Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2013–2014

30 327 Regels inzake de verwerking van politiegegevens (Wet politiegegevens)

I

BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 23 juni 2014

In deze brief schets ik een perspectief op de toekomstige omgang met politiële, justitiële en strafvorderlijke gegevens. Directe aanleiding daartoe is de evaluatie van de twee wetten die daarop betrekking hebben: de Wet politiegegevens (hierna: Wpg) en Wet justitiële en strafvorderlijke gegevens (hierna: Wjsg).[1] Deze wetten moeten worden gemoderniseerd. Zowel de taakuitvoering van politie en justitie als de bescherming van de privacy van burgers kan en moet worden versterkt. Op hoofdlijnen gaat het om het volgende:

– De verschillende regimes die van toepassing zijn op politiële, justitiële en strafvorderlijke gegevens, moeten worden geharmoniseerd. Op dit moment staan ze nog in de weg aan een goede samenwerking tussen de verschillende partijen én aan een adequate bescherming van de privacy.
– Uitgangspunt van de regelgeving moet zijn het gebruik van gegevens. In de huidige regulering staan de bewaartermijnen te veel centraal. De bewaartermijn behoort evenwel een afgeleide te zijn van de noodzaak tot gebruik van de gegevens, niet andersom. Voor een zwaarwegend doel, zoals het oplossen van cold cases bij ernstige misdrijven, moeten gegevens lange tijd kunnen worden gebruikt. Voor minder zwaarwegende doelen, bijvoorbeeld de beoordeling van een VOG aanvraag, kan en moet die termijn veel korter zijn.
– Het toezicht op het gebruik en de verstrekking van gegevens moet worden versterkt. Moderne ICT kan en moet hierbij behulpzaam zijn. Tevens moet het toezicht op de werkvloer, zowel preventief als repressief, worden versterkt en moet er via opleidingen worden

[1] «Politiegegevens» zijn de persoonsgegevens die worden verwerkt in het kader van de uitoefening van de politietaak. «Justitiële gegevens» zijn de persoonsgegevens (of gegevens over een rechtspersoon) inzake de toepassing van het strafrecht of de strafvordering. «Strafvorderlijke gegevens» zijn de persoonsgegevens (of gegevens over een rechtspersoon) die zijn verkregen in het kader van een strafvorderlijk onderzoek en die het openbaar ministerie in een strafdossier of langs geautomatiseerde weg verwerkt.

kst-30327-I
ISSN 0921 - 7371
's-Gravenhage 2014

gewerkt aan meer bewustwording van het belang van nauwgezette naleving van de regels op dit gebied.

Deze modernisering van de regelgeving en de uitvoering is ambitieus en zal de nodige tijd kosten. Zij heeft op hoofdlijnen al de instemming van de betrokken organisaties. De noodzaak van dit ambitieuze programma wordt bevestigd door de uitkomsten van twee onderzoeken die onlangs zijn uitgevoerd naar de omgang met politiële, justitiële en strafvorderlijke gegevens. In deze rapporten wordt onder meer geconstateerd dat politie en justitie op onderdelen niet voldoen aan de huidige wetgeving. Eén van de geconstateerde problemen is dat gegevens niet altijd tijdig zijn vernietigd (zoals de wetgeving voorschrijft). De betrokken organisaties nemen nu maatregelen die bijdragen aan het versneld verwijderen en vernietigen van gegevens. Ik zie toe op de voortgang van deze maatregelen en laat mij daar periodiek over informeren.

In het onderstaande licht ik mijn voornemens toe. Vooraf merk ik op dat de politietaak breder is dan de opsporing van strafbare feiten: zij omvat ook de handhaving van de openbare orde en het verlenen van hulp aan hen die deze behoeven. De verwerking van politiegegevens omvat dan ook een navenant breder terrein dan alleen de strafrechtspleging. De visie die ik in deze brief schets, start weliswaar vanuit het perspectief van de strafrechtspleging, maar beperkt zich daartoe niet.

