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

[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]*

informatie wordt verwezen naar het wetsvoorstel zelf en het voor de toepassing van ANPR opgestelde uitvoeringskader.

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.

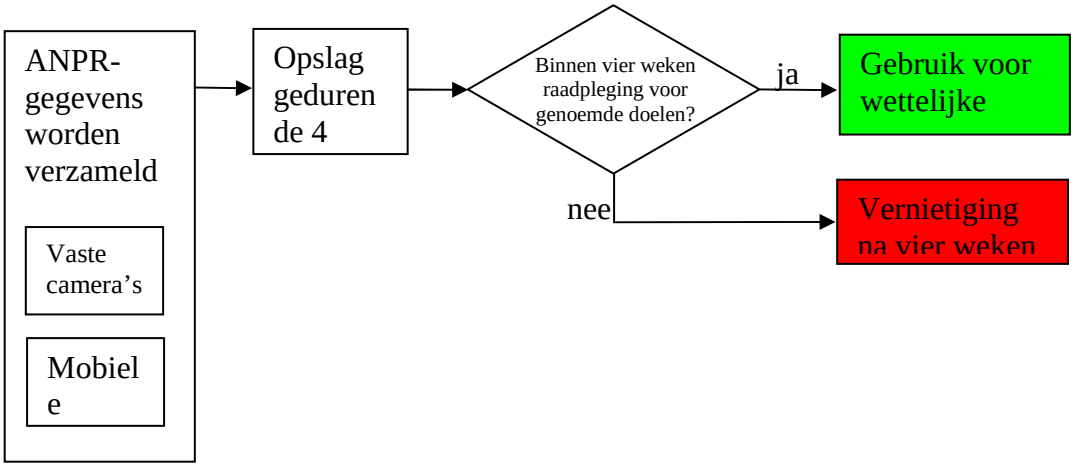
Wie heeft toegang tot de gegevens?
Opsporingsambtenaren kunnen de gegevens raadplegen voor de in het wetsvoorstel genoemde doelen. Dit kan middels een verzoek van de opsporingsambtenaar aan een van de geautoriseerde ambtenaren die met een persoonlijke toegangscode toegang heeft tot de vastgelegde gegevens.

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 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

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

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 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

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

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
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:

<u>Fase 1 - procesbenadering</u>
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.

<u>Fase 2 - actorbenadering</u>
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.

[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.

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-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

---

[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.
[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.

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 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

[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.
[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.

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)

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.

[13] International Association of Chiefs of Police (2009) *Privacy Impact Assessment Report for the Utilization of License Plate Readers*. Alexandria, Virginia, September 2009.
[14] Zie art. 138a Wetboek van Strafrecht.

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.

Stap 3: raadpleging en gebruik voor wettelijke doeleinden

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 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

[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.

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>

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.

---

[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.

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[21]. 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.

5 Risicobeheersende maatregelen

[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.
[21] Regeerakkoord VVD- CDA 'Vrijheid en verantwoordelijkheid' (2010).

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[22] 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.[23] 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

[22] Regeerakkoord VVD-CDA 'Vrijheid en Verantwoordelijkheid' (2010); vgl. het regeerakkoord VVD-PvdA 'Bruggen Slaan'(2012): 'Bij de bouw van systemen en het aanleggen van databestanden is bescherming van persoonsgegevens uitgangspunt. Daar hoort een zogenaamd privacy impact assessment (PIA) standaard bij.'

[23] **Custers, B.H.M. (2009) Kredietcrisis vraagt om scherper toezicht, *Nederlands Juristenblad*, jaargang 84, nummer 3, 23 januari 2009, p. 176.**

van vier weken oplevert danwel zou kunnen opleveren.[24] 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.[25]
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 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

[24] Flight, S. en Egmond, P. van (2011) *Hits en hints; de mogelijke meerwaarde van ANPR voor de opsporing*. Amsterdam: DSP-groep.
[25] 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.

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.[26] 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)

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

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

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.[27] 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.[28]
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.

[27] www.cbpweb.nl
[28] 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: opslag	2.1	beveiliging naar buiten (hackers en lekkers)	Klein	Groot
	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 bescherming (WBP, WPG, WSJG)	X	X						X	X	X	X		X		
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	X		X	X	X										

cameraplan															
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.