W03.12.0008/II

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

VOORSTEL VAN WET

Wij Beatrix, bij de gratie Gods, Koningin der Nederlanden, Prinses van Oranje-Nassau, enz. enz. enz.

Allen die deze zullen zien of horen lezen, saluut! doen te weten:
Alzo Wij in overweging genomen hebben, dat het wenselijk is in het Wetboek van Strafvordering regels te stellen voor het vastleggen en bewaren van kentekengegevens;
Zo is het, dat Wij, de Afdeling advisering van de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

Artikel I

Het Wetboek van Strafvordering wordt als volgt gewijzigd.
Na titel VE van het Eerste Boek wordt een titel ingevoegd, die luidt:

TITEL VF

Vastleggen en bewaren van kentekengegevens

Artikel 126jj

1. Een opsporingsambtenaar is bevoegd op of aan de openbare weg kentekengegevens van voertuigen als bedoeld in het tweede lid met behulp van een technisch hulpmiddel vast te leggen, teneinde deze gegevens met toepassing van het derde lid te kunnen raadplegen. De aanwezigheid van het technisch hulpmiddel wordt op duidelijke wijze kenbaar gemaakt.
2. Het kenteken, de locatie en het tijdstip van de vastlegging, en de foto-opname van het voertuig kunnen worden bewaard gedurende een periode van vier weken na de datum van de vastlegging.
3. De gegevens als bedoeld in het tweede lid kunnen door een opsporingsambtenaar worden geraadpleegd:
a. in geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, en een misdrijf als bedoeld in artikel 178 van de Wegenverkeerswet 1994, ten behoeve van de opsporing van dat misdrijf of
b. in geval van een voortvluchtige persoon als bedoeld in artikel 564 van het Wetboek van Strafvordering, ter aanhouding van deze persoon. De raadpleging vindt slechts plaats door politiegegevens die voor één van deze doelen worden verwerkt, geautomatiseerd te vergelijken met de gegeven als bedoeld in het tweede lid, teneinde vast te stellen of de gegevens overeenkomen. Als de gegevens

overeenkomen kunnen ze voor het desbetreffende doel verder worden verwerkt.
4. Bij of krachtens algemene maatregel van bestuur worden regels gesteld over de wijze waarop de gegevens worden geraadpleegd.

Artikel II

1. Deze wet treedt in werking op een bij koninklijk besluit te bepalen tijdstip. Artikel 126jj van het Wetboek van Strafvordering vervalt drie jaar na inwerkingtreding van de wet, tenzij bij koninklijk besluit anders wordt bepaald.
2. De Minister van Veiligheid en Justitie zendt binnen drie jaar na inwerkingtreding van deze wet aan de Staten-Generaal een verslag over de doeltreffendheid en de effecten van deze wet in de praktijk.

Lasten en bevelen dat deze in het Staatsblad zal worden geplaatst en dat alle ministeries, autoriteiten, colleges en ambtenaren wie zulks aangaat, aan de nauwkeurige uitvoering de hand zullen houden.

Gegeven

De Minister van Veiligheid en Justitie,

W03.12.0008/II

Concept december 2011

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

MEMORIE VAN TOELICHTING

ALGEMEEN DEEL

1. Inleiding

Sinds een aantal jaren wordt door verschillende politieregio's gebruik gemaakt van automatische kentekenherkenning, ook wel *automatic numberplate recognition* (ANPR) genoemd. Dit is een techniek waarbij met behulp van camera's kentekens van voertuigen in het verkeer worden vastgelegd en langs geautomatiseerde weg worden vergeleken met kentekens van voertuigen die op naam staan van personen die bekend zijn bij de politie. Automatische kentekenherkenning stelt de politie in staat aan de hand van kentekens snel en efficiënt voertuigen en personen waar te nemen die zij zoekt ter uitvoering van de politietaak. In de afgelopen decennia is de mobiliteit toegenomen. De tijd dat politieagenten door eigen kennis en waarneming een goed beeld konden hebben van wat zich in dorpen en steden afspeelt en zicht hadden op woon- en verblijfplaatsen van justitiabelen ligt achter ons. De politie is alleen door de toepassing van nieuwe technologie en de opbouw van een goede informatiepositie in staat haar taken effectief en efficiënt uit te voeren.
Er zijn circa 10 miljoen geregistreerde kentekens in Nederland. Een gerichte selectie van die kentekens die toebehoren aan personen die bijvoorbeeld vanwege de tenuitvoerlegging van een straf worden gezocht, draagt bij aan een effectieve uitvoering van de politietaak. Waar handmatig per uur hoogstens tientallen kentekens kunnen worden vergeleken, kunnen met toepassing van automatische kentekenherkenning per uur vele duizenden gegevens worden vergeleken. Dit gebeurt door op bepaalde locaties kentekens vast te leggen en te vergelijken met een referentiebestand, waarin kentekens zijn opgenomen van voertuigen waarvan het kenteken op naam is gesteld van personen tegen wie bijvoorbeeld een bevel tot vrijheidsbeneming is gegeven in verband met een onbetaalde geldboete, of aan wie een ontzegging van de rijbevoegdheid is opgelegd. Wanneer de camera een kenteken vastlegt dat is opgenomen in het referentiebestand, is er een *hit* en wordt het voertuig stilgehouden om daaraan opvolging te geven, dan wel worden de gegevens verwerkt en wordt daaraan later opvolging gegeven. Het verwerken van *hits* bij automatische kentekenherkenning voor de uitvoering van de politietaak kan, zoals hierna in paragraaf 5.3 aan de orde komt, plaatsvinden binnen de bestaande wetgeving.

Automatische kentekenherkenning kan ook worden toegepast om op een later tijdstip in de vastgelegde gegevens terug te kunnen zoeken.

Hierbij worden alle kentekens die een camera passeren – ongeacht of het gaat om *hits* - vastgelegd en bewaard. Indien later een misdrijf wordt ontdekt, kunnen de gegevens ten behoeve van de opsporing daarvan worden geraadpleegd. De politie onderzoekt dan bijvoorbeeld of de auto van de verdachte op een bepaalde plaats aanwezig is geweest. Dit kan eraan bijdragen dat de politie beter in staat is misdrijven op te lossen, zoals hierna aan de orde komt in paragraaf 4. Voor deze toepassing ontbreekt echter een toereikende wettelijke basis. Het wetsvoorstel heeft ten doel in de noodzakelijke wettelijke basis te voorzien.

2. Inhoud van het wetsvoorstel

Voorgesteld wordt in het Wetboek van Strafvordering een bevoegdheid op te nemen voor het vastleggen en bewaren van gegevens betreffende kentekens Kentekens, en de daarmee verbonden gegevens van tijd en locatie kunnen dan, ongeacht of er sprake is van een *hit,* worden vastgelegd en gedurende een periode van vier weken worden bewaard. Indien in deze periode naar voren komt dat het kan bijdragen aan de opsporing van een bepaald misdrijf om een kentekennummer van een voertuig te vergelijken met de bewaarde gegevens, is dat mogelijk. Voorgesteld wordt dat de gegevens ook mogen worden gebruikt voor het aanhouden van voortvluchtige veroordeelden of verdachten. Dit wordt nader toegelicht in paragraaf 4.

3. Toekomstige ontwikkelingen

Automatische kentekenherkenning kent ook andere toepassingsvarianten, zowel binnen de politie als andere overheidsdiensten. Deze worden geïnventariseerd. Op basis daarvan zal een meer brede inzet van automatische kentekenherkenning, zoals aangekondigd in het regeerakkoord, kunnen worden ontwikkeld (Kamerstukken II 2010/2011, 32417, nr. 14, blz. 35). Bij deze inventarisatie zal de aandacht uitgaan naar de juridische vormgeving, ontwikkelmogelijkheden en mogelijke knelpunten. Er zal een beleidsvisie over de inzet van automatische kentekenherkenning worden opgesteld. Het wetsvoorstel maakt daarvan onderdeel uit.

Voor de huidige praktijk, beschreven in paragraaf 1, wordt een uitvoeringskader opgesteld voor de praktische voorzieningen zoals de automatische opschoning van gegevens, de uniformiteit van programmatuur, het vaststellen van autorisatieniveaus en het stellen van eisen aan de integriteit van systemen. Voor de huidige praktijk zijn tevens de “Richtsnoeren voor de toepassing van automatische kentekenherkenning door de politie” van het CBP van belang (www.cbpweb.nl).

4. Het bewaren van kentekengegevens ten behoeve van de opsporing.

4.1 Noodzaak van een wettelijke regeling

In een aantal politieregio’s werden tot begin 2010 alle kentekens die een camera passeerden vastgelegd en bewaard, ongeacht of deze op het moment van vastlegging noodzakelijk waren voor de uitvoering van de politietaak. De gehanteerde bewaartermijnen verschilden,

variërend van tien dagen tot vier maanden. Gedurende deze periode werden de opgeslagen gegevens geraadpleegd voor opsporingsdoeleinden. Deze toepassing is beëindigd omdat de huidige wetgeving niet voorziet in een algemene regeling voor het bewaren van alle door de politie vastgelegde kentekens, ook indien deze op het moment van vastlegging niet noodzakelijk waren voor de uitvoering van de politietaak. Zonder wettelijke basis is dit niet toegestaan. Het College bescherming persoonsgegevens (CBP) heeft dit vastgesteld in de bevindingen over de toepassing van automatische kentekenherkenning door de Regionale politiekorpsen IJsselland en Rotterdam Rijnmond van 11 januari 2010. Het wetsvoorstel voorziet in een wettelijke basis.
Zoals in paragraaf 5 aan de orde komt, dient een bevoegdheid tot het bewaren van kentekengegevens te voldoen aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit, die voortvloeien uit het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). In het navolgende zal worden ingegaan op het belang van het bewaren van de gegevens voor de opsporing van strafbare feiten en op de randvoorwaarden waarmee het bewaren van de gegevens zal worden omgeven. In paragraaf 5 zal de voorgestelde regeling worden getoetst aan het EVRM.

4.2 Belang van de opsporing

In de politieregio's IJsselland en Rotterdam-Rijnmond is ervaring opgedaan met het gebruik van bewaarde kentekengegevens ten behoeve van de opsporing. Gebleken is dat misdrijven mede met behulp van bewaarde kentekengegevens kunnen worden opgelost. Een voorbeeld hiervan is een overval op een winkel, waarbij omstanders de verdachte hebben zien wegrijden en waarbij later blijkt dat het kenteken van het voertuig van de verdachte, kort na de overval is vastgelegd door een camera in de nabijheid van de plaats waar de overval is gepleegd. Wanneer in de loop van het opsporingsonderzoek naar voren komt dat de verdachte mogelijk hulp heeft gehad van andere personen, kan door terug te zoeken in de kentekengegevens ook worden achterhaald welke voertuigen voor en achter het voertuig van de verdachte hebben gereden. Dit kan richting geven aan het opsporingsonderzoek en bijdragen aan het bewijs. Een dergelijke onderzoekswijze is in 2008 en 2009 binnen de politieregio Rotterdam gebruikt bij de opheldering van een overval, de opheldering van een ontvoering en de opheldering van een levensdelict.

Een voorbeeld van een zaak waarin het achteraf raadplegen van bewaarde kentekengegevens heeft bijgedragen aan het bewijs van een ernstig misdrijf, betreft de uitspraak van de Rechtbank Rotterdam van 29 juli 2009 (LJN BJ4213). Het betrof een verdenking van onder andere een levensdelict en het wegmaken van het stoffelijk overschot. Het lichaam van het overleden slachtoffer werd gevonden in de buurt van een autoweg. De verdachte maakte gebruik van een transportauto. De bandensporen op de plaats delict kwamen overeen met deze auto en ook andere sporen voerden naar deze auto. Uit gegevens van een verkeersregistratiesysteem dat kentekengegevens van passerende voertuigen vastlegde en bewaarde, bleek dat deze auto gedurende een bepaalde periode bij de plaats delict was geweest. Dit droeg bij aan het bewijs dat de verdachte opzettelijk het lijk heeft weggemaakt. In hoger beroep werd in deze zaak aangevoerd dat de desbetreffende gegevens "no hits" betroffen, die direct hadden

behoren te worden verwijderd en daarom niet voor het bewijs mochten worden gebruikt. Omdat het evenwel de kentekengegevens betrof van het voertuig van het slachtoffer, ook al werd het bestuurd door de verdachte, en de gegevens waren gebruikt om duidelijkheid over diens vermissing te krijgen, oordeelde het Hof dat de verdachte zich niet op deze schending van het recht kon beroepen. De gegevens konden daarom wel gebruikt worden voor het bewijs (Gerechtshof s'Gravenhage, 16 juni 2010, LJN BM7688). De verdachte werd veroordeeld voor het wegmaken van het stoffelijk overschot, maar vrijgesproken van het levensdelict. De kentekengegevens die betrekking hadden op een ander voertuig, dat in gebruik was bij de verdachte, werden door het Hof uitgesloten van het bewijs Op dit onderdeel is de uitspraak in cassatie vernietigd, en zal het Hof opnieuw recht doen (Hoge Raad, 20 september 2011, LJN BR0554)

Een andere casus betrof de uitspraak van de Rechtbank Zwolle van 2 juli 2009 (LJN BJ2118). Dit betrof een reeks van autodiefstallen die mede met behulp van bewaarde *no hits* weren opgelost. Met behulp van de bewaarde *no hits* kon de aanwezigheid van het voertuig van de verdachte op bepaalde plaatsen en tijden worden aangetoond. De rechtbank gaf aan dat het vaste rechtspraak is dat de grondslag voor opsporingsactiviteiten die niet specifiek in de wet zijn geregeld, en die niet meer dan een beperkte inbreuk maken op grondrechten, kan worden gevonden in de algemene opsporingstaak zoals die is neergelegd in artikel 141 en 142 Sv of, indien nog geen sprake is van opsporing, artikel 2 Politiewet 1993. De rechtbank was van oordeel dat in de gegeven omstandigheden – een toename van mobiel banditisme dat met het huidige arsenaal aan technische hulpmiddelen moeilijk te bestrijden is – het gebruik van het ANPR-systeem als opsporingsmiddel als noodzakelijk en passend kon worden beschouwd. Mede gelet op de gehanteerde zorgvuldige werkwijze oordeelde de rechtbank dat de inzet van het ANPR-systeem rechtmatig was geschied en dat de daaruit verkregen gegevens tot bewijs mochten worden gebezigd. In deze zaak oordeelde het Gerechtshof Leeuwarden in hoger beroep, onder verwijzing naar de wetsgeschiedenis van artikel 8 van de Wet politiegegevens (Wpg), anders. Gegevens die een *no hit* opleveren in het kader van de uitvoering van de dagelijkse politietaak dienden direct vernietigd te worden, omdat deze gegevens niet noodzakelijk zijn voor het doel van de ANPR registratie, gelet op het ontbreken van het desbetreffende kenteken in het vergelijkingsbestand. Het Hof achtte dit een ernstig vormverzuim en oordeelt dat de gegevens van het bewijs dienden te worden uitgesloten. (Hof Leeuwarden, 16 juni 2010, LJN BM8100).

Een andere relevante uitspraak betrof Rechtbank Rotterdam 4 maart 2010 (LJN BL6649), betreffende straatroof en heling. De rechtbank verwerpt een verweer dat de officier van justitie niet-ontvankelijk moest worden verklaard omdat de politie bij de opsporing gebruik had gemaakt van zogenaamde *no hits* die hadden behoren te worden vernietigd. De politie was namelijk voor drie autokentekens nagegaan of deze door ANPR-camera's waren vastgelegd op bepaalde locaties op de dag van de straatroof en op de dagen daar vlak voor en na. De aanwezigheid van de auto's op dezes locaties en de betreffende dagen kon bijdragen aan de opheldering van de strafbare feiten. De rechtbank oordeelde dat dit niet een dusdanige schending van de rechten van de verdachte opleverde dat het openbaar ministerie niet-ontvankelijk moest worden verklaard. Overigens volgde vrijspraak in

verband met gebrek aan toereikend bewijs. Tot slot kan worden genoemd de uitspraak van de Rechtbank De Haag van 22 februari 2010 (LJN BL5236) ter zake van onder andere vrijheidsberoving en diefstal met geweld en bedreiging. De politie was nagegaan of het kenteken van de auto van de verdachte op een bepaalde datum op bepaalde plaatsen door ANPR-camera's was vastgelegd. Dit bleek het geval te zijn, hetgeen bijdroeg aan het bewijs. De rechtbank oordeelde dat gebruik was gemaakt van een *no hit* en dat daarmee gehandeld was in strijd met de artikel 8, zesde lid jo 3, eerste en tweede lid van de Wpg, zodat de resultaten niet mochten worden gebruikt voor het bewijs. Er volgde een bewezenverklaring op grond van ander beschikbaar bewijs.

4.3 Meerwaarde voor de opsporing

Cijfers over de aantallen misdrijven die per jaar kunnen worden opgelost indien alle door de politie vastgelegde kentekengegevens gedurende een bepaalde periode mogen worden bewaard, kunnen niet worden gegeven. De ervaringen met het gebruik van bewaarde kentekengegevens ten behoeve van de opsporing zijn namelijk beperkt. Slechts enkele regio's hebben deze vorm van kentekenherkenning toegepast en zij zijn daar naar aanleiding van de bevindingen van het CBP mee gestopt. Door Regioplan is onderzoek gedaan naar het gebruik en de resultaten van automatische kentekenherkenning ten behoeve van de opsporing met vaste camera's boven de A-28 bij Zwolle in 2008 en 2009. (Kamerstukken II 2010–2011, 31 051, nr. 8). In deze periode werden de no-hits nog 10 dagen bewaard. Dit was voorafgaand aan het besluit het bewaren van *no –hits* te staken wegens het ontbreken van een wettelijke basis. Uit dit onderzoek blijkt dat automatische kentekenherkenning gebruikt wordt om voertuigen te signaleren en zicht te krijgen op reisbewegingen van verdachten. Er is in de bestudeerde zaken geen sprake van het direct aanhouden van verdachten. De conclusie van de onderzoekers is dat automatische kentekenherkenning meerwaarde heeft voor de opsporing. In twaalf van de negentien onderzochte zaken leidde de inzet van automatische kentekenherkenning tot specifieke opsporingsinformatie. Daarnaast kan door automatische kentekenherkenning richting worden gegeven aan opsporingsonderzoeken, bijvoorbeeld wanneer andere aanknopingspunten ontbreken.

Vergelijkbare resultaten komen naar voren in onderzoek dat in het Verenigd Koninkrijk is gedaan naar automatische kentekenherkenning (zie het rapport "*Practice advice on the management and use of Automatic Number Plate Recognition*" van de *National Policing Improvement Agency*, www.NPIA.police.uk). Uit het onderzoek van Regioplan blijkt ook dat – hoewel de politie casuïstiek voorhanden heeft waaruit de meerwaarde van ANPR blijkt – nader onderzoek nodig is om het inzicht in de effectiviteit van ANPR toepassingen in de opsporing verder te vergroten. Dit onderzoek, waarbij onder meer de ervaringen in de regio Rotterdam Rijnmond zijn betrokken, is onder auspiciën van het WODC uitgevoerd door de DSP groep. Uit het DSP onderzoek blijkt dat ANPR een efficiënt instrument is, aangezien de oude, handmatige werkwijze is geautomatiseerd. Of ANPR ook effectief is, is lastiger te beantwoorden. ANPR levert niet alleen hits op, maar ook hints die richting geven aan opsporingsonderzoeken. De meerwaarde van ANPR voor de opsporing ligt dan volgens de

onderzoekers ook hoofdzakelijk in het richting geven van opsporingsonderzoeken en (vooralsnog) veel minder in het opleveren van bewijsmateriaal. Volgens de onderzoekers zal het wetsvoorstel niet automatisch leiden tot betere opsporing. Volgens hen komt dat naar voren in de ervaringen in het Verenigd Koninkrijk (VK) waar al geruime tijd passagegegevens mogen worden bewaard. De onderzoekers zetten dit af tegen het gebruik van automatische kentekenherkenning voor boete-inning en de inzet van schaarse politie-capaciteit. Hierover kan worden opgemerkt dat de meerwaarde van automatische kentekenherkenning voor de opsporing niet zozeer is gelegen in besparing op de inzet van politiecapaciteit maar in het verhogen van de resultaten van het opsporingsonderzoek. De in paragraaf 3 genoemde beleidsvisie zal ingaan op de bestaande en de in de toekomst gewenste inzet van automatische kentekenherkenning.

Wanneer dit wetsvoorstel kracht van wet krijgt en in werking treedt, kan inzicht worden verkregen in de aantallen misdrijven die per jaar met behulp van het bewaren van kentekengegevens kunnen worden opgelost. Nu moet worden volstaan met de resultaten van bovengenoemde onderzoeken en met de indrukken als beschreven in paragraaf 4.2, die zijn ontleend aan de jurisprudentie over de korte periode waarin de politie alle kentekens die camera's passeerden vastlegde. In het wetsvoorstel is een zogenaamde horizonbepaling opgenomen. Dit betekent dat de voorgestelde bevoegdheid tot het bewaren van kentekengegevens na inwerkingtreding van de wet in beginsel voor slechts drie jaar van kracht is, tenzij bij Koninklijk Besluit anders wordt besloten. Hiermee wordt uitvoering gegeven aan het regeerakkoord van dit kabinet, waarin is opgenomen dat voorgenomen maatregelen inzake opslag, koppeling en verwerking van persoonsgegevens zoveel mogelijk worden voorzien van een horizonbepaling. Indien na inwerkingtreding van de wet op basis van een evaluatie van de wet kan worden bevestigd dat de bevoegdheid effectief is voor de opsporing van strafbare feiten, kan worden besloten de bevoegdheid te handhaven. Hierbij zal niet alleen worden gekeken naar de resultaten voor de opsporing, maar zal ook worden onderzocht of de verwerking van de bewaarde gegevens plaatsvindt met inachtneming van de wettelijke waarborgen.