Digitalisering en de omgang met politiële, justitiële en strafvorderlijke gegevens

Digitalisering is een van de pijlers van het programma Versterking prestaties strafrechtsketen (VPS).[2] De norm in de strafrechtketen is dat in 2016 processtukken digitaal beschikbaar worden gesteld.[3] Effectieve samenwerking tussen partijen in en buiten de keten vereist immers efficiënte uitwisseling van informatie. De samenleving stelt hogere eisen, zowel ten aanzien van sociale veiligheid en het gebruik van ICT, als ten aanzien van de bescherming van de privacy. Wetgeving beoogt deze belangen te verzoenen. De twee toepasselijke wetten – de Wpg en de Wjsg – zijn, in hun onderling verband en samenhang, aan een grondige heroverweging toe. In het bijzonder twee redenen nopen daartoe.

1. De wettelijke regimes sluiten niet goed op elkaar aan. Een en hetzelfde persoonsgegeven is aan verschillende regimes voor verstrekking en bewaring onderworpen naar gelang het zich bevindt bij politie, bij het openbaar ministerie, bij de rechtbanken of bij de reclassering. Zeker in het digitale tijdperk, waarin gegevens niet meer aan een plaats gebonden zijn, is dat niet langer te rechtvaardigen. De bestaande juridische schotten bemoeilijken bovendien de verwerking van de gegevens.
2. De bewaartermijnen zijn in de regelgeving dominant. Die betreffen als zodanig echter het *bewaren* van de gegevens, niet hun *gebruik*. Gedurende de gehele bewaartermijn, die voor de ernstigste feiten kan oplopen tot 80 jaren, mag het gegeven in beginsel worden gebruikt voor alle in de wet omschreven doelen: opsporing, strafoplegging, verlenen van vergunningen, screening van personen, BIBOB, de Verklaring omtrent het gedrag, in samenwerkingsverbanden waaraan politie en openbaar ministerie deelnemen, etc. Uit oogpunt van proportionaliteit en bescherming van de privacy van betrokkenen is dat moeilijk te rechtvaardigen.

---

[2] Ik informeer u regelmatig over mijn plannen en de voortgang op dit gebied, laatstelijk in mijn brief van 14 november 2013 over VPS (Kamerstukken II 2013/14, 29 279, nr. 177).

[3] Zie mijn brief van 5 juli 2013, Kamerstukken II 2012/13, 29 279, nr. 165 (VPS), p. 5.

Vanuit de materie van deze wetten is er dus reden om na te denken over een nieuwe systematiek voor de regelgeving. Ik voel mij daarin gesterkt door de recente uitspraken van het Hof van Justitie van de EU inzake de Dataretentierichtlijn en Google.[4] Hoewel deze uitspraken geen betrekking hebben op de politiële, justitiële en strafvorderlijke gegevens, bevestigen zij wel de noodzaak om beter te regelen wie toegang heeft tot welke gegevens, voor welke doelen en gedurende welke periode. Voor de onderhavige materie wil ik hieraan als volgt – op hoofdlijnen – invulling geven.

ad 1: harmonisatie van wettelijke regimes

Ik ga de Wpg en de Wjsg in hun onderling verband en samenhang herzien. Ik overweeg om daarbij ze samen te voegen tot één wet als dat dienstig zou zijn voor de noodzakelijke samenhang en afstemming. Deze integratie zal moeten aansluiten bij de ontwikkelingen in EU-verband ten aanzien van een nieuwe Verordening en Richtlijn betreffende de bescherming van persoonsgegevens. In het bijzonder de reikwijdte van deze Europese rechtsinstrumenten is daarbij van groot belang. Hiervoor verwijs ik naar de periodieke rapportage dienaangaande.[5] Tevens zullen daarbij de relaties met het Wetboek van Strafvordering en met de Wet openbaarheid van bestuur (Wob) en andere wetten die zien op de verwerking van strafrechtelijke gegevens worden bezien, omdat er soms spanning lijkt te bestaan tussen de regimes voor openbaarmaking en voor verstrekking in deze wetgevingscomplexen; hierover ben ik reeds in gesprek met mijn ambtgenoot van Binnenlandse Zaken en Koninkrijksrelaties.

ad 2: van «bewaartermijnen» naar «gebruikstermijnen»

