WODC

Glazen privacy

Knelpuntenonderzoek uitvoering Wet politiegegevens (Wpg)

Colofon

Projectnummer WODC	*2236*
Datum	*4 oktober 2013*
Auteurs	*John Smits*
	Anna Sibma
	Josien Roodnat
	Niko Struiksma
	Roald Schel
Versie	*3.5*
Status	*definitief*
	www.arenaconsulting.nl
	www.pro-facto.nl

Geïnterviewde: *"Wij moeten transparant zijn maar ook boeven kunnen vangen; als er iets fout loopt, gaat het zonder veel nuance snel rond via twitter. Als politie bevind je je wat privacy betreft in een glazen huis".*

Glazen Privacy

Knelpuntenonderzoek Wet politiegegevens (Wpg)

Het onderzoek is verricht in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC), Ministerie van Veiligheid en Justitie te Den Haag.

Een gedrukt exemplaar van het volledige rapport is te bestellen Arena Consulting of Pro Facto. De digitale versie is te downloaden van de website van het WODC, Arena Consulting en Pro Facto .

Arena Consulting Group BV
Diepenveenseweg 152
7413 AV Deventer

E: info@arenaconsulting.nl
I: www.arenaconsulting.nl

Pro Facto BV
Ossenmarkt 5
9712 NZ Groningen

E: profacto@pro-facto.nl
I: www.pro-facto.nl

Samenvatting

Op 1 januari 2008 is de Wet politiegegevens (Wpg) in werking getreden ter vervanging van de Wet politieregisters (Wpolr). De Wpg regelt de wijze waarop politie, Koninklijke marechaussee (Kmar) en Bijzondere opsporingsdiensten (BOD-en) moeten omgaan met politiegegevens, dat wil zeggen persoonsgegevens die worden verwerkt bij de uitvoering van politietaken. Ten opzichte van de Wpolr betekent de Wpg een verruiming van de verwerkingsmogelijkheden van politiegegevens, maar tevens een aanscherping van de waarborgen voor de bescherming van de privacy. In de Wpg is bepaald dat de Minister van Veiligheid en Justitie binnen vijf jaar na de inwerkingtreding van de wet verslag uitbrengt over de doeltreffendheid en effecten van de wet in de praktijk.

Eind 2011 bleek uit door de Departementale Auditdienst (DAD) van het ministerie van Veiligheid en Justitie uitgevoerde audits dat de implementatie van de Wpg nog op veel punten tekort schoot. Onder meer als het gaat om de beveiliging, autorisaties, de registratie van verstrekking van gegevens aan derden en het interne toezicht.

Vraagstelling en opzet onderzoek

Arena Consulting en Pro Facto hebben in opdracht van het Wetenschappelijk Onderzoeks- en Documentatiecentrum (WODC) van het ministerie van Veiligheid en Justitie een nadere evaluatie verricht van de knelpunten. De vraagstelling was samengevat daarbij als volgt:

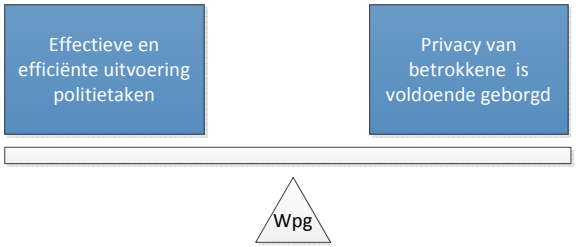
1. Wat heeft de wetgever beoogd met de Wet politiegegevens (wat is de beleidstheorie)?
2. Hoe wordt de Wet politiegegevens in de praktijk uitgevoerd; is dit volgens de doelstellingen en de verwachtingen van de wetgever en wat zijn de resultaten en knelpunten?
3. Hoe verhoudt de Wpg zich tot andere wet- en regelgeving zoals de Wet bescherming persoonsgegevens (Wbp), de Wet openbaarheid van bestuur (Wob) en internationale wet- en regelgeving?
4. Hoe kunnen de knelpunten bij de invoering van de wet en de uitvoering van de wettelijke regels verklaard worden?

Het onderzoek is uitgevoerd in de periode november 2012 tot september 2013. Daarbij zijn twee sporen bewandeld. Enerzijds is aan de hand van de in 2011 uitgevoerde audits en naar aanleiding van uitgevoerde hercontroles in 2012/2013 in beeld gebracht in welke mate de naleving van de Wpg conform de eisen van de wet is. Anderzijds is aan de hand van een groot aantal interviews in beeld gebracht welke knelpunten in relatie tot de Wpg worden ervaren bij de uitvoering van politietaken. Er zijn onder meer gesprekken gevoerd

met politie (regionale en landelijke eenheden), het ministerie van Veiligheid en Justitie, het Openbaar Ministerie (OM), het College bescherming persoonsgegevens (CBP), de Kmar en BOD-en. Daarnaast zijn literatuur en documenten gebruikt voor de reconstructie van de beleidstheorie en de reflectie op de uitkomsten van de gesprekken. Ter reflectie is daarnaast een expertmeeting georganiseerd met vertegenwoordigers van betrokken organisaties.

Globale beleidstheorie

De Wpg heeft een tweeledige doelstelling. Enerzijds voldoende (meer dan onder de Wpolr) ruimte bieden voor de verwerking (en verstrekking) van persoonsgegevens zodat een effectieve en efficiënte uitvoering van de politietaken mogelijk is. Waaronder een free-flow-of-information binnen en tussen opsporingsdiensten. Anderzijds het voldoende waarborgen van de privacy van degene waarvan gegevens worden verwerkt. Een nevendoelstelling van de Wpg is het verminderen van de administratieve lasten die werden ervaren bij de Wpolr. Het uitgangspunt van de wet is dat er voldoende balans ('nieuw evenwicht') is tussen de twee hoofddoelstellingen.



Om de privacy voldoende te borgen stelt de Wpg eisen aan:

- Geheimhouding, beveiliging en toegang (autorisatie) van gegevens
- Verwerkingstermijnen, bewaartermijnen en vernietiging
- Condities waaronder gegevens mogen worden verwerkt en verstrekt (noodzaak, doelbinding, proportionaliteit)
- Toezicht door een privacyfunctionaris, het uitvoeren van audits en protocollering
- Rechtsbescherming van de betrokkene in de vorm van recht op kennisneming
- Extern toezicht door het CBP

De verwachting van de wetgever was dat de Wpg goed zou aansluiten bij de politiepraktijk en anticipeerde op ontwikkelingen, zoals het toewerken naar een landelijke informatiehuishouding. Als belangrijkste aandachtspunt voor de implementatie werden scholing en opleiding gezien.

Conformiteit van de uitvoeringspraktijk met de wet

Uit de in 2011 uitgevoerde audits komt het beeld dat de implementatie van de Wpg – vier jaar na in werking treden van de wet – nog op veel punten tekortschiet. Dit geldt met

name voor het regelen van de autorisaties (wie mag welke gegevens verwerken?), de beveiliging van gegevens, de protocollering (vastleggen welke gegevens zijn verwerkt of verstrekt) en het hanteren van de wettelijke termijnen voor verwerking en vernietiging. Daarnaast was het uitvoeren van periodieke audits niet geborgd en vond intern toezicht niet of nauwelijks plaats. Tussen de organisaties (politiekorpsen, Kmar) waren er aanzienlijke verschillen in de mate waarin werd voldaan aan de Wpg. Geen enkele organisatie voldeed op alle punten. Het naar aanleiding van de audits ingezette verbetertraject heeft op een aantal onderdelen tot een betere naleving geleid, onder meer als het gaat om het inrichten van de auditfunctie en het proces voor het afsluiten van convenanten met het oog op verstrekkingen. De meeste eenheden waren in afwachting van landelijke modellen die – mede in het licht van de vorming van de Nationale politie – werden ontwikkeld.

Bij uitvoering van politietaken ervaren knelpunten

Door de organisaties wordt de wet in algemene zin ervaren als moeilijk te lezen en te interpreteren. Dat geldt onder meer voor begrippen als 'verwerken', de vraag wanneer het doel van een onderzoek is bereikt en de vraag onder welk verwerkingsregime politiegegevens vallen.

Knelpunten bij verwerking

Bij de verwerking van politiegegevens is een belangrijk knelpunt het wettelijke onderscheid tussen artikel 8 (dagelijkse politietaken) en artikel 9 (onderzoek). Gegevens veranderen in de praktijk van status en zijn niet statisch te plaatsen in één van de verwerkingsregimes. Het doorvoeren van de mutaties vergt veel tijd. Ook worden er voor de uitvoering van bepaalde politietaken (zoals de aanpak van zware criminaliteit en het oplossen van cold-cases) knelpunten ervaren met de bewaartermijnen. Vernietiging van gegevens vijf jaar na verwerking is volgens betrokkenen te kort en gaat ten koste van de informatiepositie. Daarnaast wordt een aantal overige knelpunten gesignaleerd bij het bepalen van het doel van een onderzoek (dat is niet altijd specifiek aan te geven), het bepalen of sprake is van geautomatiseerd vergelijken (valt een zoekopdracht daar ook onder?) en de mogelijkheden om grootschalig data-onderzoek te doen.

Knelpunten bij verstrekkingen

Bij de verstrekking van politiegegevens wordt vooral onduidelijkheid ervaren in de fase vóór een onderzoek (artikel 9) wordt gestart. Welke gegevens mogen bijvoorbeeld worden uitgewisseld bij het aftasten van de vraag of een onderzoek moet worden gestart in het kader van de samenwerking in RIEC-verband? Dit leidt in de praktijk tot terughoudendheid bij het delen van informatie waar de Wpg juist een meer actief delen van informatie voor ogen heeft. Daarnaast is er in de praktijk sprake van een stapeling van convenanten. Wat

onder welke condities aan welke organisatie mag worden verstrekt is daarmee niet geheel transparant en doelmatig. Ook zijn er landelijk verschillen in afspraken rond vergelijkbare samenwerkingsarrangementen. Als overige knelpunten komen onder meer naar voren de verschillende wettelijke kaders die van toepassing (kunnen) zijn bij gezamenlijk aangelegde bestanden in het kader van samenwerking en het gebruik van social media (etiquette bij gebruik daarvan).

Knelpunten rond rechten betrokkenen

Bij het gebruik maken van het recht op kennisnemingen worden vooral knelpunten ervaren in de administratieve last rond kennisgevingsverzoeken inzake CIE-gegevens en de toename in verzoeken om kennisnemingen om andere reden dan de wetgever heeft bedoeld (zoals rouwverwerking). Voor zover er klachten van betrokkenen zijn over de wijze van afwikkeling van kennisgevingsverzoeken gaan die vooral over de wijze waarop kennisgeving plaatsvindt (inzage, kopie stukken, telefonische mededeling) of niet verwijderde gegevens.

Knelpunten bij toezicht

Bij het toezicht zoals vastgelegd in de Wpg worden vooral de administratieve lasten van de protocollering als knelpunt ervaren, in het bijzonder als het gaat om de verstrekking van politiegegevens bij de uitvoering van dagelijkse politietaken (artikel 8 Wpg). Daarbij spelen zowel de hoeveelheid verstrekkingen als de gebrekkige ondersteuning van de ICT een rol. Het toezicht door privacyfunctionarissen komt niet goed van de grond. Het accent van de rol van de privacyfunctionaris ligt op het adviseren bij het toepassen van de Wpg.

Knelpunten in samenloop met andere wetten

Naast de Wpg gelden er andere wetten waarin de verwerking van persoonsgegevens en de bescherming van de privacy worden geregeld. In de strafketen is er vooral sprake van samenloop met de Wet justitiële en strafvorderlijke gegevens (Wjsg), het Wetboek van strafvordering (Sv) en de Wet bescherming persoonsgegevens (Wbp). In de praktijk worden er knelpunten ervaren bij het bepalen welk wettelijk regime van toepassing is en door verschillen in bewaartermijnen.

Wat betreft de rechten van betrokkenen is naast de Wpg ook de Wet openbaarheid van bestuur (Wob) van belang. De wetgever heeft in de Wpg geen relatie gelegd met de Wob. In de praktijk worden vooral knelpunten ervaren in de administratieve lasten bij de afwikkeling van Wob-verzoeken.

Verklaringen voor de knelpunten

De knelpunten bij de implementatie en aan de Wpg gerelateerde knelpunten bij de uitvoering van politietaken kunnen worden verklaard door vier hoofdfactoren:

- Kenmerken van de politieorganisatie
- De implementatiestrategie van de politie
- De opzet en inhoud van de Wpg
- Omgevingsfactoren

Verklaringen uit de politieorganisatie

Belangrijke factor voor het uitblijven van een goede implementatie is het lange tijd ontbreken van een gevoelde noodzaak bij de politieorganisatie als geheel en de leiding in het bijzonder. Daarbij was ook sprake van een 'archipel-organisatie': onder de vlag van 'politie' waren 26 korpsen autonoom verantwoordelijk voor de invoering. Er waren – tot de interventie van het CBP in 2011 – geen centrale sturende prikkels om de organisatie 'te dwingen' tot invoering. De praktijk onder het regime van de Wpolr ('privacy, dat regelen we zelf wel') werd daarmee voortgezet. Een tweede factor is de ICT. De aanname van de wetgever dat er één (de Wpg ondersteunende) ICT-voorziening zou komen, is niet bewaarheid. De verouderde en gefragmenteerde ICT met hulpstructuren voor de Wpg (i90-formulier voor de protocollering) heeft de invoering van de Wpg niet onmogelijk gemaakt maar heeft wel extra barrières opgeworpen.

Verklaringen uit de wijze van implementatie door de politie

Bij de implementatie heeft de politie gekozen voor een bedrijfstechnische benadering: het opstellen van formats, protocollen en werkinstructies. Er is weinig tot geen aandacht besteed aan kennisopbouw en bewustwording rond de essenties van de Wpg, het politiebelang met het oog op de uitvoering van politietaken en de omschakeling in het denken van professionele borging naar ook een meer bedrijfsmatige borging. Hierdoor bleef de invoering van de Wpg lange tijd vooral een ´moetje´ en kreeg de wet (mede door de slechte ICT-ondersteuning) een bureaucratisch imago.

Verklaringen uit de Wpg zelf

De Wpg zelf sluit met een aantal (organisatie)eisen niet goed aan bij (de dynamiek van) de praktijk. Dit geldt met name voor de beschotting tussen de verschillende verwerkingsregimes en het niet goed aansluiten op of vertonen van overlap met andere wetgeving (zoals Archiefwet, Politiewet, Wob en Wbp). Het relatief zware accent op organisatie-eisen en toezicht sluit niet goed aan bij de bedrijfsprocessen. Bijvoorbeeld als het gaat om het beheersbaar houden van een autorisatiematrix en protocollering. Bovendien worden diverse eisen of instrumenten in de context van toezicht geplaatst zoals protocollering en het uitvoeren van audits. Dit zijn echter primair

beheers/managementinstrumenten (waarvan de uitkomsten ook voor toezicht kunnen worden gebruikt). Door echter deze instrumenten onder (de wettelijke paragraaf) toezicht te scharen, creëert de wet een besturingsmodel van controle en afrekening. Dit heeft niet goed gewerkt in de context dat de Wpg niet verinnerlijkt was in casu de politie bij de implementatie weinig aandacht heeft geschonken aan deze verinnerlijking.

Verklaringen omgevingsfactoren

Sinds de voorbereiding en het in werking treden van de Wpg is de context waarbinnen politietaken worden uitgevoerd veranderd. Dit geldt voor de opgaven en taakstelling (zoals de rol van digitalisering bij de aard en het karakter van georganiseerde criminaliteit), voor de onderzoeksmethoden (zoals nieuwe technieken voor digitale analyses), voor het veranderende informatieaanbod en daarmee de (potentiële) informatiepositie van de politie en voor de opvattingen over privacy. Dit betekent dat grenzen van de mogelijkheden van verwerking (big data analyse, crowd analysis) en verstrekking (bijvoorbeeld via social media) in beweging zijn. Hetzelfde geldt ook voor de vraag waar de grenzen van privacy liggen als het gaat om de uitvoering van politietaken. Er is sprake van een zeker spanningsveld tussen het statische inrichtingskaraker van de Wpg en de dynamiek van ontwikkelingen waarmee de politie te maken heeft.

Conclusies en slotbeschouwing

De implementatie en naleving van de Wpg kan worden omschreven als een 'worstelende praktijk'. Het is opmerkelijk dat de verschillende betrokken partijen de achterliggende doelstellingen en hoofdlijnen van de wet breed onderschrijven, maar de invulling en toepassing vastloopt in de operationalisering en implementatie. Deels is dat terug te voeren op het in gebreke blijven van de betrokken organisaties, deels op de inhoud van de Wpg. Alhoewel er geen signalen zijn van structurele en systematische schendingen van de informationele privacy en ten gevolge daarvan inbreuken in de persoonlijke levenssfeer, zijn er wel patronen van incidenten en is de politie nog onvoldoende 'in control' als het gaat om politiegegevens.

Daar staat tegenover dat de inrichtingseisen die de Wpg stelt aan de betrokken organisaties, deels op gespannen voet staan met een doelmatige en effectieve bedrijfsvoering en uitvoering van (bepaalde) politietaken. De beleidstheorie van de Wpg is met andere woorden ook niet helemaal in balans als het gaat om het realiseren van de twee hoofddoelstellingen.

Ontschotting en naleving modelleren naar werkprocessen i.p.v. werkprocessen naar Wpg

De doelmatigheid en effectiviteit van de uitvoering van politietaken wordt gehinderd door het onderscheid in verwerkingsregimes. Wat de specifieke verwerkingsregimes regelen

(met name de artikelen 8 en 9), is in de wet in feite al in algemene zin geregeld in artikel 3 dat verwerking alleen toestaat bij gemotiveerde noodzaak, rechtmatigheid en doelbinding. Ontschotting biedt de organisatie meer mogelijkheden om de naleving van de Wpg te modelleren aan de hand van de eigen werkprocessen in plaats van de werkprocessen te moeten modelleren naar de Wpg.

Gekwalificeerde bewaartermijnen

De bewaartermijnen van vijf jaar na verwijdering moeten voor het gros van de politietaken afdoende worden geacht. Vooral de aanpak van zware criminaliteit vraagt mogelijk om langere bewaartermijnen. Het dilemma is dat vooraf niet altijd kan worden bepaald welke gegevens op een later moment relevant kunnen blijken. Alles bewaren is vanuit privacy-oogpunt geen optie. Alles na afloop van de (huidige) wettelijke bewaartermijnen vernietigen is geen verstandige keuze vanuit het oogpunt van de opsporing. De bescherming van de informationele privacy mag echter niet ondergeschikt worden aan het opsporingsbelang. Als wordt gekozen voor een verlengde bewaartermijn – en het uitstellen of afzien van vernietiging – dan zal dat op basis van een deugdelijke afweging moeten gebeuren. Bovendien zal moeten worden gezorgd voor extra beveiliging van gegevens en waarborgen bij de verwerking (speciale toestemming). Langer bewaren zal in ieder geval gepaard gaan met een stijging van de beheerskosten.

