overheidsinstanties die zij overeenkomstig hun eigen wettelijke bepalingen aan de politie verstrekken.
Ten overvloede wordt opgemerkt dat voor de ANPR-gegevens die op grond van artikel 126jj Sv worden vastgelegd en bewaard – wat dus niet aan de orde is bij de integrale acties – een aanzienlijk strikter regime geldt. De ANPR-gegevens die op grond van artikel 126jj Sv worden verwerkt, worden gescheiden van andere politiegegevens in een afzonderlijke database bewaard (artikel 9 van het ontwerpbesluit). Zoals hierboven aan de orde is gekomen mogen de gegevens uit deze 126jj Sv-database *niet* worden verstrekt aan andere Nederlandse overheidsinstanties. Dit is op het niveau van de wet vastgelegd (zie de tweede nota van wijziging: Kamerstuk 33 542, nr. 20). De enige uitzondering hierop zijn de inlichtingen- en veiligheidsdiensten. Ik kom daarop hieronder in antwoord op een vraag van de leden van de D66-fractie nog terug.

3. Toelichting op de bepalingen

De leden van de CDA-fractie wezen op de Algemene Verordening Gegevensbescherming (AVG) en vroegen of die nog van invloed is op de wijze waarop de ANPR-gegevens worden verwerkt.
Graag verhelder ik in antwoord op deze vraag dat de verwerking van ANPR-gegevens op grond van artikel 126jj Sv plaatsvindt met het oog op de opsporing en vervolging van strafbare feiten en de tenuitvoerlegging van straffen. Dat betekent dat niet de AVG, maar richtlijn 2016/680/EU over de bescherming van persoonsgegevens die worden verwerkt voor politiële en strafvorderlijke doeleinden daarop van toepassing is. Een wetsvoorstel om deze richtlijn te implementeren is inmiddels bij de Tweede Kamer aanhangig (zie Kamerstuk 34 889). De in dit wetsvoorstel voorgestelde wijzigingen van de Wpg zijn ook van toepassing op de op grond van artikel 126jj Sv verzamelde ANPR-gegevens.

Cameraplan (artikel 2)

De leden van de D66-fractie vroegen waarom voor mobiele camera's niet van tevoren kan worden vastgelegd op welke locaties zij worden geplaatst. Zij vroegen of in ieder geval de regio of gemeente waar deze camera's ingezet gaan worden kan worden vastgelegd. Ook vroegen zij om hoeveel camera's, vast of mobiel, het in totaal gaat.
Vanwege de noodzaak van een flexibele inzet van mobiele camera's is het niet mogelijk vooraf in het cameraplan op te nemen waar zij zullen worden geplaatst, ook niet in welke gemeente. Een belangrijk voordeel van mobiele camera's is namelijk dat zij kunnen «meebewegen» met zich