4.4 Bewaartermijn

Bij het bepalen van de duur van de bewaartermijn dient het hierboven beschreven belang voor de opsporing van strafbare feiten te worden afgewogen tegen het belang van de burger gevrijwaard te blijven van bemoeienis van de politie, en van de verwerking van zijn gegevens zonder dat daar directe aanleiding toe bestaat. Een bevoegdheid tot het bewaren van gegevens moet, zoals in paragraaf 5 aan de orde komt, voldoen aan de eisen van noodzakelijkheid, proportionaliteit en subsidiariteit. Dit betekent dat de bewaartermijn zodanig lang moet zijn dat dit bijdraagt aan de effectiviteit van de opsporing, maar tevens zodanig kort dat geen onnodige verwerking van gegevens van burgers plaatsvindt.
Met inachtneming hiervan wordt een bewaartermijn voorgesteld van vier weken na de datum van de eerste verwerking. Een termijn van vier weken wordt ook gehanteerd voor het bewaren van beelden van gemeentelijke toezichtcamera's. In artikel 151c, zevende lid, van de Gemeentewet is bepaald dat de beelden die in het belang van de handhaving van de openbare orde met gemeentelijke toezichtcamera's

worden vastgelegd, voor een periode van ten hoogste vier weken mogen worden bewaard en dat de gegevens mogen worden gebruikt indien er een vermoeden is dat de gegevens noodzakelijk zijn voor de opsporing van een strafbaar feit. Deze termijn wordt noodzakelijk geoordeeld voor de preventieve functie voor de openbare orde handhaving van het cameratoezicht (Kamerstukken 2004/2005, 29440, nr. 16, blz. 2). De beelden mogen worden bewaard ongeacht of daartoe op het moment van het verwerven van de beelden aanleiding bestaat. Hierbij kan worden opgemerkt dat de parallel met de Gemeentewet maar ten dele opgaat. Bij het toezicht op openbare plaatsen in een gemeente worden in het algemeen geen kentekens vastgelegd. Het bewaren van de beelden van deze camera's heeft een functie bij het achteraf oplossen van lokaal gepleegde strafbare feiten, die doorgaans kort nadat de beelden zijn vastgelegd worden ontdekt. Bij automatische kentekenherkenning is dat anders. Vastgelegde en bewaarde kentekens kunnen van belang zijn voor misdrijven die pas later, soms veel later, worden ontdekt. Om die reden kan de termijn van vier weken worden beschouwd als een korte termijn voor het doel van de opsporing van strafbare feiten. Immers, ook na de periode van vier weken kunnen strafbare feiten naar voren komen die mede met behulp van bewaarde kentekengegevens kunnen worden opgespoord. Een voorbeeld daarvan is de hiervoor besproken zaak bij de Rechtbank Rotterdam van 29 juli 2009. In deze zaak werden de kentekengegevens pas twee maanden na de ontdekking van het lijk geraadpleegd, omdat het voertuig dat sporen op de plaats delict had achtergelaten pas later werd gevonden.

In hun brief van 3 februari 2010 stelden de toenmalige ministers van Justitie en BZK een periode van 10 dagen voor. Deze termijn van 10 dagen was bepaald aan de hand van de werkwijze van de politieregio IJsselland. De termijn van 10 dagen is toereikend voor gerichte opsporingsactiviteiten, zoals het herkennen van kentekens die in verband gebracht kunnen worden met herhaaldelijk gepleegde strafbare feiten op bepaalde locaties, zoals woninginbraken. Deze termijn is echter te kort zijn voor de opsporing van strafbare feiten die niet direct worden ontdekt, of strafbare feiten waarbij pas later blijkt dat kentekengegevens kunnen bijdragen aan de opheldering daarvan. Een voorbeeld daarvan is de hiervoor besproken zaak bij de Rechtbank Rotterdam van 29 juli 2009. In deze zaak werden de kentekengegevens overigens pas twee maanden na de ontdekking van het lijk geraadpleegd, omdat het voertuig dat sporen op de plaats delict had achtergelaten pas later werd gevonden. Ook voor strafbare feiten waarvoor de politie een langere periode nodig heeft om aangiften te verwerken en te selecteren voor opsporingsonderzoek is een termijn van 10 dagen erg kort. Daarom is gekozen voor een termijn van vier weken. Ik ben van mening dat een bewaartermijn van vier weken recht doet aan enerzijds het belang van de opsporing van strafbare feiten en anderzijds de belangen van bescherming van de persoonlijke levenssfeer. Drie jaar na inwerkingtreding van de wet wordt – zoals hiervoor aan de orde kwam – de effectiviteit van de bevoegdheid beoordeeld. De duur van de bewaartermijn zal hierbij opnieuw aan de orde komen.

4.5 Welke gegevens worden bewaard?

Voorgesteld wordt dat het kenteken, de locatie en het tijdstip van vastlegging van het kenteken en de foto-opname van het voertuig

kunnen worden bewaard. De camera's die worden gebruikt voor de automatische kentekenherkenning maken een foto van de voor- of achterkant van alle voorbijkomende voertuigen. Daaruit wordt het kenteken in een bestand vastgelegd. Het kenteken is met het oog op de herkenning het belangrijkste element, maar de foto zal een groter deel van het voertuig kunnen omvatten. Zo kunnen het merk en de kleur ook worden vastgelegd. Dit kan van belang zijn om in een concrete zaak te kunnen controleren of het gaat om het gezochte voertuig. De bestuurder of eventuele passagiers zullen wellicht wel te zien zijn, maar op basis van de huidige stand van de techniek naar verwachting niet herkenbaar, aldus het CBP op blz. 10 van de hiervoor genoemde Richtsnoeren. Het openbaar ministerie wijst er in haar advies op dat de techniek het reeds mogelijk maakt bestuurders herkenbaar te fotograferen. De eisen die gehanteerd worden voor de aanschaf van ANPR-apparatuur, zoals beschreven in paragraaf 4.7. zijn evenwel gericht op de goede weergave van het kenteken en brengen met zich mee dat de herkenbaarheid van de bestuurder beperkt zal zijn.
Naast het kenteken en de foto van het voertuig, worden ook de gegevens over de locatie, de datum en het tijdstip bewaard. Met behulp van deze gegevens is het mogelijk om de aanwezigheid van een voertuig op een bepaald tijdstip op een bepaalde plaats vast te stellen en kunnen de bewaarde kentekens waarde hebben voor de opsporing van strafbare feiten. De naam van de persoon op wiens naam het kenteken staat, wordt niet bewaard. De naam wordt pas bekend wanneer in een concrete zaak over een bepaald kenteken navraag wordt gedaan bij het kentekenregister.
Hiermee wordt inhoud gegeven aan het door de Commissie Brouwer geformuleerde uitgangspunt: "selecteer voor je verzamelt en houdt het sober". Het uitgangspunt van een selectieve verzameling van gegevens (*select before you collect*) is hier van toepassing in die zin dat alleen de hoogst noodzakelijke gegevens die bij latere raadpleging noodzakelijk zijn, worden verzameld. Daarnaast geldt het uitgangspunt van een selectieve toegang tot de gegevens: alleen voor een van de twee in de wet genoemde doeleinden.

4.6 Het gebruik van de bewaarde gegevens

In het voorgestelde artikel 126jj Sv wordt bepaald dat de bewaarde gegevens kunnen worden geraadpleegd in geval van verdenking van bepaalde misdrijven en ter aanhouding van voortvluchtigen. De raadpleging vindt slechts plaats door politiegegevens die voor één van deze doelen worden verwerkt, geautomatiseerd te vergelijken met de bewaarde gegeven, teneinde vast te stellen of de gegevens overeenkomen. Dit houdt in dat alleen op basis van *hit no hit* in de bewaarde gegeven kan worden gezocht, dat wil zeggen aan de hand van reeds bij de politie bekende onderzoeksgegevens. Bij de raadpleging kunnen wel over meer locaties of tijdstippen of kentekennummers gegevens verkregen worden. Zo kan voor één kentekennummer worden nagegaan of gegevens beschikbaar zijn over locaties waar het voertuig met dit nummer is vastgelegd.
Indien in een opsporingsonderzoek informatie aanwezig is over een voertuig dat betrokken was bij het misdrijf of dat in gebruik is bij de verdachte, kan aan de hand van het bij dat voertuig behorende kenteken worden gezocht in de bewaarde gegevens. Daaruit kan naar voren komen dat het desbetreffende voertuig op bepaalde tijdstippen

op bepaalde locaties aanwezig is geweest. Dit kan bijdragen aan de opheldering van het misdrijf.
Voor de opheldering van een misdrijf kan het – indien dat aan de opheldering van het feit bijdraagt - passend en proportioneel zijn met behulp van de bewaarde gegevens de aanwezigheid van een voertuig te achterhalen, of de bewegingen van een voertuig na te gaan. Naar aanleiding van de adviezen over het wetsvoorstel is de raadpleging van de bewaarde gegevens beperkt tot misdrijven waarvoor voorlopige hechtenis is toegelaten, dat zijn de ernstiger misdrijven waarop naar de wettelijke omschrijving een gevangenisstraf van vier jaren of meer is gesteld, en enkele misdrijven uit de Wegenverkeerswet 1994. Het betreft onder andere het veroorzaken van een verkeersongeval en het verlaten van de plaats van het ongeval. Ik ben van mening dat het passend en proportioneel is om de bewaarde gegeven te raadplegen voor deze misdrijven. Verdergaande beperkingen acht ik niet noodzakelijk. De bewaarde kentekengegevens betreffen namelijk slechts het kenteken en de foto van het voertuig, en de gegevens over locatie, datum en tijdstip. De naam van de persoon op wiens naam het kenteken staat, wordt niet bewaard. Die naam wordt pas bekend wanneer in een concrete zaak de tenaamstelling van een bepaald kenteken in het kentekenregister van de Dienst wegverkeer (RDW) wordt nagetrokken. Dat gebeurt alleen indien met behulp van de bewaarde gegevens inderdaad de aanwezigheid van een voertuig op bepaalde locaties en tijdstippen is vastgesteld en dit voor het onderzoek van belang is. Overigens kan dan nog aanvullend onderzoek nodig zijn om na te gaan of bepaalde personen op bepaalde tijdstippen daadwerkelijk van het voertuig gebruik hebben gemaakt.

Tevens is bepaald dat de bewaarde gegevens kunnen worden gebruikt voor de aanhouding van een voortvluchtige verdachte of veroordeelde persoon als bedoeld in artikel 564 Sv. Wanneer informatie voorhanden is over een vluchtauto of over een voertuig dat op naam staan van een voortvluchtige, kan het natrekken van de bewegingen van deze voertuigen, door het raadplegen van de op grond van artikel 126jj bewaarde gegevens, bijdragen aan het achterhalen van de verblijfplaats van de voorvluchtige en diens aanhouding. In artikel 565 Sv is bepaald dat ook bijzondere opsporingsbevoegdheden mogen worden toegepast voor het vaststellen van de verblijfsplaats van een aan te houden persoon. Het gebruik van bewaarde kentekengegevens – als voorgesteld in artikel 126jj – kan eveneens beschouwd worden als een passende bevoegdheid voor dit doel.

In artikel 126jj vierde lid is bepaald dat de toegang tot de gegevens bij algemene maatregel van bestuur geregeld wordt. Zie hierover paragraaf 6.1.2.

4.7 Waarborgen voor een zorgvuldige toepassing

Voor een zorgvuldige toepassing van de bevoegdheid tot het bewaren van kentekengegevens is het van belang dat de gegevens worden verwerkt overeenkomstig de voorwaarden die daaraan in het voorgestelde artikel 126jj en in de Wpg worden gesteld. Zie hierover paragraaf 5.
Voor een zorgvuldige toepassing van de bevoegdheid tot het bewaren van kentekengegevens is ook de kwaliteit van de gebruikte apparatuur van belang. Voor de camera's en de hardware en programmatuur die worden gebruikt bij automatische kentekenherkenning worden

standaarden gehanteerd. Deze beschrijven de kwaliteit van de vastlegging van gegevens, het percentage passerende voertuigen dat minimaal dient te worden vastgelegd en de correctheid van de herkenning van de kentekens vanaf het vastgelegde beeld. Voor de beveiliging en integriteit van de beelden gelden de beveiligingsrichtlijnen van de Voorziening tot samenwerking Politie Nederland (vtsPN). De korpsen hanteren deze eisen in hun inkoop- dan wel aanbestedingsdocumenten. Deze eisen zullen onderdeel uitmaken van het uitvoeringskader waarin de uitwerking van de praktische voorzieningen is opgenomen.

4.8 Afbakening naar andere grondslagen voor het bewaren van kentekengegevens en andere toepassingen van automatische kentekenherkenning voor de opsporing van strafbare feiten

Thans biedt de Wpg reeds een basis voor het bewaren van kentekengegevens die noodzakelijk zijn voor de uitvoering van de politietaak. Het kan gaan om *hits*, als beschreven in paragraaf 1 maar ook om kentekengegevens die worden vergaard in het kader van een opsporingsonderzoek. Indien, bijvoorbeeld ter opsporing van herhaalde woninginbraken op bepaalde locaties, kentekens worden vastgelegd om na te gaan welke in verband gebracht kunnen worden met de gepleegde misdrijven, kunnen deze gegevens voor de duur van het onderzoek worden verwerkt op grond van artikel 9 Wpg. Het betreft gerichte gegevensverwerking voor een onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval. (Kamerstukken 2005/2006, 30327, nr. 3, blz. 43 en 44).

4.9 Camera's

De toepassing van de voorgestelde bevoegdheid kan eenvoudig plaatsvinden met behulp van de camera's die gebruikt worden voor de acties waarbij een directe opvolging aan *hits* wordt gegeven, als beschreven in paragraaf 1. Niet alleen kunnen de *hits* en de *no hits* (oftewel, alle passagegegevens) tijdens de acties worden bewaard maar ook kunnen de camera's buiten de acties om worden gebruikt voor het vastleggen van de kentekens van passerende voertuigen. In de praktijk worden hiervoor mobiele en vaste camera's gebruikt. De mobiele camera's zijn in politieauto's gemonteerd en kunnen op elke gewenste plek worden ingezet. De vaste camera's worden met toestemming van de wegbeheerder op of aan de weg gemonteerd, bijvoorbeeld aan bestaande installaties. De plaatsing en spreiding van de camera's dient zodanig te zijn dat er een optimale bijdrage wordt geleverd aan de toepassing automatische kentekenherkenning als beschreven in paragraaf 1. Een aantal weegfactoren zijn hierbij richtinggevend:

- criminele "hot spots" of criminele fenomenen in een bepaald gebied
- specifieke locaties met een bepaald risico, zoals bijvoorbeeld vliegvelden, havens, industriegebieden of grensovergangen
- wegen met intensieve verkeersstromen (personen- of goederenvervoer) of een bepaalde functie (zwaar vervoer)

Besluitvorming over het daadwerkelijke gebruik van de geplaatste ANPR-camera's vindt plaats door het bevoegd gezag. Bij de inzet van ANPR-camera's wordt tevens getoetst aan de beginselen van proportionaliteit en subsidiariteit en aan beleid ten aanzien van de

handhaving en opsporing zoals landelijk of lokaal is vastgesteld. In het uitvoeringskader, bedoeld in paragraaf 3, wordt dit nader uitgewerkt.

Tevens zullen het openbaar ministerie en de politie periodiek een cameraplan opstellen dat door de minister van Veiligheid en Justitie wordt vastgesteld. In dit plan zullen de locaties worden opgenomen waar (vaste) ANPR-camera's geplaatst zijn dan wel in de toekomst geplaatst kunnen worden.

Volgens een inventarisatie van het Landelijk Programmabureau ANPR van de politie op 9 november 2011, beschikken thans 5 korpsen over vaste ANPR camera´s en 19 korpsen over mobiele camera´s. Het betreft 119 vaste camera´s op 21 locaties en 78 mobiele camera's. Daarnaast bestaat het voornemen bij de Koninklijke Marechaussee om in 2012 op 15 locaties camera´s te plaatsen.

Een deel van de camera's die door de politie en het openbaar ministerie worden gebruikt voor verkeerscontroles, kunnen worden ingezet voor toepassing van de voorgestelde bevoegdheid tot het vastleggen en bewaren van kentekengegevens. Het gaat hierbij om de zogenaamde flitspalen en de camera's die worden gebruikt voor trajectcontroles, op 150 tot 200 locaties. Hiermee krijgt de toepassing van de bevoegdheid een grotere betekenis omdat dan op meer plaatsen in Nederland kentekengegevens van passerende voertuigen kunnen worden vastgelegd en bewaard.

Daarnaast is het denkbaar dat camera's geplaatst worden, speciaal met het oog op toepassing van de bevoegdheid tot het vastleggen en bewaren van kentekengegevens. Mocht in een regio naar voren komen dat bepaalde routes veelvuldig worden gebruikt door verdachten van bepaalde strafbare feiten, dan is voorstelbaar met het oog daarop een camera te plaatsen.

Voorzien is dat de met behulp van camera's door de politie vastgelegde kentekengegevens centraal worden bewaard door de voorziening tot samenwerking Politie Nederland (vtsPN). Daardoor kunnen kentekengegevens die met behulp van camera's in verschillende delen van het land zijn vastgelegd, landelijk worden verwerkt ten behoeve van de doelen van het voorgestelde artikel 126jj. Conform het voorgestelde vierde lid, wordt bij algemene maatregel van bestuur de toegang tot de gegevens geregeld.

5. Bescherming van de persoonlijke levenssfeer en waarborgen voor een zorgvuldige gegevensverwerking.

5.1 Algemeen: Privacy impact assessment

Voor het wetsvoorstel is een *Privacy impact assessment* (PIA) uitgevoerd, als toegezegd in het beleidsdebat met de Eerste Kamer over de rol van de overheid bij digitale dataverwerking- en uitwisseling in het kader van het rapport van de commissie-Brouwer-Korf (Handelingen I, 17 mei 2011, 27-11-49). Deze gaat als bijlage bij deze memorie van toelichting. Voor het opstellen van een PIA bestaan nog geen vaste standaarden. Wanneer voor meer wetsvoorstellen een PIA is opgesteld, zal het mogelijk zijn te bezien

of een model kan worden gekozen dat in de toekomst als standaard kan worden gehanteerd.
In deze PIA zijn de belangrijkste risico's voor de persoonlijke levenssfeer geïnventariseerd en worden enkele risicobeheersende maatregelen voorgesteld teneinde de risico's te voorkomen of te verkleinen. Het betreft onder andere beperkingen in de doelen waarvoor gegevens mogen worden verzameld en geraadpleegd, een beperkte opslagtermijn en het uitvoeren van periodieke evaluaties. Daarnaast worden maatregelen voor feitelijke beveiliging en wettelijke bescherming van de gegevens voorgesteld en is voorzien in onafhankelijk toezicht. Op een aantal van deze maatregelen - die tevens voortvloeien uit artikel 8 van het EVRM - wordt hierna in paragraaf 5.6 ingegaan. Een compleet overzicht van de maatregelen is te vinden in de bijlage. De enige maatregel die niet wordt overgenomen is het zo nu en dan uitzetten van de camera's, omdat het lastig uit te leggen is wanneer om privacyredenen een camera bleek uit te staan tijdens een incident.
De kleine en medium risico's die resteren na de genomen risicobeheersende maatregelen zijn voldoende verkleind en overzichtelijk, zodat ze als acceptabel gelden ten opzichte van de voordelen van het wetsvoorstel. In het kader van de toegezegde evaluatie van dit wetsvoorstel zal naast de effectiviteit van de maatregel nadrukkelijk ook worden bezien of de risico's die zijn benoemd zich feitelijk hebben voorgedaan en indien dat het geval is welke maatregelen zijn getroffen.

5.2 Artikel 10 van de Grondwet en artikel 8 van het EVRM

Zowel het gebruik van camera's die kentekennummers vastleggen als de verdere verwerking van kentekengegevens die langs die weg door de politie zijn vastgelegd, moeten worden beoordeeld in het licht van het recht op bescherming van de persoonlijke levenssfeer als neergelegd in artikel 10 van de Grondwet en artikel 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM). Het recht op bescherming van de persoonlijke levenssfeer houdt in dat de overheid de persoonlijke levenssfeer van burgers dient te respecteren. Onderdeel van het recht op bescherming van de persoonlijke levenssfeer is dat de burger het recht heeft met rust gelaten te worden en onbevangen zichzelf te zijn. Een beperking van dit recht is slechts mogelijk als dat in de wet is geregeld en noodzakelijk is in een democratische samenleving in het belang van onder andere de openbare veiligheid of het voorkomen van wanordelijkheden en strafbare feiten. In de rechtspraak van het Europees Hof voor de Rechten van de Mens (EHRM) komt naar voren dat deze noodzaak mede wordt bepaald aan de hand van de beginselen van proportionaliteit en subsidiariteit. Artikel 8 EVRM en de daarop gebaseerde jurisprudentie stellen ook eisen aan de kwaliteit van de wettelijke regeling. Deze moet voor de burger voldoende toegankelijk en kenbaar zijn. Dit betekent dat de regeling voldoende precies moet zijn geformuleerd, zodat de burger vooraf kan weten onder welke omstandigheden bevoegdheden mogen worden toegepast. De regeling moet bovendien waarborgen bieden tegen willekeurige inmenging door de overheid in het persoonlijke leven van de burger en tegen misbruik van bevoegdheid.

