Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

32 761 Verwerking en bescherming persoonsgegevens

Nr. 173 **BRIEF VAN DE MINISTER VOOR RECHTSBESCHERMING**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 19 november 2020

Een veilige en rechtvaardige samenleving vraagt om een overheid die zorgt voor de handhaving van de openbare orde, het voorkomen, onderzoeken, opsporen, vervolgen van strafbare feiten en de tenuitvoerlegging van opgelegde straffen en maatregelen. Voor een goede uitvoering van deze taken, is het noodzakelijk om persoonsgegevens te verwerken, zoals het verzamelen, opslaan en delen ervan. Bij de verwerking van persoonsgegevens moet de overheid zorgvuldigheid betrachten en niet meer inbreuk maken op de persoonlijke levenssfeer van burgers dan noodzakelijk is voor een goede uitvoering van de taak. De Wet justitiële en strafvorderlijke gegevens (Wjsg, uit 2002) en de Wet politiegegevens (Wpg, uit 2007) vormen samen een belangrijk onderdeel van het wettelijk kader voor de verwerking van persoonsgegevens in het politie- en justitiedomein. Dat wettelijk kader is aan vernieuwing toe.

In het domein van de rechtshandhaving worden veel persoonsgegevens verwerkt. De aard van deze gegevens is zeer divers. Het kan gaan om de gegevens van een slachtoffer dat aangifte doet van een strafbaar feit, maar ook van mensen die meldingen doorgeven, observaties van wijkagenten, camerabeelden van passanten in de openbare ruimte, verklaringen van getuigen en vanzelfsprekend ook gegevens over verdachten van een strafbaar feit, procesgegevens en gegevens van veroordeelde personen die hun straf uitzitten. Zonder deze gegevens te verwerken kunnen de betrokken organisaties hun wettelijke taken niet uitvoeren.

Sinds de invoering van beide wetten is het nodige veranderd in de samenleving waardoor de huidige wetten niet meer goed aansluiten op de realiteit van vandaag en morgen. Niet veranderd is dat het gaat om gevoelige data waar zeer zorgvuldig mee om moet worden gegaan. Dit geldt voor gegevens over verdachten en veroordeelden, maar temeer ook al die gegevens die geen vastgestelde feiten zijn: een groot deel van de gegevens bestaat bijvoorbeeld uit waarnemingen van opsporingsambtenaren. Wel genereren burgers, private en publieke organisaties veel meer

kst-32761-173
ISSN 0921 - 7371
's-Gravenhage 2020

gegevens dan 15 tot 20 jaar geleden. Dit vraagt om een wet die de mogelijkheden van de hoeveelheid gegevens die beschikbaar zijn voor de taakuitvoering optimaal benut, maar ook om een wet die zorgt voor passende waarborgen voor de bescherming van de persoonlijke levenssfeer. Daarnaast is op het gebied van gegevensverwerking steeds meer mogelijk met de inzet van moderne technologieën. Gedacht kan bijvoorbeeld worden aan de inzet van artificiële intelligentie die ervoor zorgt dat beelden van kindermisbruik worden geanalyseerd om zo achter verblijfplaatsen en daders te komen. Of aan gezichtsherkenningstechnologie. Verduidelijking van het wettelijk kader op dit punt is gewenst. Veranderd is ook de aanpak van veiligheidsproblemen in de samenleving. Er wordt steeds meer samengewerkt met andere domeinen zoals de zorg, gemeenten en het onderwijs. Om te kunnen komen tot een integrale aanpak is het noodzakelijk dat met andere domeinen gegevens worden uitgewisseld. Het wettelijk kader voor de verstrekking van gegevens vanuit het politie- en justitiedomein aan andere domeinen is ingewikkeld, en wordt ook zo ervaren in de praktijk. Dat leidt ertoe dat niet in alle gevallen optimaal gebruik wordt gemaakt van de mogelijkheden die de wet reeds biedt tot uitwisseling van gegevens. Het risico is dat het wettelijk kader en de realiteit steeds verder uit elkaar gaan lopen. Dit komt een effectieve taakuitvoering en de bescherming van de persoonlijke levenssfeer niet ten goede. Het moet voor de uitvoeringspraktijk duidelijker worden wanneer gegevens kunnen worden gedeeld en wanneer niet, zonder de noodzakelijke waarborgen ter bescherming van de persoonlijke levenssfeer te verliezen. Tot slot sluiten de Wpg en Wjsg niet goed op elkaar aan. Dat draagt niet bij aan een eenduidige gegevensverwerking binnen het politie- en justitiedomein. Ook om de samenwerking op het gebied van bijvoorbeeld digitalisering te verstevigen is het noodzakelijk om beide wetten in onderling verband te herzien. Een uniform wettelijk kader maakt het immers mogelijk dat ontwikkelde digitale toepassingen eenvoudig domein overstijgend kunnen worden gebruikt.