(snel) verplaatsende of nieuwe «criminele hotspots». Het is voor een effectieve opsporing van essentieel belang dat, wanneer een «criminele hotspot» zich verplaatst naar een andere locatie, de 126jj-camera eveneens direct kan worden verplaatst. In het cameraplan moet wel worden vastgelegd hoeveel mobiele camera's door de politie mogen worden ingezet en op wat voor soort locaties. Op dit moment zijn er – naast de 352 locaties waar vaste ANPR-camera's worden ingezet – ongeveer 200 mobiele camera's in gebruik bij de politie. Het gaat hier om vaste en mobiele camera's die worden ingezet voor de huidige inzet van ANPR. Niet al deze camera's zullen ook voor de bevoegdheid van artikel 126jj Sv kunnen worden ingezet: alleen de camera's die voldoen aan de criteria opgesomd in artikel 3 van het ontwerpbesluit, kunnen voor de bevoegdheid van artikel 126jj Sv worden ingezet. Camera's geplaatst op locaties die niet voldoen aan de criteria opgesomd in artikel 3, tweede lid, van het ontwerpbesluit vallen bij voorbaat af. Bij mobiele camera's moet daarbij bedacht worden dat ongeveer 150 van de 200 huidige mobiele camera's, camera's in voertuigen betreft. Zoals in de nota van toelichting bij het ontwerpbesluit is aangegeven zullen deze camera's naar verwachting niet worden ingezet voor de bevoegdheid van artikel 126jj Sv, omdat niet of hoogst zelden zal zijn voldaan aan het vereiste dat de (camera's in) voertuigen zich uitsluitend verplaatsen in een gebied dat voldoet aan één van de criteria opgesomd in artikel 3, tweede lid, van het ontwerpbesluit. Een aanzienlijk deel van de mobiele camera's zal dus niet voor de bevoegdheid van artikel 126jj Sv kunnen worden ingezet.
In de vragen van deze leden zie ik aanleiding om in het ontwerpbesluit vast te leggen dat jaarlijks een overzicht wordt gepubliceerd door de politie (op de website) van de locaties waar in het daaraan voorafgaande jaar mobiele camera's waren geplaatst. Zo zijn ook de locaties van mobiele camera's openbaar en raadpleegbaar voor burgers. Ik zal daartoe een vijfde lid toevoegen aan artikel 2 van het ontwerpbesluit. Zie daarvoor ook de bijlage bij deze brief. In de jaarlijkse privacy audit en in de wetsevaluatie zal aandacht worden besteed aan het aantal mobiele camera's dat is ingezet voor de bevoegdheid van artikel 126jj Sv.

Criteria voor plaatsing en inzet (artikel 3)

De leden van de D66-fractie vroegen om een nadere toelichting hoe de afweging aangaande de proportionaliteit en subsidiariteit van het plaatsen van camera's wordt gemaakt. Zij vroegen of hiervan concrete voorbeelden te geven zijn.
Bij de afweging of de plaatsing van een camera proportioneel is, spelen verschillende omstandigheden een rol. Allereerst is van belang of sprake is van een locatie die voldoet aan een van de criteria opgesomd in artikel 3, tweede lid, van het ontwerpbesluit. Dit betekent dat moet worden beoordeeld of sprake is van een voor de opsporing relevante locatie. Dat moet worden onderbouwd in het cameraplan (artikel 2, derde lid, van het ontwerpbesluit). Daarbij zal ook moeten worden betrokken of er geen andere, minder ingrijpende bevoegdheden zijn waarmee hetzelfde doel kan worden bereikt, bijvoorbeeld door surveillance of voertuigcontrole. Of dit mogelijk is zal mede afhankelijk zijn verschillende factoren, zoals de soort strafbare feiten en (de (ligging en kenmerken van) de locatie waarom het gaat. Daarnaast moet het verdere netwerk van camera's worden betrokken. Dit is relevant omdat de vastlegging van kentekengegevens met behulp van een afzonderlijke camera op zichzelf een beperkte en proportionele aantasting van de persoonlijke levenssfeer met zich mee kan brengen, maar als onderdeel van een netwerk van camera's een grotere inbreuk kan vormen. Dit betekent dat in de beoordeling wordt betrokken of de plaatsing van de camera een substantiële meerwaarde heeft ten opzichte van reeds geplaatste camera's in de nabijheid van de betreffende locatie.