Omdat het gebruik van iemands persoonsgegevens kan leiden tot een inmenging in diens persoonlijke levenssfeer, zijn er regels voor de zorgvuldige omgang met persoonsgegevens. Artikel 10, tweede lid, van de Grondwet bepaalt dat de wet regels stelt ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. De Wet politiegegevens (Wpg) geeft hieraan uitvoering voor de verwerking van politiegegevens. Deze wet is gebaseerd op de beginselen die zijn neergelegd in het Dataprotectieverdrag (Verdrag van de Raad van Europa van 28 juni 1981 tot bescherming van personen in verband met de geautomatiseerde verwerking van persoonsgegevens (Trb. 1988, 7). Deze beginselen houden in dat gegevens rechtmatig moeten zijn verkregen, alleen voor specifieke en legitieme doeleinden mogen worden opgeslagen, evenredig moeten zijn in relatie tot het doel waarvoor ze zijn opgeslagen en niet langer mogen worden bewaard dan vereist voor dit doel waarvoor ze zijn opgeslagen. Om te voorkomen dat door het verwerken van gegevens de persoonlijke levenssfeer van de burger onevenredig wordt beperkt, voorziet de Wet politiegegevens in regels voor een zorgvuldige omgang met de gegevens.

5.3 Het gebruik van camera's voor automatische kentekenherkenning

Bij automatische kentekenherkenning worden met behulp van camera's op de openbare weg waarnemingen gedaan van voertuigen die op een bepaalde plaats en tijd passeren. Het gaat om het op een enkel moment in de openbare ruimte waarnemen van het kenteken en een deel van het voertuig. In de rechtspraak wordt aangenomen dat bij kortstondige waarnemingen op de openbare weg de persoonlijke levenssfeer niet in het geding is, althans niet in die mate dat dit gebaseerd moet zijn op een speciale bevoegdheid. (EHRM, *Peck v. Verenigd Koninkrijk*, 44647/98, 28 januari 2003; HR 20 april 2004, LJN AL8449).
Hierbij is relevant dat 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 waargenomen. Het is van algemene bekendheid dat het kenteken op de kentekenplaat ertoe dient dat bestuurders van auto´s op de weg kunnen worden herkend ten behoeve van de handhaving van wet- en regelgeving. Bestuurders van voertuigen kunnen redelijkerwijs geen verwachting hebben dat zij voor de politie onopgemerkt blijven. Zoals tot uitdrukking komt in de rechtspraak van het EHRM, is voor de vraag of sprake is van inmenging in de persoonlijke levenssfeer de "*reasonable expectation of privacy*" van betrokkene van belang. Overigens is het voor automatische kentekenherkenning van belang dat een voertuig nauw verbonden kan zijn met een persoon, maar dat er geen zekerheid is dat de persoon op wiens naam het voertuig staat, daadwerkelijk gebruik maakt van het voertuig. Met behulp van automatische kentekenherkenning kan slechts iets worden gezegd over de mogelijkheid dat een bepaalde persoon op een bepaalde tijd en plaats aanwezig was, maar kan daarover geen zekerheid worden geboden, daarvoor is aanvullend onderzoek nodig.

5.4. Artikel 2 Politiewet 1993

Op grond van artikel 2 van de Politiewet 1993 heeft de politie tot taak in ondergeschiktheid aan het bevoegde gezag en in overeenstemming

met de geldende rechtsregels te zorgen voor de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. Ter uitvoering van haar taak is de politie bevoegd tot het verrichten van al die handelingen die nodig zijn voor een goede taakvervulling, binnen de wettelijke grenzen. Ter uitvoering van haar taak dient de politie opmerkzaam te zijn op personen die met het oog op die taak aandacht behoeven. Een mogelijkheid om opmerkzaam te zijn is dat de politie het oog houdt op kentekens van voertuigen die toebehoren aan deze personen. Het is een passende ontwikkeling dat de politie daarbij gebruik maakt van camera's en automatische kentekenherkenning. Zolang deze camera's worden gebruikt om uitsluitend kentekens waar te nemen van voertuigen van personen die relevant zijn voor de politietaak, bijvoorbeeld omdat zij verdachte zijn of omdat zij een straf moeten ondergaan, past dit binnen de uitvoering van artikel 2 van de Politiewet 1993. De gegevens die bij een vergelijking overeenkomen, de zogenaamde *hits,* kunnen op grond van de Wpg verder worden verwerkt. Ook het vergaren van kentekens in het kader van een lopend opsporingsonderzoek kan gebaseerd worden op artikel 2 van de Politiewet 1993. Een bijvoorbeeld hiervan is een opsporingsonderzoek naar woninginbraken in een woonwijk. Het kan bijdragen aan de opsporing van de woninginbraken om gedurende een bepaalde periode vast te leggen welke voertuigen de wijk inkomen. De verwerking van deze gegevens vindt plaats op grond van artikel 9 van de Wpg.
Artikel 2 van de Politiewet 1993 biedt dus een basis voor het waarnemen en vergelijken van kentekens van personen die ingevolge de uitvoering van de politietaak aandacht behoeven. De Wpg staat de verwerking van gegevens toe, voor zover die noodzakelijk zijn voor de uitvoering van de politietaak.

5.5 Het vastleggen en bewaren van kentekengegevens die geen hit opleveren

Het vastleggen en bewaren van zogenaamde *hits* en van kentekengegevens die anderszins noodzakelijk zijn voor de uitvoering van de politietaak past dus binnen artikel 2 van de Politiewet 1993 en het stelsel van de Wpg. Anders is dat voor het vastleggen en bewaren van kentekengegevens die niet noodzakelijk zijn voor de uitvoering van de politietaak. Dit betreft kentekens van voertuigen die toebehoren aan personen die op het moment van de vastlegging van de kentekengegevens niet de aandacht van de politie behoeven. Verwerking van die gegevens past daarom, binnen de huidige wetgeving, niet binnen de uitvoering van de politietaak van artikel 2 van de Politiewet 1993. De uitvoering van die taak kan in beginsel niet strekken tot het vastleggen van kentekengegevens van burgers, indien daartoe op dat moment geen aanleiding bestaat. Daarom is dit zonder expliciete wettelijke regeling niet mogelijk. Evenmin biedt de Wpg thans mogelijkheden om deze gegevens te verwerken. De Wpg staat slechts verwerking van gegevens toe indien deze op het moment van de eerste verwerking noodzakelijk zijn voor de uitvoering van de politietaak. Gaat het om gegevens die geen *hit* betreffen - oftewel om gegevens die op dat moment niet van belang zijn voor de uitvoering van de politietaak – maar die mogelijk op een later tijdstip wel relevant kunnen zijn, dan is verwerking op grond van de Wpg nu niet mogelijk. Om de bewaring van deze gegevens mogelijk te maken, teneinde deze achteraf ten behoeve van de opsporing van strafbare feiten te kunnen raadplegen, is dan ook expliciete wettelijke basis

vereist. Voorgesteld wordt deze neer te leggen in een nieuw artikel 126jj Sv. Deze regeling dient te voldoen aan de hiervoor genoemde eisen van artikel 8 van het EVRM.

5.6 De eisen van artikel 8 van het EVRM.

Dit betekent ten eerste dat de bevoegdheid tot het bewaren van kentekengegevens als neergelegd in het voorgestelde artikel 126jj noodzakelijk moet zijn in een democratische samenleving, in het belang van de openbare veiligheid en de voorkoming en vervolging van strafbare feiten. Hierbij heeft de staat een vrije beoordelingsruimte. Zoals in paragraaf 4 aan de orde kwam, draagt het bij aan de opsporing van strafbare feiten, indien alle kentekengegevens die door de politie met behulp van camera's worden vastgelegd, voor een periode van vier weken kunnen worden bewaard, teneinde deze achteraf te kunnen raadplegen. Misdrijven kunnen mede met behulp van bewaarde kentekengegevens worden opgelost. Ook kunnen deze gegevens specifieke opsporingsinformatie opleveren en richting geven aan opsporingsonderzoeken. Deze opbrengsten van het bewaren van *no hits* wegen zwaar in een samenleving waarin veel waarde wordt gehecht aan het verhogen van de veiligheid en de aanpak van ondermijnende en georganiseerde criminaliteit.

De noodzaak van de regeling wordt mede ingevuld aan de hand van de beginselen van proportionaliteit en subsidiariteit. Het beginsel van proportionaliteit houdt in dat het belang dat gediend wordt met de maatregel, in verhouding moet staan tot de omvang van de beperking van de persoonlijke levenssfeer. Voor de beoordeling van de omvang van deze beperking is ten eerste van belang dat de maatregel inhoudt dat slechts een beperkte set van gegevens wordt bewaard. Het gaat om het kenteken en de foto van het voertuig, en de gegevens over locatie, datum en tijdstip. Met behulp van deze gegevens is het mogelijk om de aanwezigheid van een voertuig op een bepaald tijdstip op een bepaalde plaats vast te stellen. Ook is het mogelijk aan de hand van kentekens de bewegingen van voertuigen na te gaan. Van belang voor de proportionaliteit is dat de naam van de persoon op wiens naam het kenteken staat, niet wordt bewaard. Die naam wordt pas bekend wanneer in een concrete zaak de tenaamstelling van een bepaald kenteken in het kentekenregister van de RDW wordt nagetrokken. Dit laatste gebeurt pas als bij raadpleging van de bewaarde kentekengegevens inderdaad de aanwezigheid van een voertuig op bepaalde locaties en tijdstippen is vastgesteld en dit voor het onderzoek van belang is. Aanvullend onderzoek is nodig om te kunnen vaststellen of de houder van het kenteken, of wellicht een ander, op die tijdstippen van het voertuig gebruik maakte.

Voor de beoordeling van de proportionaliteit is ten tweede van belang dat de toegang tot de bewaarde gegevens bij wet wordt beperkt de opsporing van een bepaald misdrijf of de aanhouding van een voortvluchtige verdachte of veroordeelde. Dit zijn voldoende zwaarwegende doelen, die in verhouding staan tot beperking van de persoonlijke levenssfeer, zoals ook in paragraaf 4.6 aan de orde kwam.
Voor de beoordeling van de proportionaliteit is ten derde van belang dat de
raadpleging van de gegeven slechts plaatsvindt door politiegegevens die voor één van deze doelen worden verwerkt, geautomatiseerd te

vergelijken met de bewaarde gegeven, teneinde vast te stellen of de gegevens overeenkomen. Dit houdt in dat alleen op basis van *hit no hit* in de bewaarde gegeven kan worden gezocht, dat wil zeggen aan de hand van reeds bij de politie bekende onderzoeksgegevens, en dat geen bevoegdheid bestaat tot *datamining* of het koppelen aan andere gegevensbestanden. Op deze wijze wordt het gebruik van de gegevens beperkt tot gegevens die in direct verband staan met de opsporing van het misdrijf of de aanhouding van de voortvluchtige.
Voor de beoordeling van de proportionaliteit is tenslotte van belang dat de duur van bewaartermijn is beperkt tot vier weken. In paragraaf 4.4 is besproken dat de termijn van vier weken passend is gezien het belang van de opsporing - hoewel deze kort genoemd kan worden in verband met langduriger onderzoeken naar ernstiger misdrijven – en gezien de termijn in reeds bestaande andere wetgeving terzake van het bewaren van camerabeelden.
Gelet op de voorgaande afwegingen voldoet de maatregel aan het vereiste van proportionaliteit.

Het beginsel van subsidiariteit houdt in dat het beoogde doel niet bereikt kan worden met een andere maatregel die minder ingrijpend is voor de persoonlijke levenssfeer. Hierover kan worden opgemerkt dat er geen andere maatregel is waarmee op zo'n betrekkelijk eenvoudige wijze in zwaarwegende gevallen achteraf de aanwezigheid van een voertuig op een bepaald tijdstip op een bepaalde plaats kan worden vastgesteld. De grenzen die gesteld zijn aan het gebruik van de bewaarde gegevens garanderen dat de gegevens alleen in zwaarwegende gevallen worden gebruikt. De voorgestelde maatregel voldoet hiermee aan het subsidiariteitsvereiste.

Andere eisen waaraan de regeling ingevolge artikel 8 van het EVRM moet voldoen, betreffen de kwaliteit van de wettelijke regeling. De wettelijke regeling moet voor de burger voldoende toegankelijk en kenbaar zijn. Met de voorgestelde regeling in artikel 126jj wordt aan deze eisen voldaan. In het eerste lid van het voorgestelde artikel 126jj is omschreven voor welke doelen de gegevens kunnen worden vastgelegd. Ook is voorgeschreven dat de aanwezigheid van een technisch hulpmiddel ter vastlegging van kentekengegevens op of aan de openbare weg, op duidelijke wijze kenbaar wordt gemaakt. In de artikelsgewijze toelichting wordt hier nader op ingegaan.

De wettelijke regeling moet ook waarborgen bieden tegen willekeurige inmenging door de overheid in het persoonlijke leven van de burger en tegen misbruik van bevoegdheid. Deze waarborgen komen overeen met een aantal voorzorgsmaatregelen die zijn vermeld in het *Privacy impact assessment,* zoals de beperking tot het gebruik van de gegevens voor een beperkt aantal delicten, het beperken van de toegang tot intern geautoriseerde medewerkers en het vastleggen van het gebruik, zodat inzage en rectificatie en onafhankelijk toezicht mogelijk zijn. Hiervoor biedt artikel 126jj de nodige waarborgen. In het tweede lid is omschreven om welke gegevens het precies gaat en is een bewaartermijn opgenomen. In het derde lid is limitatief vermeld dat de bewaarde gegevens slechts voor twee doelen kunnen worden gebruikt. Hierbij is het van belang dat de gegevens slechts toegankelijk zijn voor daartoe geautoriseerde ambtenaren die het doel van de raadpleging vastleggen, hetgeen bij algemene maatregel van bestuur op basis van het vierde lid nader wordt geregeld. Andere waarborgen zijn neergelegd in de Wpg. In artikel 4 van de Wpg is

bepaald dat de korpsbeheerder ervoor zorgdraagt dat de gegevens worden vernietigd, zodra de wettelijke bewaartermijn is verstreken. De Wpg voorziet er dus in dat de gegevens die op grond van het voorgestelde artikel 126jj mogen worden bewaard, na ommekomst van de in artikel 126jj voorgeschreven maximale termijn van vier weken worden vernietigd. Tevens voorziet de Wpg in een regeling van inzage en correctie en in onafhankelijk toezicht door het College bescherming persoonsgegevens. Tot de waarborgen voor een zorgvuldige gegevensverwerking behoren ook de kwaliteit van de apparatuur en programmatuur, waarop in paragraaf 4.7 is ingegaan.

6. Consultatie

Over het wetsvoorstel is advies uitgebracht door de Raad voor de rechtspraak, het College van procureurs-generaal van het openbaar ministerie, het College Bescherming persoonsgegevens, het Korpsbeheerdersberaad en de Raad van Korpschefs. Het openbaar ministerie en de politieberaden tonen zich voorstander van een regeling die het mogelijk maakt om kentekengegevens te bewaren voor een bepaalde periode en beschikbaar te houden voor de opsporing van strafbare feiten. De Raad voor de rechtspraak deelt de opvatting dat voor het vastleggen en bewaren van kentekengegevens wetgeving in formele zin is vereist en vraagt aandacht voor de waarborgen waarmee de regeling is omgeven. Het College Bescherming persoonsgegevens meent dat de noodzaak en de proportionaliteit van de regeling niet zijn aangetoond, en dat de onderbouwing van de termijn van vier weken te kort schiet.

Op enkele in de adviezen aangesneden onderwerpen wordt ingegaan op die plaatsen in de memorie van toelichting waar deze onderwerpen worden besproken. De hoofdlijnen van de adviezen bespreek ik in deze paragraaf. Daarbij bespreek ik eerst het advies van het College Bescherming persoonsgegevens (CBP).

6.1 Advies College Bescherming persoonsgegevens

6.1.1. Subsidiariteit. Het belang voor de opsporing

Het CBP beoordeelt het wetsvoorstel aan de hand van artikel 8 van het EVRM en toetst aan de hand van de beginselen van proportionaliteit en subsidiariteit of aan het vereiste van noodzakelijkheid is voldaan. Voor de beoordeling van de subsidiariteit is het van belang na te gaan of er andere bevoegdheden zijn waarmee hetzelfde resultaat kan worden bereikt. Het CBP stelt vast dat het wetsvoorstel een bevoegdheid schept waar thans nog niet in is voorzien.

Vervolgens moet - aldus het CBP – het belang van de nieuwe bevoegdheid worden onderbouwd. Het CBP meent dat uit de wijze waarop in de memorie van toelichting recente jurisprudentie wordt besproken niet kan worden afgeleid wat het belang is van de bevoegdheid. Er wordt namelijk – aldus het CBP – niet aangegeven of en waarom de *no hits* van belang waren voor de opsporing in het concrete geval. Hierover merk ik op dat in paragraaf 4.2 verschillende rechterlijke uitspraken worden besproken, waarbij over strafzaken concreet is vermeld op welke wijze de *no hits* hebben bijgedragen aan de opsporing van het strafbaar feit. Over de uitspraak van 29 juli 2009

(LJN BJ4213) vermeldt het CBP dat de verdachte werd vrijgesproken van het opzettelijk wegmaken van een lijk. Dit is echter niet het geval. Zowel in eerste als in tweede aanleg werd in deze strafzaak de verdachte veroordeeld voor het wegmaken van een lijk en speelden *no hits* hierbij een belangrijke rol.

Ook de andere uitspraken illustreren het belang van *no hits* voor de opsporing van het strafbare feit. Dat de rechter - ondanks de aanwezigheid van bewijs dat voortvloeit uit kentekengegevens - alles bijeen genomen oordeelt dat het bewijs ontoereikend is, doet daaraan niet af. (Rechtbank Rotterdam, 4 maart 2001, LJN BL6649). Evenmin wil het buiten beschouwing laten van bewijs dat voortvloeit uit kentekengegevens omdat de rechter het gebruik daarvan onrechtmatig oordeelt, waarbij de rechter op basis van ander bewijs wel tot een veroordeling komt – zeggen dat de kentekengegevens niet aan het bewijs hadden kunnen bijdragen (Rechtbank Den Haag, 22 februari 2010, LJN BL5236). Kentekengegevens kunnen dus een rol spelen als zelfstandig of aanvullend bewijsmiddel. Ook kunnen kentekengegevens bijdragen aan de inrichting van het opsporingsonderzoek. De aanwezigheid van een voertuig op een bepaalde tijd en plaats die in relatie staan tot het strafbare feit kan bijvoorbeeld aanleiding zijn onderzoek naar dit voertuig te doen en kan naar de verdachte leiden. Paragraaf 4.2 is naar aanleiding van het advies van het CBP aangevuld.

Het CBP plaatst kanttekeningen bij het onderzoek “Kentekenherkenning op de A28”. Er wordt in dit onderzoek geen onderscheid genaakt tussen het direct scannen en het terugzoeken in passage gegevens, aldus het CBP. Uit het onderzoek blijkt onvoldoende dat het bewaren van *no hits* ten behoeve van de opsporing een doorslaggevende meerwaarde heeft. Hierover kan worden opgemerkt dat het rapport mede betrekking heeft op casus waarin resultaten werden behaald door het terugzoeken in de opgeslagen gegevens.

6.1.2. Proportionaliteit

Het CBP geeft aan dat voor de toetsing van de proportionaliteit afgewogen moet worden of de verwerking evenredig is aan het beoogde doel. Het CBP meent dat het doel ‘opsporing van een strafbaar feit’ niet specifiek genoeg is om deze afweging te maken. Het CBP geeft aan dat ‘strafbaar feit’ in de wettekst niet nader wordt ingeperkt, zoals dat in het Wetboek van Strafvordering wel gebruikelijk is als het gaat om bijzondere opsporingsbevoegdheden. Ook wijst het CBP op de grootschaligheid van de gegevensverwerking, waarbij van alle passerende voertuigen het kenteken wordt vastgelegd, en niet alleen van voertuigen die van belang kunnen zijn in een opsporingsonderzoek. De gegevensvergaring vindt immers plaats om deze zo nodig achteraf te kunnen raadplegen, en staat los van vooraf bestaande verdenkingen van strafbare feiten. Vanwege deze grootschaligheid, waarbij de gegevens eenvoudig te koppelen en te vergelijken zijn, meent het CBP dat de beperking van het doel waartoe de gegevens geraadpleegd kunnen worden, des te zwaarder weegt. Naar aanleiding van dit onderdeel van het advies van het CBP is het wetsvoorstel aangescherpt. Het doel is niet de opsporing van elk strafbaar feit, maar alleen de opsporing van een misdrijf als omschreven in artikel 67, eerste lid, en een misdrijf als bedoeld in

artikel 178 van de Wegenverkeerswet 1994. Daarnaast blijft het doel van de aanhouding van een voorvluchtige veroordeelde of verdachte gehandhaafd.
Door deze beperking wordt voorkomen dat de bewaarde gegevens kunnen worden geraadpleegd voor relatief lichte strafbare feiten. Dit is van belang omdat de bewaarde gegevens op meer locaties, tijdstippen en kentekens kunnen worden geraadpleegd, zoals is beschreven in paragraaf 4.6. Verzekerd moet zijn dat deze raadpleging alleen voor voldoende zwaarwegende misdrijven plaatsvindt.
Naar aanleiding van het advies van het CBP zal bovendien bij algemene maatregel van bestuur worden bepaald dat de opsporingsambtenaar slechts de beschikking over de opgeslagen gegevens kan krijgen door een verzoek te doen aan daartoe door de Minister van Veiligheid en Justitie expliciet geautoriseerde politie-ambtenaren. In het verzoek moet worden vermeld ter opsporing van welk strafbaar feit, dan wel ter aanhouding van welke voortvluchtige persoon, het verzoek wordt gedaan. De raadpleging vindt plaats door de gegevens die in het verzoek zijn vermeld langs geautomatiseerde weg te vergelijken met de vastgelegde kentekengegevens. Deze vergelijking vindt slechts plaats aan de hand van een in het verzoek opgenomen gegevens betreffende kenteken, locatie of tijdstip. Er wordt dus gezocht op basis van *hit no hit*. Hiermee is uitgesloten dat gezocht wordt aan de hand van patronen of dat door middel van *datamining* naar patronen wordt gezocht. Ook is uitgesloten dat de opgeslagen gegevens worden gekoppeld aan andere gegevensbestanden. Zowel het verzoek om te mogen raadplegen, als het raadplegen zelf wordt vastgelegd, om achteraf het gebruik van de gegevens te kunnen monitoren.