De evaluaties van beide wetten tonen de noodzaak van herziening duidelijk aan, zoals uiteengezet in een brief van de Minister van Veiligheid en Justitie uit 2014.[1] De herziening kon na de aankondiging in 2014 niet direct worden opgepakt omdat moest worden gewacht op de totstandkoming van EU-regelgeving op het gebied van persoonsgegevens (de AVG en de Richtlijn gegevensbescherming opsporing en vervolging 2016/680[2] (hierna: de richtlijn)) en de implementatie daarvan. Nu de implementatie van de richtlijn in de Wpg en Wjsg is afgerond, is, zoals destijds al toegezegd, dit het moment om verder te kijken naar de toekomst. De richtlijn is een belangrijk uitgangspunt voor het toekomstig wettelijk kader.

De ambitie is om te komen tot een nieuw wettelijk kader voor gegevensverwerking in het politie- en justitiedomein dat bijdraagt aan een effectieve taakuitvoering, goede samenwerking in de strafrechtketen en ook met de partners daarbuiten en een goede bescherming van de persoonlijke levenssfeer van burgers.

---

[1] Kamerbrief Evaluatie Wet politiegegevens en Wet justitiële en strafvorderlijke gegevens, Kamerstuk 33 842, nr. 2.

[2] Richtlijn betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (Richtlijn 2016/680 van 27 april 2016, Pb EU L 119/89).

Ik ben gestart met een verkenning naar uitgangspunten voor een toekomstig wettelijk kader en een inventarisatie van de onderwerpen waarop stappen gezet moeten worden. In het kader van deze verkenning zijn gesprekken gevoerd met verschillende partijen waaronder de partijen uit de strafrechtketen, de Autoriteit Persoonsgegevens en een aantal maatschappelijke organisaties en partijen die dicht tegen de strafrechtketen aan werken. Naast de reeds beschikbare rapporten over dit onderwerp heb ik het WODC gevraagd een rechtsvergelijkend onderzoek uit te voeren naar het wettelijk regime in vijf EU-lidstaten. Ik verwacht dat dit onderzoek dit jaar zal worden afgerond. De uitkomsten daarvan neem ik mee in het vervolgtraject. Het verder uitwerken van de genoemde onderwerpen en deze uitgangspunten tot een toekomstig wettelijk kader voor de verwerking van politiële, justitiële en strafvorderlijke gegevens, gerechtelijke strafgegevens en tenuitvoerleggingsgegevens is geen sinecure en zal in meerdere stappen worden uitgevoerd.

In deze brief schets ik – mede namens de Ministers van Justitie en Veiligheid en Defensie – de opbrengst van mijn verkenning en het verdere proces. Allereerst zal ik daarbij de algemene uitgangspunten toelichten voor een toekomstig wettelijk kader, vervolgens ga ik in op een aantal specifieke onderwerpen die aan bod zijn gekomen tijdens de verkenning.

1. Algemene uitgangspunten

Om tot een toekomstig wettelijk kader voor gegevensverwerking in het politie- en justitiedomein te komen, is een aantal algemene uitgangspunten van belang. Deze uitgangspunten dienen als een leidraad voor de uitwerking van de specifieke onderwerpen.

Effectieve taakuitvoering en bescherming persoonsgegevens

Het toekomstig wettelijk kader zal, net als de Wpg en de Wjsg, ten dienste staan van een effectieve taakuitvoering van de bevoegde autoriteiten en een goed functionerende strafrechtketen. Voor een doeltreffende taakuitvoering is het van groot belang dat het wettelijk kader daarbij adequate waarborgen biedt voor de bescherming van de persoonlijke levenssfeer. Kernpunt is dat verwerkingen noodzakelijk en proportioneel moeten zijn, want dat komt én de effectieve taakuitvoering en de bescherming van de persoonlijke levenssfeer ten goede. Deze balans volgt niet enkel uit regelgeving, maar moet ook in de praktijk dagelijks gevonden worden.