Helder onderscheid tussen toezicht en kwaliteitsborging

De Wpg kent een zekere stapeling van (impliciete) toezichtfiguren. Mede doordat protocollering, het uitvoeren van audits en de privacyfunctionaris expliciet onder het hoofdstuk 'toezicht' worden geplaatst in de Wpg. Dit terwijl de – ook door de wetgever bedoelde – primaire functie van deze instrumenten niet toezicht is maar kwaliteitsborging. De annotatie van 'toezichtinstrumenten' werkt naar de organisaties toe niet alleen bureaucratiserend; het is zelfs niet aannemelijk dat het bijdraagt aan het beschermingsniveau van politiegegevens. Het verdient de voorkeur om een veel duidelijker onderscheid te maken in de kwaliteitsborging die de verantwoordelijkheid is van de politie en een (wettelijk) toezicht door een externe toezichthouder (CBP). Dit zowel vanuit een oogpunt van transparantie, effectiviteit van het toezicht als verinnerlijking van informationele privacy in de organisatie.

Focus op kwaliteit gegevens en professionele én bedrijfsmatige borging

Vanuit een oogpunt van privacybescherming is het belangrijkste aandachtspunten voor de politie de borging van de kwaliteit van de gegevens. Dit vraagt om een samenhangende bedrijfsmatige en professionele borging, het beschikken over een ICT die het naleven van de Wpg voldoende ondersteunt én een goede beveiliging van de gegevens. Een en ander zal gepaard moeten gaan met een heroriëntatie op de vraag hoe de administratie, zowel

voor de organisatie als geheel als voor de medewerkers, beheersbaar blijft. Er zal – in lijn met het inrichtingsplan van de Nationale politie - in elk geval moeten worden gezorgd voor een goede balans tussen bedrijfsmatige borging en de 'mores' van de medewerkers.

Politieke heroriëntatie op verwachtingen van politie, technische ontwikkelingen en privacy

Tot slot zal er ook een politieke afweging moeten worden gemaakt rond de gewenste informatiepositie van de politie (en andere opsporingsdiensten). Dit tegen de achtergrond van de veranderingen in organisatie en verschijningsvormen van criminaliteit, de verwachtingen die worden gesteld aan opsporingsdiensten, de technische mogelijkheden voor opsporing (en hulpverlening), de veranderende opvattingen over privacy en het delen van informatie én de daarmee samenhangende risico's voor de privacy. De balans tussen het effectief kunnen uitvoeren van politietaken en het beschermen van de informationele privacy zal opnieuw moeten worden opgemaakt.

Summary

On 1 January 2008 the Dutch Police Data Act took effect, replacing the Data Protection (Police Files) Act. The Police Data Act regulates how the police, Royal Netherlands Military Constabulary and the Special Investigation Services must handle police data, that is, personal data processed in the course of the police's performance of their duties. The Police Data Act is broader than the Data Protection (Police Files) Act in terms of the possibilities for processing police data, but it also tightens the safeguards for protecting privacy. There was a provision in the Police Data Act requiring the Minister of Security and Justice to issue a report within five years of the Act's effective date on the effectiveness and consequences of the Act in practice.

Audits conducted by the Ministry of Security and Justice's Departmental Audit Service showed in late 2011 that the implementation of the Act was still inadequate in many respects, including security, authorizations, registration of the provision of data to third parties, and internal control.

Questions and survey design

At the instruction of the Ministry of Security and Justice's Research and Documentation Centre, Arena Consulting and Pro Facto carried out an additional evaluation. The questions examined were summarized as follows:

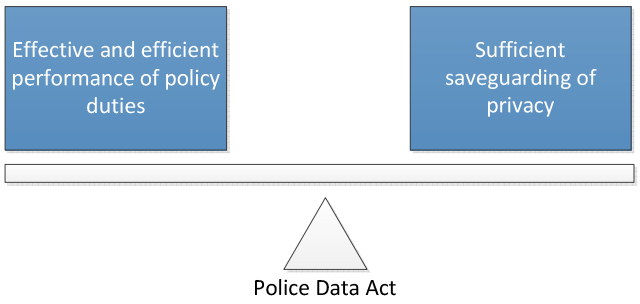
5. What was the legislative intention behind the Police Data Act (what was the policy theory)?
6. How has the Act been implemented in practice; is this consistent with the legislative goals and expectations, and what type of bottlenecks do police encounter?
7. How does the Act relate to other laws and regulations, such as the Personal Data Protection Act, the Government Information (Public Access) Act, and international laws and regulations?
8. How can the bottlenecks in implementing the Act be explained?

The survey was conducted between November 2012 and September 2013. Two tracks were followed. First, based on the audits performed in 2011 and in response to the subsequent audits conducted in 2012/2013, the degree to which compliance with the Police Data Act has been in line with the Act's requirements was analysed. Second, based on a large number of interviews, the bottlenecks experienced in carrying out police duties in relation to the Act were identified. Interviews were conducted, for instance, with the police (regional and nationwide units), the Ministry of Security and Justice, the Public Prosecution

Service, the Dutch Data Protection Authority (Dutch DPA), the Royal Netherlands Military Constabulary and the Special Investigation Services. Literature and documents were also used to reconstruct the policy theory and to reflect on the results of the interviews. For purposes of reflection as well, an expert meeting was organized with representatives of the relevant organizations.

General policy theory

The Police Data Act has two goals. On the one hand, it aims to afford sufficient latitude (more than used to be the case under the Data Protection (Police Files) Act) for processing (and providing) personal data, so that the police can carry out their duties effectively and efficiently. This includes having information flow freely within and between investigative agencies. On the other hand, the Police Data Act is intended to adequately safeguard the privacy of the persons whose data is processed. An ancillary objective of the Act is to reduce the administrative burdens experienced under the previous Act. The Police Data Act is based on the premise that there should be a proper, 'new balance' between the Act's two



primary goals.

To safeguard privacy properly, the Act imposes requirements regarding:

- the confidentiality and security of and access to (authorization for) data
- processing periods, retention periods and destruction
- the conditions under which data may be processed and furnished (necessity, purpose limitation, proportionality)
- supervision by a privacy officer, conducting audits and establishing protocols
- legal protection of interested parties in the form of a right of inspection
- external regulation by the Dutch DPA

The legislature expected that the Act would be in keeping with police practice and the anticipated developments in this area, such as the move towards nationwide information management. Training and education were viewed as the most important aspects concerning implementation.

Consistency of the implementation of the law

The audits conducted in 2011 revealed that the implementation of the Police Data Act was – four years after the Act's effective date – still deficient in many respects. This was particularly true for the regulation of authorizations (who may process which data?), the security of the data, the establishment of protocols (recording which data has been processed or furnished) and the application of the statutory periods for processing and destruction. Moreover, conducting periodic audits had not been embedded into the system, and internal control hardly took place or not at all. There were significant differences between the organizations (police corps, military constabulary) in the degree to which the Act had been complied with. Not a single organization was compliant in all areas. The action plan for improvement initiated in response to the audits has resulted in better compliance in several respects, specifically in terms of structuring the audits and the process for entering into agreements on furnishing data. Most units were waiting for nationwide models to be developed, partly in light of the creation of the national police force.

Bottlenecks experienced in carrying out police duties

The organizations felt that the Act was, generally speaking, difficult to read and interpret, including such terms as 'processing', the question of when the purpose of an investigation has been achieved and the question of under which processing regime police data falls.

Processing bottlenecks

With regard to the processing of police data, the statutory distinction between Article 8 (day-to-day police duties) and Article 9 (investigation) is a significant problem. In practice the status of data changes, and data cannot statically be placed under one of the processing regimes. Inputting changes takes a lot of time. Problems with retention periods are likewise experienced in performing certain police duties (such as combatting serious crime and solving cold cases). According to the interested parties, destruction of data five years after processing is too soon and reduces the availability of information. Several other problems were also identified with respect to determining the purpose of an investigation (which cannot always be specifically indicated), determining whether there have been computerized comparisons (does a search enquiry fall under this, too?) and the possibilities for conducting large-scale data research.

Bottlenecks relating to furnishing data

With respect to furnishing police data, the situation is especially ambiguous in the stage before an investigation (Article 9) is launched. Which data, for example, may be exchanged in getting a sense of whether an investigation must be commenced as part of cooperation with the Regional Information and Expertise Centre? As a result, there is a reluctance to

share information in those instances where the Police Data Act specifically contemplates more active sharing of information. Further, the agreements pile up on one another in practice. Thus, which data may be furnished to which organizations under which conditions is not entirely transparent or efficient. Also, the agreements about comparable cooperative arrangements differ across the country. Other problems include the different statutory frameworks which are or may apply to the jointly created files in connection with the collaboration and the use of social media (the proper etiquette in using such media).

Bottlenecks concerning the interested parties' rights

As regards the exercise of inspection rights, the problems mainly concern the administrative burden surrounding inspection requests regarding Criminal Intelligence Unit data and the increase in inspection rights for other reasons than the law intended (such as coping with grief). Insofar as the interested parties have complaints about the way inspection requests are dealt with, these primarily relate to the manner in which notice occurs (access, copies of documents, notice by telephone) or undeleted data.

Supervision bottlenecks

In terms of the supervision prescribed by the Police Data Act, the administrative burdens of establishing protocols are primarily seen as a problem, specifically as this pertains to furnishing police data while carrying out the day-to-day police duties (Article 8 of the Act). The amount of data furnished and the inadequate IT support come into play here as well. The control by privacy officers has not really got off the ground. The emphasis has been placed on the privacy officer's role in advising on the application of the Act.

Bottlenecks in conjunction with other laws

Other laws in addition to the Police Data Act regulate the processing of personal data and protection of privacy. The Police Data Act overlaps in particular with other Dutch criminal laws such as the Judicial Data and Criminal Records Act, the Criminal Code and the Personal Data Protection Act. Practical problems have been experienced in determining which statutory regime applies and of the resulting differences in retention periods.

In addition to the Police Data Act, the Government Information (Public Access) Act applies to the rights of interested parties. Lawmakers did not lay down a link in the Police Data Act to the Government Information (Public Access) Act. Practically speaking, the problems mainly revolve around the administrative burdens in handling Government Information (Public Access) Act requests.

Explanations for the bottlenecks

The bottlenecks in implementation and carrying out police duties under the Police Data Act can be explained by four main factors:

- the characteristics of the police organization
- the police's implementation strategy
- the substance and design of the Act
- external influences

Explanations based on the police organization

A major reason why proper implementation has not occurred is the long failure by the police organization as a whole and its management in particular to understand that this was necessary. The organization was archipelago-like in nature, too: under the banner of the 'police', 26 police corps were autonomously responsible for implementation. Until the Dutch DPA intervened in 2011, there were no incentives from any central authority 'forcing' the organization to put the Act into place. The practice under the Data Protection (Police Files) Act regime ('privacy, we'll take care of that ourselves') thus continued. IT is a second factor. The assumption by legislators that a single IT structure (supporting the Police Data Act) would come about has not proved true. The obsolete and fragmented IT system with auxiliary structures for the Police Data Act (i90 form for establishing protocols) has not made implementation of the Act impossible, but it has raised additional barriers.

Explanations based on the manner of implementation by the police

The police have opted for a business-oriented approach in implementing the Act: drawing up formats, protocols and working instructions. Virtually no attention has been paid to building up knowledge and awareness of the essential features of the Police Data Act, the police's interest with respect to performing their duties and the switch in mentality from professional safeguarding to more business-like safeguarding. Implementation of the Act was therefore thought of for a long time as something unpleasant which had to be done, and the Act (partly because of the poor IT support) came to be viewed as a bureaucratic hassle.

Explanations based on the Act itself

Several organizational requirements under the Police Data Act do not dovetail well with the practical dynamics. This is especially true of the partitioning between the various processing regimes and the lack of consistency or showing of overlap with other laws, such as the Public Records Act, the Police Act, the Government Information (Public Access) Act and the Personal Data Protection Act. The relatively heavy emphasis placed on organizational requirements and supervision is not really in line with the operating processes with respect, say, to keeping an authorization matrix and protocols manageable.

Various requirements or tools, such as formulating protocols and performing audits, have also been placed in the context of supervision, but these are primarily administrative/management tools (the results of which may be used for supervisory purposes, too). By categorizing these tools under the statutorily-mandated supervision, the Act has created an administrative model of control and assessment. This has not worked well in a context in which the Police Data Act has not been internalized, or the police have paid little attention to such internalization in implementing the Act.

Explanations based on external influences

The context in which police duties are carried out has changed since the Act was drafted and took effect. The tasks and responsibilities (such as the role of digitization in the nature and character of organized crime), the investigative methods (new techniques for digital analyses, for example), the change in the supply of information and thereby the potential and actual availability of information to the police, and ideas about privacy are no longer the same. Consequently, the limits on processing options (big data and crowd analyses) and furnishing data (say, through social media) are in flux. That applies, too, to the privacy limitations which the police must observe in performing their duties. A certain tension exists between the static design of the Police Data Act and the dynamic developments with which the police are faced.

Conclusions and final observations

Implementation of and compliance with the Police Data Act can be described as a 'struggle'. Remarkably, the various interested parties broadly endorse the Act's underlying goals and main elements, but the operationalization and implementation of the law has stymied its development and application. This is partly due to failures by the relevant organizations and partly to the Act's substance. Although there are no indications that informational privacy is being structurally and systematically breached, resulting in breaches in individuals' privacy, there have been patterns of incidents, and the police are still not 'in control' enough of their data.

On the other hand, the design requirements which the Act sets for the organizations concerned are partly at odds with efficient and effective operations and performance of certain police duties. In other words, the policy theory underpinning the Act is not entirely in keeping with achievement of the Act's two primary objectives.

Decompartimentalization and conformance of the models to the working processes, instead of conformance of the working processes to the Act

The distinction between processing regimes undermines the efficient and effective performance of police duties. The matters regulated by the specific processing regimes

(particularly Articles 8 and 9) are already in fact regulated generally by Article 3, which solely allows processing if there is a substantiated need, legitimacy and purpose limitation. Decompartimentalization gives the organization more options for modelling compliance with the Police Data Act based on the organization's own working processes, instead of having to model the working processes based on the Act.

Qualified retention periods

The five-year retention period after closing the processing of data should be deemed sufficient for the vast majority of police tasks. Longer retention periods may, though, be required to specifically combat serious crime. The problem is that it cannot always be determined in advance which data may prove to be relevant at a later time. From a privacy perspective, retaining everything is not an option. Destroying everything after the current statutory retention periods are over is not sensible from an investigative point of view. Still, the interest in protecting informational privacy must not be subordinated to the investigative interest. If a choice is made for a longer retention period – and postponement or abandonment of destruction – this will have to be based on a proper weighing of the interests. In addition, extra security for data and safeguarding for processing (special permission) will have to be arranged. At any rate, longer retention will be associated with increased administrative costs.

Clear distinction between supervision and quality assurance

The Police Data Act implicitly or explicitly piles up supervisory elements to a certain extent, partly because the establishment of protocols, the performance of audits and the privacy officer are expressly included under the chapter 'Supervision' in the Act. However the primary purpose of these tools as envisaged by the law too, is quality assurance and not being supervision. The inclusion of 'supervisory tools' not only makes matters bureaucratic for the organizations; it is even unlikely that it promotes protection of the police data. Preferably, a much clearer distinction should be made between the quality assurance for which the police are responsible and the statutory supervision by an external regulatory agency (the Dutch DPA). This is necessary from the standpoint of transparency, effectiveness of the supervision and internalization of informational privacy into the organization.

Focus on the quality of data and professional and business-like safeguarding within the national police

Safeguarding the quality of the data should, from a privacy protection viewpoint, be the police's most important concern. This demands cohesive, business-like and professional safeguarding, having an IT system which adequately supports compliance with the Police Data Act *and* proper securing of the data. This must go hand in hand with a new approach

to the question of how to keep the administration manageable, both for the organization as a whole and for the employees. Consistent with the plan for creating a nationwide police force, a good balance between business-like safeguarding and the employees' mores must in any event be assured.

Political reorientation to the expectations of the police, technical developments and privacy

Finally, a political assessment will have to be made regarding the desired availability of information to the police (and other investigative services). This must take into account the changes in organizations and manifestations of crime, the expectations placed on investigative agencies, the technical possibilities for investigation (and support provided), the evolving views on privacy and sharing information *and* the related privacy risks. The balance between effectively carrying out police duties and protecting informational privacy will have to be made again.

Inhoudsopgave

1 Inleiding en onderzoeksopzet

1.1 Achtergrond

Op 1 januari 2008 is de Wet politiegegevens (Wpg) in werking getreden ter vervanging van de Wet politieregisters (Wpolr). De Wpg regelt de wijze waarop politie, Koninklijke marechaussee (Kmar)[1] en Bijzondere opsporingsdiensten (BOD-en) om moeten gaan met politiegegevens, dat wil zeggen persoonsgegevens die worden verwerkt bij de uitvoering van politietaken. Ten opzichte van de Wpolr betekende de Wpg een verruiming van de verwerkingsmogelijkheden van politiegegevens, maar tevens een aanscherping van de waarborgen voor een zorgvuldige verwerking van persoonsgegevens. In de Wpg is bepaald dat de Minister van Veiligheid en Justitie binnen vijf jaar na de inwerkingtreding van de wet verslag uitbrengt over de doeltreffendheid en effecten van de wet in de praktijk.

Eind 2011/begin 2012 - vier jaar na de inwerkingtreding - zijn door de Departementale Auditdienst (DAD) van het ministerie van Veiligheid en Justitie audits uitgevoerd naar de implementatie van de Wpg door de politie en de Kmar. Uit deze audits bleek dat de praktijk nog op veel punten afweek van de eisen in de Wpg, *onder meer* als het gaat om de beveiliging, autorisaties, de registratie van verstrekking van gegevens aan derden en het interne toezicht op de naleving van de Wpg.