De gegevens worden dus niet zomaar opgenomen in politiebestanden, maar worden apart bewaard en slechts geraadpleegd indien dat nodig is voor een van de twee in de wet genoemde doelen.

Naar mijn mening wordt hiermee voorzien in passende waarborgen, gelet op de grootschaligheid van de verwerking.

6.1.3. De lengte van de bewaartermijn

Eveneens in verband met de proportionaliteit is het CBP van opvatting dat de bewaartermijn van vier weken niet goed is onderbouwd. De vergelijking met het gemeentelijk cameratoezicht gaat volgens het CBP niet op omdat het bewaren van kentekens meer risico's met zich brengt dan beelden van de openbare weg: kentekens zijn op eenvoudige wijze te verwerken, te koppelen en te vergelijken. Als risico noemt het CBP dat de kentekenhouder niet per definitie ook de bestuurder in het concrete geval hoeft te zijn. In reactie hierop kan erop worden gewezen dat het gebruik van kentekengegevens uitsluitend waarde heeft als de politie onderzoekt wie er reed met het desbetreffende voertuig en in welke relatie het voertuig staat tot de onderzochte feiten. De politie houdt er bij al haar werk rekening mee dat anderen dat de kentekenhouder van een voertuig gebruik kunnen maken. Met dit door het CBP gesignaleerde risico is de politie vertrouwd. Dit risico vormt geen reden af te zien van het gebruik van kentekengegevens, dan wel te kiezen voor een kortere bewaartermijn, maar brengt wel met zich mee dat zorgvuldig met de gegevens moet worden omgegaan. Dit is eigen aan de uitvoering van de politietaak. Hierin onderscheidt het gebruik van kentekengegevens zich niet van

het gebruik van andere gegevens die de politie ter uitvoering van haar taak vergaart. Voor de raadpleging van beelden van gemeentelijk cameratoezicht geldt evenzeer dat de beelden een indruk kunnen geven van gebeurtenissen die niet overeenstemt met wat er werkelijk is voorgevallen. Daarom dient altijd aanvullend onderzoek te worden gedaan, zoals het horen van getuigen. In die zin verschillen kentekengegevens en gegevens van cameratoezicht niet zozeer.
In ander opzicht zijn er wel verschillen tussen de beelden van gemeentelijk cameratoezicht en kentekengegevens. Beelden van cameratoezicht leggen namelijk het gedrag van personen vast, bijvoorbeeld in het uitgaansleven. In het licht van de persoonlijke levenssfeer is dit relevant, zo kan worden afgeleid uit de uitspraak van het EHRM van 2 september 2010, LJN BO2548, in de zaak Uzun tegen Duitsland. Daarin geeft het Europese Hof aan, dat observatie met behulp van GPS – waarbij alleen vervoersbewegingen wordt vastgelegd - onderscheiden moet worden van andere observatiemethoden die meer interfereren met de persoonlijke levenssfeer, omdat zij informatie onthullen over het gedrag en de opvattingen van een persoon. GPS komt in die zin overeen met het gebruik van kentekengegevens dat daarmee slechts vervoersbewegingen kunnen worden vastgelegd, en dat bovendien aanvullend onderzoek nodig is om na te gaan wie de inzittenden van het voertuig zijn.

Voor de lengte van de bewaartermijn is vooral van belang dat zowel bij het gemeentelijk cameratoezicht als bij het vastleggen van kentekengegevens, de gegevens achteraf kunnen worden geraadpleegd voor de opsporing van strafbare feiten, en dat dit bepalend is voor de duur van de bewaartermijn.

6.1.4. De eisen van proportionaliteit en subsidiariteit

Gelet op het voorgaande deel ik het oordeel van het CBP dat de proportionaliteit van de maatregel met zich meebrengt dat het doel van de vastlegging van de gegevens beperkt moet zijn tot zwaardere strafbare feiten. Het wetsvoorstel is op dit punt aangescherpt. Met inachtneming van deze aanscherping en gelet op de beperkte set van gegevens die wordt vastgelegd, de beperking van het gebruik van de gegevens voor twee nauw omschreven wettelijke doeleinden en het feit dat niet op andere wijze voorzien kan worden in een eenvoudige manier om achteraf de aanwezigheid van een voertuig op een bepaalde plaats aan te tonen, meen ik dat voldaan is aan de eisen van proportionaliteit en subsidiariteit. Verschil van inzicht met het CBP bestaat er over de waardering van het belang van de maatregel voor de opsporing van strafbare feiten.

6.2. Het gebruik van camera's

Het CBP merkt over de omvang van de vastlegging van kentekengegevens op dat in paragraaf 4.9 is geschetst welke camera's hiervoor kunnen worden gebruikt. Dit neigt, aldus het CBP, naar een landelijk dekkend cameraweb. In reactie hierop merk ik op dat het in de toekomst zou kunnen gaan om 300 of meer locaties voor vaste camera's, zodat inderdaad enige dekking rond plaatsen met veel verkeer kan worden bereikt. In paragraaf 4.9 is vermeld dat periodiek een cameraplan wordt vastgesteld.

Denkbaar is dat de politie gebruik maakt van camera-opstellingen van andere instanties, indien deze voldoen aan de technische eisen. Deze camera's maken dan onderdeel uit van het cameraplan.

De Raad voor de rechtspraak merkt op dat - nu nadere voorschriften over de plaats waar een camera wordt geplaatst ontbreken - niet uit te sluiten valt dat vastlegging van kentekengegevens op zodanige wijze plaatsvindt dat er sprake is van een inbreuk op de persoonlijke levenssfeer. Men noemt als voorbeeld dat een camera zodanig wordt geplaatst dat uitritten van woningen te zien zijn of zelfs in woningen kan worden gekeken. De Raad acht het gewenst de eisen waaraan de apparatuur voor automatische kentekenherkenning moet voldoen vast te leggen bij algemene maatregel van bestuur.
Naar aanleiding van deze opmerkingen hecht ik eraan nader in te gaan op de voorwaarden die zijn gesteld in het voorgestelde wetsartikel en de eisen waaraan de camera´s moeten voldoen. De voorwaarden die worden gesteld in het voorgestelde artikel 126jj brengen een beperkte inzet van camera's met zich mee. Belangrijk is dat de aanwezigheid van een camera op duidelijke wijze kenbaar wordt gemaakt. Dit wordt in de artikelsgewijze toelichting op artikel 126jj toegelicht. Dit betekent dat de vastlegging van kentekengegevens niet heimelijk plaatsvindt. Daarnaast is vereist dat de camera's uitsluitend kentekens vastleggen op of aan de openbare weg. Artikel 126jj voorziet niet in een bevoegdheid om kentekens vast te leggen van voertuigen die zich niet op de openbare weg bevinden. Evenmin kan de vastlegging gericht zij op uitritten van woningen. Bovendien mogen alleen kentekengegevens worden vastgelegd. Er mag dus niet in woningen worden gekeken. Welke kentekengegevens mogen worden vastgelegd, is omschreven in het tweede lid. Ter verduidelijking hiervan is - naar aanleiding van de adviezen – in het eerste lid een verwijzing naar het tweede lid opgenomen.

De raad wijst er terecht op dat de apparatuur aan bepaalde eisen moet voldoen, gelet op de bescherming van de persoonlijke levenssfeer. In paragraaf 4.7 zijn de eisen genoemd waaraan de apparatuur moet voldoen. Hierin zijn ook eisen opgenomen over het bereik van de camera. In het uitvoeringskader voor de praktijk zijn deze eisen opgenomen als voorwaarde voor de toepassing van automatische kentekenherkenning.
Deze eisen zijn geheel gericht op het gebruik van de camera voor automatische kentekenherkenning, en de verwerking van het kentekennummer. De eisen houden onder andere in dat de kentekens van passerende voertuigen volledig zichtbaar en goed leesbaar moeten zijn. Dit betekent dat de foto's die genomen worden zijn gericht op het voertuig en niet op de omgeving. Naast de hantering van deze eisen, acht ik het niet nodig bij wet of algemene maatregel van bestuur eisen te stellen
Gelet op de wettelijke voorwaarden en de eisen aan de apparatuur, worden de door de Raad voor de rechtspraak geschetste risico's mijns inziens ondervangen.

6.3 De adviezen van de Raad voor de rechtspraak, het openbaar ministerie en de politie

De Raad voor de rechtspraak en het openbaar ministerie vragen zich af of de regeling wel thuishoort in het Wetboek van Strafvordering. De Raad vraagt of de regeling niet thuishoort in de Politiewet 1993, nu het

gaat om een registratiebevoegdheid voor opsporingsambtenaren met het oog op nog onbekende en nog te plegen strafbare feiten. Het openbaar ministerie is van mening dat de regeling in de Wet politiegegevens (Wpg) thuishoort, omdat het doel waarvoor de gegevens mogen worden gebruikt niet bepalend hoeft te zijn voor de plaats van de regeling en omdat de toepassing van ANPR niet beperkt is tot het strafrecht. Ook het feit dat de plaatsing van camera's plaatsvindt na besluitvorming in de driehoek en dat de officier van justitie niet verantwoordelijk is voor de vastgelegde gegevens, wijst er volgens het advies van het openbaar ministerie op dat regeling in de Wpg passender is. Het openbaar ministerie is er geen voorstander van dat bepalingen over het verwerken van politiegegevens in andere wetten dan de Wpg worden opgenomen.
In reactie op deze adviezen wil ik toelichten waarom naar mijn mening regeling in het Wetboek van Strafvordering het meest voor de hand ligt. De regeling van de bevoegdheid tot het vastleggen en bewaren van kentekengegevens komt toe aan elke opsporingsambtenaar. Regeling in de Politiewet 1993 ligt daarom minder voor de hand. Het doel van de bevoegdheid is bovendien beperkt tot twee expliciet benoemde strafvorderlijke doeleinden. Toepassing van de bevoegdheid vindt op grond van artikel 148 Sv en artikel 13 van de Politiewet 1993 dan ook plaats onder het gezag van de officier van justitie. Weliswaar betreft het een bevoegdheid die kan worden toegepast zonder dat een strafvorderlijk onderzoek loopt, maar het doel van de bevoegdheid is om gegevens vast te leggen en te bewaren, teneinde daarin op een later moment, waarop wel een strafvorderlijk onderzoek loopt, in terug te kunnen zoeken. Nu de bevoegdheid is beperkt tot strafvorderlijke doelen is regeling in het Wetboek van Strafvordering passend.

Dit laat onverlet dat de middelen waarmee de bevoegdheid wordt toegepast – waaronder de camera's - en de gegevens die daarmee worden vergaard, beheerd worden door de korpsbeheerder, ook indien de besluitvorming over de plaatsing van vaste camera's plaatsvindt in overeenstemming met de officier van justitie. Dit komt overeen met de inzet van andere middelen ten behoeve van de opsporing van strafbare feiten, zoals politieauto's, camera's van observatieteams, of wapens. De officier van justitie heeft evenmin verantwoordelijkheid voor het beheer van de vastgelegde gegevens. Zoals ook geldt voor andere gegevens die de politie vergaart voor de uitvoering van haar taken, ligt de verantwoordelijkheid voor het beheer van de gegevens bij de korpsbeheerder, ook al vindt de vergaring plaats onder het gezag van de officier van justitie. Het is dus de taak van de korpsbeheerder toe te zien op de naleving van de voorschriften voor de verwerking van de vastgelegde gegevens, zoals neergelegd in het voorgestelde wetsartikel en in de Wet politiegegevens.
Weliswaar kan met het openbaar ministerie worden ingestemd dat het minder gewenst is bepalingen over het verwerken van politiegegevens op te nemen in andere wetten dan de Wpg, toch is dit in een enkel geval onvermijdelijk. Zo zijn in artikel 151c, zevende lid, van de Gemeentewet regels gesteld voor het verwerken van politiegegevens die worden vastgelegd met behulp van camera's ter handhaving van de openbare orde. Ook in de artikelen 126cc en 126dd van het Wetboek van Strafvordering zijn – in aanvulling op de regels van de Wpg – voor de toepassing van opsporingsbevoegdheden regels voor het verwerken van politiegegevens opgenomen.

Gelet op het voorgaande wordt het voorstel van het openbaar ministerie om de regeling op te nemen in artikel 8 van de Wet politiegegevens niet overgenomen. Naast voornoemde inhoudelijke redenen, bestaan daarvoor ook wetssystematische redenen. De Wpg geeft namelijk slechts regels voor de verwerking van eenmaal vergaarde gegevens. De Wpg kent geen bepalingen die een grondslag of bevoegdheid bieden voor het vergaren van gegevens. Het openbaar ministerie merkt in haar advies op dat artikel 2 van de Politiewet 1993 reeds een basis biedt in het kader van de algemene politietaak kentekengegevens vast te leggen. Dit is echter alleen het geval indien voor het vastleggen van kentekengegevens op het moment van vastlegging een aanleiding bestaat, zie ook paragraaf 5.4 van deze memorie van toelichting. Het voorgestelde artikel 126jj geeft daarom expliciet een basis voor de vergaring van gegevens. Er zijn dus zowel inhoudelijke als wetsystematische argumenten om de regeling op te nemen in het Wetboek van Strafvordering, en er zijn geen (doorslaggevende) argumenten die zich hiertegen verzetten.

Het openbaar ministerie plaatst kanttekeningen bij de doelomschrijving in het eerste lid en de verhouding daarvan tot de omschrijving van de gevallen waarin de opgeslagen gegevens kunnen worden gebruikt in het derde lid. Ook de Raad voor de rechtspraak maakt hierover opmerkingen. De Raad vindt de afbakening van het doel van de bevoegdheid in het eerste lid te vaag, gelet op de reikwijdte van artikel 132a Sv, en bepleit een meer concrete omschrijving van de opsporingsdoelen. Naar aanleiding van deze opmerkingen van het openbaar ministerie en de Raad voor de rechtspraak is de tekst van het eerste lid aangepast. Hiermee wordt verhelderd dat de vastlegging van gegevens plaatsvindt met het doel deze achteraf te kunnen raadplegen in geval van verdenking van een bepaald misdrijf dan wel de aanhouding van voortvluchtige personen.

De Raad voor de rechtspraak is van mening dat de enkele vastlegging van een kenteken van een voertuig weliswaar niet te beschouwen is als een inbreuk op de persoonlijke levenssfeer, maar dat onder bijkomende omstandigheden - zoals het bewaren van het kenteken gedurende enige tijd - daarvan wel sprake kan zijn. De raad meent, dat niet uitgesloten is dat de vastlegging en raadpleging van kentekengegevens op zodanige wijze plaatsvindt dat iemands gangen of de gangen van een groep personen door het hele land gedurende langere tijd kunnen worden gevolgd. Uit de rechtspraak van het EHRM kan worden afgeleid dat enige vorm van rechterlijke controle achteraf op de toepassing van automatische kentekenherkenning in een concrete zaak mogelijk moet zijn. De raad verwijst hierbij naar de uitspraak van het EHRM van 2 september 2010, LJN BO2548, in de zaak Uzun tegen Duitsland.
In reactie hierop zij vermeld dat rechterlijke controle achteraf op de toepassing van automatische kentekenherkenning in strafzaken in elk geval aan de orde is. Daarnaast staat voor de burger op grond van artikel 25 van de Wpg de weg open inzage te vragen in de vastgelegde gegevens, alsmede verwijdering te verzoeken. Tegen een weigering van een dergelijk verzoek staat bezwaar open en beroep op de rechter.

De Raad voor de rechtspraak vraagt in te gaan op de verhouding tot stelselmatige observatie, mede in relatie tot vergelijkingsbestanden CIE. Hierover merk ik op dat ten aanzien van een CIE-subject geen

stelselmatige observatie is toegestaan, tenzij dit plaatsvindt in het belang van een concreet opsporingsonderzoek, op basis van artikel 126g, of artikel 126o.
De uitspraak inzake Uzun die door de Raad voor de rechtspraak wordt aangehaald, betreft observatie van een verdachte met behulp van GPS gedurende drie maanden. In deze zaak werden van één persoon alle bewegingen vastgelegd. Dit zou kunnen worden aangemerkt als een vorm van stelselmatige observatie (artikel 126g Sv). Stelselmatige observatie houdt in dat een opsporingsambtenaar op bevel van de officier van justitie stelselmatig een persoon volgt of stelselmatig diens aanwezigheid of gedrag waarneemt. Daarmee kan een min of meer volledig beeld van bepaalde aspecten van iemands leven worden verkregen (Kamerstukken II 1996/97, 25403, nr. 3, blz. 26). Vanwege de inbreuk op de persoonlijke levenssfeer die dit met zich mee kan brengen, is het bevel van de officier van justitie vereist en is de bevoegdheid beperkt tot de opsporing van misdrijven. Door toepassing van de voorgestelde bevoegdheid tot het vastleggen van kentekengegevens wordt niet stelselmatig informatie over een bepaalde persoon vergaard. Het gaat slechts om het op een enkel moment waarnemen van een voertuig (zie ook paragraaf 5.3).
Zoals tot uidrukking komt in de rechtspraak van de Hoge Raad, wordt niet snel aangenomen dat sprake is van stelselmatige observatie (HR 26 oktober 2010, LJN BN0004, Gerechtshof Den Haag 7 maart 2007, aangehaald in HR 12 oktober 2010, LJN BM4211). Daarom zal de raadpleging van de vastgelegde gegevens niet snel het karakter dragen van stelselmatige observatie, zelfs niet indien van één bepaald kenteken alle gegevens worden geraadpleegd.

De Raad voor de rechtspraak vraagt of voor het verkrijgen van de bij een kenteken behorende gegevens in het buitenland een rechtshulpverzoek nodig is. Sinds de totstandkoming van het Verdrag van Prüm van 27 mei 2005, (Trb. 2005, 197) is geen rechtshulpverzoek meer nodig. Volgens artikel 12 van dit verdrag hebben de partijen bij het verdrag via hun nationale contactpunt toegang tot elkaars kentekenregisters. Vanuit het contactpunt in het land waar een voertuig wordt aangetroffen waarover informatie gewenst is, kan in het kader van handhaving van de openbare orde en veiligheid en ter voorkoming en opsporing van strafbare feiten, contact worden gelegd met het kentekenregister van de staat waar het voertuig staat geregistreerd. In Nederland is de RDW het nationale contactpunt.

De Raad van Korpschefs bepleit in zijn advies dat de opgeslagen kentekengegevens mogen worden gebruikt voor “de daadwerkelijke handhaving van de rechtsorde”, zodat ook gebruik mogelijk is ter voorkoming van misdrijven en terroristische dreigingen, bijvoorbeeld in het kader van het bewaken en beveiligen van personen of grootschalige evenementen. In reactie hierop zij vermeld dat het achteraf zoeken in bewaarde gegevens van belang is wanneer zich ná het moment van vastleggen incidenten hebben voorgedaan. Alleen wanneer deze incidenten bestaan uit een bepaald misdrijf of een ontvluchting, wordt gebruik gerechtvaardigd geacht. Als zich in het kader van het bewaken en beveiligen van personen of bij evenementen incidenten voordoen, betreft dit doorgaans strafbare feiten. Gaat het om misdrijven waarvoor voorlopige hechtenis is toegelaten dan mogen, volgens het voorstel, de vastgelegde kentekengegevens geraadpleegd worden. Zijn er bij het bewaken en beveiligen van personen of rond evenementen vooraf risico’s bekend die verbonden zijn met personen met bepaalde voertuigen dan kan

met een vergelijkingsbestand worden gewerkt, en is het niet nodig om achteraf *no hits* te raadplegen. Denkbaar is ook dat er een onderzoek loopt in het kader van bewaken en beveiligen en dat kentekengegevens op grond van artikel 9 van de Wpg kunnen worden verwerkt.
De Raad van Korpschefs bepleit de reikwijdte van het wetsvoorstel te verbreden tot andere soorten sensoren, die geautomatiseerde waarnemingen kunnen doen. Hiervan is afgezien, omdat onvoldoende inzicht bestaat in het gebruik van andere soorten sensoren.

7. Financiële gevolgen

Voor het bewaren van kentekengegevens kan gebruik worden gemaakt van dezelfde camera's als voor de automatische kentekenherkenning waarbij opvolging wordt gegeven aan *hits.* In paragraaf 4.9. kwam dit aan de orde. In het door de Minister van Veiligheid en Justitie vast te stellen cameraplan komt aan de orde of de ingebruikneming van ANPR-camera's op nieuwe locaties nodig of gewenst is, voor zover het budget dat toelaat. De kosten voor de camera-opstellingen, zowel mobiel als vast, worden gedragen door de korpsen.
.
De kosten voor het bewaren van kentekengegevens als beschreven in paragraaf 4 vergen een additionele investering van 0,8 mln euro. Deze is nodig om te voorzien in de capaciteit voor het bewaren van kentekengegevens gedurende een periode van vier weken, uitgaande van de hiervoor genoemde aantallen camera's. De kosten voor het bewaren van de kentekengegevens worden gedragen door de korpsen.