De noodzaak van *gebruik* van de informatie moet in de regelgeving voorop staan, de noodzaak van *bewaring* volgt daaruit. Immers, «(d)e regulering van opslag en verwerking van gegevens is van minder belang dan de regulering van het handelen dat is gebaseerd op digitale gegevens; de nadruk van het stelsel moet daarom verschuiven van de verantwoordelijkheden met betrekking tot de opslag naar extra verantwoordelijkheden met betrekking tot gebruik jegens een persoon».[6] Uit oogpunt van proportionaliteit moet worden gedifferentieerd naar de verschillende doelen waarvoor de gegevens mogen worden gebruikt en moet de termijn gedurende welke dat mag, worden bepaald door het doel. Aan dat gebruik kunnen wel nadere voorwaarden worden verbonden, bijvoorbeeld dat het alleen is toegestaan voor bepaalde categorieën zeer ernstige delicten, of alleen voor opsporingsdoelen, of dat de expliciete toestemming van een officier van justitie daartoe is vereist, of dat andere regels gelden voor gegevens die de politie heeft verzameld in het kader van haar niet-strafrechtelijke taken (handhaving van de openbare orde, hulpverlening). Gehandhaafd blijft uiteraard dat de gegevens na ommekomst van een nader te bepalen termijn zullen moeten worden vernietigd.

moderne ICT gaat bijdragen aan de oplossingen

Gegevens worden nu nog op tal van plaatsen vastgelegd. Dat bemoeilijkt een eenduidige toepassing van de regels voor verstrekken en bewaren. In

---

[4] Resp. HvJ EU 8 april 2014 (zaken C 293/12 en C 594/12) en HvJ EU 13 mei 2014 (zaak C-131/12).
[5] Laatstelijk: brief van de Staatssecretaris van Veiligheid en Justitie van 19 december 2013, Kamerstukken II, 2013/14, 32 761, nr. 57.
[6] Aldus Ybo Buruma: Het recht op vergetelheid. Politiële en justitiële gegevens in een digitale wereld. In: De staat van informatie (WRR, 2011), p. 210 resp. 206.

het kader van de eerder genoemde digitalisering van de strafrechtsketen wordt toegewerkt naar een situatie dat niet langer informatie wordt «rondgepompt». Gegevens moeten eenmalig worden vastgelegd en beheerd en meervoudig gebruikt. Het gaat om de verantwoordelijkheid voor de informatie, voor het beheer ervan (inclusief de beveiliging) en voor de systemen waarin de informatie wordt verwerkt. In de strafrechtsketen wordt momenteel een systematiek ontwikkeld die inhoudt dat gegevens of documenten die niet meer mogen worden gewijzigd, worden opgeslagen in speciaal daartoe bestemde voorzieningen. De verantwoordelijkheid voor het gegeven of document blijft berusten bij degene die het gegeven heeft vastgelegd resp. het document heeft gemaakt, zij gaat niet over op de beheerder van de voorziening. De wet – dus niet de «eigenaar» – bepaalt wie kennis mag nemen van het gegeven of document. Indien een functionaris of organisatie een gegeven of document «van een ander» nodig heeft, kan hij dat «ophalen» uit de bedoelde voorziening (mits hij daartoe gerechtigd is). De ketenorganisaties sturen elkaar in beginsel niet langer documenten toe, maar signaleringen dat een zaak of bewerking door hen is afgerond en dat een gegeven of document klaarstaat voor de opvolgende schakel in de keten. Die opvolgende schakel kan het, zoals gezegd, «ophalen» uit de speciaal daartoe bestemde voorziening en daarmee de bewerking van de zaak in de keten het passende vervolg geven. Aldus wordt het redundant opslaan van gegevens tegengegaan. Daarmee wordt ook een rem gezet op het oneigenlijk gebruik van informatie (gegevens of documenten). Iedere verwerking wordt bovendien gelogd. De geschetste systematiek is neergelegd in een set van richtinggevende principes die reeds door alle betrokken organisaties zijn onderschreven. Met deze aanpak worden privacywaarborgen zo veel mogelijk ingebouwd in de informatievoorziening van politie en justitie, overeenkomstig de visie van dit kabinet dat bij de bouw van systemen en het aanleggen van databestanden bescherming van persoonsgegevens uitgangspunt moet zijn («privacy by design»).[7] Er bestaan al technische voorzieningen voor wat in de informatica wordt genoemd «regelgestuurde toegang tot informatie» («rule based access»). Ik laat de mogelijkheden voor de toepassing daarvan binnen de strafrechtsketen onderzoeken.

