Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

29 754 Terrorismebestrijding

Nr. 389 **BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 24 juni 2016

1. Inleiding

In het Kamerdebat van 7 april jl. over de aanslagen in Brussel (Handelingen II 2015/16, nr. 74, items 2 en 7) bespraken wij de mogelijkheden van Nederlandse opsporings- en inlichtingendiensten om ten behoeve van terrorismeonderzoek gebruik te maken van gegevens van andere publieke of private organisaties, zoals telecomgegevens en camerabeelden. Ik zegde daarbij toe uw Kamer te zullen informeren over de mogelijkheden om in het kader van terrorismebestrijding deze gegevens te kunnen opvragen en te zullen nagaan of die mogelijkheden voor de Nederlandse diensten toereikend zijn om effectief op te kunnen treden.

Daarop heeft een inventarisatie plaatsgevonden, waarbij de volgende gegevens zijn betrokken:
- telefoon- en overige gegevens van internet- en telecommunicatiebedrijven
- reisgegevens;
- beelden van cameratoezicht;
- kentekenplaatherkenning (ANPR)-gegevens;
- financiële gegevens (pin- en creditcardgegeven).

In deze brief schets ik een aantal intensiveringen en maatregelen die ik, mede naar aanleiding van de tijdens het Kamerdebat gemaakte opmerkingen, heb genomen of in voorbereiding heb om ten behoeve van terrorismebestrijding gegevens voor opsporings- en inlichtingendoeleinden te kunnen bewaren en raadplegen. Het gaat om de volgende voorstellen:
- *Bewaarplicht van telecommunicatiegegevens*
  Een conceptwetsvoorstel is in procedure gebracht (Raad van State heeft advies uitgebracht), waarin aanvullende waarborgen worden voorzien voor de bewaring van bepaalde telecommunicatiegegevens voor de opsporing en vervolging van ernstige misdrijven. Het wetsvoorstel zal binnenkort aan uw Kamer worden voorgelegd.

kst-29754-389
ISSN 0921 - 7371
's-Gravenhage 2016

– *Reisgegevens*
  De Europese *PNR-richtlijn* verplicht de lidstaten om binnen twee jaar te regelen dat luchtvaartmaatschappijen PNR-gegevens verstrekken aan een in te richten passagiersinformatie-eenheid. Deze voorziening wordt met urgentie geïmplementeerd in de Nederlandse wetgeving.
– *Passagegegevens*
  Onderzocht wordt op welke wijze gegevens kunnen worden ontsloten voor de inlichtingen- en veiligheidsdiensten. Daarnaast is een wetsvoorstel bij uw Kamer aanhangig dat het mogelijk maakt om alle passagegegevens gedurende vier weken te bewaren; een tweede nota van wijziging zal op korte termijn worden ingediend.
– *Tegengaan anoniem gebruik van betaal-, bel- en simkaarten*
  In het Actieplan van de Europese Commissie ter versterking van de strijd tegen terrorismefinanciering is voorgesteld om de bepalingen uit de vierde Europese anti-witwasrichtlijn die betrekking hebben op het anonieme gebruik van *betaal-, bel- en simkaarten* aan te scherpen. Deze strengere regels worden met urgentie geïmplementeerd in de Nederlandse wetgeving.
– *Inlichtingenbevoegdheden*
  Het wetsvoorstel voor de nieuwe *Wet op de inlichtingen- en veiligheidsdiensten*, waarvan mijn ambtgenoot van BZK eerste ondertekenaar is, ligt momenteel ter advisering voor aan de Raad van State. Het wetsvoorstel introduceert onder andere nieuwe bevoegdheden voor de inlichtingen- en veiligheidsdiensten, waaronder de mogelijkheid van onderzoeksopdracht-gerichte interceptie in het kabelgebonden domein.

Ik licht deze voorstellen nader toe in paragraaf 2 van deze brief. Met deze aanpassingen worden de mogelijkheden verruimd om gegevens op te vragen en te bewaren ten behoeve van onderzoek naar onder andere terroristische activiteiten. Hiermee worden de mogelijkheden vergroot om sneller tot opheldering van strafbare feiten en tot aanhouding van verdachten te komen, ook waar het gaat om terrorisme.