In overeenstemming met het geldende internationale en EU-recht

Vanzelfsprekend zal het nieuwe wettelijk kader moeten voldoen aan de eisen die voortvloeien uit de richtlijn. Er wordt zo veel mogelijk aangesloten bij de begrippen en systematiek zoals in die richtlijn zijn opgenomen. Daarnaast moet het wettelijk kader uiteraard in overeenstemming zijn met geldende mensenrechtelijke en grondwettelijke eisen en aansluiten bij andere Europese regelgeving zoals de AVG.[3] Bovendien zal aangesloten worden bij ontwikkelingen in EU-verband o.a. ten aanzien van privacy en regulering van het gebruik van artificiële intelligentie.

[3] Hierbij valt te denken aan EVRM, de Europol en Eurojust verordeningen, de verordeningen in het kader van Grenzen en Veiligheid, de ontwikkelingen rond het Europees OM (EOM), het Europees Arrestatiebevel (EAB), de ECRIS-richtlijn, de ECRIS-TCN-Verordening en telecommunicatie/dataretentiewetgeving.

Nalevingsvriendelijk: verduidelijken en vereenvoudigen

Het toekomstig wettelijk kader moet nalevingsvriendelijk zijn. Daarvoor is het belangrijk dat het wettelijk kader aansluit bij de (toekomstige) realiteit van de praktijk en duidelijkheid biedt. Een wens tot verduidelijking is er bijvoorbeeld voor bepaalde verwerkingen die gepaard kunnen gaan met een meer dan geringe inbreuk op de persoonlijke levenssfeer. Hierbij kan bijvoorbeeld gedacht worden aan de diverse varianten van camerabeelden gemaakt in de publieke ruimte; voor de verwerking van bijvoorbeeld ANPR en gegevens afkomstig van gemeentecamera's en bodycams zijn in de loop van de tijd van elkaar afwijkende waarborgen ontwikkeld waardoor naleving ingewikkelder is dan nodig. Daarnaast zijn enkele termen die worden gehanteerd in de wetten onduidelijk en sluiten niet aan bij de praktijk, gedacht kan worden aan de termen «geautomatiseerd vergelijken» en «in combinatie verwerken». Tegelijkertijd moet de wet ook vereenvoudigd worden met als doel ruimte te laten voor ontwikkelingen die per organisatie of taak anders kunnen zijn, de wet moet dus niet te rigide zijn. Vereenvoudigen leidt echter niet altijd tot meer duidelijkheid en omgekeerd; hier moet een balans in gevonden worden.

Toekomstbestendig

Het wettelijk kader moet niet enkel op de korte termijn toepasbaar zijn, maar ook verder in de toekomst. Dit maakt dat de wet niet te veel geënt moet zijn op de huidige praktijk, de technologische mogelijkheden en de huidige staat van veiligheid in ons land, maar rekening moet houden met veranderingen in de toekomst. Techniekonafhankelijk wetgeven zal dan ook een belangrijk thema zijn. Het toekomstig wettelijk kader zal bijvoorbeeld ruimte moeten bieden voor de ontwikkeling van digitaal procederen in de strafrechtketen, maar ook moeten passen op de realiteit van vandaag.

2. Specifieke onderwerpen

Een aantal specifieke onderwerpen is tijdens de verkenning door meerdere partijen benadrukt en moet in de stappen die volgen dan ook expliciet worden meegenomen. Hieronder licht ik de meest in het oog springende onderwerpen uit.