Deze leden wezen op de passage in de nota van toelichting bij het criterium, opgenomen in artikel 3, tweede lid, onder c, waarin staat dat er geen concreet vermoeden hoeft te zijn van een concreet te verwachten individueel strafbaar feit. Wat daarmee bedoeld wordt, zo beantwoord ik de vraag van deze leden daarnaar, is dat er niet al sprake hoeft te zijn van een concreet vermoeden bij de opsporingsinstanties dat op tijdstip X een bepaald strafbaar feit Y op locatie Z is gepleegd. Voldoende is dat bekend is dat op de betreffende locatie of op soortgelijke locaties bijvoorbeeld met enige regelmaat drugs worden verhandeld. Dat kan bijvoorbeeld gelden voor grote parkeerplaatsen langs snelwegen of grensovergangen. Het is dus zeker niet zo dat dit criterium het mogelijk maakt om camera's op alle locaties in Nederland plaatsen. De plaatsingscriteria beogen de locaties waar camera's geplaatst kunnen worden uitdrukkelijk te beperken tot voor de opsporing mogelijk relevante locaties. Door middel van het jaarlijkse cameraplan wordt steeds voorafgaande aan de inzet inzicht verschaft over de plaatsing van de vaste camera's en het gebruik van mobiele camera's. Omdat het niet mogelijk is om in het cameraplan aan te geven op welke locaties mobiele camera's worden ingezet, zal dit achteraf op de website van de politie worden gepubliceerd, zo zegde ik hierboven toe naar aanleiding van een eerdere vraag van deze leden reeds toe. Ik zal dit, zoals gezegd, ook vastleggen in het ontwerpbesluit. Zie daarvoor de bijlage bij deze brief[1].

Geen woningen of gezichten (artikel 5)

De leden van de D66-fractie vroegen naar de bewaartermijn van vier weken. In antwoord op deze vraag verhelder ik graag dat deze bewaartermijn in de wet is vastgelegd (art. 126jj, tweede lid, Sv). Met de bewaartermijn van vier weken is aangesloten bij de bewaartermijn voor cameratoezicht in de Gemeentewet. De bewaartermijn geeft de opsporing de tijd om na de constatering van een strafbaar feit terug te kijken in de gegevens, terwijl tegelijkertijd – vanuit een oogpunt van de bescherming van de persoonlijke levenssfeer van burgers – wordt voorkomen dat deze gegevens onnodig lang worden bewaard. Tijdens de parlementaire behandeling is uitvoerig gesproken over de lengte van de bewaartermijn. Door verschillende partijen in de Tweede Kamer zijn amendementen ingediend. Er waren amendementen van het lid Van Toorenburg (CDA) (Kamerstuk 33 542, nr. 25) en van de leden Van Wijngaarden (VVD) en Van der Staaij (SGP) (Kamerstuk 33 542, nr. 32) om de bewaartermijn te verlengen tot zes maanden, evenals een amendement van de leden Segers (CU) en Verhoeven (D66) om de bewaartermijn te verkorten tot twee weken (Kamerstuk 33 542, nr. 40). Voor geen van deze amendementen bestond een meerderheid, zodat deze zijn verworpen. De lengte van de bewaartermijn zal, zoals is toegezegd, onderdeel uitmaken van de evaluatie van de wet.

In antwoord op een volgende vraag van deze leden benadruk ik dat het niet mogelijk is – ook niet bij wijze van uitzondering – om met toestemming van de officier van justitie af te wijken van de bepaling dat personen onherkenbaar moeten worden gemaakt. De suggesties uit de adviezen van de politie en de NVvR om het in uitzonderingsgevallen mogelijk te maken om van deze bepaling af te wijken zijn niet overgenomen. Naar aanleiding van de vraag van deze leden zal ik dit in de nota van toelichting bij het ontwerpbesluit verhelderen.

De leden van de D66-fractie vroegen verder om een overzicht van alle instanties die direct toegang hebben tot de gegevens.