Door de inbreng van vele leden van uw Kamer tijdens het debat van 7 april jl. voel ik mij gesteund in deze aanpak. Deze aanpak en de bijbehorende (voorgenomen) maatregelen zijn noodzakelijk om bij het voorkomen van aanslagen en bij de opsporing van strafbare feiten, gedragingen te zien of te ontdekken die van tevoren niet konden worden vastgesteld of redelijkerwijs konden worden voorzien. Dit geldt niet alleen voor onderzoek naar aan terrorisme gerelateerde misdrijven, maar ook bij de aanpak van criminaliteit en mensenhandel. In dergelijke gevallen kan dan bijvoorbeeld, dankzij raadpleging van bewaarde gegevens, gereconstrueerd worden waar (potentiële) daders zich ophouden of hoe hun reisbewegingen zijn (geweest). In combinatie met andere informatiebronnen kan het daardoor ook makkelijker worden om alsnog verblijfplaatsen te achterhalen en om zicht te krijgen op gehanteerde modi operandi. Ook kunnen zo eerder (nog niet bekende) contacten en/of medeplichtigen in beeld worden gebracht. Tenslotte kunnen zo ook afwijkende gedragingen of patronen in gedragingen rondom objecten van onze vitale infrastructuur beter in de gaten worden gehouden. Gelet op de inbreng van vele leden van uw Kamer tijdens het debat van 7 april jl. reken ik op uw steun voor en/of medewerking bij een voortvarende behandeling van de voorgestelde maatregelen.

Ik hecht dan ook zeer aan een voorspoedig verloop van de daarvoor benodigde procedures en zal alles in het werk stellen om de wijzigingen zo snel als mogelijk in werking te kunnen laten treden.

2. Intensivering van en maatregelen met betrekking tot de mogelijkheden om gegevens te raadplegen voor onderzoek

In de bijlage[1] treft u een overzicht aan van de huidige mogelijkheden om gegevens te bewaren en te raadplegen ter voorkoming van (o.a.) terroristische activiteiten en ten behoeve van opsporingsonderzoek. Hieronder wordt ingegaan op een aantal intensiveringen van en (voorgenomen) maatregelen met betrekking tot de mogelijkheden om gegevens voor opsporings- en inlichtingendoeleinden te bewaren en te raadplegen.

Dataretentie

De *Wet bewaarplicht telecommunicatiegegevens* voorziet in de bewaring van telefoon- en internetgegevens, specifiek ten behoeve van de opsporing en vervolging van ernstige criminaliteit. Deze wet vormde de implementatie van de Europese *richtlijn dataretentie*.

Nadat het Europese Hof van Justitie de *richtlijn dataretentie* met terugwerkende kracht ongeldig heeft verklaard, is sinds maart 2015 ook de *Wet bewaarplicht telecommunicatiegegevens* door de rechter buiten werking gesteld. De aanbieders zijn daardoor niet meer gehouden bepaalde telecommunicatiegegevens gedurende de wettelijke bewaartermijnen te bewaren ten behoeve van de opsporing en vervolging van ernstige strafbare feiten. Op dit moment mogen aanbieders gegevens alleen ten behoeve van eigen bedrijfsvoering bewaren. De termijn die ze daarvoor hanteren is voor de meeste gegevens een half jaar. De gegevens die de aanbieders voor de eigen bedrijfsvoering bewaren, kunnen door het Openbaar Ministerie op basis van het *Wetboek van Strafvordering* worden gevorderd.

Inmiddels is een conceptwetsvoorstel is in procedure gebracht (Raad van State heeft advies uitgebracht), waarin extra maatregelen worden voorgesteld om buiten twijfel te stellen dat de Wet bewaarplicht telecommunicatiegegevens in overeenstemming is met het Europees kader ten aanzien van de bescherming van de privacy. In het wetsvoorstel wordt een bewaartermijn voorgesteld van een half jaar voor internetgegevens en een jaar voor telefoniegegevens, inclusief bepaalde vormen van internettelefonie.