Toepassingsbereik toekomstig wettelijk kader

Er wordt opnieuw gekeken naar de organisaties die onder het toekomstig wettelijk kader hun gegevens gaan verwerken, de zogenoemde bevoegde autoriteiten.[4] De organisaties en functionarissen die als bevoegde autoriteiten opereren zijn politie, Koninklijke Marechaussee, Rijksrecherche, bijzondere opsporingsdiensten, buitengewoon opsporingsambtenaren, Openbaar Ministerie, Rechtspraak, Hoge Raad, Centraal Justitieel Incasso Bureau, Dienst Justitiële Inrichtingen, Justitiële Informatiedienst en Financiële Inlichtingen Eenheid. Deze partijen verwerken gegevens momenteel onder het regime van de Wpg en/of de Wjsg. Een aantal andere partijen in de strafrechtketen verwerkt persoonsgegevens onder het regime van de AVG. Ik ben met hen in gesprek, om te bezien of zij in het toekomstig wettelijk kader als bevoegde autoriteit, in de zin van de richtlijn, moeten worden aangemerkt. Indien dat bijdraagt aan een betere aansluiting op de gegevensverwerking in de strafrechtketen en meer duidelijkheid biedt, dan ben ik daar een voorstander van. Het gaat hierbij bijvoorbeeld om het Nederlands Forensisch Instituut en de reclasserings-

[4] Bevoegde autoriteit zoals bedoeld in artikel 3, lid 7 van de richtlijn gegevensbescherming opsporing en vervolging.

organisaties. Tegelijkertijd ben ik ook gebonden aan de kaders van de richtlijn. Verwerkingen van persoonsgegevens bij bijvoorbeeld bestuursrechtelijke beslissingen (zoals vergunningsverlening en vreemdelingentoezicht) vallen niet onder de reikwijdte van deze richtlijn en blijven dus ook buiten het toepassingsbereik van het toekomstig wettelijk kader.

Delen van gegevens

Een ander belangrijk onderwerp is het delen van gegevens. Er wordt steeds meer gewerkt vanuit een integrale aanpak, waarbij niet enkel de vervolging van strafbare feiten of de tenuitvoerlegging centraal staat, maar bijvoorbeeld ook het voorkomen van strafbare feiten waarbij gemeenten, zorgpartners of onderwijsinstellingen een belangrijke rol kunnen spelen. Om dit mogelijk te maken moet een zorgvuldige uitwisseling van gegevens mogelijk zijn. Dit betreft zowel het delen van gegevens binnen het politie- en justitiedomein, als het delen met samenwerkingspartners in andere domeinen en het buitenland. Enerzijds is de gegevensdeling noodzakelijk om maatschappelijke vraagstukken op te lossen, maar anderzijds betreffen het hier gevoelige gegevens over onder andere verdachten, melders, getuigen en (overleden) slachtoffers en soms ook onbekende betrokkenen. Daarnaast is er vaak sprake van vastlegging van waarnemingen, en niet altijd van vastgestelde feiten. Die gegevens moeten dan ook als zodanig behandeld worden. Er moet worden verkend op welke wijze het uitwisselen van gegevens zorgvuldig kan plaatsvinden. Er wordt daarbij onderscheid gemaakt tussen het delen van gegevens tussen bevoegde autoriteiten en het delen van gegevens met andere instanties dan bevoegde autoriteiten binnen Nederland, alsmede een onderscheid tussen landen uit de Europese Unie en «derde landen» bij het verwerken van gegevens buiten Nederland. Het algemene uitgangspunt «nalevingsvriendelijk» is hier bij uitstek op van toepassing. De huidige regels worden als niet passend bij de praktijk, te ingewikkeld en multi-interpretabel beschouwd.

Ruimte voor inzet van innovatieve technologieën

Het kabinet heeft eerder al aangegeven dat moderne vormen van gegevensverwerking kansen bieden voor het bevorderen van de veiligheid in Nederland.[5] Denk hierbij aan het inschatten van risico's om tijdig preventieve maatregelen te treffen, het inzichtelijk maken hoe criminelen te werk gaan, het *real time* volgen van ontwikkelingen in crisissituaties of de mogelijkheden voor *crowd control* bij grootschalige manifestaties. Zoals gezegd hoort daar de bescherming van de persoonlijke levenssfeer en persoonsgegevens hand in hand bij. Uw Kamer is eerder geïnformeerd over mogelijke wettelijke waarborgen bij het verwerken van data[6], daarnaast is onder meer een Strategisch Actieplan voor AI[7] gepresenteerd. Ook de ontwikkelingen binnen de Europese Unie op dit onderwerp worden door mijn departement op de voet gevolgd. Algemene grondslagen en waarborgen voor de inzet van deze technologieën dienen, vertaald naar het politie- en justitiedomein, een goede plek te krijgen in het toekomstig wettelijk kader. Hierbij wordt opgemerkt dat de waarborgen die zullen worden gesteld voor innovatieve technologieën in het toekomstig wettelijk kader niet identiek zullen zijn aan die bij andere sectoren, vanwege het belang van heimelijkheid en geheimhouding die

---

[5] Kamerstuk Kabinetsreactie op WRR-rapport big data in een vrije en veilige samenleving, Kamerstuk 26 643, nr. 426.