ARTIKELSGEWIJZE TOELICHTING

Artikel 126jj

Eerste lid

Dit artikel bepaalt dat een opsporingsambtenaar bevoegd is tot het vastleggen van kentekens ten behoeve van de opsporing van bepaalde misdrijven en het achterhalen van voortvluchtige veroordeelden en verdachten. In paragraaf 4 is ingegaan op het belang voor de opsporing van bepaalde misdrijven. Over het achterhalen van voortvluchtigen kan worden opgemerkt dat de politie tot taak heeft verdachten en veroordeelden tegen wie een bevel tot vrijheidsbeneming is afgegeven, aan te houden. Dit is een taak ten dienste van de justitie, als bedoeld in artikel 1, eerste lid, onder g, van de Politiewet 1993.

De voorgestelde bevoegdheid wordt opgenomen in het Wetboek van Strafvordering omdat de bevoegdheid kan worden aangewend voor strafvorderlijke doeleinden. De bevoegdheid houdt in dat door een opsporingsambtenaar gegevens kunnen worden vastgelegd zonder dat sprake is van verdenking van een strafbaar feit. Indien er wel een verdenking bestaat van een strafbaar feit, staat artikel 9 van de Wpg reeds toe dat gegevens die ter opsporing van dat strafbare feit noodzakelijk zijn voor de duur van dat onderzoek kunnen worden verwerkt.

De kentekens worden vastgelegd met een technisch hulpmiddel, in de huidige toepassing is dat een camera. In paragraaf 4.7 is ingegaan op de kwaliteitseisen die daarvoor in de praktijk worden gehanteerd. De gegevens worden conform artikel 1, onderdeel f, van de Wpg verwerkt onder verantwoordelijkheid van de beheerder van het politiekorps dat de camera's gebruikt.
De aanwezigheid van een technisch hulpmiddel ter vastlegging van kentekens wordt op duidelijke wijze kenbaar gemaakt. Omdat de kentekens van alle voertuigen die het technisch hulpmiddel passeren, worden vastgelegd, is het passend dat het vastleggen niet heimelijk plaatsvindt. Overheidsoptreden behoort kenbaar te zijn. Ook het Dataprotectieverdrag verlangt dat een burger – behoudens bijzondere gevallen – ervan op de hoogte moet zijn als hem betreffende gegevens worden verwerkt. In haar advies geeft het openbaar ministerie aan het ermee eens te zijn dat het vastleggen van gegevens niet heimelijk gebeurt, maar vraagt verheldering wat "duidelijk kenbaar maken" betekent in de praktijk en wat het gevolg is als de aanwezigheid van het technisch hulpmiddel niet op duidelijke wijze is kenbaar gemaakt. De aanwezigheid van het technisch hulpmiddel kan kenbaar worden gemaakt door het plaatsen van een bord langs de weg. Niet kenbaar hoeft te zijn waar het technisch hulpmiddel precies is opgesteld. Ook kan de aanwezigheid worden kenbaar gemaakt op de website van de politie of door het gebruik van een politieauto waarvan kenbaar is dat daarin een camera is aangebracht die kentekengegevens vastlegt. De kenbaarheid is een van de randvoorwaarden voor een zorgvuldige toepassing van de bevoegdheid tot het vastleggen van kentekengegevens, zie paragaaf 5. Of – indien aan deze voorwaarde niet (geheel) is voldaan is - de vastlegging onrechtmatig is, zal de rechter, indien dit hem wordt voorgelegd, beoordelen aan de hand van de feiten en omstandigheden van het geval

De bevoegdheid is niet slechts toebedeeld aan politie-ambtenaren. Ook andere opsporingsambtenaren, bijvoorbeeld werkzaam bij bijzondere opsporingsdiensten (BOD-en), kunnen de bevoegdheid toepassen. Het ligt in de rede dat politiekorpsen en BOD-en onderling het gebruik van camera's afstemmen. De Raad voor de rechtspraak vraagt in zijn advies of het wel voldoende is om er vanuit te gaan dat politiekorpsen en bijzondere opsporingsdiensten het gebruik van camera´s afstemmen. In reactie hierop kan worden verwezen naar hetgeen hierboven is vermeld over het opstellen van een cameraplan. Inderdaad is er regie nodig op de plaatsing van camera´s. Dat gebeurt onder meer via het door de minister van Veiligheid en Justitie vast te stellen cameraplan.

Tweede lid en derde lid

Naast de bevoegdheid gegevens vast te leggen, neergelegd in het eerste lid, worden in het tweede lid voorschriften gegeven over de verwerking van de vastgelegde gegevens.
Op de verwerking van de gegevens is in beginsel de Wpg van toepassing, maar op een aantal punten geeft het voorgestelde artikel 126jj Sv een eigen regeling. Het tweede lid bepaalt dat de gegevens gedurende een periode van vier weken mogen worden bewaard en het derde lid bepaalt voor welke doelen de gegevens mogen worden gebruikt. De regels voor de bewaartermijn en het gebruik zijn dus neergelegd in het Wetboek van Strafvordering, en vormen een lex specialis ten opzichte van de regels van de Wpg. Voor het overige zijn

de regels van de Wpg van toepassing. Dit betreft bijvoorbeeld de bepalingen over de rechten van de betrokkene en het toezicht op de gegevensverwerking. Ook voor gegevens die worden verwerkt in verband met het gemeentelijk cameratoezicht, geldt zo'n eigen regeling naast de regeling van de Wpg, zie artikel 151c van de Gemeentewet.

De gegevens die worden bewaard zijn de kentekens zelf en de met de kentekens samenhangende gegevens betreffende locatie, tijstip en de opname van het voertuig. De camera's die gebruikt worden voor automatische kentekenherkenning maken een foto van hetzij de achterkant, hetzij de voorkant van het voertuig.

De bewaarde gegevens mogen voor de twee in het derde lid genoemde doelen worden gebruikt. Dit is toegelicht in paragraaf 4.6. Indien de bewaarde gegevens worden geraadpleegd in verband met de verdenking van een misdrijf en de gegevens informatie opleveren voor de opsporing van het feit, maakt de opsporingsambtenaar hiervan op grond van artikel 152 Sv een proces-verbaal op.

Vierde lid

Bij algemene maatregel van bestuur zal worden bepaald op welk wijze de gegevens worden geraadpleegd. De opsporingsambtenaar kan slechts de beschikking krijgen over de opgeslagen gegevens door een verzoek te doen aan de ambtenaren die daartoe door de Minister van Veiligheid en Justitie expliciet zijn geautoriseerd. In het verzoek is vermeld ter opsporing van welk misdrijf, dan wel ter aanhouding van welke voortvluchtige persoon, het verzoek wordt gedaan. De geautoriseerde ambtenaren hebben met behulp van aan hen toegekende toegangscodes toegang tot de gegevens. Zij voldoen aan een verzoek door de gegevens die in het verzoek zijn vermeld langs geautomatiseerde weg te vergelijken met de vastgelegde kentekengegevens. Wanneer de gegevens waarop het verzoek betrekking heeft aanwezig zijn in het bestand, verstrekken zij deze aan de opsporingsambtenaar die het verzoek heeft gedaan. De vergelijking vindt slechts plaats aan de hand van in het verzoek opgenomen gegevens betreffende kenteken, locatie of tijdstip. Daarbij wordt een kenmerk vastgelegd aan de hand waarvan kan worden herleid ten behoeve van welke opsporingsambtenaar en op grond van welk verzoek de gegevens zijn verwerkt. Jaarlijks wordt een verslag gemaakt over het aantal malen dat gegevens zijn verstrekt, voor welk doel dit is gebeurd en aan welk arrondissementsparket of politiekorps dan wel andere opsporingsdienst. Tevens wordt jaarlijks een *audit* gehouden naar de goede toepassing hiervan.

De Minister van Veiligheid en Justitie

Bijlage - Privacy Impact Assessment ANPR

1 Inleiding

Deze bijlage hoort bij de Memorie van Toelichting van het wetsvoorstel tot aanpassing van het Wetboek van Strafvordering in verband met de regeling van het vastleggen en bewaren van kentekengegevens door de politie. Het vastleggen van kentekengegevens vindt plaats met camera's voor automatische nummerplaatherkenning (in het Engels Automatic Number Plate Recognition, ANPR).[1] Deze bijlage bevat een Privacy Impact Assessment (PIA) van bovengenoemd wetsvoorstel zoals door de Staatssecretaris van Veiligheid en Justitie is toegezegd aan de Eerste Kamer naar aanleiding van de motie Franken d.d. 17 mei 2011.[2]
Een PIA is een risicoanalyse, in het bijzonder gericht op privacyrisico's en aanverwante risico's, zoals voor de zorgvuldige verwerking van persoonsgegevens. Er bestaat geen uniforme aanpak voor het uitvoeren van een PIA, maar in het buitenland zijn wel verschillende voorbeelden beschikbaar van PIA's op het gebied van ANPR.[3] Teneinde zo volledig mogelijk de risico's van het wetsvoorstel in kaart te brengen is voor de opzet gekozen die is beschreven in paragraaf 3.
Deze PIA richt zich specifiek op de in het wetsvoorstel opgenomen bevoegdheid kentekengegevens voor specifiek omschreven doelen vast te leggen en maximaal vier weken te bewaren. Dat houdt in dat de risico's van een bepaalde keuze in beeld worden gebracht.[4] Het voordeel hiervan is dat de analyse een stuk concreter wordt en er niet in talloze verschillende scenario's hoeft te worden gedacht. Daarbij dient wel opgemerkt te worden dat de keuze voor een bewaartermijn van vier weken uiteraard van invloed is op de inschatting van de privacyrisico's. Deze PIA is niet gericht op de andere mogelijkheden die ANPR als zodanig biedt, maar beperkt zich tot de toepassing die wordt geregeld in het wetsvoorstel.
Het voorgenomen gebruik van ANPR zoals het is geregeld in dit wetsvoorstel wordt kort weergegeven in paragraaf 2. Daar komt onder meer aan bod welke gegevens worden bewaard, wie toegang heeft tot die gegevens en waarvoor de gegevens mogen worden gebruikt. Vervolgens wordt in paragraaf 3 uiteengezet hoe deze PIA is opgezet. Hier wordt toegelicht wanneer iets als een risico moet worden gezien, om wiens risico's het gaat en welke opzet is gekozen om een zo volledig mogelijk beeld van de aard en omvang van die risico's te verkrijgen. In paragraaf 4 wordt het wetsvoorstel getoetst volgens dit model. Daarbij wordt tevens een inschatting gemaakt van de zwaarwegendheid van de risico's: is de kans dat de risico's zich voordoen klein of groot en als ze zich voordoen, hoe groot is dan de impact? In paragraaf 5 worden risicobeheersende maatregelen besproken die worden ingezet om de risico's te vermijden of te verkleinen. Paragraaf 6 sluit af met een overzicht en conclusies.

2 Het wetsvoorstel

In deze paragraaf wordt kort samengevat wat het wetsvoorstel waarvoor de PIA wordt uitgevoerd inhoudt. De hier geboden informatie is zeer summier, voor meer gedetailleerde informatie wordt verwezen naar het wetsvoorstel zelf en het voor de toepassing van ANPR opgestelde uitvoeringskader.

---

[1] Wetsvoorstel tot wijziging van het Wetboek van Strafvordering in verband met de regeling van het vastleggen en bewaren van kentekengegevens door de politie.
[2] Kamerstukken I 2010/2011, 31052, nr. D.
[3] Zie bijvoorbeeld: IACP (2009) *Privacy Impact Assessment Report for the Utilization of License Plate Readers*, Alexandria, Virginia: International Association of Chiefs of Police.
[4] Zie ook: *Data Protection Impact Assessments for EU Member State law enforcement information exchange initiatives [draft version]*

Wat is ANPR?
ANPR houdt in dat op camerabeelden kentekenplaten van voertuigen als zodanig worden herkend. Met bijbehorende software worden de cijfers en letters op de kentekenplaten vervolgens 'gelezen', d.w.z. herkend welke cijfers en letters er op het kenteken staan. Het herkende kenteken kan vervolgens worden vastgelegd.

Wat beoogt het wetsvoorstel?
Het wetsvoorstel regelt de bevoegdheid van de opsporingsambtenaar om op of aan de openbare weg met behulp van een technisch hulpmiddel (ANPR-camera's) de kentekens van passerende voertuigen en de met de kentekens samenhangende gegevens betreffende locatie en tijdstip en de opname van het voertuig vast te leggen en gedurende een periode van vier weken na de datum van de vastlegging te bewaren. Hiermee realiseert het wetsvoorstel een wettelijke titel voor het vastleggen en tijdelijk bewaren van passagegegevens.
Aangezien het vastleggen van kentekengegevens die op het moment van vastlegging direct noodzakelijk zijn voor de uitvoering van de politietaak reeds binnen de bevoegdheden van de politiewet valt, is met dit wetsvoorstel vooral een nadere regeling gegeven voor gegevens die op het moment van vastlegging niet direct noodzakelijk zijn voor de uitvoering van de politietaak.

Welke gegevens worden bewaard?
Van passerende voertuigen worden de kentekens en de met de kentekens samenhangende gegevens betreffende locatie en tijdstip en de opname van een voertuig bewaard gedurende vier weken, ongeacht of de kentekens op het moment van vastlegging direct noodzakelijk zijn voor de uitvoering van de politietaak.

Waarvoor worden de gegevens gebruikt?
De gegevens kunnen worden geraadpleegd door een opsporingsambtenaar in geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, en een misdrijf als bedoeld in artikel 178 van de Wegenverkeerswet 1994, ten behoeve van de opsporing van dat misdrijf of in geval van een voortvluchtige persoon als bedoeld in artikel 564 van het Wetboek van Strafvordering, ter aanhouding van deze persoon. De raadpleging vindt slechts plaats door politiegegevens met betrekking tot de verdenking van het misdrijf of de voortvluchtige persoon geautomatiseerd te vergelijken met de vastgelegde ANPR-gegevens, teneinde vast te stellen of de gegevens overeenkomen. Als de gegevens overeenkomen, kunnen ze voor het desbetreffende doel verder worden verwerkt.

Wie heeft toegang tot de gegevens?
Opsporingsambtenaren kunnen de gegevens raadplegen voor de in het wetsvoorstel genoemde doelen. Dit kan middels een verzoek van de opsporingsambtenaar aan een van de geautoriseerde ambtenaren die met een persoonlijke toegangscode toegang heeft tot de vastgelegde gegevens.

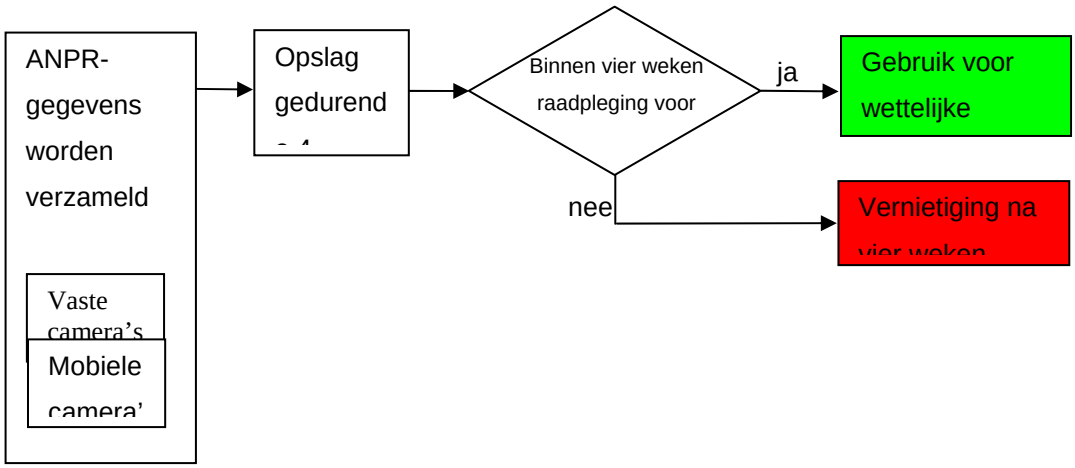
Hoe lang worden de gegevens bewaard?
De gegevens worden vier weken bewaard en worden daarna vernietigd. Indien de gegevens in deze periode van vier weken geraadpleegd worden en nodig zijn voor een van de in het wetsvoorstel opgenomen doelen, kunnen ze voor dit doel verder worden verwerkt met inachtneming van de Wet politiegegevens. De betreffende gegevens worden in dat geval elders opgeslagen; de oorspronkelijke gegevens worden hoe dan ook na vier weken vernietigd.

Zijn de ANPR-gegevens persoonsgegevens?
Ja, in beginsel zijn ANPR-gegevens persoonsgegevens in de zin van art. 1 sub a Wet bescherming persoonsgegevens.[5] Omdat de gegevens echter worden verwerkt door

[5] Kentekengegevens voldoen voor de overheid aan de definitie van persoonsgegevens, zoals

politie- en andere opsporingambtenaren, is niet de WBP, maar de WPG van toepassing, overeenkomstig art. 1 sub a en art. 46 WPG en art. 2 lid 2 sub b WBP.

Hoe loopt het proces van ANPR-gegevens verwerken?
In onderstaand schema is vereenvoudigd het proces van vastleggen van ANPR-gegevens weergegeven:



Merk op de gegevens na vier weken altijd worden verwijderd uit het bestand met passagegegevens. Als de gegevens na vier weken mogen worden gebruikt voor de wettelijke doelen, dan worden de gegevens elders opgeslagen.

3 Onderzoeksopzet

In deze PIA worden de risico's, met name de privacyrisico's, van het wetsvoorstel in kaart gebracht. Door de risico's vroegtijdig in beeld te brengen, kan bij het ontwerp reeds rekening worden gehouden met risicobeheersende maatregelen waar dat nodig is. Zo kunnen onnodige en ongewenste inbreuken op de privacy en andere burgerrechten worden voorkomen. Tevens kan deze analyse mogelijk bijdragen aan het vertrouwen van burgers in de wijze waarop politie en justitie gegevens verzamelen en verwerken en omgaan met privacy en gegevensbescherming. Beoogd is om met deze PIA ook het bewustzijn rondom privacyvraagstukken en de transparantie betreffende het verzamelen en verwerken van gegevens te vergroten.

Wat is een risico?
In deze PIA worden met risico's bedoeld de *mogelijke negatieve gevolgen* voor bescherming van de persoonlijke levenssfeer en de zorgvuldige verwerking van persoonsgegevens die zich kunnen voordoen bij het vastleggen en gebruiken van ANPR-gegevens conform het wetsvoorstel. Risico's hangen daarmee enerzijds af van de kans

---

beschreven in art. 1 WBP. Het criterium is of de identiteit van de persoon redelijkerwijs en zonder onevenredige inspanning kan worden vastgesteld, zie *CBP Richtsnoeren ANPR, de toepassing van automatische kentekenherkenning door de politie*, juli 2009, p. 14. Het is niet doorslaggevend of het identificeren daadwerkelijk plaatsvindt. Kentekengegevens zijn voor de overheid betrekkelijk eenvoudig te herleiden tot een natuurlijk persoon, de eigenaar/kentekenhouder, als gevolg van de veelheid aan systemen waarop een beroep kan worden gedaan. Voor particulieren ligt dit anders: de RDW verschaft niet zonder meer gegevens over een eigenaar/kentekenhouder. Verzekeraars kunnen die relatie vaak weer wel leggen op basis van de hun beschikbare gegevens.

dat een gevolg zich voordoet en anderzijds van de impact die dat gevolg heeft als het zich eenmaal voordoet. Kortom, de risico's die in deze PIA worden beschreven *kunnen* zich voordoen, sommigen zijn waarschijnlijker dan anderen, maar ook als de gevolgen nooit daadwerkelijk plaatsvinden zijn het risico's.

Risico = Kans * Impact

Deze gangbare definitie biedt ook meteen een aanknopingspunt om de ernst van risico's vast te stellen.[6] Een risico is groot als de kans op ernstige gevolgen groot is, maar kan ook groot zijn als er een grote kans is op kleine nadelige gevolgen of als er een zeer kleine kans is op zeer ernstige gevolgen:

	Grote kans	Kleine kans
Grote impact	Groot risico	Mogelijk groot risico
Kleine impact	Mogelijk groot risico	Klein risico

Als algemene voorbeelden zouden kunnen dienen fietsendiefstal en moord: de kans dat iemand slachtoffer wordt van een fietsendiefstal is veel groter dan de kans dat iemand slachtoffer wordt van een moord. Wat betreft de impact is het echter duidelijk andersom.
Dit model biedt eveneens aanknopingspunten voor risicobeheersende maatregelen. Immers, deze kunnen gericht zijn op het vermijden of verkleinen van de kans dat het nadelige effect zich voordoet of gericht zijn op het vermijden of verkleinen van de impact van dat nadelige gevolg. Bijvoorbeeld bij een woninginbraak kan de kans worden verkleind door goed hang- en sluitwerk en voldoende verlichting, maar kan ook de impact worden verkleind door weinig contact geld en juwelen in huis te hebben. Meer over risicobeheersende maatregelen is te vinden in paragraaf 5.