Reisgegevens

Luchtvaartmaatschappijen verzamelen zogenoemde «Passenger Name Record» (PNR)-gegevens voor hun eigen bedrijfsvoering. In het belang van een opsporingsonderzoek kunnen deze gegevens, op grond van het *Wetboek van Strafvordering*, door de officier van justitie bij de luchtvaartmaatschappijen worden gevorderd. De officier van justitie kan PNR-gegevens ook vorderen bij de Douane, voor zover deze beschikt over PNR-gegevens in het kader van haar goederencontroletaak.
De Koninklijke Marechaussee verkrijgt op basis van de Vreemdelingenwet 2000 zogenoemde «Advance Passenger Information» (API)-gegevens van bepaalde inkomende vluchten ten behoeve van de grensbewaking en het tegengaan van illegale immigratie.

De PNR-richtlijn, die op 4 mei jl. is gepubliceerd, verplicht de lidstaten om binnen twee jaar te regelen dat luchtvaartmaatschappijen PNR-gegevens verstrekken aan een in te richten passagiersinformatie-eenheid. Deze eenheid krijgt tot taak PNR-gegevens te verwerken ten behoeve van daartoe aangewezen instanties die bevoegd zijn om terroristische

[1] Raadpleegbaar via www.tweedekamer.nl

misdrijven of ernstige criminaliteit te voorkomen, op te sporen, te onderzoeken of te vervolgen. Ook zal worden voorzien in de uitwisseling van de gegevens tussen de passagiersinformatie-eenheden van de lidstaten en met Europol.

Ik ben voornemens om het wetsvoorstel dat nodig is voor de implementatie van de PNR-richtlijn begin 2017 bij uw Kamer in te dienen. In lijn met de verklaring die de JBZ-raad heeft uitgebracht op 4 december 2015 inzake de toepassing van de richtlijn op intra-EU-vluchten (Kamerstuk 32 317, nr. 375), zal het wetsvoorstel betrekking hebben op zowel extra- als intra-EU-vluchten. Reisbewegingen van buiten de EU vinden niet altijd rechtstreeks plaats naar de lidstaat van de eindbestemming, maar gaan ook indirect via andere lidstaten. Het opknippen van een reis via een andere lidstaat van de EU is een door criminelen vaker gebruikte methode om onopgemerkt te blijven. Het is daarom van groot belang ook inzicht te hebben in de reisbewegingen die binnen de EU plaatsvinden om zo zware criminelen en terroristen te kunnen onderkennen.

Om te borgen dat de samenwerking tussen de passagiersinformatie-eenheden zo optimaal mogelijk zal zijn, wordt als onderdeel van de CT-acties in de «Roadmap to enhance information exchange and information management including interoperability solutions in the Justice and Home Affairs area», die voorligt in de JBZ-raad van 9 en 10 juni, voorgesteld een operationele werkgroep in te richten waaraan in elk geval de hoofden van de (toekomstige) passagiersinformatie-eenheden deelnemen.

Kentekenplaatherkenning

Ook kentekenplaatherkenning (ANPR) levert een bijdrage aan de opsporing van misdrijven. ANPR is een effectief opsporingsmiddel om gericht te zoeken naar een bepaald voertuig. Naar verwachting beschikken eind dit jaar alle politie-eenheden over ANPR-camera's. Vanzelfsprekend zullen deze camera's ook voor de bestrijding van terrorisme worden ingezet voor zover de huidige wetgeving dat toelaat. In dat verband worden ook de mogelijkheden onderzocht die er zijn om ANPR-gegevens voor de AIVD te ontsluiten.

Momenteel wordt kentekenplaatherkenning ingezet bij de opsporing van misdrijven voor zover dat binnen de huidige wettelijke kaders is toegestaan. Daarvoor is in beginsel nodig dat het kenteken van een voertuig waarin de politie is geïnteresseerd, op een opsporingslijst wordt geplaatst. Dit kenteken wordt vergeleken met de kentekens van voertuigen die een camera passeren. De passagebeelden van die kentekens die overeenkomen met een kenteken op een opsporingslijst (de «hits») mogen bewaard worden voor de duur van het opsporingsonderzoek. Daarnaast is het binnen het huidige wettelijke kader toegestaan om onder bepaalde aanvullende omstandigheden (als de ernst van het feit dit rechtvaardigt en er sprake is van een nader van tevoren gedefinieerd doel en een specifiek gebied) gedurende een beperkte periode alle passagegegevens te bewaren, ook van voertuigen die niet op een opsporingslijst voorkomen. Thans bezie ik de concrete mogelijkheden om gedurende een beperkte periode en in relevante gebieden, bijvoorbeeld in grensstreken, passagegegevens te bewaren van kentekens die niet op opsporingslijsten voorkomen. Dit wordt momenteel nader uitgewerkt en met de politie en het openbaar ministerie besproken.