organisatie, toezicht, bewustwording

De mogelijkheden van ICT zijn noodzakelijk, maar niet voldoende. Rechtmatig gebruik van gegevens dient allereerst op de werkvloer zelf gestalte te krijgen. Het moet worden verankerd in opleidingen, in bewustwording, in de cultuur, in werkprocessen, in omgangsvormen, in het leidinggeven, in functioneringsgesprekken, in beoordelingen, via protocollen en managementafspraken. En het moet worden aangevuld met effectief toezicht op het gebruik van gegevens door medewerkers. Proactief toezicht moet worden verankerd in de ondersteunende en sturende processen, repressief toezicht via audits, via rapportages van privacyfunctionarissen of functionarissen voor de gegevensbescherming binnen de organisaties en extern door het College Bescherming Persoonsgegevens (CBP). Dat het interne toezicht versterking behoeft is in het afgelopen jaar reeds besproken met alle partijen in de strafrechtsketen en door hen ook erkend. Ik heb hun gevraagd met praktische en effectieve maatregelen te komen om daaraan invulling te geven.
Een nieuw concept in dit opzicht is de Gegevensautoriteit. Hiermee wordt gedoeld op een functionaliteit binnen een organisatie of domein die betrekking heeft op het opstellen van standaarden voor en het houden van toezicht op de naleving daarvan en eventueel ook op de verwerking van gegevens binnen de organisatie of het domein. Het concept is in het

[7] Kamerstukken II, 2012/13, 33 410 («Bruggen slaan»), nr. 15, p. 27.

afgelopen jaar in onderzoek genomen binnen mijn ministerie. In de loop van dit jaar verwacht ik conclusies te kunnen trekken en effectief invulling te kunnen geven aan de nieuwe functionaliteit. De politie heeft in haar inrichtingsplan ook voorzien in een Gegevensautoriteit.

lange termijn

Met het vorenstaande is in potentie een ambitieus en omvangrijk programma geschetst. Vergaande digitalisering van de strafrechtketen is een zaak van lange adem, schreef ik in mijn brief van 23 november 2012.[8] De herziening van het Wetboek van Strafvordering en het introduceren van het digitaal dossier in 2016 hebben de komende jaren alle prioriteit. De hiervóór gegeven schets zal nog nader moeten worden doordacht en vervolgens in kleine stapjes moeten worden gerealiseerd. Ook zullen de praktische, financiële en technische implicaties van de nieuw op te stellen regelgeving goed in kaart (moeten) worden gebracht via ex-ante uitvoeringstoetsen, privacy impact assessments e.d.

De evaluaties van de Wpg en de Wjsg

Bij mijn brieven van 13 januari jl. heb ik u het rapport over de Wet politiegegevens aangeboden.[9] Hierbij bied ik u het rapport over de Wet justitiële en strafvorderlijke gegevens[10] aan. In het tweede deel van deze brief ga ik nader in op deze beide evaluaties.[11] Overeenkomstig artikel 47 Wpg heb ik het CBP geconsulteerd over de evaluatie van de Wpg. Het CBP geeft in zijn brief van 13 februari 2014 ervan blijk het door de onderzoekers geschetste beeld te herkennen. Het CBP bepleit om eerst alle aandacht te richten op de knelpunten die zijn toe te schrijven aan oorzaken binnen de politieorganisatie en pas daarna op knelpunten in de structuur van de Wpg. De opvatting van het CBP dat de eerste prioriteit behoort te liggen bij het Wpg-conform maken van de uitvoeringspraktijk door de politie, onderschrijf ik gaarne. Dit staat echter niet in de weg aan het denken over een betere omgang met politiële, justitiële en strafvorderlijke gegevens en over de wijzigingen die het wettelijk kader daartoe zou moeten ondergaan, zoals ik hierboven heb geschetst.