---

[1] Raadpleegbaar via www.tweedekamer.nl

Zoals eerder, naar aanleiding van een vraag van de leden van de GroenLinks-fractie, is opgemerkt is in dit verband de tweede nota van wijziging van belang (Kamerstuk 33 542, nr. 20). Middels die tweede nota van wijziging is expliciet in de wet vastgelegd dat de gegevens die op grond van artikel 126jj Sv worden bewaard niet verstrekt kunnen worden aan derden. De bepalingen uit de Wpg die een dergelijke gegevensverstrekking mogelijk zouden maken, zijn niet van toepassing op de hier bedoelde gegevens, zo wordt bepaald in artikel 126jj, vijfde lid, Sv. Hierop bestaan twee uitzonderingen. Allereerst kunnen de gegevens wel aan buitenlandse autoriteiten worden verstrekt. Dit kan slechts onder dezelfde voorwaarden als gesteld in artikel 126jj Sv. Dat betekent dat de gegevens alleen kunnen worden verstrekt bij een concrete zoekvraag (kenteken en/of locatie en tijdstip), ter opsporing van een ernstig misdrijf of ter aanhouding van een voortvluchtige. Ik verwijs naar artikel 13 van het ontwerpbesluit. Van belang is dat het gaat om een *verstrekking* van gegevens. De buitenlandse autoriteiten hebben zelf géén toegang tot de database met de gegevens. De tweede uitzondering vormen de inlichtingen en de veiligheidsdiensten; aan die diensten zullen de gegevens, die op grond van artikel 126jj Sv worden bewaard, kunnen worden verstrekt met het oog op de uitvoering van de Wet op de inlichtingen- en de veiligheidsdiensten 2002 (Wiv 2002). Deze wet zal binnenkort worden vervangen door de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017). Vanwege het mogelijk belang van de bewaarde kentekengegevens voor de nationale veiligheid, bijvoorbeeld in het kader van terrorismebestrijding, is bij eerdergenoemde tweede nota van wijziging expliciet in artikel 126jj Sv vastgelegd dat de gegevens, die op grond van artikel 126jj Sv worden bewaard, aan de inlichtingen- en veiligheidsdiensten kunnen worden verstrekt met het oog op de uitvoering van de taken van de diensten.

Raadpleging (artikel 7)

De leden van de SP-fractie vroegen waarom er niet is gekozen voor een voorafgaande machtiging door de rechter-commissaris bij de raadpleging van de gegevens. Zij verwezen naar de uitspraak Digital Rights van het Hof van Justitie van de Europese Unie (HvJEU 8 april 2016, C-293/12 en C-594/12).
Naar aanleiding van deze vraag merk ik op dat deze betrekking heeft op de regeling van artikel 126jj Sv. Op grond van het wetsvoorstel zoals dat was ingediend bij de Tweede Kamer, konden opsporingsambtenaren de vastgelegde gegevens zonder voorafgaand bevel van de officier van justitie raadplegen. In de door deze leden genoemde uitspraak, heb ik evenwel aanleiding gezien om dit bij tweede nota van wijziging te wijzigen, en de toegang afhankelijk te maken van een bevel van de officier van justitie.
Bij de keuze voor de officier van justitie is van belang dat de bewaarregeling van telecommunicatiegegevens zoals die in de Digital Rights uitspraak centraal stond en de regeling van artikel 126jj Sv op belangrijke punten van elkaar verschillen. Zie hierover ook Kamerstuk 33 542, C, blz. 6 e.v. en Kamerstuk 33 542, F, blz. 4 e.v. Belangrijke verschillen vormen de aard van de gegevens – (verkeers)gegevens betreffende vertrouwelijke communicatie (Digital Rights) tegenover kentekengegevens (ANPR) – en de «reasonable expectation of privacy». Met dit laatste wordt bedoeld dat het feit dat de ANPR-gegevens worden vastgelegd langs de openbare weg maakt dat de verwachting van de burgers over in hoeverre zij (of hun voertuigen) worden waargenomen, anders is dan bij (verkeers)gegevens over vertrouwelijke communicatie. Dit leidt ertoe dat de inbreuk die op de persoonlijke levenssfeer wordt gemaakt met het vastleggen en bewaren van ANPR-gegevens anders moet worden gewaardeerd dan de inbreuk die daarop wordt gemaakt met het vastleggen en bewaren van telecom-