Met het oog op de evaluatiebepaling in de Wpg en de constateringen uit de audits als vertrekpunt hebben Arena Consulting en Pro Facto in opdracht van het Wetenschappelijk Onderzoeks- en Documentatiecentrum (WODC) van het ministerie van Veiligheid en Justitie de Wpg geëvalueerd. *Het accent lag op het nader in kaart brengen van de knelpunten bij de implementatie en de uitvoering van de politietaken en het verklaren van deze knelpunten.* Het onderzoek is gestart in november 2012 en afgerond in september 2013.

1.2 Vraagstelling van het onderzoek

De centrale onderzoeksvragen luiden als volgt[2]:

1. Wat heeft de wetgever beoogd met de Wet politiegegevens (wat is de beleidstheorie)?
    a. Wat zijn de doelstellingen van de Wpg?
    b. Hoe zijn de doelstellingen en verwachtingen geformuleerd voor de specifieke onderdelen autorisaties, verwerking, bewaartermijnen, verstrekkingen, kennisneming, toezicht en organisatorische waarborgen?
    c. Welke verwachtingen waren er ten aanzien van de uitvoerbaarheid en mogelijke neveneffecten?

[1] Er is gekozen voor de schrijfwijze van onder meer de Politiewet 2012, de Wpg en de Ambtsinstructie voor de politie en de Koninklijke marechaussee. In het gangbare taalgebruik wordt meestal Koninklijke Marechaussee, dus met dubbele hoofdletter gehanteerd.

[2] Dit is een beperkte herstructurering en samenvatting van de oorspronkelijke en meer gedetailleerde vraagstelling.

2. Hoe wordt de Wet politiegegevens in de praktijk uitgevoerd; is dit volgens de doelstellingen en de verwachtingen van de wetgever en wat zijn de resultaten en knelpunten?
   a. Is de uitvoeringspraktijk conform de wettelijke kaders?
   b. Welke knelpunten worden in de praktijk ervaren, met name als het gaat om autorisaties, verwerking, bewaartermijnen, verstrekkingen, kennisneming, toezicht en organisatorische waarborgen?
   c. Welke (onvoorziene) neveneffecten worden ervaren bij de uitvoering van politietaken?

3. Hoe verhoudt de Wpg zich tot aanpalende wet- en regelgeving zoals de Wet bescherming persoonsgegevens (Wbp), de Wet openbaarheid bestuur (Wob) en internationale wet- en regelgeving?

4. Hoe kunnen de knelpunten bij de invoering van de wet en de uitvoering van de wettelijke regels verklaard worden?

Op basis van het voorgaande worden conclusies getrokken over het wettelijk kader en de uitvoeringpraktijk inzake de verwerking van politiegegevens.

1.3 Centrale begrippen

De Wpg heeft betrekking op de bescherming van de privacy bij de verwerking van politiegegevens die in het kader van de uitvoering van de politietaak, als bedoeld in de artikelen 3 en 4, eerste lid, van de Politiewet 2012, in een bestand zijn opgenomen of die bestemd zijn daarin te worden opgenomen.[3]

Privacy

Het begrip *privacy* wordt veelal gebruikt om te verwijzen naar de mogelijkheid van mensen om ongestoord zichzelf te kunnen zijn.[4] De wet- en regelgeving ter bescherming van persoonsgegevens vindt haar oorsprong in het grondrecht van de burger op eerbiediging van zijn persoonlijke levenssfeer.[5]

Op Europees niveau is het recht op eerbiediging van privéleven, familie- en gezinsleven onder andere neergelegd in artikel 8 EVRM. In het tweede lid van dit artikel zijn de voorwaarden neergelegd waaronder een beperking op de privacy mag plaatsvinden. Een beperking van het privacyrecht mag alleen plaatsvinden voor zover dit bij de wet is

[3] Artikel 2 lid 1 en artikel 1 onder a en b Wpg.
[4] *Elektronische overheid en privacy. Bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid*, College bescherming persoonsgegevens, Den Haag, juli 2002, p. 9.
[5] Idem.

voorzien, deze noodzakelijk is in een democratische samenleving en deze beperking ten slotte plaatsvindt in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen. Een aantasting is noodzakelijk als sprake is van een dringende noodzaak ('pressing social need') en als de aantasting voldoet aan de vereisten van proportionaliteit en subsidiariteit.

Artikel 10 van de Grondwet stelt dat iedereen recht heeft op eerbiediging van zijn persoonlijke levenssfeer. De bescherming van persoonsgegevens is daarvan een onderdeel. Het tweede lid van artikel 10 Grondwet bepaalt dat wettelijke regels moeten worden gesteld ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. Personen hebben aanspraak op kennisneming en verbetering van over hen vastgelegde gegevens en het gebruik dat daarvan wordt gemaakt (artikel 10 lid 2 Grondwet). Het recht op eerbiediging van de persoonlijke levenssfeer kan in bepaalde gevallen worden beperkt.

Een conceptuele uitwerking van het begrip 'persoonlijke levenssfeer' (of: privacy) is lastig. Dit komt doordat de betekenis van dit begrip veranderlijk, flexibel en contextafhankelijk is. Denk daarbij aan de vraag wat tot de persoonlijke levenssfeer moet worden gerekend. Daarbij spelen ook de normen en waarden van de betrokkene een rol. In de literatuur wordt aangegeven dat ´privacy´ vooral fungeert als een geaccepteerd instrument in normatieve argumentaties waaraan verschillende waarden ten grondslag liggen. Het begrip privacy is daarmee een relatief begrip dat context- en functieafhankelijk is[6].

Politiegegevens: informationele privacy

De Wpg heeft betrekking op informationele privacy. Bij de informationele privacy gaat het om de bescherming tegen ongewenste openbaarmaking van informatie over de persoonlijke levenssfeer. Informationele privacy heeft enerzijds het doel bij te dragen aan indirecte bescherming van de fysieke en relationele privacy. Daarnaast dienen principes van een behoorlijke omgang met persoonsgegevens, zoals juistheid en vertrouwelijkheid, een breder doel dan privacy alleen. Andere belangrijke argumenten voor zorgvuldigheid zijn het voorkomen van schade door misbruik (bijv. identiteitsfraude), de economische waarde (de burger kent vaak de waarde niet die zijn of haar persoonsgegevens hebben en hoe die waarde wordt benut) en het voorkomen van discriminatie.[7]

---

[6] Zie bijvoorbeeld Bert-Jaap Koops en Anton Vedder, Opsporing versus privacy: de beleving van burgers. IteR-reeks nr. 45. Den Haag, 2001.

[7] *Elektronische overheid en privacy. Bescherming van persoonsgegevens in de informatie-infrastructuur van de overheid*, College bescherming persoonsgegevens, Den Haag, juli 2002, p. 9.

Volgens de Wpg zijn politiegegevens persoonsgegevens, d.w.z. gegevens betreffende geïdentificeerde of identificeerbare natuurlijke personen die bij de uitoefening van de politietaken, bedoeld in de artikelen 3 en 4 van de Politiewet 2012, worden verwerkt.[8]

Verwerken

Onder het verwerken van persoonsgegevens wordt op grond van artikel 1 onder c van de Wpg verstaan: *'elke handeling of elk geheel van handelingen met betrekking tot politiegegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, vergelijken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van politiegegevens'*.

Politietaken

De Wpg heeft alleen betrekking op de uitvoering van politietaken. De Politiewet (artikel 3) omschrijft dit als '*de daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven'.* In de praktijk wordt daarbij veelal een onderscheid gemaakt in enerzijds dagelijkse politietaken als preventie, handhaving openbare orde en hulpverlening en anderzijds de opsporing van strafbare feiten. In grote lijnen lopen hierin ook de scheidslijnen in de politieorganisatie tussen 'blauw' en recherche.

De Wpg heeft niet alleen betrekking op de politie, maar ook op andere organisaties die politietaken uitvoeren. Daaronder worden naast de Kmar ook de volgende BOD-en verstaan**:**[9]

1. NVWA-IOD: de nieuwe Voedsel en Waren Autoriteit – Inlichtingen- en Opsporingsdienst van het ministerie van Economische Zaken, Landbouw en Innovatie;
2. FIOD: de Fiscale Inlichtingen- en Opsporingsdienst van het ministerie van Financiën;
3. Inspectie SZW: de directie Opsporing van het ministerie van Sociale Zaken en Werkgelegenheid;
4. ILT-IOD: de Inspectie Leefomgeving en Transport – Inlichtingen- en Opsporingsdienst van het ministerie van Infrastructuur en Milieu.

De Wpg geldt sinds 2010 ook voor de Openbare Lichamen Bonaire, Sint Eustatius en Saba.[10]

[8] Artikel 1 onder a Wpb.
[9] Art. 2 Wet bijzondere opsporingsdiensten en Besluit Wpg bijzondere opsporingsdiensten.
[10] Wet van 30 september 2010, Stb. 2010, 362 in werking op 10 oktober 2010.

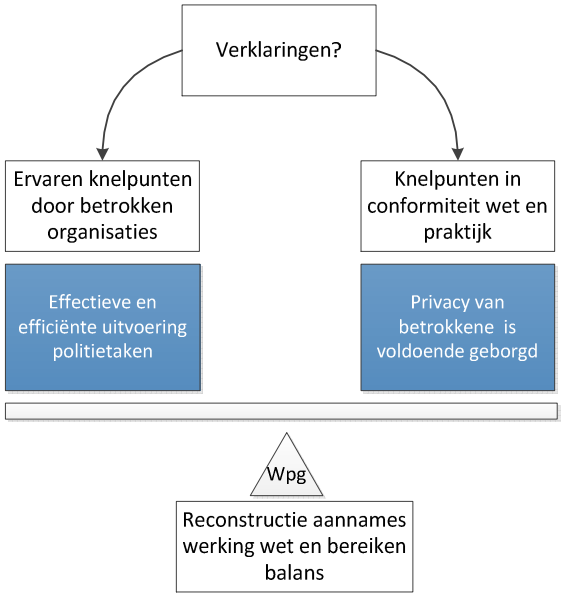
1.4 Globaal onderzoeksmodel

De focus van het onderzoek heeft gelegen op het verkennen van de knelpunten rond de Wpg bij de uitvoering van politietaken en op het verklaren van deze knelpunten. De knelpunten zijn daarbij belicht vanuit twee invalshoeken:

1. De mate waarin de Wpg knelpunten oplevert voor de *uitvoering van politietaken* door politie, Kmar, BOD-en en Openbaar Ministerie (OM)
2. *Conformiteit tussen wet en praktijk*, te weten de mate waarin de vereisten in de Wpg ook zijn geborgd bij de organisaties die onder de Wpg vallen.

Achter de eerste invalshoek ligt de vraag besloten of de Wpg volgens de betrokken organisaties bijdraagt aan een effectieve en efficiënte uitvoering van politietaken of in elk geval daarvoor geen belemmeringen vormt. Achter het tweede invalshoek ligt de vraag besloten of – uitgaande van de beleidstheorie van de Wpg – de bescherming van persoonsgegevens in de uitvoering van de wet is geborgd bij de organisaties die onder de Wpg vallen en of daarmee (de risico's op) een ongewenste aantasting van de persoonlijke levenssfeer zoveel mogelijk worden beperkt. In paragraaf 1.5 is nader gespecificeerd hoe dit is gemeten.

Figuur 1.1: Globaal onderzoeksmodel met drie centrale onderzoeksobjecten: de reconstructie van de beleidstheorie van de Wpg, de knelpunten die zich in de praktijk voordoen (vanuit het perspectief van de wet en vanuit het perspectief van betrokken organisaties) en de verklaringen voor deze knelpunten.



Beleidstheorie als vertrekpunt

Vertrekpunt van het onderzoek was de beleidstheorie van de Wpg, meer specifiek de achterliggende doelstellingen en de aannames over hoe de inrichting van de wet bijdraagt aan het realiseren van deze doelstellingen.

De doelstelling van de Wpg is tweeledig, te weten voldoende ruime mogelijkheden bieden om politiegegevens te kunnen verwerken met het oog op de uitvoering van politietaken en anderzijds een afdoende bescherming van de privacy. De aanname daarbij was dat de wijze waarop de Wpg is uitgewerkt, ervoor zorgt dat deze twee doelstellingen voldoende in balans zijn. Deze aannames zijn in het kader van het onderzoek nader onderzocht en gereconstrueerd. Deze reconstructie is mede gebruikt als raamwerk voor de dataverzameling (vraagstelling in de interviews) en de analyse (zijn de aannames van de wetgever ook in de praktijk gerealiseerd?).

Afbakening

Een gedetailleerde analyse van de organisatie van de politie in het licht van de uitvoering van de Wpg zelf, bijvoorbeeld met betrekking tot de opzet in extenso van de ICT, is geen onderdeel van het onderzoek. Wel zijn de knelpunten die door politie, Kmar en andere relevante organisaties meer in algemene zin met de ICT worden ervaren in het onderzoek betrokken. Het onderzoek is evenmin gericht op het in beeld brengen of het (op onderdelen) niet naleven van bepaalde regels van de Wpg tot een aantasting van de persoonlijke levenssfeer van de betrokken personen heeft geleid. Er heeft mede op basis van enkele interviews wel een reflectie van de onderzoeksresultaten plaatsgevonden vanuit privacy-optiek.

Context onderzoek

Het onderzoek heeft plaatsgevonden in de periode dat de uitkomsten van de audits naar de uitvoering van de Wpg net bekend waren bij de korpsen. Daarnaast speelde in de onderzoeksperiode de (voorbereiding van de) inrichting van de Nationale politie. Het onderzoeksobject was gedurende de onderzoeksperiode derhalve in beweging. Dit betekent bijvoorbeeld dat, terwijl het onderzoek liep, de politie ook bezig was met een verbeterslag naar aanleiding van de audits uit 2011/2012 én met de algehele herinrichting van de organisatie. De beschreven knelpunten bij de implementatie betreffen de stand van zaken eind 2012/begin 2013.

1.5 Onderzoeksaanpak

Het onderzoek is een kwalitatief bestuurskundig onderzoek dat grotendeels is uitgevoerd aan de hand van documentenanalyse en interviews. Er is daarbij aandacht geschonken aan zowel de meer juridische als de meer organisatorische facetten van de naleving van de

Wpg. De analyse is uitgevoerd op het niveau van de gereconstrueerde beleidstheorie. Dat houdt in dat juridisch en bedrijfsmatig niet in detail is getreden . Onderstaand is uiteengezet hoe daarbij te werk is gegaan.

Reconstructie beleidstheorie

De reconstructie van de beleidstheorie omvat een vereenvoudigde weergave van de aannames van de wetgever over de werking van de Wpg: hoe wordt deze geacht bij te dragen aan het effectief en efficiënt kunnen uitvoeren van politietaken met inachtneming van voldoende bescherming van de privacy van betrokkenen?

De reconstructie is uitgevoerd aan de hand van een analyse van primaire documenten over de (totstandkoming van de) Wpg (wettekst, memorie van toelichting, correspondentie etc.) en secundaire literatuur zoals eerder uitgevoerd onderzoek naar de Wpg en de privacywetgeving. Daarnaast zijn gesprekken gevoerd met personen die betrokken waren bij het tot stand komen van de Wpg, de implementatie van de Wpg of daar onderzoek naar hebben gedaan. Er is onder meer gesproken met penvoerders van de Wpg, (voormalig) projectleiders Wpg bij de politie, de politieleiding, het CBP, onderzoekers van de departementale auditdienst van het ministerie van Veiligheid en Justitie en wetenschappers. De gesprekken zijn tevens gebruikt voor een eerste oriëntatie op de knelpunten en verklaringen daarvoor.

In kaart brengen in welk mate de Wpg wordt nageleefd

Zoals aangegeven zijn in 2011/2012 bij alle organisaties die onder de Wpg vallen audits uitgevoerd. Een groot deel van deze audits is uitgevoerd door de departementale auditdienst van het ministerie van Veiligheid en Justitie. De BOD-en en het voormalige regiokorps Zeeland hebben de audit langs een andere weg uitgevoerd.

De auditrapportages – en annotaties daarop – zijn door ons gebruikt als basis om in beeld te brengen in hoeverre de praktijk in overeenstemming is met de wet. Meer specifiek is gekeken in welke mate de Wpg in formele zin wordt nageleefd en of dit naleven is geborgd in de organisatie. In de audits – en daarmee ook in het voorliggende onderzoek – is slechts beperkt gekeken naar de mate waarin bij de uitvoering van politietaken ook in materiële zin, dat wil zeggen conform de vastgestelde protocollen en processen, wordt gewerkt. Doordat de uitkomsten van de hercontroles nog konden worden meegenomen in het onderzoek, is het beeld van de formele naleving van wet de situatie van medio 2013.

In kaart brengen van door organisaties ervaren knelpunten

Om de door de betrokken organisaties ervaren knelpunten bij de uitvoering van politietaken in beeld te brengen, is een groot aantal gesprekken gevoerd. Centrale gesprekspunten waren:

- de ervaren veranderingen vergeleken met de situatie vóór de Wpg in werking trad.
- de wijze waarop de implementatie is verlopen.
- de ervaren knelpunten bij de uitvoering van politietaken in relatie tot de Wpg.
- de verklaringen die de betrokkenen hebben voor knelpunten.

De respondenten zijn geselecteerd aan de hand van een gestratificeerde steekproef op basis van organisatietype en functie van de respondenten. De organisaties zijn geselecteerd op basis van twee criteria:

- De organisatie staat te boek als een 'good practice'.
- Spreiding in organisatiekenmerken.

De aanname bij het eerste criterium was dat als een 'good practice' knelpunten ervaart, de oorzaken daarvan mogelijk minder in de wijze van implementatie en organisatie moeten worden gezocht en daarmee terug te voeren zijn op de wet of externe factoren. De selectie van de 'good practices' is gemaakt op basis van de uitkomsten van de audits uit 2011. Bij het tweede criterium is het uitgangspunt dat de organisaties waar interviews worden afgenomen zoveel mogelijk van elkaar moeten verschillen om te kunnen beoordelen of knelpunten en gevolgen en verklaringen daarvoor ook verschillen. Op grond daarvan is geselecteerd op type organisatie, grootte en regionale spreiding.

Dit heeft geleid tot de selectie van drie politie-eenheden, te weten een relatief grotere territoriale eenheid (Amsterdam-Amstelland), een relatief kleinere territoriale eenheid (Limburg) en de landelijke eenheid (onderdelen recherche en de dienst Landelijke Informatie Organisatie, LIO)[11]. Daarnaast is de Kmar geselecteerd omdat het vergeleken met de politie een 'a-typische' organisatie is. Per organisatie is gesproken met:

- Leidinggevenden.
- Projectleiders implementatie Wpg.
- Privacyfunctionarissen.
- Rechercheurs.
- Agenten uit de uniformdienst[12].
- Gegevensanalisten/informatiemakelaars.
- Overige functionarissen.