Het is evenwel nuttig en passend om deze bestaande bevoegdheid uit te breiden met een helder wettelijk kader op grond waarvan het mogelijk wordt om gedurende vier weken *alle* passagegegevens te bewaren, ook

van voertuigen die niet op een opsporingslijst voorkomen. Daarvoor is het *wetsvoorstel ANPR* van betekenis (Kamerstuk 33 542) dat een nieuw artikel in het Wetboek van Strafvordering (artikel 126jj) introduceert. Met behulp van dit wetsvoorstel kunnen gedurende vier weken alle passagegegevens worden bewaard, ook als er op het moment van vastlegging van de beelden nog geen concrete verdenking is. In geval van een voortvluchtige persoon kan de bewaarde informatie dan alsnog ter aanhouding van deze persoon worden geraadpleegd. Ook kan deze informatie worden geraadpleegd ter opsporing van verdachten van een misdrijf waarvoor een bevel voor voorlopige hechtenis kan worden gegeven, jegens wie pas een verdenking is gerezen nadat het misdrijf is gepleegd. De bevoegdheid om kentekens gedurende vier weken te kunnen bewaren biedt aldus de mogelijkheid om in een later stadium de gegevens te raadplegen ten behoeve van het oplossen van ernstige misdrijven of het aanhouden van voortvluchtige personen.

Dit wetsvoorstel is door mijn ambtsvoorganger in 2013 aan uw Kamer voorgelegd. Op 3 april 2014 heeft de eerste termijn van de mondelinge behandeling plaatsgevonden (Handelingen II 2015/16, nr. 71, items 4 en 7). De tweede termijn van de behandeling van het *wetsvoorstel ANPR* is door uw Kamer aangehouden vanwege de reactie van de regering op het arrest van het Hof van de Europese Unie tot ongeldigverklaring van de richtlijn dataretentie (*Kamerstuk* 33 542, nr. 16). In die reactie is een tweede nota van wijziging aangekondigd voor het *wetsvoorstel ANPR*, waarin zal worden bepaald dat de daartoe geautoriseerde opsporingsambtenaar de bewaarde kentekengegevens uitsluitend op bevel van de officier van justitie kan raadplegen.

In het licht van de gedachtewisseling met uw Kamer over de recente gebeurtenissen in Parijs en Brussel, komt het mij voor dat een spoedige hervatting van de behandeling van dit wetsvoorstel aangewezen is. Daartoe zal de betreffende tweede nota van wijziging bij het wetsvoorstel ANPR binnenkort aan uw Kamer worden voorgelegd.

Camerasysteem @migoboras

Het camerasysteem @migoboras van de koninklijke Marechaussee wordt ingezet ten behoeve van terrorismebestrijding bij het opvolgen van (politie)meldingen over terrorismeverdachten, de zogenaamde Quick Alerts. In samenspraak tussen de Koninklijke Marechaussee, politie en Openbaar Ministerie is een procedure opgesteld voor het aanzetten van het systeem ten behoeve van het inwinnen van passagedata na calamiteiten (waaronder aanslagen) met een groot maatschappelijke impact of belang, waarbij de mogelijkheid bestaat van grenspassage door betrokkenen/verdachten, zowel nationaal als internationaal (aangrenzende landen). Tot slot heeft de inzet van @migoboras voor de rechtshandhaving die sinds kort mogelijk is een meerwaarde bij de aanpak van terrorisme. Het signaleren en tegenhouden van uitreizigers die Nederland willen verlaten dan wel terugkeerders die vanuit het buitenland voet op Nederlandse bodem zetten kan met de hier boven omschreven inzet ondersteund worden.

Bij separate brief wordt u nader geïnformeerd over de ontwikkelingen rondom de inzet van het camerasysteem @migoboras voor de rechtshandhaving, mede ten behoeve van terrorismebestrijding.