[6] Kamerbrief Waarborgen tegen risico's van data-analyses door de overheid, Kamerstuk 26 643, nr. 641.

[7] Kamerbrief Strategisch Actieplan voor Artificiële Intelligentie, Kamerstuk 26 643 nr. 640.

nodig kunnen zijn in het veiligheidsdomein. De eisen die de richtlijn stelt zullen leidend zijn.

Bewaren van gegevens

Er moeten ook stappen worden gezet op het vraagstuk rondom het bewaren van en toegankelijkheid tot gegevens. Bekend is dat de huidige wettelijke bewaartermijnen in sommige gevallen tekort schieten voor een goede taakuitvoering, te denken valt aan het onderzoeken van cold cases[8] of het behandelen van tot herziening van een onherroepelijke veroordeling en verzoeken om nader onderzoek naar het bestaan van gronden voor de herziening van een onherroepelijke veroordeling. Daarnaast sluiten bewaartermijnen niet op elkaar aan en zijn ze ingewikkeld om in de praktijk toe te passen. Tegelijkertijd is het niet wenselijk dat gegevens oneindig bewaard blijven, dit zou een niet noodzakelijke en niet proportionele inbreuk op de persoonlijke levenssfeer van de betrokkene(n) zijn. Het is van belang dat we als samenleving nadenken en in gesprek gaan over de keuzes die we op dit soort thema's willen maken.

Zoals reeds aangekondigd bij de reactie op de wetsevaluaties[9], moet het uitgangspunt van de regelgeving de noodzaak van het gebruik van gegevens zijn. In de huidige regulering staan de bewaartermijnen te veel centraal, dit moeten gebruikstermijnen worden. De noodzaak van het gebruik van gegevens voor een gerechtvaardigd doel moet centraal staan. Uit deze gebruikstermijnen volgt wanneer de gegevens moeten worden vernietigd. Voor een zwaarwegend doel, zoals het onderzoeken van cold cases bij ernstige misdrijven, moeten gegevens lange tijd kunnen worden gebruikt. Voor andere doelen, bijvoorbeeld de handhaving van de openbare orde, kan en moet die termijn veel korter zijn. Deze gedachte die in 2014 reeds werd aangekondigd wordt in de komende periode verder verkend en uitgewerkt.

Eenduidige waarborgen en toezicht

De Wpg en Wjsg kennen niet hetzelfde stelsel van toezicht en controle. Zo kent de Wpg een uitgebreid systeem van interne en externe audits terwijl in de Wjsg geen auditverplichting is opgenomen. In het toekomstig wettelijk kader zal dit gelijkgetrokken worden. Hetgeen de richtlijn voorschrijft op het gebied van toezicht en de rechten van de betrokkene geldt uiteraard onverkort. Daarnaast wordt gekeken op welke punten aanvullingen of veranderingen nodig en wenselijk zijn in het Nederlandse stelsel. In dit kader wordt bijvoorbeeld gekeken naar een aantal soorten gegevens waarvoor nu aanvullende regels ter bescherming van de persoonlijke levenssfeer gelden, zoals gegevens die zijn verkregen door cameratoezicht en ANPR. Onderzocht wordt in hoeverre de aanvullende regels die specifiek voor deze toepassingen in wet zijn opgenomen kunnen worden geüniformeerd met overige verwerkingen van persoonsgegevens, zonder het huidige niveau van bescherming te verlagen.

Hierbij wordt gestreefd naar een sluitende set aan waarborgen, effectief toezicht op de naleving van het toekomstig wettelijk kader waarbij het intern en extern toezicht goed op elkaar aansluiten.
Daarbij moet uiteraard wel rekening worden gehouden met de bijzondere eisen op het gebied van onafhankelijkheid van enkele organisaties.