[11] Bij de eenheid Limburg heeft het accent gelegen op het voormalige korps Limburg Noord dat relatief positief uit de audits kwam.
[12] Waar in de tekst verder wordt gesproken over 'agenten' wordt bedoeld 'agenten uit de uniformdienst'; waar wordt gesproken over 'rechercheurs' worden bedoeld agenten die niet in de uniformdienst zitten.

Hierdoor kon vanuit verschillende perspectieven en samenhangend worden gekeken naar de uitvoeringspraktijk in het algemeen en de knelpunten die worden ervaren bij de uitvoering van politietaken in het bijzonder.

Expertmeeting en reflectiegesprekken

Op basis van een eerste analyse zijn de voorlopige onderzoeksbevindingen geformuleerd en voorgelegd tijdens een expertmeeting. Daarbij waren vertegenwoordigers van de politie, het OM, de Kmar, het Landelijk Informatie en Expertise Centrum (LIEC) en gemeenten aanwezig. Centraal in de expertmeeting stond de herkenbaarheid van de voorlopige bevindingen en de duiding (verklaring) daarvan. Naast de expertmeeting zijn nog enkele bilaterale reflectiegesprekken gevoerd met het OM, het ministerie van Veiligheid en Justitie en de politie. In de afsluitende fase is een aantal meer specifieke reflectiegesprekken gevoerd, gericht op de vraag hoe de bevindingen moeten worden gezien in het licht van de (risico's voor de) privacybescherming. In dat kader is gesproken met de Nationale Ombudsman, de Nederlandse Orde van Advocaten[13] en het College bescherming persoonsgegevens (CBP)[14].

1.6 Leeswijzer

De rapportage is opgebouwd uit drie onderdelen.

Deel I: Achtergrond, beleidstheorie en inhoud Wpg

Hoofdstuk 2 gaat in op de achtergrond en beleidstheorie van de Wpg. Meer specifiek gaat het daarbij om de vraag welke aannames de wetgever had over de werking van de wet in de praktijk. Hoofdstuk 3 geeft een korte samenvatting van de inhoud en opzet van de wet.

Deel II: Knelpunten in de praktijk

In deel II gaan we in op de uitvoeringspraktijk. Daarbij wordt enerzijds (in hoofdzaak) op basis van de audits uit 2011/2012 en de hercontroles uit 2012/2013 in beeld gebracht in hoeverre de Wpg is verankerd in de uitvoeringspraktijk. Anderzijds wordt aan de hand van interviews beschreven welke knelpunten politie, OM, Kmar en BOD-en in relatie tot de Wpg ervaren bij de uitvoering van politietaken. We gaan achtereenvolgens in op de algemene uitgangspunten van de Wpg (hoofdstuk 4), de verwerking van politiegegevens (hoofdstuk 5), de verstrekking van politiegegevens (hoofdstuk 6), de rechtsbescherming (hoofdstuk 7) en het toezicht (hoofdstuk 8). Deze hoofdstukken volgen daarmee de eerste 5 paragrafen van de Wpg. In hoofdstuk 9 gaan we in op de relatie tussen de Wpg en andere wetgeving, meer specifiek de Wet openbaarheid van bestuur (Wob).

---

[13] In dat verband is ook Bits of Freedom (BoF) benaderd voor een gesprek. BoF wenste echter niet aan het onderzoek mee te werken. Met de politie(project)leiding, het ministerie van V&J en het CBP zijn zowel gesprekken gevoerd bij de start van het onderzoek als in de reflectiefase.

[14] Er is gesproken met twee door de Nederlandse Orde van Advocaten benaderde advocaten. Zie bijlage 2.

Deel III: Nadere analyse en conclusies

Deel III bestaat uit drie hoofdstukken. Hoofdstuk 10 gaat in op de verklaringen voor de knelpunten bij de implementatie van de Wpg en uitvoering van politietaken in relatie tot de Wpg. In hoofdstuk 11 worden de vier centrale onderzoeksvragen beantwoord. De rapportage sluit in hoofdstuk 12 af met een slotbeschouwing.

De bijlagen bevatten een overzicht van de geraadpleegde literatuur en documenten, een schematische weergaven van de transitie van Wpolr naar Wpg, de geïnterviewde personen, de deelnemers aan de expertmeeting, de leden van de begeleidingscommissie van het onderzoek en een lijst met gebruikte afkortingen.

DEEL I: Achtergrond, beleidstheorie en inhoud Wpg

2 Achtergrond en beleidstheorie Wet politiegegevens

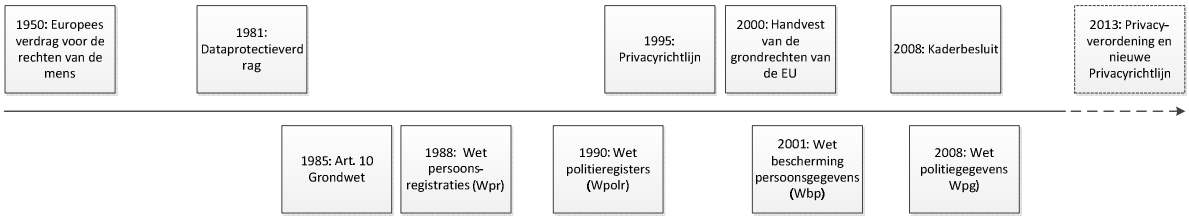
2.1 Inleiding

Dit hoofdstuk gaat in op achtergrond en beleidstheorie van de Wpg. We staan stil bij het globale juridische kader van de privacywetgeving (paragraaf 2.2), de voorloper van de Wpg, te weten de Wet politieregisters (paragraaf 2.3), de algemene doelstellingen en beleidstheorie van de Wpg (paragraaf 2.4) en de meer specifieke aannames (paragrafen 2.5 tot en met 2.8). We sluiten af met samenvattende bevindingen (paragraaf 2.9).

2.2 Privacywetgeving

Zowel op Europees als op nationaal niveau gelden regelingen over privacy en de verwerking van persoonsgegevens. De ontwikkeling daarvan de afgelopen decennia is samengevat als volgt.

Figuur 2.1: Globale tijdlijn ontwikkeling privacywetgeving



Europese regelgeving

De basis voor de nationale regelgeving over het verwerken van persoonsgegevens is gelegd in het Europees Verdrag voor de Rechten van de Mens (EVRM) uit 1950. In artikel 8 van dit verdrag is onder andere het recht op eerbiediging van het privéleven neergelegd.[15] In het Data-protectieverdrag van 1981[16] is meer specifiek de privacy bij de geautomatiseerde verwerking van persoonsgegevens geregeld. Ontwikkelingen in ICT en informatiegebruik, bijvoorbeeld de mogelijkheden om informatie uit verschillende bestanden te combineren en het gebruik van persoonsgegevens voor marketingdoeleinden, leidden in 1995 tot de Europese Privacyrichtlijn[17]. In het Handvest van de Grondrechten[18] van de Europese Unie (2000) zijn het recht op privacy (artikel 7) en de aanspraak op de bescherming van persoonsgegevens (artikel 8) verder uitgewerkt en in het zogenaamde Kaderbesluit (2008)[19] de bescherming van persoonsgegevens bij politiële en justitiële samenwerking in

[15] Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden.
[16] Verdrag van de Raad van Europa ter bescherming van personen met het oog op de geautomatiseerde verwerking van persoonsgegevens. Dit verdrag wordt ook wel het Verdrag van Straatsburg of Conventie 108 genoemd.
[17] Richtlijn 95/46/EG betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (24 oktober 1995).
[18] Handvest van de Grondrechten van de Europese Unie, 7 december 2000, PbEG 2000, C364/1.
[19] Kaderbesluit 2008/977/JBZ van de Raad van de Europese Unie van 27 november 2008, PbEU 2008, L350/60.

strafzaken.[20] Op dit moment (medio 2013) is een voorstel van de Europese commissie in behandeling om de eerdergenoemde Privacyrichtlijn te vervangen door een Europese verordening. De opsporing en vervolging van strafbare feiten en de tenuitvoerlegging van straffen vallen niet onder de reikwijdte van de ontwerpverordening. Voor de verwerking van persoonsgegevens in het kader van die taken komt een aparte richtlijn.

Nederlandse verankering

In 1983 is in artikel 10 van de Nederlandse Grondwet vastgelegd dat de wet regels stelt ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens. Dit heeft in 1988 geleid tot de Wet persoonsregistraties (Wpr) en, na de totstandkoming van de Europese Privacyrichtlijn, in 2001 tot de Wet bescherming persoonsgegevens (Wbp). De Wbp geeft de voorwaarden waaronder persoonsgegevens rechtmatig verwerkt kunnen worden en geeft waarborgen aan de personen wier gegevens verwerkt worden. Hierbij gaat het bijvoorbeeld om het recht van betrokkenen om inzage en correctie. Als toezichthouder van de Wbp is het CBP ingesteld.

2.3 Privacywetgeving politie

Keuze voor separate wet voor privacybescherming bij gebruik politiegegevens

De Nederlandse wetgever heeft van meet af aan gekozen voor aparte privacywetgeving voor de politie. Dit in tegenstelling tot de meeste Europese landen die de algemene privacywetgeving die voortvloeit uit de Privacyrichtlijn van toepassing hebben verklaard op gegevensverwerking door de politie.[21] De wetgever noemt zes redenen:[22]

1. Het gaat om gegevens die vaak niet van de persoon zelf afkomstig zijn; de persoon heeft vaak ook geen toestemming verleend voor het gebruik.
2. Het gaat vaak om het gebruik van gevoelige gegevens, bijvoorbeeld vanwege betrokkenheid bij criminaliteit.
3. De verhouding tussen politie en burger is niet gelijkwaardig, daarbij moet ervoor worden gewaakt dat de belangen van de burger niet ondermijnd worden.
4. Er was en is sprake van steeds meer mogelijkheden om gegevens te koppelen. De wetgever vond het wenselijk om zeker bij persoonsgegevens die door de politie worden gebruikt, extra waarborgen in te bouwen.
5. Politiegegevens brengen een beperkte inzage door de burger met zich mee.
6. De gevoeligheid van de inhoud van de gegevens vereist dat wettelijk is vastgelegd wie verantwoordelijk is voor het beheer en gebruik.

[20] Dit Kaderbesluit is op 1 april 2012 in de Wpg (en de Wjsg) geimplementeerd, Wet van 6 oktober 2011, Stb. 2011, 490.
[21] Egelkamp en Mein 2003 en Mac Gillavry 2005.
[22] *Kamerstukken II 2005/2006*, 30 327, nr. 3, p. 2 en 3.

Strekking wet politieregisters

In 1990 trad de Wet politieregisters (Wpolr) in werking. Centraal in deze wet stond het begrip politieregister. Hieronder werd verstaan '*een samenhangende verzameling van op verschillende personen betrekking hebbende persoonsgegevens die langs geautomatiseerde weg wordt gevoerd of met het oog op een doeltreffende raadpleging van die gegevens systematisch is aangelegd, en die is aangelegd ten dienste van de uitvoering van de politietaak (artikel 1 onder c Wpolr)*'.

Een politieregister mocht slechts worden aangelegd voor een bepaald *doel* en voor zover dit *noodzakelijk* was voor een goede uitvoering van de politietaak. Voor elk politieregister moest worden vastgelegd wat doel, soort gegevens en moment van verwijdering waren.

Onder de Wpolr gold een *gesloten verstrekkingsregime*; politiegegevens mochten alleen worden verstrekt aan de personen binnen de politie die waren belast met de uitvoering van de politietaak en aan personen en instanties die in de Wpolr en het Besluit politieregisters (Bpolr) waren genoemd. Het Bpolr regelde wanneer van verstrekkingen aantekening moest worden gemaakt, de zogenaamde *protocolplicht*.

Geregistreerden hadden het recht om kennis te nemen van de vastgelegde gegevens en konden verzoeken gegevens aan te passen of te verwijderen. Bij klachten konden zij zich wenden tot de korpsbeheerder, de rechter of de Registratiekamer, de voorloper van het CBP. Er konden voor een onderzoek voor de duur van zes maanden tijdelijke registers worden ingesteld (met mogelijkheid van verlenging). Hierbij gold geen reglementsplicht.

Heroverwegingen

Met het in werking treden van de Wbp, ontstond de behoefte de Wpolr daarmee begripsmatig in lijn te brengen en een aantal knelpunten in de Wpolr op te lossen:

- De behoefte aan ruimere mogelijkheden tot het verwerken van gegevens over personen die (nog) niet als verdachte zijn aangemerkt of aan te merken. De verwerkingstermijn van deze politiegegevens was in de Wpolr begrensd tot vier maanden. Dat werd als te kort ervaren.
- De Wpolr was onvoldoende toegesneden op het verwerken van gegevens om zicht te verkrijgen op maatschappelijke problemen die samenhangen met criminaliteit.
- De uitvoering van politietaken werd belemmerd doordat met een bepaald doel verzamelde gegevens maar beperkt gebruikt konden worden voor andere doelen.
- Het gesloten verstrekkingsregime van de Wpolr sloot niet aan bij de behoefte om gegevens te kunnen verstrekken aan instanties waarmee de politie samenwerkt.[23]

[23] *Kamerstukken II 2005/2006*, 30 327, nr. 3, p. 3.

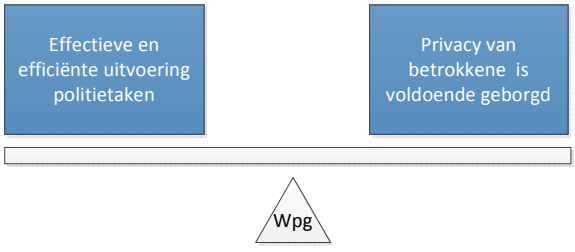
Deze knelpunten werden gezien in het licht van de ontwikkelingen in de informatie- en communicatietechnologie en de samenleving en het karakter van (georganiseerde) criminaliteit. De gedachte was dat de politie systematischer kon werken doordat een landelijke informatiehuishouding voor de gehele Nederlandse politie werd ontwikkeld. Door de informatisering waren de mogelijkheden tot het leggen van verbanden tussen gegevens toegenomen. Daarnaast was het belang van een goede informatiehuishouding gestegen doordat het politiewerk complexer werd. Deze complexiteit ontstond volgens de wetgever door de groei en toename in mobiliteit en geschakeerdheid van de bevolking, bestuurlijke en maatschappelijke schaalvergroting en internationalisering. Ook wat betreft (georganiseerde) criminaliteit. De behoefte om informatie uit te wisselen met andere (ook buitenlandse) instanties nam toe.[24] De aanpassingen in de Wpolr om een en ander mogelijk te maken, zouden dusdanig ingrijpend zijn dat de wetgever besloot van herziening af te zien en een nieuwe wet op te stellen, de Wet politiegegevens (Wpg).

2.4 Wet politiegegevens (Wpg)

Doelstellingen Wpg

De in 2008 in werking getreden Wpg heeft een tweeledige doelstelling. Enerzijds meer ruimte bieden voor de verwerking (inclusief verstrekking) van persoonsgegevens van de Wpolr. Dat moet een een effectieve en efficiënte uitvoering van de politietaken mogelijk maken. Anderzijds het waarborgen van de privacy van degene waarvan gegevens worden verwerkt. Deze dubbele doelstelling van de Wpg heeft een zekere ambivalentie. De verruiming van de verwerkingsmogelijkheden kan immers op gespannen voet staan met de bescherming van de privacy. Het uitgangspunt van de wet is dat er voldoende balans ('nieuw evenwicht') tussen deze twee doelstellingen moet zijn[25].

Figuur 2.2: Doelstellingen Wpg, balans tussen effectieve uitvoering politietaken en bescherming privacy van degene waarvan gegevens worden verwerkt.



Naast deze hoofddoelstellingen beoogt de Wpg een harmonisatie van de privacyregelgeving die geldt bij de uitvoering van politietaken met de algemene privacywetgeving, in het

[24] *Kamerstukken II 2005/2006*, 30 327, nr. 3, p. 2 en 3.
[25] *Kamerstukken II 2005/2006*, 30 327, nr. 3, p. 1.

bijzonder de Wbp. Een nevendoelstelling van de Wpg is ook het verminderen van de administratieve lasten die werden ervaren bij de Wet politieregisters.

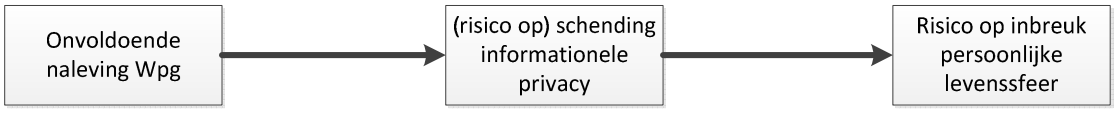
2.5 Beknopte beleidstheorie

De Wpg wil de knelpunten die zich voordeden bij de uitvoering van de Wpolr wegnemen en tevens een raamwerk bieden om de politietaken (qua gebruik van persoonsgegevens) in het licht van de maatschappelijke en technologische ontwikkelingen effectief en efficiënt te kunnen uitvoeren. Dit betekende op verschillende onderdelen een verruiming van de verwerkingsmogelijkheden. Onder meer waar het gaat om de duur van de periode waarin gegevens mogen worden verwerkt (en bewaard), het doel waarvoor gegevens mogen worden verwerkt, de personen van wie gegevens mogen worden verwerkt en de mogelijkheden om gegevens aan derden te verstrekken. Dit binnen de conditie dat de rechtsbeginselen van privacy voldoende in acht worden genomen. Daarbij gaat het om:

- Doelbinding: verwerking vindt alleen plaats voor specifiek omschreven doel.
- Proportionaliteit: inbreuk privacy staat in verhouding tot doel verwerking.
- Transparantie: verwerking is navolgbaar.
- Rechtmatigheid: verwerking in overeenstemming met geldige regels en besluiten.
- Noodzakelijkheid: het verwerken is noodzakelijk voor het specifieke doel.

Deze rechtsbeginselen zijn in de Wpg verankerd, door waarborgen in de vorm van bijvoorbeeld autorisaties en beveiliging. De gedachte van de Wpg is dat de gestelde eisen een waarborg zijn tegen (risico's op) inbreuken in de informationele privacy en als mogelijk gevolg daarvan aantasting van de persoonlijke levenssfeer en schade. De (impliciete) aanname is dat de bescherming van de informationele privacy en de persoonlijke levenssfeer in de basis voldoende is gewaarborgd als de Wpg wordt nageleefd[26].