Tegengaan terrorismefinanciering

Tegen de verschillende verschijningsvormen van de financiering van terrorisme kan met behulp van diverse strafbepalingen worden opgetreden (artikel 421 en artikel 140a van het Wetboek van Strafrecht en de Sanctiewet). Opsporingsdiensten en het openbaar ministerie komen bij elke verdenking van terrorismefinanciering in actie. Daarnaast is een belangrijke rol weggelegd voor de Financial Intelligence Unit-Nederland (FIU) die meldingen van ongebruikelijke transacties ontvangt van instellingen in de zin van de Wet ter voorkoming van witwassen en financieren van terrorisme en die bevoegd is gegevens te raadplegen om deze ongebruikelijke transacties nader te onderzoeken en deze gegevens te delen met opsporings- en inlichtingendiensten. Daarbij kan de FIU, wanneer een meldplichtige instelling (bijvoorbeeld een bank) een melding van een ongebruikelijke transactie doet of anderszins is betrokken bij die transactie ook om nadere informatie omtrent de betrokken persoon/ entiteit vragen. Momenteel maken FIU en politie structurele afspraken om sneller te kunnen schakelen met politiegegevens voor terrorismebestrijding.

Analyse van de financiering van de aanslagen in Parijs toonde het gebruik aan van prepaid cards. Ik vind dan ook dat er een eind moet komen aan het anonieme gebruik van dergelijke kaarten. In het Actieplan ter versterking van de strijd tegen terrorismefinanciering van de Europese Commissie is mede om die reden voorgesteld om de bepalingen uit de vierde anti-witwasrichtlijn die betrekking hebben op prepaid cards, opnieuw te bezien en aan te scherpen. Het gaat hierbij om alle vormen van prepaid cards, zoals creditcards, cadeaukaarten en sim-kaarten.

Doelstelling van het Actieplan is het intensiever bestrijden van de financiering van terrorisme door bestaande EU-regels aan nieuwe dreigingen aan te passen en het beleid en de praktijken in overeenstemming te brengen met internationale normen. Het gaat daarbij onder meer om wijzigingen van de vierde anti-witwasrichtlijn die gericht zijn op:
– strengere normen inzake prepaid (betaal-, bel- en sim-) cards;
– invoering van centrale registers van bank- en betaalrekeningen of centrale systemen voor ontsluiting van bankgegevens;
– toegang door financiële inlichtingeneenheden tot de gegevens uit deze centrale registers of systemen en
– intensievere gegevensuitwisseling tussen FIU's.

De vierde anti-witwasrichtlijn wordt geïmplementeerd in de Wet ter voorkoming van witwassen en financieren van terrorisme.

Verkend wordt ook aanpassing van Verordening 1889/2005, onder meer om de bevoegdheden van de Douane uit te breiden tot het controleren van cash geld in post en vracht. Nu bestaat die bevoegdheid alleen als personen cash geld in- of uitvoeren.

Een aanscherping van normen met betrekking tot vooraf betaalde instrumenten zoals prepaid cards kan gevolgen hebben voor in het bijzonder de telecomsector en retailsector, omdat prepaid kaarten in deze sectoren regelmatig worden gebruikt. Het is daarbij zaak dat risico's op onder meer financieren van terrorisme effectief worden tegengegaan maar dat tegelijkertijd een eventuele aanscherping van maatregelen zo wordt ingericht dat administratieve lasten zo beperkt mogelijk blijven en de voordelen niet teniet worden gedaan. Datzelfde geldt voor het bestrijden van illegaal grensoverschrijdend vervoer van cash geld. Voor beide trajecten geldt dat bezien zal worden hoe de te treffen maatregelen effectief zijn voor het tegengaan van het financieren van terrorisme,

terwijl tegelijkertijd gezorgd wordt dat de sector en de gebruikers niet onevenredig worden belast.

Bevoegdheden inlichtingen en veiligheidsdiensten

Het wetsvoorstel voor de nieuwe *Wet op de inlichtingen- en veiligheidsdiensten*, waarvan mijn ambtgenoot van BZK eerste ondertekenaar is, ligt momenteel ter advisering voor aan de Raad van State. Deze wet levert na inwerkingtreding op dat de bevoegdheden van de inlichtingen- en veiligheidsdiensten worden gemoderniseerd en dat er wettelijke waarborgen voor inzet van die bevoegdheden nauwgezet worden vastgelegd. Met dit wetsvoorstel krijgen de inlichtingen- en veiligheidsdiensten onder andere de bevoegdheid om zogenoemde onderzoeksopdrachtgerichte interceptie te verrichten in het kabelgebonden domein.