---

[8] Kamerbrief Aanpak van cold cases, Kamerstuk 29 628 nr. 859.
[9] Kamerbrief Evaluatie Wet politiegegevens en Wet justitiële en strafvorderlijke gegevens, Kamerstuk 33 842, nr. 2, p. 1–3.

Verkrijgen van gegevens

De bevoegdheid tot het verkrijgen van gegevens is in andere wetten dan de Wpg en Wjsg geregeld. Het gaat dan met name om het Wetboek van Strafvordering, maar ook de Gemeentewet (camerabeelden) en de Politiewet 2012 regelen bevoegdheden voor het verkrijgen van gegevens. Ook het toekomstig wettelijk kader zal enkel zien op de verdere verwerking van verkregen gegevens.

Wel moet worden geconstateerd dat er steeds meer persoonsgegevens gegenereerd worden over menselijke aanwezigheid en gedrag in de publieke ruimte. Dergelijke gegevens kunnen van groot belang zijn voor de openbare veiligheid en de voorkoming van strafbare feiten. Omdat de vraag onder welke voorwaarden gegevens mogen worden verwerkt, verweven is met de vraag onder welke voorwaarden ze mogen worden verzameld, komt dit onderwerp ook naar voren in de gesprekken die worden gevoerd over het vernieuwd wettelijk kader. Deze opmerkingen worden verzameld.

Regelgeving BES

In de gesprekken die de afgelopen tijd zijn gevoerd, is door verschillende partijen gevraagd om aandacht te besteden aan het wettelijk kader dat geldt op Bonaire, Sint Eustatius en Saba (BES), hierna Caribisch Nederland. In dit kader is het van belang dat de richtlijn niet van toepassing is op de gegevensverwerking in Caribisch Nederland en in de Caribische landen. De huidige Wpg bevat een wettelijke regeling die geldt op de BES maar die beperkt is tot de gegevensverwerking in het politiedomein. Zoals ik in mijn brief van 13 maart jl.[10] heb aangegeven, onderschrijf ik het belang van een goed gegevensbeschermingsregime in Caribisch Nederland en de Caribische Landen. De sociaalgeografische verbinding tussen Caribisch Nederland en de Caribische landen brengt met zich mee dat harmonisatie van het gegevensbeschermingsniveau uitermate wenselijk is. Om die reden heeft het Justitieel Vierpartijen Overleg (hierna: JVO) in juli 2018 besloten tot een verkenning naar de vraag of harmonisatie mogelijk is, en zo ja, wat daarvoor nodig is. Een soortgelijke verkenning is uitgevoerd met het oog op de doorgifte van politie- en justitiegegevens aan Caribisch Nederland en de Caribische Landen. Ook hieruit komt naar voren dat harmonisatie binnen het politie- en justitiedomein gewenst en noodzakelijk is. Een gezamenlijk traject in Koninkrijksverband gericht op het gegevensbeschermingsniveau in Caribisch Nederland en in de Caribische Landen heeft daarbij de voorkeur en is ook de inzet van het kabinet. Daarover zal in het eerstvolgende JVO nader overleg en het vervolg van dit traject plaatsvinden. Over de uitkomsten van dat overleg wordt uw Kamer separaat geïnformeerd.

Lopende trajecten

Het aansluiten bij lopende trajecten is ook van groot belang. Zo is er de afgelopen jaren hard gewerkt aan de modernisering van het Wetboek van Strafvordering en de digitalisering van de strafrechtketen.[11] In 2018 werd de Minister van Justitie en Veiligheid geadviseerd[12] om te bewerkstelligen dat het nieuwe Wetboek van Strafvordering in samenhang met de nieuwe Wet politiegegevens het opsporingsonderzoek zal reguleren. Het

---

[10] Kamerstuk 32 761, nr. 161.

[11] Zie ook de Kamerbrief Digitalisering strafrechtketen waarin onder meer de achtergrond en doelen van het digitaliseringstraject worden toegelicht. Kamerstuk 29 279, nr. 548.

[12] Rapport van de Commissie modernisering opsporingsonderzoek in het digitale tijdperk «Regulering van opsporingsbevoegdheden in een digitale omgeving», p. 25.