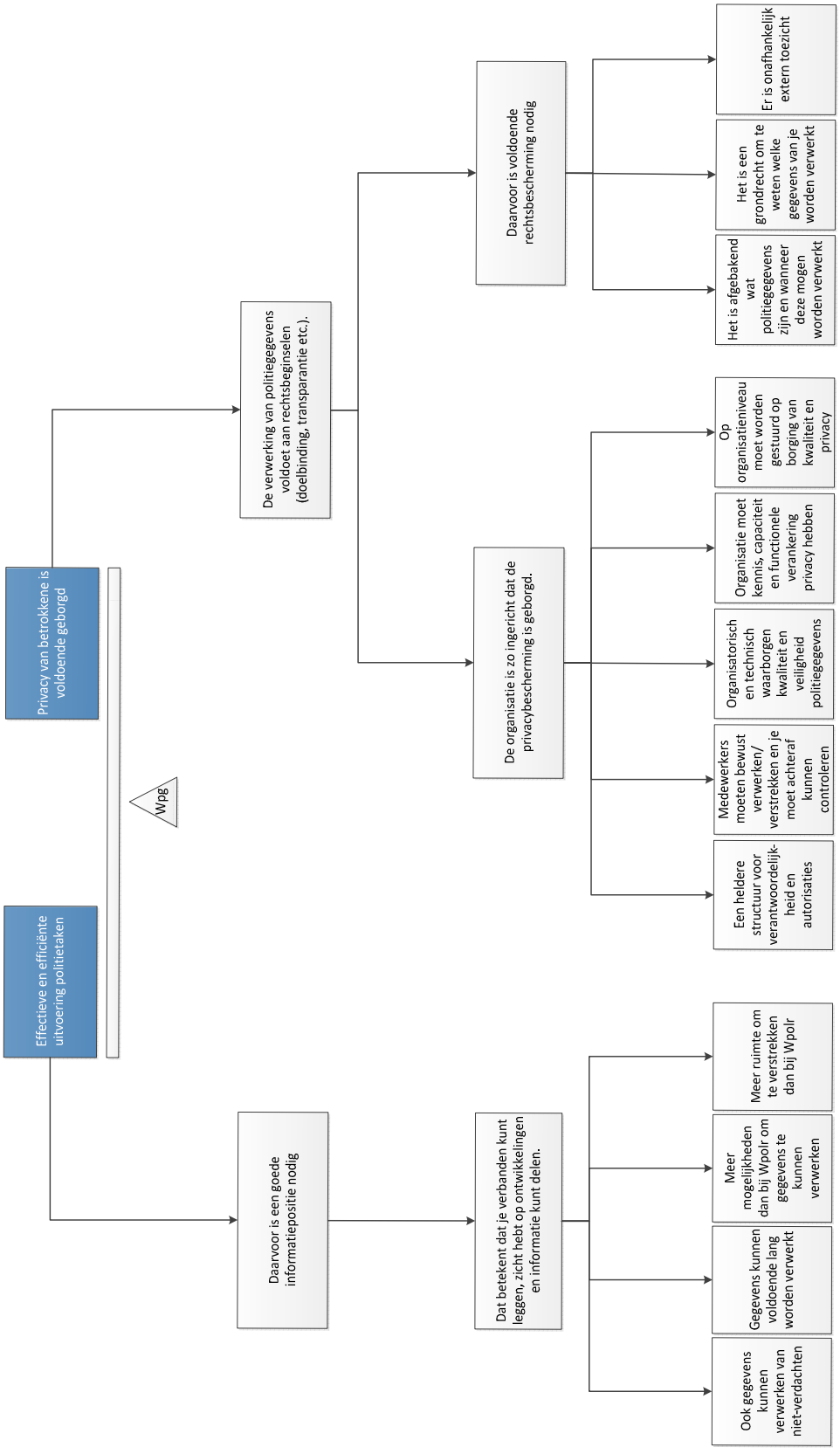
Figuur 2.3: Achterliggende aannames relaties tussen onvoldoende naleving Wpg en risico's voor



Daarbij staat niet voor alle normen of waarborgen in de Wpg het overtreden ervan direct gelijk aan het ook feitelijk plegen van inbreuk op de informationele privacy of de persoonlijke levenssfeer van betrokkenen. Van een directe inbreuk kan sprake zijn bij bijvoorbeeld het onterecht verstrekken of het verstrekken van onjuiste gegevens. Van een verhoogd risico op een inbreuk is in de beleidstheorie van de Wpg bijvoorbeeld sprake als de autorisaties niet goed zijn geregeld. In de navolgende paragrafen gaan we meer in detail op de aannames in.

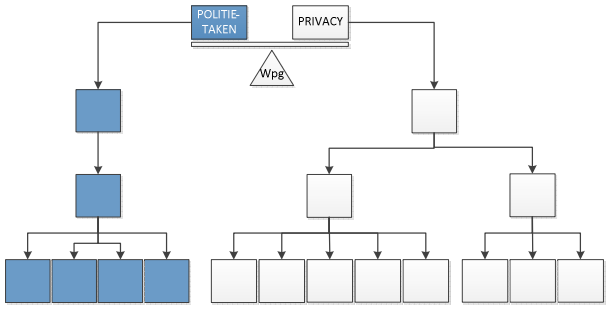
[26] Het wel naleven hoeft daarbij nog geen absolute garantie te zijn dat er geen schendingen plaatsvinden. Het is een basisbescherming.

Figuur 2.4: Beknopte beleidstheorie Wpg



2.6 Ruimte voor verwerking en verstrekking van politiegegevens

Ten opzichte van de Wpolr biedt de Wpg een verruiming van de mogelijkheden om politiegegevens te verwerken. Dit moet leiden tot een betere informatiepositie en daarmee een effectievere uitvoering van politietaken. Meer specifiek liggen daarbij de volgende aannames in de wet besloten.



Verwerken gegevens van niet-verdachten

In de eerste plaats biedt de Wpg de mogelijkheden om ook gegevens te verwerken over personen die geen verdachte zijn. Dat biedt meer ruimte om zicht te krijgen op de context en het netwerk rond verdachten. Bijvoorbeeld als het gaat om het functioneren van netwerken rond mensenhandel of hennepteelt.

Voldoende ruime verwerkings- en bewaartermijnen

In de tweede plaats mogen gegevens langer worden verwerkt en bewaard dan voorheen mogelijk was. Dit is bijvoorbeeld van belang om inzicht te hebben in de achtergrond van personen (bij de uitvoering van dagelijkse politietaken) of het oppakken van cold-cases. De aanname daarbij is dat voor dagelijkse politietaken een operationele beschikbaarheid van gegevens van maximaal vijf jaar voldoende moet zijn. Gedurende het eerste jaar kunnen de gegevens vrijelijk worden geraadpleegd, daarna kunnen de gegevens alleen worden bevraagd op basis van gegevensvergelijking. Dit impliceert dat de bevrager een met de politietaak samenhangende aanleiding heeft voor de raadpleging, bijvoorbeeld een naam of adres. Voor gegevens die worden verwerkt in het kader een onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval, is de beschikbaarheid er zolang het onderzoek loopt. Na de verwerkingsperiode worden gegevens verwijderd en bewaard met het oog op de afhandeling van klachten of de verantwoording van verrichtingen (art. 14 Wpg). Daarna worden de gegevens vernietigd. Grosso modo zijn politiegegevens gedurende tien jaar actief (verwerken) of passief (‘achter schot’) beschikbaar voor de uitvoering van politietaken[27]. In hoofdstuk 3 wordt dit meer in detail beschreven.

Door deze beschotting en verschillen in verwerkingstermijnen denkt de wetgever dat er een voldoende balans is tussen enerzijds voldoende tijd om gegevens te kunnen werken en anderzijds voldoende bescherming van de privacy.

[27] Vernietiging is niet aan de orde als gegevens opnieuw worden verwerkt. Vernietiging is voorts niet aan de orde als politiegegevens als onderdeel van het cultureel erfgoed moeten worden gezien of van belang zijn voor historisch onderzoek. In plaats van vernietiging vindt dan bewaring plaats op basis van de Archiefwet 1995.

Ruimere verwerkingsmogelijkheden

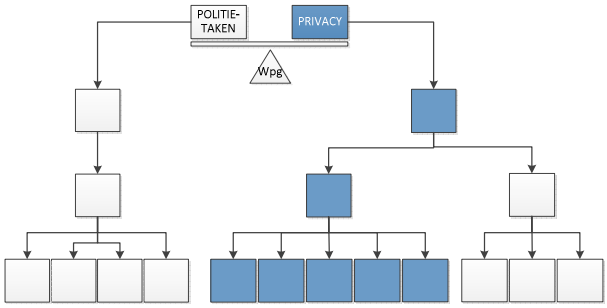
In de derde plaats wordt het mogelijk politiegegevens van verschillende onderzoeken geautomatiseerd te vergelijken of in combinatie te verwerken (mits het doel duidelijk is aangegeven). Hierdoor kunnen verbanden worden gelegd tussen bijvoorbeeld de gegevens van de wijkagent, die worden verwerkt met het oog op de uitvoering van de dagelijkse politietaak en de gegevens van een opsporingsonderzoek. Ook kunnen de bevindingen uit meerdere onderzoeken worden gecombineerd om een betere tactische informatiepositie te krijgen.

Verstrekking van politiegegevens

De Wpg biedt meer ruimte dan de Wpolr om politiegegevens te verstrekken aan derden. Dit kan bijdragen aan het versterken van de informatiepositie van derden die – zelfstandig of in samenwerking met de politie – een rol hebben bij bijvoorbeeld de bestrijding van criminaliteit of de hulpverlening. Door het uitwisselen, delen en combineren van gegevens verbetert het zicht op maatschappelijke problemen en risico's en wordt een integrale aanpak mogelijk gemaakt.

2.7 Treffen organisatorische voorzieningen en waarborgen

De Wpg gaat ervan uit dat de bescherming van de privacy moet zijn geborgd in de organisatie. Daarbij legt de wetgever expliciet de verantwoordelijkheid bij de leiding van de organisatie. Meer specifiek liggen daarbij de volgende aannames in de wet besloten.



Een heldere verantwoordelijkheids- en autorisatiestructuur

Door de verantwoordelijkheid expliciet in de wet vast te leggen kan de verantwoordelijke (korpschef/politiechef) worden aangesproken op de wijze waarop de organisatie met privacy omgaat. Dit moet prikkelen tot het ook feitelijk nemen van deze verantwoordelijkheid. Bijvoorbeeld door te zorgen dat de technische en professionele condities zijn ingevuld en privacy in de (aansturing van de) primaire processen is geborgd.

De verantwoordelijke moet via autorisaties borgen dat geen gegevens worden verwerkt door iemand voor wie deze gegevens vanuit de taakuitoefening niet relevant zijn. Dit wordt niet alleen van belang geacht voor de bescherming van de privacy maar ook in het belang van de opsporing. De gegevens moeten immers toegankelijk zijn en worden gedeeld. Bij voorkeur worden de autorisaties daarbij niet alleen organisatorisch maar ook technisch

ingevuld (toegang tot gegevens in systemen). De autorisaties moeten daarbij het doelgerichte verwerken in goede banen leiden.

In de wijze waarop de verantwoordelijke de autorisaties inricht (zowel inhoudelijk als organisatorisch) wordt hij of zij – binnen de kaders van zorgvuldigheid en evenredigheid – tot op zekere hoogte vrij gelaten. Nadere regels over de autorisaties zijn opgenomen in het Besluit politiegegevens (paragraaf 2).

Bewustzijn en transparantie verhogen via opleiding en protocollering

De wetgever vindt dat er voldoende bewustzijn over het omgaan met privacy moet zijn in de organisatie als geheel. Enerzijds acht hij daarvoor (aanvullende) scholing nodig: kennis is de basis van bewustzijn[28]. Anderzijds neemt de wetgever aan dat deze bewustwording vooral ook in het primaire proces moet plaatsvinden, dat wil zeggen bij het uitvoeren van politietaken. Protocollering moet daarin bijdragen. Protocollering houdt in dat bepaalde verwerkingen en verstrekkingen moeten worden vastgelegd. Meer specifiek welke gegevens aan wie en met welk doel zijn verstrekt of met welk doel gegevens (verder) zijn verwerkt. Dit 'dwingt' de medewerker om bewuster met bijvoorbeeld verstrekkingen om te gaan. Aan de andere kant wordt daarmee ook de transparantie en navolgbaarheid van de verstrekkingen verhoogd. Bijvoorbeeld met het oog op het uitvoeren van (privacy)audits, extern toezicht of de rechtsbescherming van degene over wie gegevens zijn verwerkt. Daarnaast is protocollering volgens de wetgever van belang om de kwaliteit van gegevens te borgen. Bijvoorbeeld als het gaat om het informeren van instanties of personen indien verstrekte gegevens niet correct blijken (of verouderd zijn) en aangepast moeten worden.

Technische en organisatorische waarborgen veiligheid data

De technische en professionele waarborgen moeten ervoor zorgen dat gegevens ook veilig zijn, dat wil zeggen fysiek en professioneel zijn afgeschermd. Het eerste gaat ervan uit dat systemen (encryptie, opslag, kopieerbeveiligingen etc.) en toegang tot en mobiliteit van fysieke media (dossiermappen, USB-sticks, HD's etc.) voldoende beveiligd zijn. Het tweede doet een appèl op (het sturen door de leiding op) de professionaliteit van de medewerkers waar het gaat om geheimhouding.

Waarborgen van tijd en kennis

De organisatie moet volgens de wetgever beschikken over specifieke (juridische) deskundigheid als het gaat om privacy. Door het aanstellen van een privacyfunctionaris kan dit worden geborgd. Enerzijds ondersteunt deze de verantwoordelijke (leidinggevende) door het monitoren, rapporteren, toezichthouden en adviseren over de mate waarin de

[28] Tweede Kamer, 2005-2006, 30 327 nr. 3, p.19

verwerking van politiegegevens aan de Wpg voldoet. Anderzijds geeft deze voorlichting aan de medewerkers over het toepassen van de Wpg en het verbeteren daarvan.

Sturing op borging privacy via audits

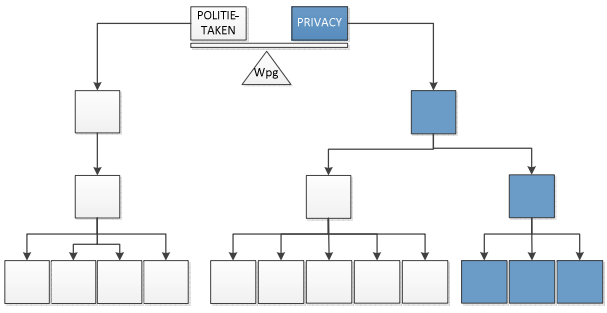
Van de verantwoordelijke casu quo leidinggevende wordt verwacht dat hij of zij op zodanige wijze sturing geeft aan de organisatie dat de bescherming van persoonsgegevens deel uitmaakt van de reguliere managementcyclus[29]. Het monitoren/evalueren en het uitvoeren van periodieke audits zijn volgens de wetgever belangrijke instrumenten die passen binnen de doelstelling van de politie om de kwaliteit van de organisatie als geheel te borgen.

De organisatie wordt door de Wpg verplicht om privacy-audits uitvoeren. Behalve dat de audits (praktische) verbeterpunten kunnen opleveren, dragen ze volgens de wetgever ook bij aan de bewustwording van de organisatie als het gaat om de bescherming van persoonsgegevens bij de verwerking van politiegegevens. Dat moet op zijn beurt weer een prikkel zijn voor de (verbetering) van de borging van de bescherming van politiegegevens.

De periodieke monitoring en evaluatie kan de politieorganisatie zelf uitvoeren. De privacy-audits moeten door een onafhankelijke auditor worden uitgevoerd. De auditrapportages moeten ook worden toegestuurd aan het CBP. Daarmee wordt enerzijds externe transparantie beoogd en anderzijds een vermindering van de toezichtlast: de gedachte is dat het CBP terughoudender invulling geeft aan haar toezichtrol naarmate de politie beter invulling geeft aan de auditcyclus. Bovendien wordt aangenomen dat de externe controle (met mogelijke sanctionering) een extra prikkel is om op de juiste wijze met politiegegevens om te gaan.

2.8 Rechtsbescherming

Degene wiens politiegegevens worden verwerkt, moet voldoende rechtsbescherming genieten. Aparte aandacht daarvoor in de Wpg is volgens de wetgever nodig vanwege het karakter van de relatie tussen politie en burger en de aard en het specifieke gebruik van de gegevens. Doordat politiegegevens veelal direct of indirect zijn gekoppeld aan (mogelijk) criminele activiteiten en/of verstoring van de openbare orde, is sprake van een hoge gevoeligheid.



[29] Tweede Kamer, 2005-2006, 30 327 nr. 3, p.89

Begrenzingen aan verwerking en verstrekking

De Wpg stelt grenzen aan de aard van de persoonsgegevens die mogen worden verwerkt, de condities waaronder deze mogen worden verwerkt en aan wie ze mogen worden verstrekt.

Politiegegevens mogen alleen worden verwerkt voor zover dat noodzakelijk is voor de bij of krachtens de Wpg geformuleerde doeleinden. De politiegegevens moeten rechtmatig zijn verkregen en moeten, gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, terzake dienend en niet bovenmatig zijn. Gebruik voor een ander doel is alleen mogelijk als de Wpg daarin uitdrukkelijk voorziet, de verwerking niet onverenigbaar is met het oorspronkelijke doel en de verwerking voor dat andere doel noodzakelijk is en in verhouding staat tot dat doel. De verdere verwerking is alleen mogelijk door personen en instanties die bij of krachtens de wet met het oog op een zwaarwegend algemeen belang zijn aangewezen. [30]

Aan de verantwoordelijke is een doorlopende inspanningsverplichting opgelegd om maatregelen te treffen om de verwerkte politiegegevens juist en nauwkeurig te laten zijn.[31] Politiegegevens die onjuist of onvolledig zijn, moeten worden verbeterd, vernietigd of aangevuld.

Bij de uitvoering van de politietaken speelt samenwerking en uitwisseling van gegevens met andere overheidsinstanties als hulpverleningsinstellingen, belastingdienst of gemeenten een belangrijke rol. Het gaat bij de informatie-uitwisseling zowel om de versterking van de informatiepositie van de politie en die van de betreffende instanties als om de gezamenlijke informatiepositie. Met het oog op de bescherming van de privacy geldt het principe van doelbinding en proportionaliteit. De Wpg benoemt de instanties waarvoor de verstrekkingsmogelijkheid generiek geldt. Bijvoorbeeld het OM, burgemeesters, inlichtingendiensten en politie en gezagsdragers op de BES-eilanden.