Wiens risico's?
Deze PIA richt zich vooral op de risico's voor burgers. Het gaat dan om de bescherming van hun persoonlijke levenssfeer en de zorgvuldige verwerking van hun gegevens, maar ook om de bescherming van aanverwante rechten, beginselen en waarden, zoals vrijheid, veiligheid, integriteit, transparantie, rechtszekerheid, betrouwbaarheid en non-discriminatie. Door deze PIA breder op te zetten dan alleen zuivere privacyrisico's, wordt een breder beeld verkregen.
In deze PIA ligt niet de nadruk op risico's voor de overheid of overheidsinstellingen. Als de politie op basis van onjuiste ANPR-gegevens verkeerde beslissingen neemt, dan is dat in de eerste plaats een risico voor de burger die onjuist en wellicht onheus wordt bejegend en pas daarna een risico voor de politie in termen van reputatie en vertrouwen en eventuele aansprakelijkheid. Dat laatste is zeker ook belangrijk, maar de nadruk in deze analyse ligt op risico's voor burgers.
De risico's in deze analyse worden zoveel mogelijk geduid in individuele en/of maatschappelijke risico's. Daar waar ANPR bijvoorbeeld technische risico's met zich meebrengt, zoals bovengenoemde onjuiste gegevens, wordt dat niet als een op zichzelf staand probleem gezien, maar vooral als de oorzaak van individuele problemen (zoals onterechte boetes) of maatschappelijke problemen (zoals verminderde rechtszekerheid). Hetzelfde geldt voor organisatorische risico's, bijvoorbeeld wanneer grote groepen mensen toegang krijgen tot ANPR-gegevens. Een individueel risico is dan bijvoorbeeld privacy (weten waar je buurman of een bekende Nederlander was) en een mogelijk maatschappelijk risico is dan een geringe beveiliging van gegevens (meer mensen die bij gegevens kunnen vergroot de kans op lekken).
Door op deze wijze risico's te inventariseren is getracht zoveel mogelijk aan te sluiten op de bedoeling van bovengenoemde motie Franken.

De gekozen systematiek

[6] http://en.wikipedia.org/wiki/Risk_management

Op welke wijze een risicoanalyse ook wordt uitgevoerd, het is onmogelijk om van een resulterende inventarisatie van risico's aan te tonen dat die compleet is. Een risicoanalyse is kijken naar de toekomst om vervolgens onderbouwd een inschatting te maken. Volledig kan die echter nooit zijn, omdat zich altijd onverwachte omstandigheden kunnen voordoen. Echter, wanneer een risicoanalyse breed, systematisch en zorgvuldig wordt uitgevoerd, kan het ontstane landschap van potentiële risico's wel *zo volledig mogelijk* zijn. Door een brede en systematische aanpak wordt in elk geval aannemelijk dat geen grote risico's ontbreken.
Door risico's breder op te pakken dan enkel privacyrisico's wordt de brede aanpak verder vorm gegeven. De systematische en zo volledig mogelijke aanpak wordt vormgegeven door de volgende twee fasen te doorlopen bij de uitvoering van de PIA:

Fase 1 - procesbenadering
Stap voor stap wordt het proces van ANPR-gegevens doorlopen en per stap wordt bezien welke specifieke risico's mogelijk aanwezig zijn. Door alle stappen in het proces systematisch na te lopen neemt de kans af dat bepaalde risico's over het hoofd worden gezien.

Fase 2 - actorbenadering
Tevens zijn alle betrokken partijen (zie hieronder) gevraagd naar welke risico's zij zien. Door alle betrokken partijen te vragen naar risico's wordt voorkomen dat te eenzijdig of vanuit te nauw perspectief risico's worden geïnventariseerd. Op deze manier wordt getracht tot een zo volledig mogelijk beeld te komen.

Methodologisch gezien zou een van beide fasen voldoende moeten zijn voor het uitvoeren van een PIA. Niettemin is voor twee fasen gekozen, ter extra controle.

De gekozen uitvoering
Voor het uitvoeren van de risicoanalyse zijn de volgende onderzoeksmethoden gebruikt:

- Literatuurstudie van in binnen- en buitenland beschikbare risicoanalyses, in het bijzonder privacy impact assessments en in het bijzonder gericht op camera's en automatische kentekenherkenning. De geraadpleegde literatuur is terug te vinden in de voetnoten van dit document.
- Interviews met vertegenwoordigers van organisaties binnen en buiten het justitiedomein die betrokken zijn bij het wetsvoorstel ANPR. Denk daarbij aan politie, OM, CJIB, NCTb, Koninklijke Marechaussee, Rijkswaterstaat, IVW, RDW, VROM-inspectie, Inspectieraad, AIVD, belastingdienst, douane en nVWA. Daarnaast is gesproken met onafhankelijke deskundigen, onder meer uit de wetenschap. In paragraaf 4.2 worden de resultaten beschreven.
- Workshop met een groep vertegenwoordigers van de verschillende betrokken organisaties uit het justitiedomein ter toetsing en validatie. Tijdens deze workshop (gehouden op 24 oktober 2011) zijn onder meer de aard en omvang van de risico's geëvalueerd. De resultaten zijn terug te vinden paragraaf 4 en 6.

4 Risico's

4.1 Procesbenadering

In deze paragraaf worden per processtap de verschillende risico's benoemd.

Stap 1: verzamelen

Risico 1.1 onjuiste of incomplete gegevens

Bij de toepassing van ANPR zijn er verschillende betrouwbaarheidsrisico's. Deze kunnen het best worden toegelicht aan de hand van de verschillende stappen waaruit een ANPR-

systeem bestaat. De eerste stap is dat een ANPR-camera een kenteken herkent in de beelden die worden gefilmd. Een kenteken kan dan verkeerd worden gelezen, bijvoorbeeld omdat een kenteken vies is, omdat het te donker of regenachtig is of omdat een ander voertuig het kenteken deels blokkeert (occlusie). Het kenteken wordt dan onjuist of onvolledig herkend omdat de camerabeelden van matige kwaliteit zijn. Maar ook bij kwalitatief goede beelden kunnen onjuistheden in de herkenning optreden, wanneer de herkenningsalgoritmen de beelden verkeerd interpreteren. Sommige letters en cijfers kunnen eerder worden verwisseld, zoals de letters P en R, letter A en cijfer 4, cijfers 3 en 8 en cijfer 0 en letter Q.
Als een kenteken verkeerd wordt herkend, heeft dat vervelende gevolgen. Immers, als kenteken 43-PP-BC wordt herkend als kenteken 43-PR-BC dat te boek staat als behorend bij een voortvluchtig persoon, dan zou dat tot gevolg kunnen hebben dat de politie op het verkeerde spoor wordt gezet (false positive). Omgekeerd zou het gezochte voertuig behorend bij de voortvluchtige persoon niet worden herkend en zou de politie dit spoor missen (false negative).
Verkeerde herkenning en matching zijn vooral technische problemen. Met betere technologie kunnen de foutmarges flink worden gereduceerd. Daarnaast kunnen deze risico's verder worden beheerst door niet uitsluitend te vertrouwen op de technologie, maar altijd een menselijke schakel in de beslissingen te houden. Met een extra handmatige controle kan snel worden vastgesteld dat een voertuig onjuist is herkend, nog voordat een voertuig wordt stilgehouden.
Niet alleen aan de kant van herkenning en matching van kentekens kan iets misgaan, ook bij de vergelijking met politiegegevens kan de betrouwbaarheid een risico vormen.[7] Immers, de politiegegevens kunnen ook onjuist of onvolledig zijn. Wanneer bijvoorbeeld een gestolen voertuig weer terecht is, maar dit (nog) niet is aangepast in de bestanden met politiegegevens, dan kan dit onjuiste resultaten opleveren bij de geautomatiseerde vergelijkingen.
Volgens Bosma et al. heeft het zorgvuldig verzamelen en verwerken van gegevens, inclusief het actualiseren van gegevens, niet altijd de aandacht die het verdient.[8] Wanneer gegevens of (delen van) databanken met elkaar worden vergeleken, kan het voor burgers lastig zijn de bron van onjuiste gegevens te vinden. Zo kan het voorkomen dat iemand die een onjuistheid laat rectificeren bij een organisatie, de volgende dag opnieuw met die onjuistheid wordt geconfronteerd, bijvoorbeeld omdat 'snachts de gegevensbestanden zijn geactualiseerd aan de hand van een centrale database. De rectificatie wordt dan simpelweg overschreven door de eerdere onjuistheid.[9]
Uit de literatuur, de interviews en de workshop kwam naar voren dat zowel de kans als de impact van dit risico op medium moeten worden ingeschat. Bij de inschatting van de impact werd door enkelen overwogen dat deze groot is als fouten zich kunnen voortplanten in het proces van verwerking van ANPR-gegevens, terwijl anderen overwogen dat kans en impact juist klein zijn, omdat er verder in het proces nog op vele plekken ingegrepen kan worden om mogelijke onjuistheden recht te zetten.

Risico 1.2 onvoldoende transparantie over verzamelen

Het gebruik van ANPR kan weinig transparant zijn. Zowel de mobiele als de vaste camera's kunnen onzichtbaar of onopvallend worden geplaatst, zodat burgers niet weten dat hun kentekens worden geregistreerd. Als burgers hier geen weet van hebben, zullen *chilling effects* (zie hieronder) niet optreden. Daarentegen ontbreken bij heimelijk ANPR-

[7] In het Verenigd Koninkrijk bleek dat de betrouwbaarheid van de gegevens die gebruikt werden voor ANPR zeer varieerde. Zie UK Home Office/Association of Chief Police Officers (2004) *Driving Crime Down: Denying Criminals Use of the Roads,* PA Consulting Group October 2004, p. 102.

[8] Bosma, H. et al., *Data voor Daadkracht;, gegevensbestanden voor veiligheid: observaties en analyse,* Rapport van de adviescommissie Informatiestromen Veiligheid, april 2007.

[9] Zie ter illustratie Rapport 2009/199 van de Nationale ombudsman d.d. 23 september 2009 over de zaak Kowsoleaa.

gebruik ook meteen alle middelen voor burgers om bezwaar te maken of onjuiste of onvolledige gegevens te laten rectificeren. Toch kan informeren onmogelijk en/of onwenselijk zijn in bepaalde gevallen. De kans op dit risico wordt op medium geschat, maar de impact klein.

Risico 1.3 strijd met het gelijkheidsbeginsel

Een betrouwbare overheid dient zich te houden aan de vooraf vastgestelde regels, dat is voor ANPR niet anders. Strijd met bijvoorbeeld het gelijkheidsbeginsel is denkbaar als ANPR systematisch op bepaalde locaties wordt ingezet maar op andere locaties niet. Een dergelijke aanpak zou bovendien kunnen leiden tot self-fulfilling prophecies.
De kans op dit risico wordt als klein ingeschat, omdat de inzet van ANPR weliswaar is gericht op hotspots (d.w.z. plekken waar zodanig veel criminaliteit plaatsvindt dat de mate van voorspelbaarheid groot wordt)[10], maar dat daarvoor geen discriminerende criteria worden gehanteerd. Gelijke gevallen worden gelijk behandeld. De impact wordt ook als klein ingeschat.

Risico 1.4 verplaatsingseffecten

Dit betreft primair een risico voor de overheid. Zodra breder bekend wordt waar en hoe ANPR wordt ingezet, zullen mensen mogelijk hun gedrag daarop aanpassen. Criminelen die niet gevonden willen worden zullen trachten te voorkomen dat ze langs een ANPR-camera rijden of trachten te voorkomen dat ze bij een ANPR-camera gesignaleerd worden. Het eerste kan worden voorkomen door bijvoorbeeld andere routes te kiezen, waar geen camera's aanwezig zijn.
De kans op verplaatsingseffecten wordt als medium ingeschat. Naar verwachting zullen sommige bestuurders ANPR proberen te ontwijken. Dit blijkt ook uit ANPR-toepassingen in het buitenland.[11] Als dat zich voordoet, is de impact voor de overheid groot. Immers, dan verliest het instrument ANPR een deel van zijn toegevoegde waarde. Voor de burger is de impact overigens gering. Verplaatsingseffecten zijn weliswaar een risico, maar niet of nauwelijks gerelateerd aan privacy.

Risico 1.5 meer diefstal kentekens en voertuigen

Naast bovengenoemde territoriale verplaatsingseffecten (andere routes, etc.) is er ook het risico dat criminelen vaker gebruik zullen maken van meerdere kentekens om niet getraceerd te worden. Dat is onder meer mogelijk door vooraf voertuigen of kentekens te stelen of door gebruik te maken van geleende of gehuurde auto's. In het Verenigd Koninkrijk, waar ANPR op grotere schaal wordt toegepast, zijn steeds meer voorbeelden van gekloonde auto's, diefstal van auto's of kentekens en van voertuigen die verlaten of uitgebrand worden teruggevonden na afloop van een misdrijf.
De kans op dit risico is groot. Naar verwachting zullen criminelen die van ANPR op de hoogte zijn zich hiertegen indekken. Hoewel er geen onderzoek bekend is naar dit effect, lijken geluiden uit het Verenigd Koninkrijk dit te bevestigen. Als dit risico zich voordoet, heeft dat grote impact voor de overheid (immers ANPR verliest een deel van zijn toegevoegde waarde en er komt een criminaliteitsprobleem bij) en voor de burger die zich geconfronteerd ziet met gestolen kentekenplaten of voertuigen.

Risico 1.6 identiteitsfraude en identiteitsverwisseling

Een belangrijk punt is dat het instrument ANPR gericht is op de *identificatie van voertuigen*, terwijl voor de opsporing van bepaalde misdrijven of het aanhouden van een

[10] Sherman, L. W. (1995) Hot Spots of Crime and Criminal Careers of Places, In: *Crime Prevention Studies*, J. Eck and D. Weisburd (eds), Vol. 4, p. 36.
[11] Lum, C., Merola, L., Willis, J., Cave, B. (2010) *License Plate Recognition Technology (LPR); Impact Evaluation and Community Assessment*. Washington DC: George Mason University, p. 32.

voortvluchtige persoon juist de *identificatie van personen* behorende bij die voertuigen gewenst is. Het koppelen van het voertuig aan een persoon vindt gewoonlijk plaats via het kentekenregister van de RDW. De geregistreerde kentekenhouder hoeft echter niet de bestuurder te zijn.
Dit kan vanuit het perspectief van de bestuurder onbedoeld of opzettelijk zijn. Als een auto bijvoorbeeld wordt uitgeleend kunnen controlerende instanties onbedoeld een andere bestuurder aantreffen dan degene naar wie ze op zoek zijn. Het kan echter ook zijn dat de bestuurder of kentekenhouder opzettelijk heeft getracht een onjuiste koppeling tussen bestuurder en kenteken voor te doen komen, teneinde te vermijden dat zijn identiteit wordt achterhaald. Dit is een vorm van identiteitsfraude.[12] Dit is bijvoorbeeld het geval wanneer overvallers eerst een auto stelen om vervolgens met die auto een ramkraak te plegen (zie ook het risico op toename van diefstallen van kentekens en voertuigen). De sporen van het voertuig leiden dan naar de kentekenhouder in plaats van naar de overvallers.
Naast het risico een verkeerde identiteit van personen aan voertuigen te koppelen, is er ook het risico dat in het geheel geen identiteit aan een voertuig kan worden gekoppeld. Dit is bijvoorbeeld het geval wanneer iemand het kenteken van het voertuig verwijderd of onherkenbaar maakt. Dit risico is niet specifiek voor ANPR en reeds onderkend door een wettelijke verplichting kentekens te voeren.
De kans op identiteitsfraude is klein. ANPR kan zelfs worden gebruikt om katvangers te pakken, zodat de kans nog kleiner wordt. Als identiteitsfraude echter plaatsvindt, dan is de impact voor de betroffen burger groot.

Risico 1.7 chilling effects

Het gebruik van ANPR kan een zogenoemd *chilling effect* hebben.[13] Hiermee wordt gedoeld op de mogelijkheid dat mensen zich anders gaan gedragen zodra ze denken dat ze in de gaten worden gehouden. ANPR kan dus gedrag beïnvloeden, hetgeen juist de bedoeling is bij bepaalde ongewenste of verboden gedragingen. Bij andere gedragingen is dit juist niet de bedoeling. Niettemin kunnen mensen zich zeer oncomfortabel voelen onder de gedachte dat ze in de gaten worden gehouden. Als gevolg daarvan kunnen ze hun gedrag aanpassen, hetgeen kan leiden tot zelfcensuur en remmingen.
De kans op chilling effects is klein. Er werd tijdens de workshop overwogen dat ANPR weliswaar het gedrag van burgers beïnvloedt, maar op een positieve manier, namelijk door een groter gevoel van veiligheid en meer legitimiteit van de politie (d.w.z. meer publieke steun voor de politie en haar optreden). Mensen kunnen zich door de toegenomen veiligheid vervolgens ook juist vrijer gaan gedragen. Mocht het risico op chilling effects zich niettemin voordoen, dan wordt de impact als medium ingeschat.

<u>Stap 2: opslag</u>

Risico 2.1 beveiliging naar buiten (hacken en lekken)

---

[12] Grijpink, J.H.A.M. (2003) Identiteitsfraude als uitdaging voor de rechtstaat, *Privacy & Informatie,* jaargang 6, nr. 4, 2003, p. 148- 153. Grijpink, J.HAM. (2005) Two barriers to realizing the benefits on biometrics; a chain perspective on biometrics, and identity fraud as biometrics' real challenge, *Computer law and security report,* jrg. 21, nr. 2 en 3, 2005, p. 138-145,249-256. *Van* der Meulen, N.5. (2006) *The Challenge of Countering Identity Theft: Recent Developments in the United States, the United Kingdom, and the Eurapean Union.* Report commissioned by the NICC, 2006. Harper, J. (2006) *Identity Crisis; How Identification is Overused and Misunderstood*, CATO Institute, Washington DC,2006.

[13] International Association of Chiefs of Police (2009) *Privacy Impact Assessment Report for the Utilization of License Plate Readers*. Alexandria, Virginia, September 2009.

Zodra gegevens worden opgeslagen, ontstaat de mogelijkheid dat die gegevens ongewenst worden verspreid. Behalve binnen de organisatie (zie het risico beveiliging naar binnen hieronder) is er ook een beveiligingsrisico naar buiten toe. ANPR-gegevens kunnen onbedoeld buiten de organisatie terechtkomen door onzorgvuldigheid, bijvoorbeeld als een medewerker een gegevensdrager laat rondslingeren of door kwaadwillenden, bijvoorbeeld als een medewerker opzettelijk gegevens lekt of verkoopt of als personen die geïnteresseerd zijn in de opgeslagen gegevens proberen zich (onrechtmatige) toegang te verschaffen tot de computersystemen. Dit laatste is overigens wel strafbaar als computervredebreuk.[14]
De kans op dit risico is als klein ingeschat, maar de impact groot. Als zou blijken dat een ANPR-databank van de overheid te kraken is, dan is dat schadelijk voor het vertrouwen van de burger in de overheid en voor de privacy van die burger.

Risico 2.2 overload aan gegevens

Door het wetsvoorstel wordt de opslag van grote hoeveelheden gegevens mogelijk gemaakt. Dit kunnen zulke grote hoeveelheden gegevens zijn dat ze niet meer hanteerbaar zijn. Technisch is de opslag van de gegevens geen groot probleem, maar de ordening teneinde gegevens te kunnen terugvinden zou lastig en tijdrovend kunnen blijken. Een ander risico is dat de gegevens mogelijk weliswaar veel waardevolle informatie bevatten, maar dat er onvoldoende capaciteit is om de resultaten opvolging te kunnen geven.
Tijdens de interviews en de workshop werd geconcludeerd dat het inderdaad gaat om grote hoeveelheden gegevens, maar niet om een onhanteerbaar grote hoeveelheid gegevens. Kans en impact worden als klein ingeschat, omdat er technisch gezien geen problemen zijn deze hoeveelheden gegevens te verwerken. Omdat de gegevens selectief worden bevraagd, zijn er naar verwachting ook geen te grote hoeveelheden vergelijkingsresultaten.

<u>Stap 3: raadpleging en gebruik voor wettelijke doeleinden</u>

Risico 3.1 privacyinbreuken

Het meest genoemde risico van ANPR is inbreuk op de privacy. Daarmee wordt gerefereerd aan een gevoel van zich onbespied weten.[15] Privacy gaat over het beschermen van iemands persoonlijke levenssfeer. Het beeld wordt dan geschetst dat middels het gebruik van ANPR (soms tamelijk indringend) inzicht kan worden verkregen in het leven van een persoon, in het bijzonder diens reisbewegingen.
De privacygevoeligheid is onder meer afhankelijk van de hoeveelheden en soorten gegevens, de duur en het centraal of decentraal vastleggen ervan. Naarmate er grotere hoeveelheden gevoelige gegevens langer en centraal worden opgeslagen en verwerkt, zal een systeem meer privacyrisico's meebrengen, waaronder een meer integraal persoonsbeeld en toenemende beveiligingsrisico's.[16]
Soms wordt gesteld dat er in het geheel geen privacyrisico is als gegevens in computersystemen worden gezet en vervolgens niet (of in de meeste gevallen niet) worden bekeken. Vanuit de risicodefinitie uit paragraaf 3 is dit onjuist: als de gegevens in potentie *kunnen* worden bekeken, is er een privacyrisico (kans), ongeacht of de gegevens wel of niet daadwerkelijk worden bekeken (impact). Bovendien kan worden

[14] Zie art. 138a Wetboek van Strafrecht.
[15] Zie bijvoorbeeld Warren, S.D. en Brandeis, L.D. (1890) The right to privacy; the implicit made explicit, *Harvard Law Review*, p. 193-220. Warren en Brandeis spreken over 'the right to be let alone'. Zie ook Westin, A. (1967) *Privacy and Freedom.* London: Bodley Head. Westin spreekt over ´a person´s right to determine for himself when, how, and to what extent Information about him is communicated to others´.
[16] Merk op dat kortere en/of decentrale opslag juist weer andere risico's met zich meebrengen, zoals minder overzicht, besturingsproblemen en beperkte koppelbaarheid als systemen verschillend werken.

gesteld dat gegevens die toch niet worden bekeken uiteraard ook niet hoeven worden opgeslagen.
Het privacyrisico bestaat niet alleen voor bedoeld gebruik, maar ook voor onbedoelde effecten. Zo bestaat het risico dat gegevens bij een ander terechtkomen (bijvoorbeeld een medewerker die het dossier van de buurman wel eens wil zien) of voor iets anders worden gebruikt (bijvoorbeeld wanneer de ene organisatie ANPR-gegevens opvraagt van de andere organisatie). Deze beide risico's worden hieronder besproken onder de noemers ongeautoriseerde toegang door medewerkers en function creep.
De kans dat burgers het gevoel hebben dat hun privacy wordt aangetast wordt als groot ingeschat. De impact werd echter als klein ingeschat, omdat burgers weliswaar dit gevoel kunnen hebben, bijvoorbeeld zonder goede voorlichting, maar dat dit feitelijk niet aan de orde is. Gegevens zijn slechts voor een beperkte groep opsporingsambtenaren onder bepaalde omstandigheden voor bepaalde doelen bevraagbaar.