municatiegegevens. De keuze voor de officier van justitie als autoriteit die over de raadpleging beslist, past tegen die achtergrond beter binnen het wettelijke stelsel. Een vereiste machtiging door de rechter-commissaris geldt op basis van de huidige wetgeving namelijk niet voor de inzet van bijzondere opsporingsbevoegdheden zoals de stelselmatige observatie, de stelselmatige inwinning van informatie en de infiltratie. Ook bij dergelijke 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 – wordt volstaan met een bevel van de officier van justitie. 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 afluisteren (artikel 126l Sv). Ook de bewaring van telecommunicatiegegevens die in de Digital Rights uitspraak centraal stond, heeft betrekking op (verkeers)gegevens rond vertrouwelijke communicatie. Bij ANPR gaat het niet om dergelijke vertrouwelijke communicatie, maar om kentekengegevens die langs de openbare weg worden vastgelegd. Daarom kan worden volstaan met een bevel door de officier van justitie. Tijdens de behandeling van het wetsvoorstel in de Tweede Kamer zijn overigens geen amendementen ingediend die zagen op een machtiging van de rechter-commissaris tot raadpleging binnen de voorgestelde bewaartermijn van vier weken. Ook in de bovengenoemde amendementen waarin werd voorgesteld de bewaartermijn te verlengen, werd voor de raadpleging binnen de eerste vier weken na vastlegging volstaan met een bevel van de officier van justitie.
Uiteraard zal de officier van justitie steeds een zorgvuldige afweging maken of aan de voorwaarden voor raadpleging is voldaan en of deze raadpleging noodzakelijk en proportioneel is. De uitkomst van deze afweging wordt vastgelegd in het bevel: op grond van artikel 126jj, vierde lid, Sv, moet de officier van justitie in het bevel onder meer opnemen voor welk doel de gegevens worden geraadpleegd, in het kader van welk concreet opsporingsonderzoek en waarom de raadpleging noodzakelijk is. Het aantal keer dat de gegevens zijn geraadpleegd zal onderdeel uitmaken van de privacy audit, die in plaats van vierjaarlijks (zie artikel 6:5 van het Besluit politiegegevens (Bpg)), jaarlijks wordt uitgevoerd (zie artikel 15 van het ontwerpbesluit), en van de wetsevaluatie. Zowel de jaarlijkse privacy audit als de wetsevaluatie zullen aan Uw Kamer worden toegezonden.

Centrale opslag (artikel 9)

De leden van de SP-fractie vroegen te verduidelijken wanneer gegevens vernietigd worden als zij gebruikt worden bij een onderzoek.
Als gegevens die op grond van artikel 126jj Sv worden bewaard, zo beantwoord ik deze vraag, relevant zijn in het kader van een opsporingsonderzoek, dan geldt voor die betreffende gegevens hetzelfde bewaarregime als voor de overige politiegegevens in dat opsporingsonderzoek. Dat betekent dat zij overeenkomstig de artikelen 8 en 9 van de Wet politiegegevens verwerkt worden. Op grond van die bepalingen kunnen die gegevens dan worden bewaard gedurende vijf 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). De verwijderde politiegegevens worden gedurende een termijn van vijf jaar bewaard ten behoeve van verwerking met het oog op de afhandeling van klachten en de verantwoording van verrichtingen en vervolgens vernietigd of gearchiveerd (art. 14 Wpg).

Als de kentekengegevens door de inlichtingendiensten zijn opgevraagd, zo beantwoord ik een volgende vraag van deze leden, dan worden zij verder verwerkt op grond van de wetgeving die van toepassing is op de verwerking van persoonsgegevens door die diensten en gelden de daarin opgenomen bewaartermijnen. Op grond van die wetgeving worden de gegevens verwijderd die, gelet op het doel waarvoor zij worden verwerkt, hun betekenis hebben verloren. De verwijderde gegevens worden vernietigd, tenzij wettelijke regels omtrent bewaring daaraan in de weg staan (art. 43, eerste en derde lid, Wiv 2002; artikel 20, eerste en derde lid, Wiv 2017). De wet voorziet in de mogelijkheid van archivering, als de gegevens ouder zijn dan twintig jaar (art. 44 Wiv 2002, art. 21 Wiv 2017). Het toezicht op de rechtmatigheid van de uitvoering van hetgeen bij of krachtens de Wiv 2002 is gesteld wordt uitgeoefend door de commissie van toezicht betreffende de inlichtingen- en veiligheidsdiensten (art. 64 Wiv 2002, art. 97, derde lid, onder a, Wiv 2017). Dit toezicht omvat de naleving van de wettelijke regels rond de vernietiging van informatie.