Daarnaast biedt de wet de mogelijkheid om via een algemene maatregel van bestuur of besluit van de minister[32] gegevens te verstrekken. Verder heeft de verantwoordelijke de mogelijkheid om tot verstrekking over te gaan met het oog op een zwaarwegend algemeen belang. Daarbij moet wel worden vastgelegd wat het doel van die verstrekking is (bijvoorbeeld via een convenant).

[30] Artikel 3 Wpg.
[31] Artikel 4 Wpg.
[32] Minister van Veiligheid en Justitie of Minister van Binnenlandse Zaken en Koninkrijksrelaties.

Recht op kennisneming

Uitgangspunt van de Wpg is dat persoonsgegevens toehoren aan degene op wie deze gegevens betrekking hebben. Degene over wie politiegegevens worden verwerkt heeft dus het recht om te weten of en zo ja welke gegevens van hem of haar zijn verwerkt[33]. Dit geeft degene over wie gegevens worden verwerkt de rechtspositie om te toetsen of de politiegegevens juist en rechtmatig (verkregen) zijn én om zo nodig aanpassing af te dwingen.

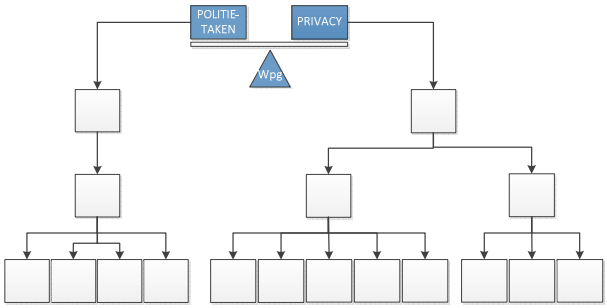
Het recht op kennisneming kan worden beperkt in het belang van een goede uitvoering van de politietaak, de bescherming van rechten van de betrokkene of van de rechten en vrijheden van derden of de veiligheid van de staat (art. 27, eerste lid, Wpg). Dit recht is samen met inhoudelijke beperkingen (reikwijdte wet, uitsluiting bepaalde persoonsgegevens, bewaartermijnen, doelbinding etc.) bij de verwerking, mede de basis om de juistheid en rechtmatigheid van (de verwerking van) politiegegevens te waarborgen. Ook hier heeft de wetgever gezocht naar een balans tussen het belang van de uitvoering van de politietaken en het fundamentele recht op privacy.

Extern toezicht

Het externe toezicht is primair belegd bij het CBP. Daarbij heeft het CBP op grond van de Wpg en de Algemene wet bestuursrecht ook sanctiemiddelen (bestuursdwang, dwangsom, boete) als onvoldoende naleving van de Wpg daar aanleiding toe geeft. Het CBP kan daarnaast optreden als bemiddelaar optreden bij een geschil inzake het recht op kennisneming.

2.9 Bereiken balans

Zoals aangegeven wil de wetgever met de Wpg een balans zien te bereiken tussen enerzijds een zo ruim mogelijke verwerking en verstrekking van politiegegevens en anderzijds de bescherming van de privacy. Samengevat voorziet de Wpg daarin als volgt.



Geconditioneerde verruiming verwerkings- en verstrekkingsmogelijkheden

De mogelijkheden om politiegegevens te verwerken of te verstrekken zijn in de Wpg ruimer dan in de Wpolr. Ten opzichte van de Wpolr mogen politiegegevens bovendien langer worden verwerkt en bewaard. Daar staat tegenover dat de organisatie in de

[33] Art. 8 en 13 EVRM.

bedrijfsprocessen elementen als de noodzaak, proportionaliteit, doelbinding etc. borgt. Als extra waarborg is een beschotting aangebracht tussen de verwerking in het kader van de uitvoering van dagelijkse politietaken en het doen van onderzoek, bijvoorbeeld in verband met de handhaving van de rechtsorde.

Organisatorische waarborgen versus vrijheid om die zelf in te vullen

De Wpg stelt eisen aan het toezicht en de organisatorische en technische waarborgen bij de organisatie die politiegegevens verwerkt. Daar staat tegenover dat de organisatie in grote lijnen vrij wordt gelaten in de wijze waarop zij dit organiseert. Bijvoorbeeld ook hoe de autorisatiestructuur er precies uitziet (wat mag een wijkagent wel of niet zien?).

Minder extern toezicht bij beter intern toezicht

De Wpg bepaalt dat er intern en extern toezicht is op de naleving van wettelijke regels over het verwerken van politiegegevens. Dit toezicht moet een prikkel zijn om de bescherming van de privacy te borgen en waar nodig te (blijven) verbeteren. Daar staat tegenover dat als de organisatie het interne toezicht (via privacyfunctionaris of functionaris gegevensbescherming) goed regelt, de externe toezichthouder meer op afstand kan blijven en zich vooral kan richten op meer structurele knelpunten. Dat kan de toezichtlast verlagen.

2.10 Aannames en verwachtingen

Verwacht werd dat de politie door de Wpg doelmatiger en doeltreffender gegevens zou kunnen verwerken.[34] Het aantal regels werd verminderd en de administratieve lasten werden gereduceerd door het vervallen van de onder de Wpolr geldende reglementsplicht en het registerbegrip.

Door qua opzet zoveel mogelijk aan te sluiten bij de Wbp en de Wet justitiële en strafvorderlijke gegevens, werd gestreefd naar eenvormigheid van wetgeving. Keuze voor één wettelijk kader voor de verwerking van politiegegevens was in lijn met de wens van de politie[35].

Ten tweede werd verwacht dat de politie op basis van de Wpg beter zou kunnen samenwerken met andere instanties. De bestaande knelpunten zouden weggenomen door een opener verstrekkingenregime en door meer duidelijkheid over de mogelijkheden om gegevens te verstrekken aan samenwerkingspartners.[36]

---

[34] *Kamerstukken II 2005/2006*, 30 327, nr. 3, p. 17.

[35] Brief Raad van Hoofdcommissarissen et al van 4 oktober 2004 aan de minister van Justitie; in eerder concept van de wet vielen niet alle politietaken onder de nieuwe wet, maar zou een deel onder de Wet bescherming persoonsgegevens (Wbp) komen te vallen. De politie pleitte in de brief voor óf één lex specialis voor de politie óf het laten vallen van politiegegevens onder de Wbp (zoals ook in andere EU-landen gebeurd is.)

[36] *Kamerstukken II 2005/2006*, 30 327, nr. 3, p. 18.

De wetgever ging ervan uit dat de politie binnen afzienbare tijd over één ICT-systeem (of in elk geval over een gekoppelde landelijke informatiehuishouding) zou beschikken. Daarbij was wel de onderkenning dat dit systeem er nog niet direct zou zijn en dat er tijdelijke voorzieningen nodig zouden zijn[37].

Voorts ging de wetgever ervan uit dat de Wpg goed aansluit bij de politiepraktijk, in het bijzonder de uitvoering van dagelijkse politietaken en het doen van onderzoek.

In de voorbereiding van de Wpg heeft de minister van Justitie onderzoek laten doen naar de uitvoerbaarheid van de wet. Dit onderzoek onderschreef in grote lijnen de uitgangspunten van de wet en concludeerde dat de wet voldoende aansloot bij de bestaande politiepraktijk en ontwikkelingen (bijvoorbeeld rond datamining). Aanbevelingen richtten zich vooral op een aantal verduidelijkingen, de bewaartermijnen in verband met cold-cases en de invulling van de landelijke informatievoorziening[38].

De wetgever verwachtte dat er de nodige bijscholing nodig zou zijn voor de medewerkers omdat een meer proces- en ketengerichte manier van werken werd verwacht (in vergelijking tot de Wpolr). In het verlengde zouden ook opleidingen bij de politieacademie moeten worden aangepast. Zowel in algemene zin als specifiek voor de opleiding van privacyfunctionaris/functionaris gegevensbescherming[39].

Wat de financiële consequenties van de wet betreft heeft/geeft de wetgever geen duidelijkheid. In de memorie van toelichting wordt slechts aangegeven dat deze in samenspraak met de politie nader in kader moeten worden gebracht[40].

2.11 Samenvattende bevindingen

De Wpg is in 2008 in werking getreden en was bedoeld als modernisering van de wetgeving inzake het omgaan met persoonsgegevens bij het uitvoeren van politietaken. Enerzijds om de regels voor de uitvoering van politietaken te stroomlijnen met nieuwe Europese en nationale wetgeving (Wbp). Anderzijds om een aantal knelpunten in de bestaande wetgeving (Wpolr) weg te nemen.

De Wpg moest daarbij zowel meer ruimte bieden voor het verwerken en verstrekken van politiegegevens als voldoende rechtsbescherming bieden voor degene over wie gegevens worden verwerkt.

---

[37] Tweede Kamer, 2005-2006, nr. 30 327 nr. 3 p. 18.
[38] Rietveld et al, 2004, p.40 e.v.
[39] Tweede Kamer, 2005-2006, nr. 30 327 nr. 3 p. 19.
[40] Idem

Met de verruiming van de verwerkingsmogelijkheden moest de politie beter in staat zijn zicht te krijgen op ontwikkelingen en netwerken en informatie met partners te delen. Het laatste zowel met het oog op de (gezamenlijke) informatiepositie als het met het oog op de integrale aanpak en samenwerking bij bijvoorbeeld de aanpak van de georganiseerde criminaliteit. Dit ook tegen de achtergrond van ontwikkelingen op ICT-gebied en maatschappelijke ontwikkelingen als toenemende mobiliteit en diversiteit en het karakter van criminaliteit (netwerkvormen, internationalisering etc.).

Het bieden van voldoende rechtsbescherming moet worden bereikt door begrenzing van welke gegevens mogen worden verwerkt en aan wie die mogen worden verstrekt (doelbinding, noodzaak, verwerkings- en bewaartermijnen etc.), het recht op kennisneming en correctie van gegevens voor degene over wie persoonsgegevens worden verwerkt, zelfcontrole (zoals audits) en door onafhankelijk extern toezicht (met sanctiemogelijkheid). De aanname was daarbij dat naast de instrumentele werking, deze rechtsbescherming ook zou bijdragen aan de bewustwording bij de organisatie die politiegegevens verwerkt.

De wetgever heeft daarbij getracht een balans te realiseren tussen deze twee hoofddoelstellingen door:

- Geconditioneerde ruimere verwerkings- en verstrekkingsmogelijkheden (verwerkings- en bewaartermijnen, verwerkingsregimes voor dagelijkse politietaken en onderzoek).
- Het stellen van specifieke organisatorische eisen (autorisatiestructuur, protocollering, audits e.a.) maar door vrij te laten hoe deze worden ingevuld.
- Vermindering van de externe toezichtlast naarmate de verwerkende organisatie het interne toezicht beter regelt.

De verwachting van de wetgever was dat de Wpg goed zou aansluiten bij de politiepraktijk en anticipeerde op ontwikkelingen, zoals het toewerken naar een landelijke informatiehuishouding. Als belangrijkste aandachtspunt voor de implementatie werden scholing en opleiding gezien.

3 Inhoud Wet politiegegevens

3.1 Inleiding

In dit hoofdstuk wordt ingegaan op de inhoud van de Wpg. De Wpg is onderverdeeld in zeven paragrafen:

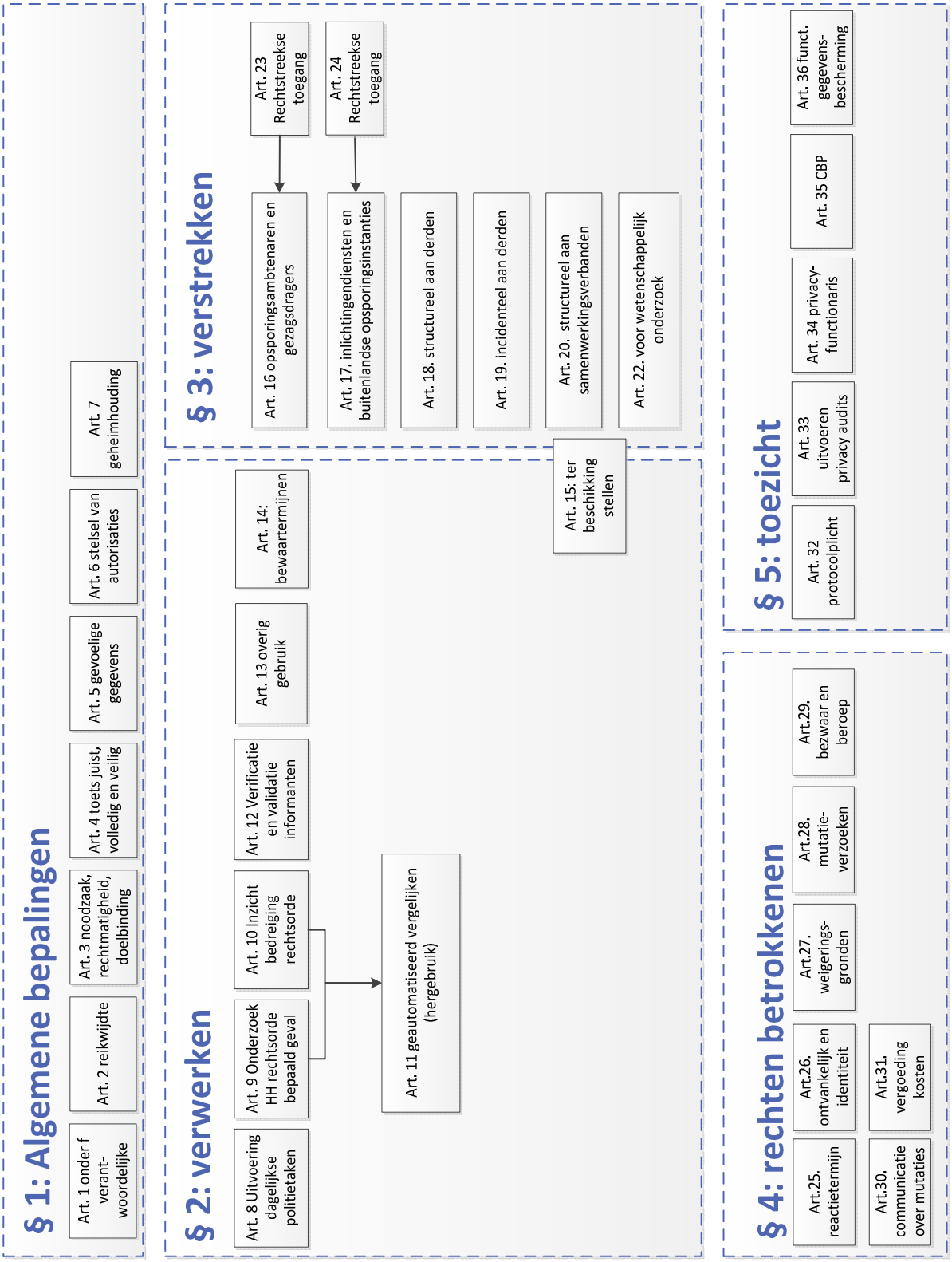
1. Algemene bepalingen (art. 1-7)
2. De verwerking van politiegegevens (art. 8-15)
3. De verstrekking van politiegegevens (art. 16-24)
4. Rechten van de betrokkene (art. 25-31)
5. Toezicht (art. 32-36)
6. Wijziging van andere wetten (art. 37-45)
7. Slotbepalingen (art. 46-52)

Een aantal onderwerpen is nader uitgewerkt in het Besluit politiegegevens (Bpg), het Besluit politiegegevens bijzondere opsporingsdiensten en het Besluit verplichte politiegegevens[41]. Daarnaast zijn ministeriële regelingen vastgesteld, zoals de Regeling periodieke audit politiegegevens en de Regeling aanwijzing wetgeving ex artikel 4:2 Besluit politiegegevens.

De belangrijkste bepalingen uit de Wpg worden hierna per paragraaf toegelicht. In paragraaf 3.2 wordt ingegaan op de algemene bepalingen, waarna in paragraaf 3.3 de verwerkingsdoeleinden worden besproken. Paragraaf 3.4 gaat over het verstrekken van politiegegevens en paragraaf 3.5 over de rechten van betrokkenen. In paragraaf 3.6 wordt ingegaan op het toezicht op de naleving.

[41] Het Besluit verplichte politiegegevens heeft op 1 januari 2013 de Regeling opsporingsinformatie regionale politiekorpsen alsmede de Regeling criminele inlichtingen eenheden (verder: Regeling CIE) vervangen. Het besluit stelt regels omtrent de doeleinden waarvoor de politie en de rijksrecherche, met inachtneming van de Wet politiegegevens, gegevens verwerken, de categorieën van gegevens die daartoe worden verwerkt, de terbeschikkingstelling en verstrekking van gegevens alsmede de wijze van verwerking.

Figuur 3.1: Belangrijkste paragrafen Wpg



3.2 Algemene bepalingen

In de eerste paragraaf van de Wpg zijn allereerst definities gegeven en is de reikwijdte van de wet weergegeven. In paragraaf 1.3 is hier al op ingegaan. Daarnaast zijn verschillende rechtsbeginselen (zie paragraaf 2.3) in deze paragraaf verankerd. In artikel 3 is het beginsel van doelbinding neergelegd. De noodzakelijkheid, rechtmatigheid, doelbinding en transparantie van de verwerking komen in artikel 3 tot uitdrukking.

In artikel 4 Wpg is aan de verantwoordelijke een doorlopende inspanningsverplichting opgelegd maatregelen te treffen om de verwerkte politiegegevens juist en nauwkeurig te laten zijn.[42] Er moeten maatregelen worden getroffen om gegevens te verwijderen of te vernietigen als ze niet langer noodzakelijk zijn voor het verwerkingsdoel. Er moet worden gezorgd voor een passend beveiligingsniveau en de informatisering moet voldoende waarborgen bevatten om te voorkomen dat gegevens langer in de systemen blijven dan op grond van de wet geoorloofd is. In de Wpg zijn verwijdering- en vernietigingsverplichtingen opgenomen (zie paragraaf 3.3). Tevens volgt uit de combinatie van artikel 4 met artikel 10 en 12 dat verwerkte gegevens periodiek geschoond dienen te worden.