Risico 3.2 function creep, détournement de pouvoir

Hoewel het voorliggende wetsvoorstel strikt afgebakend is wat betreft de doelen waarvoor ANPR gegevens mogen worden geraadpleegd, wordt in de literatuur nogal eens het risico van function creep genoemd. Daarbij kan worden gedacht aan het gebruik van gegevens voor andere doelen binnen de eigen organisatie of via verstrekking aan een andere organisatie.
Het verstrekken van gegevens door de ene organisatie aan een andere organisatie is niet vanzelfsprekend, zelfs niet als zowel verstrekkende als ontvangende partij een overheidsorganisatie is. Het verstrekken van gegevens is via verschillende wetgeving, zoals de WBP en de WPG, gereguleerd en aan voorwaarden onderhevig. Bij een voornemen tot het verstrekken van gegevens is altijd van belang wat er met die gegevens wordt gedaan door de ontvangende partij. Het kan immers zijn dat de gegevens voor een ander doel worden gebruikt door de ontvangende partij dan waarvoor de verstrekkende partij ze gebruikte. Als gegevens voor een ander doel worden gebruikt dan waarvoor ze oorspronkelijk verzameld waren, is sprake van zogeheten *function creep*. Function creep verschilt van beveiligingsrisico's: bij function creep gaat het niet om ongewenste verspreiding van gegevens, maar om verspreiding van gegevens die initieel niet bedoeld was en dus ook geen rol heeft gespeeld in afwegingen rond proportionaliteit en subsidiariteit.
Function creep kan ook binnen een organisatie plaatsvinden. Zo kan de politie gegevens verzamelen voor opsporingsonderzoek X, terwijl later dezelfde gegevens ook nuttig blijken voor opsporingsonderzoek Y.
Function creep is (onder meer) een probleem voor proportionaliteit en subsidiariteit. Door gegevens uit de ene context te gebruiken in een andere context kan het zijn dat niet aan deze eisen is voldaan. Daarnaast brengt het problemen met betrekking tot transparantie met zich mee: het is voor burgers steeds lastiger te volgen wat er met zijn of haar gegevens gebeurt. Daarmee is het ook lastiger om onjuistheden te corrigeren.
Het feit dat gegevens ergens beschikbaar zijn brengt inherent een risico van function creep met zich mee. Bij grotere hoeveelheden gegevens kunnen de risico's groter zijn, evenals bij gegevens die zich lenen voor meerdere toepassingen.
Zonder risicobeheersende maatregelen wordt de kans en impact van function creep als groot ingeschat. Onderkend wordt dat men soms geneigd is gegevens, als die beschikbaar zijn, ook in een andere context te gebruiken. Eveneens wordt onderkend dat dat schadelijk is voor de overheid en de burger. De burger moet erop kunnen vertrouwen dat ANPR-gegevens niet anders worden gebruikt dan waarvoor een zorgvuldig afgewogen wettelijke basis bestaat.

Risico 3.3 beveiliging naar binnen (ongeautoriseerde medewerkers)

Als gegevens eenmaal worden verzameld en opgeslagen, dan is er het risico dat ze in verkeerde handen komen, ook zonder dat er door buitenstaanders in de systemen wordt ingebroken. Het kan zijn dat medewerkers binnen een organisatie graag willen kijken

naar de gegevens van anderen waarin ze zijn geïnteresseerd, bijvoorbeeld van familie of bekenden of van bekende Nederlanders. In deze betekenis hangt het beveiligingsrisico sterk samen met het privacyrisico.
Kans en impact van dit risico wordt als groot ingeschat. Daarbij werden tijdens de interviews en de workshop argumenten genoemd die vergelijkbaar zijn met de argumenten hierboven bij function creep.

Risico 3.4 onvoldoende transparantie over gegevensgebruik en rechten

Gebrekkige transparantie kan niet alleen een risico zijn met betrekking tot het plaatsen van de camera's, maar ook met betrekking tot het gebruik van de verzamelde gegevens. De gemiddelde Nederlander staat geregistreerd in 250 tot 500 bestanden.[17] In het algemeen is dat niet bekend bij de gemiddelde Nederlander, laat staan dat hij weet om welke bestanden het gaat en wat daarin over hem vermeld is. Voor een burger is zulke kennis een minimale voorwaarde om gegevens te kunnen rectificeren of bezwaar te maken tegen bepaalde toepassingen of verwerkingen van gegevens.
Hoe de verzamelde gegevens worden verwerkt kan eveneens weinig transparant zijn. Het gevolg is wel dat er een risico ontstaat op situaties, waarin personen op onverwachte momenten kunnen worden geconfronteerd met optreden jegens hen op basis van de verzamelde gegevens.[18] Op zulke momenten kan voor zo iemand onduidelijk zijn wat zijn rechten zijn en hoe hij die kan uitoefenen.
De kans op dit risico wordt als groot ingeschat. Onderkend wordt dat burgers weinig zicht hebben op het gebruik van gegevens en hun rechten, zelfs na voorlichting door de overheid. De impact wordt echter als klein ingeschat, omdat de transparantie en rechten voor burgers feitelijk wel aanwezig zijn voor de burger die meer wil weten c.q. zijn rechten wenst uit te oefenen.

Risico 3.5 interpretatiefouten en het onschuldbeginsel onder druk

In beginsel is iemand onschuldig tot het tegendeel wordt bewezen. ANPR kan op gespannen voet staan met dit onschuldbeginsel in onze rechtsstaat. Immers, indien een bepaald kenteken bij de vergelijking met politiegegevens een match oplevert, kan daarmee iemand als verdachte in beeld komen. Tegelijkertijd is nog onduidelijk wat dit zegt: zoals hierboven beschreven kunnen politiegegevens bijvoorbeeld onjuist of onvolledig zijn. Bij al te snelle conclusies (bijvoorbeeld in geval van een onjuiste match, een andere bestuurder of een onterechte vermelding in de politiegegevens) heeft de persoon in kwestie het nadeel van de twijfel en zal uitleg moeten verschaffen over wat er mogelijk is misgegaan (hetgeen extra lastig is als hij niet bekend is met de verzamelde gegevens en wat daarmee wordt gedaan). Het risico is daarmee aanwezig dat ANPR-technologie als te betrouwbaar wordt ingeschat, zonder nadere kwalificatie en nuancering ("hij moet het wel hebben gedaan, er is immers een hit!").
Voor het gebruik van ANPR als bewijsmateriaal kan overigens het omgekeerde gelden. Teneinde te voorkomen dat een onschuldige onterecht wordt veroordeeld, kan het zijn dat een rechter bij enige kans op foutmarges (en die is er vrijwel altijd) meer zekerheid wil ten aanzien van het bewijsmateriaal en zodoende ANPR-materiaal niet wil meenemen in de bewijsvoering (zelfs niet als dat statistisch gezien significant is).
De kans op interpretatiefouten wordt als klein ingeschat, hoewel een deelnemer aan de workshop wel wees op het gevaar van tunnelvisie. Als zich dat voordoet, kan de impact voor de burger groot zijn.

<u>Stap 4: vernietiging</u>

[17] Schermer, B.W. en Wagemans, T. (2009) *Onze Digitale Schaduw*, Den Haag: College Bescherming Persoonsgegevens, 23 januari 2009.
[18] Solove, D. (2004) *The Digital Person*, New York: New York University Press. Solove hier spreekt over Kafka in plaats van Big Brother.

Risico 4.1: geen tijdige vernietiging

Er is een risico dat de gegevens na vier weken niet worden vernietigd. Denkbaar is dat opsporingsambtenaren 'voor de zekerheid' dusdanig veel gegevens opvragen dat grote hoeveelheden gegevens onnodig langer worden bewaard dan vier weken.
Wanneer een digitaal gegeven vernietigd wordt, blijven er altijd restanten van het gegeven achter, waarbij het gegeven onder bepaalde omstandigheden weer te reconstrueren is (met speciale software). Door het gegeven meer malen te overschrijven met andere gegevens kan het risico van reconstructie wel worden verminderd, maar nooit volledig worden weggenomen. Vernietigen betekent het zodanig elektronisch vernietigen van gegevens dat deze niet meer door een gebruiker en/of beheerder van een database met reguliere programmatuur en reguliere autorisatie zichtbaar kunnen worden gemaakt. Als gegevens 'onder water" worden bewaard en met behulp van een speciale autorisatie zichtbaar kunnen worden gemaakt, zijn de gegevens niet vernietigd.[19]
Zonder adequate technische maatregelen wordt de kans op dit risico medium ingeschat. De impact wordt eveneens op medium geschat.

4.2 Actorbenadering

Bij de voorbereiding van dit wetsvoorstel is met vertegenwoordigers van organisaties binnen en buiten het justitiedomein die betrokken zijn bij een toepassing van ANPR, overleg gevoerd.[20] In dit overleg is ook gesproken over de privacyaspecten van dit wetsvoorstel.
Daarnaast is uiteraard gesproken over de impact van een bredere toepassing van ANPR, zoals genoemd in het regeerakkoord. Voor het onderhavige wetsvoorstel heeft dit deel van deze interviewresultaten geen consequenties. Hetzelfde geldt voor de privacyaspecten die samenhangen met een bredere toepassing dan nu in het wetsvoorstel is voorzien, voor zover deze het doel van het onderhavige wetsvoorstel overstijgen zijn de gemaakte opmerkingen niet als concreet risico in deze PIA meegenomen.

Samengevat komen de reacties erop neer dat door geïnterviewden wordt onderkend dat:

- Er risico's bestaan ten aanzien van de juistheid van de referentiedata en passagegegevens.
- Er risico's bestaan rond het (on)geautoriseerd bevragen van de passagegegevens.
- Er risico's bestaan rond het beheer en de beveiliging van de gegevensbestanden.
- Er risico's bestaan rond het vernietigen van de gegevens na afloop van de wettelijke bewaartermijn van vier weken.
- Er risico's bestaan ten aanzien van het rijgedrag van personen die cameraregistratie willen vermijden (ontwijken van camera's door alternatieve routes te kiezen, rijden over de vluchtstrook of ander gevaarlijk rijgedrag).
- Er risico's bestaan rond ongeautoriseerde overdracht van gegevens (function creep).

De reactie van de betrokken partijen zijn gebruikt bij de analyse zoals deze hieronder is gemaakt. Door alle betrokken partijen te vragen naar risico's is getracht te voorkomen dat te eenzijdig of vanuit te nauw perspectief risico's worden geïnventariseerd. Op deze manier is getracht tot een zo volledig mogelijk beeld te komen.

---

[19] Willemsen, C. (2010) *Haalbaarheidsstudie Centrale Bewaking Wettelijke Bewaartermijnen*, Justitiële Informatiedienst, Ministerie van Justitie.
[20] Denk daarbij aan politie, OM, CJIB, NCTb, Koninklijke Marechaussee, Rijkswaterstaat, IVW, RDW, VROM-inspectie, Inspectieraad, AIVD, belastingdienst, douane en nVWA. Daarnaast is gesproken met onafhankelijke deskundigen, onder meer uit de wetenschap.

5 Risicobeheersende maatregelen

Nu de risico's in kaart zijn gebracht, kan worden bezien welke maatregelen kunnen worden genomen om deze risico's te beheersen. In beginsel zijn er vier manieren om met risico's om te gaan:

1. Voorkomen (kans en/of impact wegnemen)
2. Verminderen (kans en/of impact afzwakken)
3. Uitbesteden (risico's elders onderbrengen)
4. Accepteren (op de koop toe nemen wanneer het gevolg zich voordoet)

Merk op dat het derde punt, het uitbesteden van risico's (meestal aan verzekeraars) bij dit wetsvoorstel geen optie is. Merk verder op dat bij het tweede punt (verminderen van risico's) altijd een resterend risico overblijft waarvoor acceptatie moet worden afgewogen. Hieronder worden de risicobeheersende maatregelen niet gepresenteerd in dezelfde volgorde als de risico's, aangezien de risico's en maatregelen niet een op een aan elkaar gekoppeld zijn; sommige maatregelen werken door op meerdere risico's. In paragraaf 6 is hiervan een overzicht gegeven.

Horizonbepalingen en periodieke evaluaties

In lijn met het regeerakkoord van het huidige kabinet worden maatregelen inzake opslag, koppeling en verwerking van persoonsgegevens voorzien van een zogenaamde horizonbepaling, waarin staat dat de betreffende wetgeving of stukken daarvan aflopen op een bepaalde datum. Op dat moment moet expliciet worden besloten om de wetgeving te verlengen. In het huidige wetsvoorstel is een horizonbepaling van drie jaar opgenomen.
Een horizonbepaling heeft meerdere voordelen.[21] De gebruikers van de nieuwe bevoegdheden zullen het gebruik van het instrument scherp in de gaten (moeten) houden en de resultaten registreren. Immers, als ze dat niet doen, kunnen ze een verlenging van de bevoegdheden onvoldoende onderbouwen tegen de tijd dat de bevoegdheden aflopen. Daarnaast kan door goede registraties en evaluaties kan de toegevoegde waarde van een bevoegdheid duidelijk worden. Dit kan leiden tot een (nog beter) toegesneden set met instrumenten voor opsporingsambtenaren. Tot slot dwingen horizonbepalingen ook tot een periodieke evaluatie. Bij elke verlenging ontstaat zo discussie over nut en noodzaak, waardoor zorgvuldiger wordt geëvalueerd.
Bij elke periodieke evaluatie wordt de aard en omvang van alle risico's zoals benoemd in deze PIA doorgelicht om te bezien of er veranderingen in het risicobeeld zijn opgetreden en of de risicobeheersende maatregelen adequaat zijn. In dit opzicht zijn de horizonbepaling en de periodieke evaluaties een risicobeheersende maatregel voor alle geïdentificeerde risico's.

Evidence-based aanpak

ANPR wordt pas ingezet voor een bepaalde toepassing als het aantoonbaar iets oplevert. Daartoe is voor dit wetsvoorstel onderzocht wat de inzet van ANPR met een bewaartermijn van vier weken oplevert danwel zou kunnen opleveren.[22] De belangrijkste conclusie van dit onderzoek is dat de toegevoegde waarde van ANPR *voor de opsporing* hoofdzakelijk ligt in het richting geven van het opsporingsonderzoek.[23]
Door ANPR alleen te gebruiken voor toepassingen die aantoonbaar iets opleveren wordt de inzet beperkt, hetgeen het risico op een overload van gegevens en de mogelijkheden

---

[21] **Custers, B.H.M. (2009) Kredietcrisis vraagt om scherper toezicht, *Nederlands Juristenblad*, jaargang 84, nummer 3, 23 januari 2009, p. 176.**
[22] Flight, S. en Egmond, P. van (2011) *Hits en hints; de mogelijke meerwaarde van ANPR voor de opsporing*. Amsterdam: DSP-groep.
[23] Merk op dat ANPR ook toegevoegde waarde kan hebben op andere terreinen, zoals bijvoorbeeld bij (directe) handhaving. Deze toepassingen vallen niet binnen het wetsvoorstel waarover deze PIA is uitgevoerd.

tot function creep verkleint. Ook het risico van niet tijdig vernietigen wordt kleiner, omdat de impact van niet tijdig vernietigen afneemt als er minder gegevens verzameld zijn.

Beperkt aantal delicten (geen generieke bevoegdheden)

Het wetsvoorstel beperkt het gebruik van ANPR-gegevens tot een specifiek aantal delicten, namelijk:

a. in geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, en een misdrijf als bedoeld in artikel 178 van de Wegenverkeerswet 1994, ten behoeve van de opsporing van dat misdrijf of
b. in geval van een voortvluchtige persoon als bedoeld in artikel 564 van het Wetboek van Strafvordering, ter aanhouding van deze persoon

Hiermee wordt tegemoet gekomen aan de eisen van proportionaliteit en subsidiariteit. Door het gebruik van ANPR-gegevens te beperken wordt ook het risico op chilling effects geadresseerd. Immers, slechts in geval van een zwaarder delict worden de gegevens gebruikt. Door deze beperking worden weliswaar niet minder gegevens verzameld (immers de camera's slaan alles op), maar mogen de gegevens slechts beperkt worden geraadpleegd. Daarmee neemt de kans op privacyinbreuken af en worden de mogelijkheden tot function creep kleiner.

Beperkte opslagtermijn

In het wetsvoorstel is gekozen voor een opslagtermijn van vier weken. Deze beperkte opslagtermijn heeft tot gevolg dat beperkt passagegegevens worden vastgelegd. Daarmee neemt de kans op privacyinbreuken af en worden de mogelijkheden tot function creep kleiner. Bij hacken of lekken van gegevens neemt de impact af.

Selectieve inzet bij hotspots

Als het uitgangspunt is dat ANPR slechts wordt ingezet op plaatsen, tijdstippen en manieren die iets opleveren, betekent dat automatisch dat ANPR op andere plaatsen, tijdstippen en manieren niet wordt ingezet. Met andere woorden, ANPR wordt slechts selectief ingezet. Om te weten op welke plaatsen, tijdstippen en manieren dit is, zijn regelmatige evaluaties nodig, zoals hierboven reeds is besproken. Het verdient vanuit deze optiek aanbeveling om de inzet van mobiele ANPR-camera's regelmatig te wisselen van plaats en tijdstip, zodat verschillen in resultaten duidelijk worden.
Deze selectieve inzet bij hotspots betekent ook een variabele/mobiele aanpak. Dit komt tegemoet aan het gelijkheidsbeginsel, omdat niet systematisch altijd maar op dezelfde plek ANPR wordt ingezet. Daarnaast verkleint het de kans op verplaatsingseffecten en toename van kenteken- en voertuigdiefstallen. Immers, de mobiele/variabele aanpak geeft een element van onvoorspelbaarheid en bijbehorende hogere pakkans. De selectieve inzet kan ook potentiële chilling effects verkleinen, mits duidelijk is waar de hotspots zijn.
Door gerichte ANPR-inzet worden minder gegevens verzameld, hetgeen het risico op een overload van gegevens en de mogelijkheden tot function creep verkleint. Ook het risico van niet tijdig vernietigen wordt kleiner, omdat de impact van niet tijdig vernietigen afneemt als er minder gegevens verzameld zijn.

Aan/uitzetten

Met name vanuit privacyoverwegingen wordt wel eens gesuggereerd dat het raadzaam kan zijn de (vaste) ANPR-systemen af en toe uit te zetten. Daarmee wordt tegemoet gekomen aan de (privacy-)stelling dat de bewegingen van voertuigen altijd en overal worden vastgelegd. Daarnaast zorgt het af en toe uitzetten van vaste ANPR-systemen

richting kwaadwillenden voor een zekere onvoorspelbaarheid. Als een ANPR-systeem op een bepaalde locatie voortdurend aanstaat, is er een aanzienlijke kans op verplaatsingseffecten.
Een belangrijk argument tegen het zo nu en dan uitzetten van de camera's is dat er op die momenten mogelijk belangrijke informatie gemist wordt. Uiteindelijk is het lastig uit te leggen dat op het tijdstip van een incident een camera om privacyredenen niet aan stond, terwijl de camera's juist bedoeld zijn om dergelijke incidenten op te lossen.

Random locaties

Naast het gericht inzetten van ANPR bij hotspots is het aan te bevelen om tevens op willekeurige (random) locaties ANPR in te zetten. Het hanteren van een aanpak met (vaste) hotspots heeft namelijk vrijwel altijd twee gevolgen waardoor ze op den duur ineffectief worden als er geen actualisatie plaatsvindt. In de eerste plaats zullen degenen die niet vastgelegd willen worden door ANPR-camera's (zoals criminelen) hun gedrag daarop aanpassen, bijvoorbeeld door andere routes te nemen of door voertuigen en/of kentekens te stelen kort voordat ze hun misdrijven plegen.
In de tweede plaats zal ANPR, als het effectief is, de doelgroep verkleinen. Immers, verdachten die aan de hand van ANPR-beelden worden opgespoord en vervolgd, kunnen van de zoeklijsten worden gehaald. Naarmate er meer successen zijn, zullen zulke zoeklijsten dus kleiner worden, zolang ze niet worden geactualiseerd.
Random locaties kunnen laten zien welke verschuivingen in gedrag hebben plaatsgevonden. Daarmee wordt het risico op verplaatsingseffecten kleiner. Daarnaast komen random locaties tegemoet aan het risico van strijd met het gelijkheidsbeginsel

Breach notification

In het regeerakkoord van het huidige kabinet van 30 september 2010 is (op p. 42) het voornemen geformuleerd te komen tot verdere verbetering van informatieveiligheid en bescherming van persoonsgegevens door het invoeren van een nieuwe meldplicht. Het kabinet komt, zo staat in het regeerakkoord, met een voorstel voor een meldplicht in geval van verlies, diefstal of misbruik van persoonsgegevens waarbij alle datalekken worden gemeld aan de nationale toezichthouder die boetes kan opleggen indien de meldplicht niet wordt nageleefd. De gedachte achter een dergelijke meldplicht, ook wel *breach notification* genoemd, is enerzijds dat burgers goed geïnformeerd worden als er iets misgaat met gegevens die op hen betrekking hebben en anderzijds dat organisaties scherper zullen opletten dat er zorgvuldig wordt omgesprongen met gegevens om reputatieschade te voorkomen.
Breach notification kan in het geval van ANPR een bijdrage leveren aan het voorkomen van situaties van verlies, diefstal of misbruik van gegevens (het risico van hacken en lekken). Het zal, naar verwachting, organisaties die ANPR-gegevens verzamelen of verwerken aanmoedigen adequate beveiligingsmaatregelen te treffen en te voorkomen dat gegevens voor andere doeleinden worden gebruikt dan waarvoor bedoeld (function creep).