Beveiligingseisen (artikel 10, 11 en 12)

De leden van de D66-fractie vroegen welk eisen er worden gesteld aan de persoonsgebonden authenticatie. Zij vroegen of maatregelen als 2factor-authentication worden toegepast en of de gegevens versleuteld worden opgeslagen.
De verwerking van ANPR-gegevens op grond van de bevoegdheid van artikel 126jj Sv moet in de eerste plaats voldoen aan de algemene beveiligingseisen opgenomen in de Wpg. Daarnaast gelden de specifieke beveiligingsvoorschriften van de artikelen 10, 11, en 12 van het ontwerpbesluit. De eerdergenoemde richtlijn gegevensbescherming opsporing en vervolging (richtlijn (EU) 2016/680) bevat gedetailleerde voorschriften omtrent de beveiliging van persoonsgegevens (art. 29 van de richtlijn). Dit omvat het treffen van maatregelen om te verhinderen dat onbevoegden toegang krijgen tot verwerkingsapparatuur, de gegevensdragers lezen, kopiëren, wijzigen of verwijderen, persoonsgegevens invoeren of opgeslagen persoonsgegevens inzien, wijzigen of verwijderen, of geautomatiseerde verwerkingssystemen gebruiken met behulp van datatransmissieapparatuur. Ter implementatie van de richtlijn zullen de Wpg en het Bpg worden aangepast. Het wetsvoorstel ter implementatie is inmiddels bij de Tweede Kamer aanhangig (zie Kamerstuk 34 889). De aangepaste regels van de Wpg en het Bpg zullen ook van toepassing zijn op de ANPR-gegevens die op grond van artikel 126jj Sv worden verwerkt. De eisen ten aanzien van persoonsgebonden authenticatie hangen dan ook nadrukkelijk samen met de eisen die gesteld worden aan de identificatie, authenticatie en autorisatie voor de verwerking van politiegegevens in het algemeen. De wettelijke eisen ten aanzien van autorisatie bij de verwerking van persoonsgegevens zijn reeds door de politie nader uitgewerkt in het Informatiebeveiligingskader Politie en het Autorisatiebeleid Politie. Daarin worden de organisatorische en beheersmatige kaders gegeven waar de autorisatievoorzieningen aan moeten voldoen. Binnen de politie geldt een landelijk autorisatiemodel waarin identificatie en authenticatie van gebruikers plaatsvinden op basis van landelijke voorzieningen en autorisaties worden verleend op basis van centraal beheerde rollen en attributen. De methoden en technieken die voor identificatie en authenticatie worden toegepast, moeten afdoende zijn om de onderkende informatiebeveiligingsrisico's te kunnen beheersen. Om onnodige beveiligingsrisico's te voorkomen kan op deze plaats geen nadere informatie worden gegeven over de methoden en technieken die bij de beveiliging van de kentekengegevens in het centrale opslagsysteem worden toegepast. Om die reden kan evenmin nader worden ingaan op de vragen over authenticatiemethoden en de encryptie van gegevens.

Jaarlijkse audit (artikel 15)

De leden van de GroenLinks-fractie gaven aan het op prijs te stellen dat er een jaarlijkse privacy-audit wordt uitgevoerd. Graag zeg ik aan hen toe dat deze audits ook aan Uw Kamer worden gezonden.
Op de vraag van deze leden wie deze audits zal uitvoeren en wat de rol van de Autoriteit persoonsgegevens (AP) is, antwoord ik dat de privacy audits onder verantwoordelijkheid van de korpschef worden uitgevoerd. De controleresultaten van deze privacy audit worden aan de AP gestuurd (zie artikel 33 Wpg).