Net als in de Wbp worden aan de verwerking van gevoelige gegevens extra eisen gesteld. Dergelijke gegevens die betrekking hebben op iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, of het lidmaatschap van een vakvereniging, mogen alleen worden verwerkt in aanvulling op de verwerking van andere politiegegevens en voor zover dit voor het verwerkingsdoel onvermijdelijk is.[43]

Artikel 4, lid 3, Wpg brengt voor de verantwoordelijke de plicht mee ervoor te zorgen de gegevens adequaat te beveiligen tegen onrechtmatige verwerking. De beveiligingsplicht van artikel 4 Wpg is onder andere ingevuld doordat elke politiefunctionaris moet worden geautoriseerd op het niveau van zijn of haar functie.[44] Hierdoor kan worden voorkomen dat gegevens toegankelijk zijn voor personen voor wie dat uit hoofde van hun taak of functie niet noodzakelijk is. Nadere regels over de categorieën van personen die voor bepaalde gegevensverwerkingen geautoriseerd kunnen worden en de deskundigheidseisen die aan hen gesteld kunnen zijn gegeven in paragraaf 2 van het Besluit politiegegevens. Autorisatiematrices dienen een overzicht te bieden van de autorisaties per functie.

In artikel 7 Wpg is een geheimhoudingsplicht neergelegd. Deze geldt intern[45], maar ook extern[46] voor de ontvangers van politiegegevens. Er gelden uitzonderingen op de

[42] MvT, p. 32 en Muijen p. 51.
[43] Artikel 5 Wpg.
[44] Artikel 6 Wpg en Muijen 2012, p. 58.
[45] Artikel 7 lid 1 Wpg.
[46] Artikel 7 lid 2 Wpg.

geheimhoudingsplicht, bijvoorbeeld als de bepalingen van paragraaf 3 Wpg verstrekking toelaten of de politietaak in bijzondere gevallen tot verstrekking noodzaakt.

3.3 Verwerking

In de Wpg staat het beginsel van doelbinding voor de verwerking van politiegegevens centraal. In de Wpg zijn diverse doeleinden geformuleerd in verband waarmee politiegegevens mogen worden verwerkt:

- Art. 8 lid 1 Wpg: verwerking en met het oog op de uitvoering van de dagelijkse politietaak (deze verwerkingen worden veelal door "blauw" gedaan en zijn gericht op vastlegging van handhavings- en onderzoeksbevindingen);
- Art. 9 lid 1 Wpg: gerichte verwerking ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval (het gaat om verwerkingen door de recherche voor een concreet onderzoeksdoel);
- Art. 10 lid 1 a, b en c Wpg[47]: gerichte verwerking met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (deze verwerkingen worden gedaan door medewerkers van de Criminele Inlichtingen Eenheid (CIE)[48], de Regionale Inlichtingen Dienst (RID) of speciaal daartoe geautoriseerde ambtenaren van politie);
- Art. 12 lid 1 Wpg: verwerking met het oog op de controle op en het beheer van een informant evenals de beoordeling en verantwoording van het gebruik van informantgegevens (deze verwerkingen worden door de medewerkers van de CIE gedaan);
- Art. 13 lid 1 Wpg: verwerking ten behoeve van de ondersteuning van de politietaak (deze verwerkingen zijn veelal verdere verwerkingen van gegevens die onder andere zijn verkregen en initieel verwerkt met een art. 8 Wpg of 9 Wpg doel).
- Art. 14 Wpg: Afhandeling klachten en verantwoording verrichtingen en hernieuwde verwerking als uit bewaarde politiegegevens de noodzaak voortvloeit tot nieuw onderzoek.

Voor deze doelen gelden verschillende eisen als het gaat om verwerkings-, verwijderings- en vernietigingstermijnen.

[47] Artikel 10 lid 1 omvat drie gerichte verwerkingen met het oog op het verkrijgen van inzicht in de betrokkenheid van personen, namelijk bij 1) het beramen of plegen van bepaalde misdrijven, 2) bepaalde thematische verwerkingen, en 3) ernstige schendingen van de openbare orde.

[48] De taak van de CIE is het verzamelen, registreren en analyseren van informatie over strafbare feiten en verdachten. Als enige politieonderdeel mogen zij daarbij gebruikmaken van informanten, te weten mensen die anoniem informatie aan de politie verstrekken.

Tabel 3.1: Artikelsgewijs overzicht van verwerkings-, verwijderings- en vernietigingstermijnen

Art.	Verwerking	Verwijdering	Vernietiging
8	Eerste jaar: basisverwerking Na 1 jaar: alleen geautomatiseerd vergelijken en analyse Na verwijdering: voor afhandeling klachten en verantwoording verrichtingen	Zodra niet langer noodzakelijk voor uitvoering dagelijkse politietaak, uiterlijk vijf jaar na datum eerste verwerking	Vijf jaar na verwijdering
9	Zolang de gegevens noodzakelijk zijn voor het doel van het onderzoek Na verwijdering: voor afhandeling klachten en verantwoording verrichtingen	Verwijdering als de gegevens niet langer noodzakelijk zijn voor het doel van het onderzoek of nog een half jaar verwerken	Vijf jaar na verwijdering
10	Zolang de gegevens noodzakelijk zijn voor het verwerkingsdoel Na verwijdering: voor afhandeling klachten en verantwoording verrichtingen	Zodra niet langer noodzakelijk voor het verwerkingsdoel, uiterlijk vijf jaar na datum laatste noodzakelijke verwerking	Vijf jaar na verwijdering
12	Zolang de gegevens noodzakelijk zijn voor het verwerkingsdoel Vier maanden na eerste verwerking: ter beschikking stellen mogelijk voor verdere verwerking		Vernietiging zodra niet langer noodzakelijk, uiterlijk 10 jaar na datum laatste verwerking
13	Afhankelijk van hetgeen hierover in een reglement is bepaald.[49]	Afhankelijk van hetgeen hierover in een reglement is bepaald.	Afhankelijk van hetgeen hierover in een reglement is bepaald.

[49] Muijen 2012, p. 111. Er kan afgeweken worden van de termijnen die oorspronkelijk gelden. Als geen afwijkende termijn noodzakelijk wordt geacht, is het oorspronkelijke regime (bv. art. 8 Wpg) bepalend, tenzij de noodzaak voor de ondersteunende taak eerder vervalt. Als verdere werking noodzakelijk is, maar het oorspronkelijke regime vernietiging voorschrift, kan een langere verwerkingstermijn worden gekozen. Deze termijn is dan tevens de vernietigingstermijn.

3.4 Verstrekken

Politiegegevens kunnen intern en extern aan anderen worden verstrekt.[50]

Ter beschikking stellen van politiegegevens

Bij de interne verstrekking gaat het om het ter beschikking stellen van politiegegevens aan personen die zijn geautoriseerd voor het verwerken van politiegegevens. De Wpg gaat uit van een 'free flow of information' hetgeen betekent dat de politiegegevens, die worden verwerkt ten behoeve van de in paragraaf 3.3 beschreven doelen, aan andere politieambtenaren die deze gegevens nodig hebben voor een goede uitvoering van hun taak ter beschikking worden gesteld.[51] Slechts in bijzondere gevallen kan de ter beschikkingstelling van politiegegevens worden geweigerd of aan voorwaarden worden gebonden.[52] De free flow of information geldt voor de politie, de Kmar en de BOD-en.[53]

Externe verstrekking

Van de (interne) ter beschikkingstelling kan de (externe) verstrekking van politiegegevens worden onderscheiden. In de Wpg worden bepaalde doelen of taken geformuleerd die verenigbaar zijn en van zodanig belang dat deze de verstrekking van politiegegevens aan derden rechtvaardigen. Aldus kan de verstrekking van politiegegevens aan derden plaatsvinden indien dit voortvloeit uit een wettelijke verplichting of voor zover dit noodzakelijk is met het oog op een zwaarwegend algemeen belang.[54]

Uitgangspunt van de Wpg is meer mogelijkheden te bieden voor verstrekking van politiegegevens aan derden. Het gesloten verstrekkingenregime van de Wpolr is daarom verruimd[55]. De Wpg voorziet in verplichte verstrekking van gegevens door de politie aan de gezagsdragers en aan bepaalde opsporingsambtenaren buiten de politie. Tevens zijn in het Besluit politiegegevens ontvangstgerechtigde instanties aangewezen. Het betreft de instanties waarmee de politie regulier samenwerkt, zoals de partners in de strafrechtketen. Ten slotte biedt de wet ruimte aan de verantwoordelijke korpsbeheerder om in geval van een zwaarwegend algemeen belang, in overeenstemming met het bevoegd gezag gegevens te verstrekken aan niet in de algemene maatregel van bestuur genoemde instanties. Het kan hierbij gaan om incidentele verstrekkingen in bijzondere gevallen, dan wel verstrekkingen in het kader van een structureel samenwerkingsverband tussen een of meer politiekorpsen en andere instanties. Hiermee is beoogd ruimte te bieden voor door de

[50] Artikel 1 onder d Wpg.
[51] Artikel 15 eerste lid Wpg.
[52] Artikel 2:13 Bpg.
[53] De mogelijkheid voor de BOD-en om informatie uit te wisselen is uitgebreid in 2010 met de invoering van het Besluit politiegegevens bijzondere opsporingsdiensten. Een aantal bepalingen van de Wpg zijn uitgezonderd.
[54] MvT, p. 3 en 69.
[55] MvT, p. 1 en 2.

praktijk gewenste verstrekkingen in het kader van de samenwerking van de politie met derden, bijvoorbeeld ten behoeve van de aanpak van jeugdcriminaliteit.[56]

3.5 Rechten van betrokken

De Wpg kent aan betrokkenen het recht toe een verzoek tot kennisneming in te dienen over de eigen persoonsgegevens die de politie (mogelijk) heeft verwerkt en de mogelijkheid in rechte op te komen tegen een weigering om deze gegevens kenbaar te maken.[57] Een verzoek om kennisneming kan eventueel worden gevolgd door een verzoek tot verbetering, aanvulling, verwijdering of afscherming van de gegevens.[58] Onder afschermen wordt verstaan het markeren van opgeslagen politiegegevens met als doel de verwerking ervan in de toekomst te beperken.[59] Een verzoek om kennisneming kan worden afgewezen als dat noodzakelijk is in het belang van de goede uitvoering van de politietaak, de bescherming van de rechten van de betrokkene of van de rechten en vrijheden van derden, of de veiligheid van de staat.[60]

3.6 Toezicht

In de Wpg is op verschillende manieren voorzien in toezicht op de naleving ervan.

Protocolplicht

De Wpg verplicht tot schriftelijke vastlegging van:

1. de doelen van de onderzoeken, bedoeld in artikel 9 lid 2;
2. de gegevens die op grond van het bepaalde bij of krachtens artikel 13 lid 4, worden vastgelegd;
3. de toekenning van de autorisaties, bedoeld in artikel 6;
4. de geautomatiseerde vergelijking of het in combinatie met elkaar verwerken van politiegegevens, bedoeld in de artikelen 8 lid 3, en 11 lid 1, 2 en 4;
5. de hernieuwde verwerking van politiegegevens op grond van artikel 9 of 10, bedoeld in artikel 14 lid 3;
6. de verstrekking van politiegegevens op grond van paragraaf 3 met uitzondering van de verstrekking, bedoeld in artikel 17 lid 1 en artikel 24 lid 1 en 2, indien dit zich niet verdraagt met het belang van de staatsveiligheid;
7. verwerkingen ten aanzien waarvan aanwijzingen bestaan dat zij door onbevoegden of anderszins onrechtmatig zijn verricht;
8. een geautomatiseerde vergelijking van gegevens als bedoeld in artikel 11 lid 5.[61]

---

[56] *Kamerstukken II 2005/2006*, 30 327, nr. 3, p. 4.
[57] Art. 25 Wpg.
[58] Art. 28 Wpg.
[59] Art. 1 onder n Wpg. Deze bepaling is opgenomen in het kader van de implementatie van het Kaderbesluit dataprotectie.
[60] Artikel 27 Wpg.
[61] Artikel 32 Wpg.

Naast deze protocolplicht geldt in verband met de vereiste juistheid en nauwkeurigheid voor de verwerking van politiegegevens op grond van de artikelen 9, 10 en 12 eveneens de verplichting de herkomst van de gegevens en de wijze van verkrijging te vermelden.[62] Deze verplichting geldt niet voor gegevens die op grond van artikel 8 worden verwerkt.

Audits

Op grond van de Wpg[63], het Bpg en de Regeling periodieke audit politiegegevens is de verantwoordelijke verplicht periodiek privacy audits te verrichten, waarvan de controleresultaten aan het CBP moeten worden gestuurd. De eerste audit moet twee jaar na inwerkingtreding van de wet worden uitgevoerd en vervolgens moet eens per vier jaar een audit worden uitgevoerd. Als uit de audit blijkt dat niet aan de Wpg wordt voldaan, moet binnen een jaar een hercontrole worden uitgevoerd op de betreffende onderdelen. Als wederom niet wordt voldaan, moet opnieuw een hercontrole worden uitgevoerd net zolang tot aan de wettelijke vereisten is voldaan of de termijn van de reguliere audit is aangebroken.[64]

Intern toezicht

Conform artikel 34 Wpg is de verantwoordelijke verplicht een privacyfunctionaris aan te stellen binnen zijn of haar organisatie. De privacyfunctionaris houdt voor de verantwoordelijke toezicht op de juiste verwerking van politiegegevens binnen de organisatie, houdt een overzicht van de schriftelijke vastlegging van gegevens (protocolleringsplicht) bij en stelt jaarlijks een verslag op met zijn/haar bevindingen. De privacyfunctionaris zal vooral een belangrijke rol kunnen spelen in de advisering in privacyvraagstukken en het stimuleren van het privacybewustzijn binnen de organisatie, dankzij zijn/haar deskundigheid op het gebied van het privacyrecht. [65]

De mogelijkheid bestaat een functionaris gegevensbescherming aan te stellen.[66] Deze functionaris heeft een onafhankelijke positie en kent formele bevoegdheden in de zin van afdeling 5.2 van de Algemene wet bestuursrecht doordat hij/zij de status van wettelijk erkend toezichthouder heeft. De functionaris kan inzage in stukken vorderen en ziet toe op de verwerking van persoonsgegevens.[67]

[62] Artikel 3 lid 4 Wpg.
[63] Artikel 33 Wpg.
[64] Muijen 2012, p. 197.
[65] Muijen 2012, p. 201.
[66] Artikel 36 Wpg.
[67] Muijen 2012, p.201-202

Extern toezicht

Het externe toezicht op de verwerking van persoonsgegevens is belegd bij het CBP.[68] Bij niet naleving van de wet kan het CBP een bestuurlijke boete opleggen. Het CBP heeft hiervoor beleidsregels vastgesteld.[69]

3.7 Samenvattende bevindingen

De Wpg stelt regels voor een rechtmatige verwerking van politiegegevens. Politiegegevens mogen alleen worden verwerkt als het noodzakelijk is voor een goede uitvoering van de politietaak en de gegevens moeten rechtmatig zijn verkregen en juist zijn. De verwerking mag alleen plaatsvinden voor een bepaald doel en moet proportioneel zijn.

Politiegegevens moeten binnen de politie, de Kmar en BOD-en ter beschikking worden gesteld aan geautoriseerde personen, de zogenoemde 'free flow of information'. Voor de verstrekking aan derden zijn verschillende regels opgenomen. Het verstrekkingenregime is opener dan onder de Wpolr.

Voor ontvangers van politiegegevens geldt een geheimhoudingsplicht.

Betrokkenen hebben het recht een verzoek om kennisneming in te dienen, dat gevolgd kan worden door een verzoek tot verbetering, aanvulling, verwijdering of afscherming van de gegevens.

In de wet is op verschillende manieren voorzien in toezicht op de naleving. Zo moeten diverse verwerkingen geprotocolleerd worden, moeten er periodiek audits worden uitgevoerd en is voorzien in intern en extern toezicht.

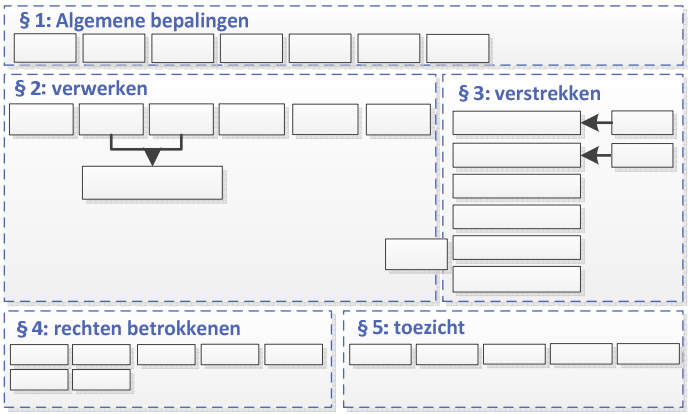
[68] Artikel 35 Wbp.
[69] Cbp 2009.

Deel II: Knelpunten in de uitvoeringspraktijk

Deel II van de rapportage gaat in op de knelpunten die zich in de praktijk voordoen. Meer specifiek de knelpunten in de (borging van de) formele naleving van de Wpg en de knelpunten die betrokken organisaties in relatie tot de Wpg ervaren bij de uitvoering van politietaken. De mate van (borging van) formele naleving is bepaald aan de hand van de audits uit 2011/2012 en de hercontroles die in 2013 zijn uitgevoerd. De knelpunten zijn in beeld gebracht aan de hand van gesprekken met medewerkers van twee territoriale eenheden van de (nationale) politie, onderdelen van de landelijke eenheid van de politie en de Kmar. Daarnaast zijn (groeps)gesprekken gevoerd met het OM, een vertegenwoordiging van BOD-en, het LIEC, de Nederlandse Orde van Advocaten, de Nationale Ombudsman en het CBP[70].

De beschrijving van de praktijk volgt in grote lijnen de structuur van de Wpg:

- Algemene bepalingen Wpg (hoofdstuk 4)
- Verwerking (hoofdstuk 5)
- Verstrekking (hoofdstuk 6)
- Rechten van betrokkenen (hoofdstuk 7)
- Toezicht (hoofdstuk 8)



Er is een apart hoofdstuk gewijd aan de samenloop van de Wpg met andere wetgeving, in het bijzonder de Wob(hoofdstuk 9).

Elk hoofdstuk beschrijft voor genoemde onderdelen van de Wpg a) de strekking van de Wpg op het betreffende punt, b) de formele naleving van de Wpg zoals deze uit de audits blijkt (borging van de Wpg) en c) de knelpunten die in de praktijk worden ervaren. Bij het laatste worden ook voorbeelden uit de praktijk gegeven.

In dit hoofdstuk wordt nog geen specifieke analyse gemaakt van de oorzaken van de knelpunten en wordt ook niet ingegaan op de vraag of geïnterviewden bijvoorbeeld een juiste uitleg van de Wpg geven. Hoofdstuk 10 gaat nader op de verklaringen in[71].