3. Afsluiting

In het voorgaande heb ik, conform mijn toezegging, op een rij gezet op welke wijze ik voornemens ben een aantal regelingen die betrekking hebben op het bewaren en raadplegen van gegevens voor opsporings- en inlichtingendoeleinden aan te passen.

Zoals ik aangaf worden met deze aanpassingen de mogelijkheden verruimd om gegevens op te vragen en te bewaren ten behoeve van onderzoek naar onder andere terroristische activiteiten. Ik hecht dan ook zeer aan een voorspoedig verloop van de daarvoor benodigde procedures.

De Minister van Veiligheid en Justitie,
G.A. van der Steur

Bijlage

Huidige mogelijkheden om gegevens te raadplegen

Voor zover in de brief waar deze bijlage toe behoort, daar al niet – ter introductie van nieuwe ontwikkelingen – op in is gegaan, bevat deze bijlage een overzicht aan van de huidige mogelijkheden om gegevens te raadplegen ter voorkoming van (o.a.) terroristische activiteiten en ten behoeve van opsporingsonderzoek.

A. Algemeen

Opsporingsbevoegdheden

Het OM kan gegevens van onder andere aanbieders van telecom- en internetbedrijven vorderen op basis van het *Wetboek van Strafvordering* / de *Wet bevoegdheden vorderen gegevens*. Op basis hiervan heeft het OM bevoegdheden waarmee (rechts)personen kunnen worden verplicht bepaalde opgeslagen of vastgelegde gegevens te verstrekken. Daarbij is sprake van drie domeinen:
– de bijzondere bevoegdheden tot opsporing.
– de bijzondere bevoegdheden tot opsporing voor het onderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband;
– de bijzondere bevoegdheden tot opsporing van terroristische misdrijven.

Afgezien van het verschillend toepassingsbereik zijn de drie domeinen inhoudelijk vrijwel gelijk.

Kern van de drie domeinen is de getrapte vordering van opgeslagen of vastgelegde gegevens:
– de opsporingsambtenaar kan ingeval van verdenking van een misdrijf de mogelijkheid identificerende gegevens vorderen;
– de officier van justitie mag in geval van verdenking van een misdrijf waarvoor een bevel voor voorlopige hechtenis kan worden gegeven, ook andere dan identificerende gegevens, met uitzondering van gevoelige gegevens, vorderen;
– bij misdrijven die een ernstige inbreuk op de rechtsorde opleveren, kan de officier van justitie, met machtiging van de rechter-commissaris, ook gevoelige gegevens vorderen;

Het als tweede genoemde domein gaat uit van dezelfde driedeling, zij het dat voor de toepassing van deze bevoegdheden sprake moet zijn van een geval waarin «uit feiten of omstandigheden een redelijk vermoeden voortvloeit dat in georganiseerd verband misdrijven waarvoor een bevel voor voorlopige hechtenis kan worden gegeven, worden beraamd of gepleegd die gezien hun aard of de samenhang met andere misdrijven die in dat georganiseerd verband worden beraamd of gepleegd een ernstige inbreuk op de rechtsorde opleveren». In het derde domein moet sprake zijn van «aanwijzingen van een terroristisch misdrijf».

Voor de drie domeinen kent de wet daarnaast nog een aantal aanvullende bevoegdheden, onder andere:
– de officier van justitie kan de vordering in bepaalde gevallen ook aanwenden voor toekomstige gegevens of kan de directe verstrekking van toekomstige gegevens te vorderen;
– de vorderingen tot het verstrekken van identificerende gegevens, andere dan identificerende gegevens en toekomstige gegevens kunnen ook worden gericht tot de aanbieder van een openbare telecommunicatiedienst;
– de mogelijkheid de bevriezing van gegevens te vorderen (art. 126ni en 126ui).