(gemoderniseerde) Wetboek van Strafvordering en het (gemoderniseerde) gegevensregime voor het politie- en justitiedomein dienen in samenhang het opsporingsonderzoek te reguleren op een manier die een goede balans biedt tussen enerzijds de effectiviteit van de rechtshandhaving en anderzijds rechtsbescherming in de vorm van afdoende waarborgen die inbreuken op grondrechten kunnen legitimeren als deze noodzakelijk zijn in een democratische samenleving. Verder loopt momenteel het wetgevingstraject met betrekking tot de Wet gegevensverwerking door samenwerkingsverbanden.[13] Daarnaast vloeit vanaf 2022 uit EU-wetgeving de verplichting voor EU-lidstaten voort om aan Europeanen en derdelanders een overzicht van de door de lidstaten geregistreerde justitiële gegevens te verschaffen indien daarom door het individu wordt verzocht. Met deze, en ook de andere ontwikkelingen vanuit de EU zal rekening worden gehouden in het komende traject.

3. Vervolgstappen

Het komen tot een toekomstig wettelijk kader vergt een grote inspanning van alle betrokken partijen en vraagt om een zorgvuldig proces waarbij rekening wordt gehouden met de zienswijze en belangen van alle betrokkenen. Mede om die reden zijn (mogelijk toekomstige) bevoegde autoriteiten al in een vroegtijdig stadium betrokken. Daarnaast ben en blijf ik ook in gesprek verschillende belanghebbende partijen zoals de samenwerkingspartners van de bevoegde autoriteiten en maatschappelijke organisaties op het gebied van mensenrechten. Ook zal ik Europese ontwikkelingen en wetenschappelijke inzichten op dit gebied betrekken in het vervolgtraject.

In deze eerste fase – de beleidsvormingsfase – staat het verder uitwerken van de bovengenoemde uitgangspunten en onderwerpen centraal. Dit gaat zowel om het verkennen van de mogelijkheden voor een effectieve taakuitvoering en samenwerking in de strafrechtsketen als het verkennen van de juiste waarborgen ter bescherming van de persoonlijke levenssfeer van betrokkenen. Tijdens deze fase wordt ook gestart met het in kaart brengen van de financiële consequenties en de implementatiegevolgen. Dit zal leiden tot een uitgebreidere nota waarin de contouren van het toekomstig wettelijk kader zullen worden geschetst. Ik verwacht dat deze contourennota in de loop van 2021 naar de Tweede Kamer zal worden gestuurd.

Onderkend wordt dat in deze vroege fase nog niet de financiële impact becijferd kan worden, omdat deze brief er toe strekt uw Kamer te informeren over de richting waarin en het proces waarlangs de beleidsontwikkeling richting een wetsvoorstel plaatsvind. Wel is – gegeven eerdere ervaringen met dergelijk grote trajecten – de verwachting dat de impact, met name ten aanzien van de implementatie, substantieel zal zijn gezien de grote rol van informatie voor handhaving van de openbare orde, onderzoek, opsporing, vervolging van strafbare feiten en tenuitvoerlegging van straffen en maatregelen. De inschatting van de financiële consequenties en implementatiegevolgen moeten in gezamenlijkheid met de betrokken organisaties en het departement worden gemaakt. Afhankelijk van de keuzes in de beleidsvoorbereiding en van de raming van de kosten die uit deze keuzes voortvloeien, zal er dekking op basis van het voorstel worden gezocht.

[13] Daarnaast wordt uiteraard ook rekening gehouden met trajecten zoals Uitwisseling Persoonsgegevens en Privacy (UPP).

Op het moment dat de beleidsuitgangspunten uitgekristalliseerd zijn en aan de vereiste randvoorwaarden kan worden voldaan, waaronder ook de benodigde financiële dekking, wordt er gestart met het wetgevingstraject. Zonder de vereiste randvoorwaarden, zal de vernieuwing van het wettelijk kader voor gegevensverwerking door politie en justitie geen doorgang kunnen vinden. Het totale proces zal naar verwachting drie tot vier jaar in beslag nemen. Na de totstandkoming van het wettelijk kader moet dit geïmplementeerd worden. Vervolgens zal de naleving ervan het voorwerp zijn van aanhoudende zorg voor alle betrokken partijen.

De Minister voor Rechtsbescherming,
S. Dekker