Hieronder vat ik eerst de bevindingen van de onderzoekers kort samen. Daarna geef ik mijn reactie, in aanvulling op hetgeen in het eerste deel van deze brief al is gesteld. Vooraf merk ik op dat de beide onderzoeken zich vooral hebben gericht op de ervaringen en meningen van mensen in de praktijk. De geïnterviewden hebben de gelegenheid gehad om desgewenst commentaar te leveren op het verslag van het met hen gehouden interview. De evaluatie van de Wpg heeft daarnaast vooral gebruik gemaakt van de rapportages van de Departementale auditdienst (DAD) van het Ministerie van Veiligheid en Justitie.

bevindingen van de onderzoekers inzake de Wpg:

– Er is sprake van «een worstelende praktijk». De doelstellingen en de hoofdlijnen van de wet worden weliswaar breed onderschreven, maar de invulling en de toepassing ervan loopt vast in de operationalisering

[8] Kamerstukken II, 2012/13, 29 279, nr. 156, p. 2.
[9] Kamerstukken I, 2013/14, 30 327, H; en Kamerstukken II, 2013/14, 33 842, nr. 1.
[10] Ter inzage gelegd op de afdeling Inhoudelijke ondersteuning onder griffie nr. 155429.
[11] Daarmee voldoe ik aan mijn verplichtingen uit hoofde van de artikelen 47 Wet politiegegevens resp. 76 Wet justitiële en strafvorderlijke gegevens.

en de implementatie. De oorzaak hiervan ligt deels in de complexiteit van de wetgeving, deels in de politieorganisatie van voor 1 januari 2013.[12]
– De Wpg wordt ervaren als moeilijk te lezen en te interpreteren. Zij sluit ook op een aantal punten niet goed aan bij de praktijk. De inrichtingseisen die de wet stelt aan de betrokken organisaties staan deels op gespannen voet met een doelmatige en effectieve bedrijfsvoering en uitvoering van (bepaalde) politietaken.
– In het oude politiebestel is een landelijke informatiehuishouding niet goed van de grond gekomen. Daarnaast kan op het gebied van kennis en bewustwording van de Wpg bij politiemedewerkers het nodige verbeteren. Wel is de laatste tijd op beide punten een aanzienlijke vooruitgang geboekt. De vorming van de nationale politie doet zich hier gevoelen. Er is een nieuwe Wpg-implementatiestrategie ingezet, die inmiddels haar vruchten afwerpt.
– De gesignaleerde tekortkomingen in de uitvoering van de Wpg gaan vooral ten koste van een effectieve en efficiënte uitvoering van politietaken. Met betrekking tot de bescherming van de privacy is de onderzoekers niet gebleken van klachten die wijzen op een systematische aantasting van de persoonlijke levenssfeer. Van een aantal wettelijke eisen die de naleving van de Wpg als geheel en de uitvoering van politietaken bemoeilijken, is niet aannemelijk dat zij aanvullend bijdragen aan de bescherming van de informationele privacy.

bevindingen van de onderzoekers inzake de Wjsg:

– Er is sprake van in de loop der jaren organisch gegroeide wetgeving. Hierdoor zijn – volgens de onderzoekers – de doelen van de wet niet expliciet vastgelegd[13] en is niet vast te stellen of de wet de beoogde doelen waarmaakt.
– De praktische werkbaarheid van de wet blijkt goed binnen de «klassieke strafrechtsketen» (opsporing door politie, vervolging door openbaar ministerie, berechting en tenuitvoerlegging), maar staat onder druk bij nieuwe samenwerkingsvormen zoals Veiligheidshuizen, RIEC's[14], ZSM[15].
– De verstrekkingsregimes van politiële, justitiële en strafvorderlijke gegevens zijn niet op elkaar afgestemd, waardoor het kan lonen om langs te gaan (te «shoppen») bij verschillende loketten.
– Het toezicht op de omgang met de ontvangen gegevens is (te) beperkt. Het ongeoorloofd doorbreken van de geheimhoudingsplicht die voor elk van de genoemde wettelijke regimes geldt, blijft vrijwel altijd zonder gevolgen. Dit betreft zowel de doorverstrekkingen door partijen binnen de strafrechtsketen als de doorverstrekkingen door partijen buiten de strafrechtsketen.
– De justitiële en de strafvorderlijke gegevens worden aan het einde van de bewaartermijn niet (of niet altijd) vernietigd. Wel worden ze voor gebruikers ontoegankelijk gemaakt c.q. afgeschermd. De feitelijke inbreuk op de rechten van geregistreerden is daardoor miniem.