De richtlijn gegevensbescherming, die op 14 april 2016 is aangenomen door het Europees Parlement, bevat regels voor het gebruik van gegevens door rechtshandhavingsinstanties bij het voorkomen, onderzoeken, opsporen en vervolgen van wetsovertredingen, of de uitvoering van straffen – inclusief het voorkomen van gevaar voor de openbare orde en veiligheid. De richtlijn is ook van toepassing op de gegevensuitwisseling voor deze doeleinden met andere EU-landen en stelt – voor het eerst – minimum standaarden voor gebruik van persoonlijke gegevens door de opsporingsdiensten in elke lidstaat. De samenwerking tussen de rechtshandhavingsinstanties van de lidstaten wordt, ook bij terrorismebestrijding, door deze standaarden makkelijker en efficiënter.

Op de verwerkingen (van politie-, justitiële en overige) gegevens zijn de regimes van toepassing van de Wet politiegegevens, de Wet bescherming persoonsgegevens en de Wet justitiële en strafvorderlijke gegevens.

Inlichtingenbevoegdheden

Om dreigingen tegen de nationale veiligheidsbelangen tijdig te onderkennen, kunnen de inlichtingendiensten onder andere gegevens opvragen bij aanbieders van openbare telecommunicatienetwerken en openbare telecommunicatiediensten. Doordat de huidige wet niet techniekonafhankelijk is terwijl de technologie zich onmiskenbaar heeft ontwikkeld, wordt de taakuitvoering van de diensten op dit ogenblik ernstig belemmerd zonder dat dit destijds de bedoeling van de wetgever was.

B. Opsporing specifiek

Voor zover er rondom gegevens bijzondere regiems gelden, worden deze hieronder toegelicht.

Reisgegevens

PNR-gegevens worden door de luchtvaartmaatschappijen verzameld en gebruikt voor hun eigen bedrijfsvoering. In het belang van een opsporingsonderzoek kunnen deze gegevens, op grond van het Wetboek van Strafvordering, door de officier van justitie bij de luchtvaartmaatschappijen worden gevorderd. De officier van justitie kan PNR-gegevens ook vorderen bij de Douane, voor zover deze beschikt over PNR-gegevens in het kader van haar goederencontroletaak. Een vordering bij de Douane kan via de technische voorziening TRIP op geautomatiseerde wijze worden uitgevoerd.

De KMar verkrijgt op basis van de Vreemdelingenwet 2000 (Vw) API-gegevens van bepaalde inkomende vluchten ten behoeve van de grensbewaking en het tegengaan van illegale immigratie. Het gebruik van API-gegevens is mogelijk voor de toepassing van artikel 14 van de Schengengrenscode op grond waarvan toegangsweigering van onderdanen van derde landen kan plaatsvinden, omdat niet is voldaan aan de voorwaarden die zijn neergelegd in artikel 6, eerste lid, onder d en e, van de Schengengrenscode (SIS-signalering of nationale signalering vanwege bedreiging voor de openbare orde, de volksgezondheid of de nationale veiligheid). Ook is het gebruik van API-gegevens mogelijk op grond van artikel 3, aanhef en eerste lid, onder b, van de Vw. Op grond van deze bepaling is toegangsweigering mogelijk bij gevaar voor de openbare orde of de nationale veiligheid in de gevallen die niet onder de Schengengrenscode vallen (zoals bij EU-burgers).

Camerasysteem @migoboras

De Koninklijke Marechaussee zet het camerasysteem @migoboras in ter ondersteuning van het Mobiel Toezicht Veiligheid (MTV). Met MTV wordt beoogd illegaal verblijf na grensoverschrijding, mensensmokkel, en document- en identiteitsfraude in een zo vroeg mogelijk stadium te bestrijden. Het systeem @migoboras bestaat uit vaste en mobiele camera's geplaatst aan de doorgaande hoofdwegen in het grensgebied met België en Duitsland. Het systeem wordt ingezet voor analyse ten behoeve van het opstellen van toezichtsprofielen, het observeren en selecteren voor stilhouden van voertuigen (aan de hand van waarneming van de kentekenplaat, de snelheid, tijd en plaats van de voertuigpassage) en assistentie bij het opvolgen van (politie)meldingen. Kentekens en kenmerken van voertuigen worden enkel voor de duur van de MTV-controle bewaard ten behoeve van het stilhouden van het betreffende voertuig. De gegevens worden daarna vernietigd.