Beveiligingsmaatregelen tegen hacken en lekken

Zowel de verzamelde ANPR-gegevens als eventuele analyseresultaten dienen adequaat beveiligd te worden. Dit om te voorkomen dat onbevoegden de gegevens kunnen inzien of eventueel zelfs zouden kunnen aanpassen. Werken op basis van need-to-know, dat wil zeggen dat iemand geen ruimere inzage in gegevens krijgt dan nodig is om zijn taak te vervullen, heeft daarbij de voorkeur (zie hieronder de interne autorisatieregels).
Beveiliging van gegevens in de opsporing is geen nieuwe zaak. Voor ANPR-gegevens hoeft beveiliging dan ook geen nieuwe problemen op te leveren. Daarbij wordt een model gebruikt waarin opsporingsambtenaren niet zonder meer alle beschikbare ANPR-gegevens kunnen inzien, maar slechts (in bepaalde gevallen) raadpleging mogelijk is door politiegegevens geautomatiseerd te vergelijken met ANPR-gegevens. De beveiliging

wordt ondersteund met een duidelijk verstrekkingenregime, opdat niet via de achterdeur alsnog gegevens worden gelekt naar andere organisaties die mogelijk gegevens minder goed hebben beveiligd of op hun beurt doorgeven aan anderen. De Wet Politiegegevens en het Besluit Politiegegevens verschaffen dit regime. Op naleving hiervan dient te worden toegezien. Een goede beveiliging verkleint de risico's op identiteitsfraude, hacken en lekken en privacyinbreuken.

Interne autorisatieregels (need to know)

Bovenstaande geldt voor beveiliging naar buiten toe. Naar binnen toe dient er ook een adequate beveiliging te zijn tegen ongeautoriseerde medewerkers. Vandaar dat voor het CIOT-model is gekozen. Een opsporingsambtenaar kan bij de geautoriseerde collega's vragen om te onderzoeken of bepaalde politiegegevens overeenkomen met de vastgelegde ANPR-gegevens. Bovendien wordt door de geautoriseerde medewerker van elke aanvraag vastgelegd welke opsporingsambtenaar de aanvraag doet en met welke reden. Ook bij de beheerder van het gegevensbestand wordt vastgelegd welke geautoriseerde medewerker de aanvraag doet, op welk tijdstip en met welke reden. Op deze wijze is er een extra controle ingebouwd om na te gaan of een opsporingsambtenaar ook voldoende reden heeft ANPR-gegevens op te vragen (need to know). Vastlegging van de aanvragen maakt controle achteraf mogelijk. Schending van integriteitsregels wordt hiermee zichtbaar. Nieuwsgierigheid wordt hiermee afgehouden. Door deze beperking van inzage wordt het risico op privacyinbreuken en op function creep verkleind.

Strafbaarstelling computervredebreuk

Naast een goede beveiliging is ook de bestaande strafbaarstelling van computervredebreuk (art. 138a Wetboek van Strafrecht) een stok achter de deur tegen hacken. Voor zover deze strafbaarstelling hackers niet reeds weerhoudt van het inbreken in ANPR-bestanden, kan zij worden gebruikt om hackers te vervolgen en te berechten. Het tegengaan van hacken verkleint eveneens de kans op privacyinbreuken.

Wettelijke bescherming

Het voorliggende wetsvoorstel stelt duidelijke regels omtrent onder meer het beperkt verzamelen van gegevens, de doelen waarvoor ANPR-gegevens mogen worden geraadpleegd en de bewaartermijn van vier weken. Naast deze regels zijn er ter wettelijke bescherming ook de algemene regels voor het verwerken van politiegegevens in de WPG. Naast technische bescherming (beveiliging) is ook zulke juridische bescherming wenselijk voor ANPR-gegevens. ANPR-gegevens zijn in dit wetsvoorstel politiegegevens. Daarmee vallen ze respectievelijk onder het beschermingsregime van de Wet Politiegegevens (WPG). Als de gegevens in een later stadium worden gebruikt in de strafdossiers, kunnen ze vallen onder het beschermingsregime van de Wet Justitiële en Strafvorderlijke Gegevens (WJSG). In deze regimes zijn waarborgen gesteld voor het verwerken van gegevens. Waarborgen waar het dan om gaat betreffen onder meer:

- beperkt verzamelen (art. 3 WPG, art. 39b lid 1 WJSG),
- kwaliteit van gegevens (art. 4 lid 1 WPG, art. 4 WJSG),
- vooraf duidelijke doelen formuleren (art. 6-10 WPG, art. 2 WJSG),
- doelbinding (art. 3 WPG, art. 39b lid 2 WJSG),
- beveiligingsmaatregelen treffen (art. 4 lid 2 WPG, art. 7 WJSG),
- transparantie (art. 21 WPG, art. 18 en 43 WJSG),
- rectificatiemogelijkheden (art. 24 WPG, art. 22 en 46 WJSG)
- verantwoordelijkheid (art. 1 onder g WPG, art. 39a WJSG).

Deze waarborgen komen tegemoet aan onder meer het risico op onjuiste en/of incomplete gegevens (de kwaliteitswaarborg), het risico op onvoldoende transparantie over welke gegevens worden verzameld en wat daarmee gebeurt (de

transparantiewaarborg), het risico op hacken en lekken (de beveiligingswaarborg), het risico op een overload aan gegevens (de beperkt-verzamelenwaarborg), het risico op privacyinbreuken (vrijwel alle waarborgen) en het risico op function creep (de doelbindingswaarborg)
Wat betreft het risico op strijd met het gelijkheidsbeginsel kan nog de Algemene wet gelijke behandeling (Awgb) worden genoemd. Deze wet verbiedt het maken van direct of indirect onderscheid in bepaalde situaties op grond van bepaalde criteria, zoals levensovertuiging en nationaliteit. Het gebruik van ANPR-gegevens kan weliswaar in potentie leiden tot indirect onderscheid, maar heeft vrijwel geen raakvlakken met de terreinen de Awgb bestrijkt, zoals arbeidsverhoudingen en -omstandigheden.

Heldere juridische grondslag

Met dit wetsvoorstel wordt een heldere juridische grondslag gegeven voor het gebruik van ANPR. Dat maakt duidelijk welke toepassingen zijn toegestaan, maar maakt ook meteen duidelijk welke toepassingen niet zijn toegestaan.[24] Daarmee wordt transparantie geboden over welke gegevens worden vastgelegd en waarvoor deze gegevens worden gebruikt. Door het gebruik voor vooral zwaardere delicten wordt ook spanning met het gelijkheidsbeginsel verminderd evenals het risico op privacyinbreuken. Door duidelijkheid wat wel en niet is toegestaan is ook de kans op function creep kleiner. Aangezien dit wetsvoorstel ook de opslagtermijn ondubbelzinnig beperkt tot vier weken, neemt de kans af dat gegevens niet tijdig worden vernietigd.

Inzage en rectificatie (waar mogelijk)

Inzage en rectificatie kan de kans op onjuiste/incomplete gegevens, op interpretatiefouten en op identiteitsfraude verkleinen (burgers zijn immers het beste op de hoogte van hun eigen gegevens en kunnen snel beoordelen of iets onjuist is). Daarom zijn de mogelijkheden voor inzage en rectificatie in de WPG van belang. Daarnaast komt inzage en rectificatie tegemoet aan het risico op onvoldoende transparantie omtrent welke gegevens worden vastgelegd en waarvoor de ANPR-gegevens worden gebruikt. Tot slot verkleint inzage en rectificatie de kans op het niet tijdig vernietigen van gegevens. Het biedt burgers immers de mogelijkheid om mee op te letten of de opslagtermijn van vier weken ook daadwerkelijk wordt nageleefd.

Menselijke schakel (geen volledig geautomatiseerde beslissingen)

Op grond van art. 42 lid 1 WBP kan niemand worden onderworpen aan een besluit waaraan voor hem rechtsgevolgen zijn verbonden of dat hem in aanmerkelijke mate treft, indien dat besluit alleen wordt genomen op grond van een geautomatiseerde verwerking van persoonsgegevens. In het kader van dit wetsvoorstel is het gebruik van ANPR-gegevens zo geregeld dat er altijd een menselijke schakel in beslissingen is ingebouwd en er geen sprake is van volledig geautomatiseerde beslissingen (ongeacht of het persoonsgegevens betreft).
Naast de hierboven besproken mogelijkheden tot inzage en rectificatie (waar mogelijk) wordt daarom altijd na raadpleging van de ANPR-gegevens door de opsporingsambtenaren interpretaties gemaakt en conclusies getrokken. Bovendien wordt bij het aanhouden van verdachten steeds goed gekeken of het inderdaad de juiste persoon betreft, eventueel door het stellen van aanvullende vragen. Deze combinatie van automatisering en mensenwerk verkleint de kans op vergissingen en interpretatiefouten. Daarnaast wordt mogelijke identiteitsfraude zo eerder opgemerkt.

Zorgvuldig cameraplan

[24] Merk op dat art. 2 Politiewet het gebruik van ANPR niet uitsluit voor, bijvoorbeeld handhavingsacties met directe opvolging waarbij geen no-hits worden opgeslagen.

In het kader van dit wetsvoorstel wordt tevens een gedetailleerd cameraplan ontwikkeld. Hierin is vastgelegd hoeveel ANPR-camera's de politie en de KMar nu ter beschikking heeft (momentopname), om wat voor camera's het gaat (zoals vaste en mobiele varianten) en waar de vaste camera's zijn opgesteld. Ook wordt in het cameraplan vermeld welke nieuwe cameralocaties zijn voorzien (voor zover nu bekend). Ook wordt aangegeven welke criteria kunnen worden gebruikt bij het voorbereiden van een besluit over het aanpassen van het aantal cameralocaties. De vaste camera's in het cameraplan zorgen voor het observeren van de belangrijkste corridors en mogelijke alternatieve routes om verplaatsingseffecten tegen te gaan. De mobiele camera's in het cameraplan zorgen voor extra flexibiliteit en onvoorspelbaarheid richting criminelen.
In het cameraplan worden verder ook technische eisen opgenomen waaraan de camera's moeten voldoen. Dit verkleint de kans op fouten bij het registreren van kentekens.

Voorlichting en scholing van de politie

Er bestaan veel misverstanden rondom ANPR. Er zit soms veel ruimte tussen de mogelijkheden die ANPR in potentie biedt en de daadwerkelijk gebruikte ANPR-toepassingen. Met dit wetsvoorstel en deze privacy impact assessment is getracht de voorgenomen inzet van ANPR zo concreet mogelijk te maken, teneinde zoveel mogelijk duidelijkheid te verschaffen waar het hier om gaat. Naar het brede publiek zal daarnaast aanvullende voorlichting worden verstrekt om transparantie te bieden over welke gegevens worden vastgelegd en waarvoor die gegevens worden gebruikt. Door heldere voorlichting neemt ook de kans af op eventuele chilling effects. Daarnaast zal de politie verder geschoold worden in het gebruik van ANPR.

Onafhankelijk toezicht

Als laatste risicobeheersende maatregelen wordt gezorgd voor onafhankelijk toezicht op de uitvoering en naleving van het gebruik van ANPR zoals dat in het wetsvoorstel is geregeld. In casu zijn er twee toezichthouders. Het College Bescherming Persoonsgegevens (CBP) houdt toezicht op de naleving en toepassing van de WBP, de WPG en de WJSG.[25] De Inspectie Openbare Orde en Veiligheid (IOOV) houdt namens de minister van Veiligheid en Justitie toezicht op de wijze waarop instanties, waaronder opsporingsinstanties, hun taak uitoefenen en de wet- en regelgeving naleven met het oog op een veilige samenleving.[26]
Beide toezichthouders kunnen onafhankelijk onderzoek doen naar de naleving en uitvoering van het gebruik van ANPR, waaronder bijvoorbeeld onderzoeken naar de effectiviteit, naar ongewenste neveneffecten, en naar praktische zaken, zoals een juiste gegevensverwerking. Bij dit toezicht kunnen risico's worden gesignaleerd, zowel nieuwe risico's die in deze impact assessment nog niet in kaart zijn gebracht, als veranderingen in bekende risico's, zoals in dit document zijn beschreven. Daarmee hebben de onafhankelijke toezichthouders een risicobeheersende functie op alle risico's.

[25] www.cbpweb.nl
[26] www.ioov.nl

6 Conclusies

In onderstaande tabel zijn de risico's uit paragraaf 4 nogmaals samengevat. Tijdens de interviews en de evaluerende workshop met vertegenwoordigers van organisaties die betrokken zijn bij het gebruik van ANPR zijn de kans en impact van de verschillende risico's ingeschat. Daartoe zijn de kansen en de impact geclassificeerd in drie categorieën, te weten klein, medium en groot.

	Risico	Omschrijving	Kans	Impact
Stap 1 verzamelen	1.1	onjuiste of incomplete gegevens	Medium	Medium
	1.2	onvoldoende transparantie (verzamelen)	Medium	Klein
	1.3	strijd met het gelijkheidsbeginsel	Klein	Klein
	1.4	verplaatsingseffecten	Medium	Groot (voor overheid)
	1.5	meer diefstal kentekens en voertuigen	Groot	Groot (voor burger) Groot (voor overheid)
	1.6	identiteitsfraude	Klein	Groot
	1.7	chilling effects	Klein	Medium
Stap 2:	2.1	beveiliging naar buiten	Klein	Groot

opslag		(hackers en lekkers)		
	2.2	overload aan gegevens	Klein	Klein
Stap 3: raadpleging en gebruik	3.1	privacyinbreuken	Groot	Klein
	3.2	function creep/détournement de pouvoir	Groot	Groot
	3.3	beveiliging naar binnen (ongeautoriseerde medewerkers)	Groot	Groot
	3.4	onvoldoende transparantie (gegevensgebruik en rechten)	Groot	Klein
	3.5	Interpretatiefouten/onschuldbeginsel	Klein	Groot
Stap 4: vernietiging	4.1	geen tijdige vernietiging	Medium	Medium

Vervolgens zijn in onderstaande tabel de verbanden weergegeven tussen de verschillende risico's (genummerd 1.1 tot en met 4.1) en de bijbehorende risicobeheersende maatregelen. In de tabel is goed te zien dat sommige maatregelen bijdragen aan het voorkomen of verkleinen van meerdere risico's. Of de maatregelen vooral de kans of de impact (of beide) van een risico beïnvloeden is terug te lezen in paragraaf 5, waar alle maatregelen zijn toegelicht.
Het aan- en uitzetten van ANPR-camera's is een risicobeheersende maatregel die regelmatig wordt genoemd om de kans op privacyinbreuken te verkleinen. Hoewel dit juist is, is er toch voor gekozen deze maatregel niet in gebruik te nemen. Voor de afwegingen, zie paragraaf 5.

Merk op dat de genoemde risicobeheersende maatregelen niet alleen potentiële maatregelen zijn, maar tevens maatregelen die in het kader van dit wetsvoorstel daadwerkelijk zijn ingevoerd of zullen worden ingevoerd. Voor de stand van zaken en verdere praktische zaken met betrekking tot de implementatie wordt verwezen naar het uitvoeringskader.

	1.1	1.2	1.3	1.4	1.5	1.6	1.7	2.1	2.2	3.1	3.2	3.3	3.4	3.5	4.1
Horizonbepaling en periodieke evaluaties	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Evidence-based aanpak									X		X				X
Beperkt aantal delicten							X			X	X				
Beperkte opslagtermijn								X		X	X				
Selectieve inzet			X	X	X		X		X		X				X
Aan/uitzetten	Niet van toepassing														
Random locaties			X	X											
Breach notification								X			X				
Beveiliging tegen hacken en lekken						X		X		X					
Interne autorisatieregels (need to know)										X		X			
Strafbaarstelling computervredebreuk								X		X					
Wettelijke	X	X						X	X	X	X		X		

bescherming (WBP, WPG, WSJG)															
Heldere juridische grondslag		X	X							X	X		X		X
Inzage en rectificatie (waar mogelijk)	X	X				X							X	X	X
Menselijke schakel						X								X	
Zorgvuldig cameraplan	X		X	X	X										
Voorlichting		X					X								
Onafhankelijk toezicht	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Tot slot is onderzocht in hoeverre de risicobeheersende maatregelen de genoemde risico's voorkomen danwel verkleinen. In onderstaande tabel zijn de risico's voor en na de genomen maatregelen ingeschat.

Risico	Omschrijving	Kans na maatregelen	Impact na maatregelen
1.1	onjuiste of incomplete gegevens	Klein	Klein
1.2	onvoldoende transparantie (verzamelen)	Klein	Klein
1.3	strijd met het gelijkheidsbeginsel	Klein	Klein
1.4	verplaatsingseffecten	Medium	Medium
1.5	meer diefstal kentekens en voertuigen	Medium	Medium
1.6	identiteitsfraude	Klein	Klein
1.7	chilling effects	Klein	Klein
2.1	beveiliging naar buiten (hackers en lekkers)	Klein	Medium
2.2	overload aan gegevens	Klein	Klein
3.1	privacyinbreuken	Klein	Klein
3.2	function creep/détournement de pouvoir	Klein	Klein
3.3	beveiliging naar binnen (ongeautoriseerde medewerkers)	Medium	Medium
3.4	onvoldoende transparantie (gegevensgebruik en rechten)	Medium	Klein
3.5	Interpretatiefouten/onschuldbeginsel	Klein	Medium
4.1	geen tijdige vernietiging	Klein	Klein

Uit de tabel blijkt dat de risico's aanzienlijk verkleind zijn, maar niet altijd volledig voorkomen. De grootste risico's zijn in elk geval gereduceerd tot medium risico's en veel medium risico's zijn gereduceerd tot kleine risico's volgens deze inschatting. Hieronder wordt de aard van de medium risico's samengevat:

Verplaatsingseffecten en diefstal van kentekens/voertuigen
Onderkend wordt dat zelfs na de genomen risicobeheersende maatregelen aannemelijk is dat een (kleine) groep criminelen zal proberen ANPR-camera's te vermijden danwel te slim af te zijn. Door een goed cameranetwerk, random locaties en het snel verwerken/registreren van gestolen kentekenplaten en voertuigen wordt de kans op deze risico's beheersbaar gehouden, maar volledig voorkomen is waarschijnlijk onmogelijk. Als er sprake is van diefstal van kentekens of voertuigen, dan wordt de impact beheersbaar gehouden door snel en adequaat optreden van de politie, maar voor de burger is het leed dan al deels geschied.

Beveiliging naar binnen en naar buiten
Door alle genoemde beveiligingsmaatregelen en ook de strafbaarstelling van computervredebreuk wordt de kans op beveiligingsrisico's aanzienlijk verkleind. Voor de beveiliging naar buiten zijn echter meer maatregelen denkbaar dan voor de beveiliging naar binnen. Niettemin kan elke beveiligingsexpert zeggen dat een 100 % garantie op veiligheid niet bestaat. Als zich beveiligingsproblemen voordoen, zelfs al is de kans daarop klein, dan in de impact daarvan serieus te nemen. De impact van deze risico's wordt echter wel beheerst door het feit dat er slechts beperkt gegevens beschikbaar zijn per kenteken, zodat niet meteen een indringend beeld van iemands handel en wandel kan worden verkregen. Het risico bestaat dus veeleer uit schade aan het vertrouwen dat de burger in de overheid heeft.

Onvoldoende transparantie
Zelfs met veel voorlichting blijft de kans aanwezig dat burgers weinig zicht hebben op hoe ANPR wordt gebruikt en wat hun rechten zijn. Dat kan nadelig zijn voor de beeldvorming rondom ANPR. Daar staat tegenover dat zulke beeldvorming mogelijk feitelijk onjuist is, omdat het gebruik van ANPR zo transparant mogelijk wordt gemaakt en inzage en rectificatie waar mogelijk worden geboden. Omdat transparantie van het werk van de politie in concrete opsporingsonderzoeken echter niet altijd mogelijk is, blijft hier een 'restrisico'.

Interpretatiefouten
Ondanks alle voorzorgsmaatregelen blijft het mensenwerk. Dat brengt met zich mee dat zich interpretatiefouten en zelfs tunnelvisie kunnen voordoen. De kans daarop wordt weliswaar als klein ingeschat, maar als dat gebeurt, kan de impact daarvan toch ernstig zijn. De menselijke schakel in het proces kan dan juist weer mitigerend werken.

De kleine en medium risico's die resteren na de genomen risicobeheersende maatregelen zijn voldoende verkleind en overzichtelijk dat ze als acceptabel gelden ten opzichte van de voordelen van het wetsvoorstel. In het kader van de toegezegde evaluatie van dit wetsvoorstel zal naast de effectiviteit van de maatregel nadrukkelijk ook worden bezien of de risico's die zijn benoemd zich inderdaad ook feitelijk hebben voorgedaan en indien dat het geval is welke maatregelen zijn getroffen.