reactie op de beide rapporten

De maatregelen die ik in het eerste deel van deze brief heb geschetst, komen al in belangrijke mate tegemoet aan de door de onderzoekers

---

[12] De Wpg is overigens, anders dan haar titel suggereert, niet alleen van toepassing op de politie, maar ook op de Koninklijke marechaussee en de vier bijzondere opsporingsdiensten.
[13] Volgens vaste rechtspraak van de Afdeling bestuursrechtspraak van de Raad van State zijn de doelen overigens wel duidelijk genoeg.
[14] Regionale Informatie- en Expertise Centra.
[15] Zo Snel, Slim, Selectief, Simpel, Samen en Samenlevingsgericht Mogelijk.

gesignaleerde knelpunten. Hieronder beschrijf ik nog een aantal aanvullende maatregelen voor de kortere termijn met betrekking tot enkele specifieke knelpunten.

Wjsg: justitiële gegevens

Sinds 1 oktober 2010 schrijft deze wet voor dat de justitiële gegevens na ommekomst van de bewaartermijn moeten worden «vernietigd». In 2005 heeft de Departementale auditdienst (DAD) van mijn ministerie reeds – onder de oude wet – de vraag opgeworpen of de praktijk binnen het het Justitieel Documentatiesysteem (JDS) wel adequaat invulling gaf aan de plicht tot (toen nog) «verwijderen» van de gegevens. Dat heeft niet geleid tot aanpassing van het systeem. Ook de wijziging van de wet in 2010 heeft niet geleid tot aanpassing van het systeem. De justitiële gegevens worden echter wel (en werden altijd al) na afloop van de wettelijke bewaartermijnen onbereikbaar gemaakt voor de gebruikers van het JDS. De Justitiële Informatiedienst zal nog dit jaar voorzieningen treffen waardoor de gegevens ook niet meer toegankelijk zullen zijn voor de functioneel beheerders van het systeem. Daarmee wordt in elk geval bereikt dat de gegevens geen rol meer kunnen spelen in de rechtspleging en de rechtshandhaving.

Wjsg: strafvorderlijke gegevens

Voor de «strafvorderlijke» gegevens gelden dezelfde bewaartermijnen als voor de justitiële gegevens. Vijf van de tien parketten, waaronder de vier grootste, zijn sinds 2012 begonnen met een inhaalslag voor het schonen en vernietigen van de papieren dossiers; deze actie wordt nog dit jaar afgerond. Het plan van aanpak voor de overige vijf parketten is nu in ontwikkeling; streven is om de vernietiging in 2015 te realiseren. De digitale bedrijfsprocessystemen van het openbaar ministerie, COMPAS en GPS, zijn ontworpen en gebouwd voordat de wet vernietiging van gegevens voorschreef en eveneens niet aangepast aan de wetswijziging van 1 oktober 2010. COMPAS zal worden uitgefaseerd als het digitaal procesdossier is ingevoerd en GPS-maatwerk in gebruik is genomen; gestreefd wordt naar medio 2016.[16] De bewaartermijnen van de in GPS geregistreerde misdrijfzaken zijn voorlopig nog niet verstreken. Voor een gedeelte van de overtredingen in GPS is dat echter wel het geval. Het OM onderzoekt hoe deze strafvorderlijke gegevens kunnen worden vernietigd en zal mij binnen twee maanden hierover rapporteren.

Wpg: politie

De onderzoekers adviseren de verwerkingsregimes van de artikelen 8 en 9 Wpg te «ontschotten» en de bewaartermijnen van bepaalde categorieën politiegegevens te verruimen. In de sfeer van de kwaliteitsborging en het toezicht bevelen zij aan om protocollering, monitoring/evaluatie en auditing niet langer op te vatten als toezichtsinstrumenten, maar meer onderdeel te laten zijn van de reguliere managementcyclus. Deze aanbevelingen zullen worden meegenomen bij de hiervoor aangekondigde heroverweging van de beide wetten.[17]
De problematiek van het ten onrechte niet vernietigen van gegevens doet zich ook voor bij politiegegevens. Dit is reeds opgemerkt door de Departementale auditdienst (DAD) van mijn ministerie bij gelegenheid van

[16] Zie mijn brief van 12 november 2013, Kamerstukken II, 2013/14, 29 279, nr. 178.
[17] Daarmee wordt tevens uitvoering gegeven aan het voornemen uit het Regeerakkoord om voor een nader te bepalen categorie van gegevens de bewaartermijn te verlengen omdat en voor zover dat kan bijdragen aan het oplossen van oude, onopgeloste zaken. Zie Kamerstukken II, 2012/13, 33 410 («Bruggen slaan»), nr. 15, p. 26.

de privacy-audit van deze dienst uit 2011–2012 bij de toenmalige korpsen. Op basis van de voortgangsrapportage Wpg 2013 van de politie heb ik de korpschef gevraagd extra aandacht te geven aan de bewaartermijnen van gegevens. Binnen het bijgestelde Aanvalsprogramma Informatievoorziening van de politie, de vorming van de nationale politie en het project implementatie Wpg worden maatregelen genomen die leiden tot het correct verwijderen en vernietigen van gegevens. Bij de implementatie van de nieuwe informatievoorziening voor de politie (Operationeel Politie Proces, OPP, en Basisvoorziening Informatie, BVI) zullen maatregelen voor verwijdering en vernietiging van gegevens worden geborgd in opleidingen, gestandaardiseerde werkprocessen en monitoringsinstrumenten. Naleving van de Wpg wordt «by design» opgenomen in de nieuwe gegevensarchitectuur. Vooruitlopend op deze nieuwe voorzieningen ligt de focus op de twee grootste systemen van de politie: de Basisvoorziening Handhaving (BVH) en SummIT, het huidige systeem ter ondersteuning van de opsporing. Ten aanzien van deze systemen zullen in 2015 respectievelijk eind 2014 verbetermaatregelen zijn getroffen die eraan bijdragen dat operationele medewerkers de voorschriften van de Wpg in acht nemen. Bij het oplossen van geconstateerde problemen is overigens steeds een punt van overweging of dit nog moet plaatsvinden in de huidige, veelal verouderde, systemen, dan wel dat de oplossing ligt in de structurele vernieuwing binnen het bijgestelde Aanvalsprogramma.

Wpg: Koninklijke marechaussee, Bijzondere opsporingsdiensten

Uit audits van de Auditdienst Defensie (2013) en PricewaterhouseCoopers Advisory NV (2012) blijkt dat ook de Koninklijke marechaussee ten onrechte justitiële en politiegegevens niet altijd heeft vernietigd. De Minister van Defensie heeft de Koninklijke marechaussee opdracht gegeven de ten onrechte niet-vernietigde gegevens alsnog te vernietigen. Deze inhaalslag moet handmatig worden uitgevoerd.
Naar aanleiding van de privacy-audits bij de politie en de bijzondere opsporingsdiensten heb ik de problematiek inzake het vernietigen van politiegegevens onder de aandacht gebracht van mijn ambtgenoten onder wie de bijzondere opsporingsdiensten ressorteren.
Eind 2014 start een externe audit betreffende de naleving van de Wpg door de politie, de Koninklijke marechaussee en de vier bijzondere opsporingsdiensten. Naar aanleiding van de uitkomsten daarvan zal ik u verder informeren over de effectiviteit van de door de betrokken organisaties ingezette maatregelen.

samenwerkingsverbanden

In verschillende samenwerkingsverbanden waarin ook politiële, justitiële en strafvorderlijke gegevens worden uitgewisseld, wordt in toenemende mate met convenanten en privacyprotocollen gewerkt. Ik zal deze werkwijze krachtig verder bevorderen.

tot slot

De wetgeving (Wpg en Wjsg) heeft ten doel het grondrecht van de privacy te beschermen en tegelijkertijd het mogelijk te maken dat informatie optimaal wordt benut bij de uitvoering van de overheidstaken op het gebied van veiligheid en justitie. Hier gaan rechtsstatelijkheid, integriteit en professionaliteit hand in hand met doeltreffendheid en doelmatige bedrijfsvoering. Ik hecht aan deze belangen groot gewicht en acht daarom de in de brief aangekondigde maatregelen ten volle gerechtvaardigd.

De Minister van Veiligheid en Justitie,
I.W. Opstelten