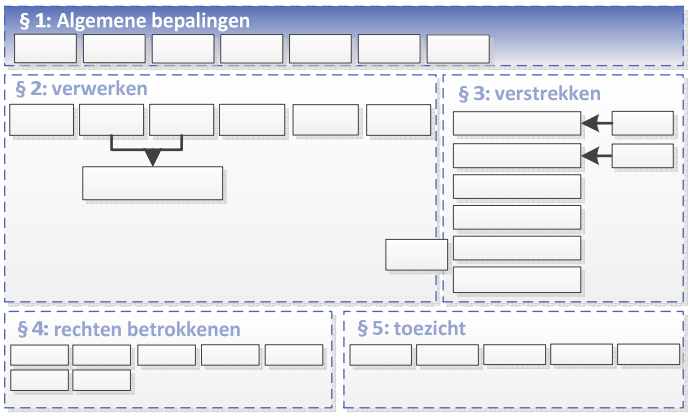
Elk hoofdstuk sluit af met een korte samenvatting.

[70] Bits of Freedom is benaderd voor een gesprek, maar wenste daar niet aan mee te werken.
[71] Op enkele plaatsen is wel in een voetnoot aangegeven als het beeld van betrokkenen in de interviews evident afwijkt van wat de Wpg feitelijk toestaat, verbiedt of beoogt.

4 Algemene bepalingen

4.1 Inleiding

De Wpg bevat algemene bepalingen ('beginselen') waaraan de inrichting van de organisatie van de politie, de Kmar en BOD-en moet voldoen. Meer specifiek gaat het om:



- Een verantwoordelijke die zorgt dat aan de Wpg wordt voldaan en daarop aanspreekbaar is (art. 1 Wpg).
- Waarborgen van de noodzaak, rechtmatigheid en doelbinding en juistheid en volledigheid van (gevoelige) politiegegevens en de beveiliging van politiegegevens (art. 3, 4 en 5 Wpg)
- Een systeem van autorisaties wat betreft de verwerking van politiegegevens (art. 6 Wpg)
- Geheimhoudingsplicht (art. 7 Wpg)

4.2 Centrale rol voor de verantwoordelijke

De Wpg noemt 'de verantwoordelijke' als degene die erop moet toezien dat de Wpg geïmplementeerd en nageleefd wordt. De verantwoordelijke is daarop ook aanspreekbaar[72]. Met de totstandkoming van de Nationale politie is de 'verantwoordelijke' de korpschef conform art. 27 Politiewet 2012. Tot 1 januari 2013 waren de 25 regionale korpsbeheerders de verantwoordelijke voor hun regionale politiekorps en de minister van Veiligheid en Justitie, in hoedanigheid van beheerder, voor het Korps landelijke politiediensten (KLPD). Voor de Kmar is de minister van Defensie de verantwoordelijke. De verantwoordelijkheid voor de (sturing op de) implementatie en het toezien op de naleving kan binnen de organisatie worden gemandateerd aan de politiechef of een ander lid van de eenheidsleiding.

Knelpunten uit de audits

In de audits uit 2011 is getoetst of de (toenmalige) korpsen een mandaatregeling hebben opgesteld waarin de verantwoordelijke de (toenmalige) korpschef heeft gemandateerd voor het implementeren van maatregelen om te voldoen aan de Wpg. In 2011 was zo'n besluit bij 92% van de korpsen voorhanden. Bij de overige korpsen zou dat besluit op korte

[72] Artikel 1 onder f Wpg.

termijn worden genomen[73]. Bij de hercontrole in 2013 hadden alle eenheden de mandaatregeling geïmplementeerd maar had één eenheid deze nog niet formeel vastgesteld[74].

Knelpunten uit de interviews

In de interviews is gevraagd naar de knelpunten die zich hebben voorgedaan bij de implementatie van de Wpg en de rol van de leiding (verantwoordelijke) daarbij.

Wie is de verantwoordelijke?

Om te beginnen geven verschillende geïnterviewden aan dat het niet altijd duidelijk is wie de verantwoordelijke is. Enerzijds omdat niet altijd scherp is af te bakenen welke organisatie verantwoordelijk is. Dit gold tot 1 januari 2013 met name voor het verwerken van dezelfde gegevens door verschillende politiekorpsen. Daar komt bij dat het niet altijd duidelijk is welk wettelijk regime van toepassing is, omdat een politiegegeven zich ook bij het OM of de rechter kan bevinden en naast de Wpg dan ook de Wjsg of Sv van toepassing kunnen zijn.

Dagelijkse leiding beperkt meegenomen in Wpg

De operationele verantwoordelijkheid voor de invoering van en het toezicht op de Wpg ligt bij de dagelijkse leiding. De mate waarin leidinggevenden zijn 'meegenomen' in de implementatie van de Wpg lijkt beperkt. Er zijn specifiek voor leidinggevenden voorlichtingsdagen gegeven, maar volgens diverse geïnterviewden was de belangstelling daarvoor zeer beperkt.

Een leidinggevende die deze voorlichtingsdagen heeft bijgewoond, betwijfelt of die voorlichting heeft bijgedragen aan duidelijkheid over de consequenties van de Wpg voor de organisatie en werkwijze. De wet is in zijn ogen moeilijk te bevatten voor een niet-ingewijde. De uitleg was in zijn ogen zeer proceduregericht en detaillistisch. Hij had graag een 'A4' gehad met de essentie van de Wpg die een leidinggevende kan overbrengen aan de medewerkers.

Beperkte kennis en regie bij dagelijkse leiding

Het voorgaande (weinig belangstelling voor voorlichting, detaillistische insteek) verklaart mogelijk dat verschillende geïnterviewden aangeven dat (ook) leidinggevenden weinig kennis hebben van de Wpg. Dat draagt er op zijn beurt volgens hen aan bij dat de Wpg weinig prioriteit heeft bij de leiding en de Wpg als taak van de privacyfunctionaris wordt gezien. Door het buiten de lijn plaatsen van de verantwoordelijkheid werd er volgens de

[73] DAD audits, 2012.
[74] Landelijke rapportage hercontrole Wpg, 2013.

betrokkenen weinig sturing gegeven op het werken conform de Wpg en het borgen van de kwaliteit van de gegevens.

4.3 Rechtsbeginselen en beveiliging

Politiegegevens mogen op grond van art. 3 Wpg alleen worden verwerkt als dat noodzakelijk is voor de in de wet genoemde doelen, als ze rechtmatig zijn verkregen en als ze met het oog op het doel van de verwerking toereikend, terzake dienend en niet bovenmatig zijn.[75].

Op basis van art. 4 Wpg moet de verantwoordelijke erop toezien dat de gegevens juist en volledig zijn en dat de gegevens afdoende zijn beveiligd.[76]

Gevoelige gegevens over bijvoorbeeld godsdienst of gezondheid mogen op grond van art. 5 Wpg alleen (aanvullend) worden verwerkt en indien dit onvermijdelijk is voor het doel van de verwerking[77].

Knelpunten uit de audits

Bedrijfsmatige borging noodzaak en doelbinding vindt selectief plaats

Uit de audits bleek dat in 2011 de borging van hetgeen is genoemd in de artikelen 3 (noodzaak, rechtmatigheid en doelbinding) en 4 (juistheid en volledigheid) beperkt was. De auditoren constateerden onder andere dat in dit verband procesbeschrijvingen of richtlijnen vaak ontbraken. Ze stelden ook vast dat in de praktijk niet altijd werd getoetst aan de noodzaak van verwerking en, voor zover dat wel gebeurde, het begrip 'noodzaak' ruim werd uitgelegd. De borging van de naleving was volgens de auditoren hoger naarmate de (gevolgen van de) verwerking ingrijpender konden zijn voor de betrokkene.

Rechtmatigheid verwerking procedureel niet maar materieel wel geborgd

De auditoren stelden voorts vast dat de rechtmatigheid van de gegevens en de verwerking procedureel niet volledig waren geborgd in de werkprocessen. De auditoren geven aan dat dit in de praktijk niet (structureel) tot feitelijke schending van de rechtmatigheid van de verwerking leidt. Toetsing door de rechter en de 'drive' van politie om een procesdossier overeind te houden, spelen daarbij volgens de auditoren een rol[78].

Verouderde ICT knelpunt voor beveiliging

Bij ruim 95% van de korpsen bleek de fysieke beveiliging (toegang tot gebouwen, ruimtes etc.) en de ICT (BVO, BVH en regionale systemen), niet te voldoen aan de eisen van de

[75] Artikel 3 Wpg.
[76] Artikel 4 Wpg.
[77] Artikel 5 Wpg.
[78] DAD audits, 2012.

Wpg[79]. Op het moment van de hercontrole van de audits in de eerste helft 2013, wordt gewerkt aan nieuwe ICT-voorzieningen (TrueBlue voor artikel 8 verwerkingen en SummIT voor artikel 9 verwerkingen) die wel moeten voldoen. Die zijn echter nog niet operationeel. De fysieke beveiliging werd ook bij de hercontrole als onvoldoende beoordeeld[80].

Verwerking gevoelige gegevens inmiddels geborgd

De helft van de korpsen had volgens de audits in 2011 de verwerking van gevoelige gegevens onvoldoende geborgd. Zo bleken er niet altijd procesbeschrijvingen of richtlijnen te zijn voor het omgaan met dit soort gegevens. De auditoren stelden voorts vast dat soms verwerking plaatsvond, terwijl de noodzaak onvoldoende duidelijk en/of onderbouwd was[81]. Bij de hercontrole is vastgesteld dat inmiddels wel voldaan wordt aan de eisen van artikel 5 Wpg[82].

Knelpunten uit de interviews

Toetsing van noodzaak en doelbinding naar geest of letter?

Ook geïnterviewden geven aan dat er nog geen systematische toetsing plaatsvindt van noodzaak en doelbinding. Deels wordt dat geweten aan het punt dat de auditoren constateren: het is niet vastgelegd in de werkprocessen. Daarnaast wordt door geïnterviewden opgemerkt dat het bij 'juistheid, noodzakelijkheid, volledigheid en rechtmatigheid' om open normen gaat. Dat wil zeggen dat er geen afgebakende grenzen zijn voor wanneer sprake is van noodzakelijkheid etc. Deze grenzen zijn volgens de betrokkenen ook niet altijd vooraf goed te bepalen. Bij de start van een onderzoek kan het precieze verwerkingsdoel niet altijd worden gegeven. Over gevoelige gegevens als in artikel 5 zijn door de geïnterviewden geen specifieke punten genoemd.

Door groot aantal mutaties is volgens betrokkenen enige ruis in gegevens onvermijdelijk

Geïnterviewden voeren ook een praktisch knelpunt op bij het toepassen van artikel 3 en 4. Volgens een geïnterviewde van de politie zijn er jaarlijks wel een miljoen mutaties in de systemen. Je kunt volgens de betrokkenen niet alles (in detail) controleren. Ze geven aan dat voor de verwerking van artikel 8 gegevens bovendien geen bronvermelding hoeft plaats te vinden.

Gevolg daarvan is dat er volgens de geïnterviewden vooral in BVH enige ruis zit qua juistheid en nauwkeurigheid. Dit komt volgens hen ook omdat in de systemen ook persoonlijke interpretaties en notities zijn opgenomen. Deze kunnen van belang zijn voor

[79] DAD audits, 2012.
[80] Landelijke rapportage hercontrole Wpg, 2013.
[81] DAD audits, 2012.
[82] Landelijke rapportage hercontrole Wpg, 2013.

de sfeertekening van een situatie of persoon waarvan gegevens worden verwerkt, maar zijn in wezen een subjectieve invulling.

Onvoldoende ondersteuning systemen complicerend bij borging

De politie werkt in de kern met twee basissystemen voor de verwerking van politiegegevens: de Basisvoorziening Handhaving (BVH) en de Basisvoorziening Opsporing (BVO). In grote lijnen wordt BVH gebruikt voor de ondersteuning van dagelijkse politietaken en BVO voor rechercheonderzoek. Verschillende geïnterviewden noemen als knelpunt voor het borgen van hetgeen is genoemd in artikel 3, 4 en 5 het niet ondersteunen van de Wpg door BVH en BVO. Ook kan men niet alle typen gegevens kwijt in de systemen. Bijvoorbeeld geluid- en beeldmateriaal en gegevens van personen met een andere status dan de systeemopties (verdachte, getuige, etc.) in de systemen. Het eerste heeft tot gevolg dat er 'hulpsystemen' ontstaan waarin deze gegevens wel kunnen worden verwerkt. Het tweede heeft tot gevolg dat er een status moet worden toegekend aan een persoon die feitelijk niet overeenstemt met de werkelijke status. Daarnaast geven geïnterviewden aan dat er een zekere angst is dat (belangrijk geachte) gegevens wordt vernietigd (vijf jaar na verwijdering). Om dat te voorkomen, wordt volgens de geïnterviewden gewerkt met schaduw/kopie-bestanden.

Extra onzekerheid over gegevens uit het buitenland?

Over de juistheid en rechtmatigheid van informatie uit het buitenland kan volgens diverse geïnterviewden onzekerheid bestaan omdat controle hiervan extra lastig is. Ook wordt soms informatie uit het buitenland breed binnen de organisatie uitgezet, waarvan de rechtmatigheid en juistheid ook niet altijd bekend is.

Volledige zekerheid rechtmatigheid, juistheid en volledigheid volgens betrokkenen lastig

Het geheel maakt volgens diverse betrokkenen (informatiebeheerders, privacyfunctionarissen) de borging vooraf en toetsing achteraf van de rechtmatigheid, juistheid en volledigheid niet eenvoudiger. Gezien de hoeveelheid informatie en aantallen mutaties en de tijd die met controle gepaard gaat, is het volgens geïnterviewden niet mogelijk de systemen meer dan incidenteel te controleren op noodzaak, rechtmatigheid, doelbinding, juistheid en volledigheid.

Wpg heeft volgens betrokkenen bewustzijn rond kwaliteit gegevens verhoogd

Wel wordt aangegeven dat de Wpg een zekere mate van bewustwording heeft gecreëerd dat persoonsgegevens juist en nauwkeurig moeten zijn. De mogelijkheid dat betrokkenen onder bepaalde voorwaarden hun eigen gegevens kunnen inzien, speelt hierin ook een rol. Volgens de geïnterviewden is dit bewustzijn er niet in alle lagen van de organisatie.

4.4 Autorisaties

Art. 6 Wpg schrijft voor dat de verantwoordelijke een systeem van autorisaties laat opzetten en onderhouden waarin wordt geregeld wie toegang heeft tot welke gegevens[83]. Dit vanuit de optiek dat een medewerker alleen toegang heeft tot gegevens die hij of zij vanuit de taakuitvoering nodig heeft. Daarmee wordt niet alleen het aantal mensen dat toegang heeft tot bepaalde gegevens beperkt, maar wordt ook de afscherming van gegevens in relatie tot het opsporingsbelang geborgd. Een autorisatie moet beschrijven tot welke gegevens welke medewerker toegang heeft. Het doel daarvan is volgens de wetgever drieledig:

1. helderheid voor de medewerker;
2. het bieden van een basis voor de inrichting van de ICT;
3. aanknopingspunt voor controle en toezicht.

Het systeem moet daarbij een onderscheid maken tussen de aard van de verwerking (raadplegen, muteren, toevoegen, combineren, verwijderen etc.) en de (risico's van de) taken waarmee de geautoriseerde is belast. In de wijze waarop dat wordt geregeld heeft de verantwoordelijke een zekere vrijheid, vooral voor de autorisaties bij de uitvoering van dagelijkse politietaken. De gedachten van de wetgever gingen wel uit naar een autorisatiematrix, waarin een koppeling wordt gelegd tussen autorisatie op basis van de Wpg en het functie/taakprofiel van een medewerker.

Knelpunten uit de audits

Uit de audits blijkt dat in 2011 70-80% van de korpsen voldeed aan de verschillende eisen voor autorisaties zoals het hebben van een autorisatiematrix, een beschrijving van het proces voor het aanvragen van een autorisatie en het (bewaren van het) protocolleren van een afgegeven autorisatie. Het beheer van de afgegeven autorisaties (wijziging, verwijdering) was bij slechts 15% van de korpsen op orde. Dit met uitzondering van het beheer van de autorisaties voor CIE- en RID-gegevens dat bij vrijwel alle korpsen op orde was.

In de audits is aangegeven dat naast de systemen ook persoonlijke mappen worden gebruikt en gedeeld, waar geen autorisaties aan verbonden zijn[84].

Ook bij de hercontrole in 2013 wordt nog niet voldaan aan de eisen voor het beheer van de autorisaties. Als motief is daarbij aangevoerd dat er een (nieuwe) landelijke autorisatiematrix en handreiking worden opgesteld (mede in het licht van de

[83] Artikel 6 Wpg.
[84] DAD audits, 2012.

vereenvoudiging van het functiehuis bij de politie). In afwachting daarvan hebben de meeste eenheden afgezien van het opstellen van een specifieke autorisatiematrix[85].

Knelpunten uit de interviews

Spanningsveld statische autorisatiematrix en dynamiek uitvoering politietaken

Geïnterviewden geven aan dat het beheer van een autorisatiematrix zoals de wetgever dat voor ogen heeft, complex is. Om te beginnen was in de situatie van vóór 1 januari 2013 sprake van een zeer grote verscheidenheid aan functies. Een geïnterviewde spreekt over 1.300 verschillende en niet altijd even scherp afgebakende functieomschrijvingen binnen de eenheid. Het is volgens hem moeilijk om op basis daarvan tot een hanteerbare en beheersbare autorisatiematrix te komen[86].

Daarnaast kan een medewerker volgens geïnterviewden in verschillende rollen betrokken zijn in zaken of tijdelijk in een ander organisatieonderdeel worden geplaatst. Er is dus niet sprake van een eenduidig autorisatieprofiel op functieniveau. Een leidinggevende en een informatieanalist geven bijvoorbeeld aan dat rechercheurs die thematisch werken niet bij collega's uit andere teams die aan hetzelfde thema werken in de dossiers kunnen kijken, waardoor mogelijke (netwerk)relaties of verbanden tussen zaken of personen kunnen worden gemist.

Ook in het (proces van het) autoriseren worden knelpunten ervaren. Zo geeft een informatiemanager aan dat de autorisaties nog niet eenduidig worden toegepast. Soms is het ook lastig op voorhand in te schatten welke gegevens relevant zijn voor medewerkers met een generieke taakstelling. Het komt volgens hem ook voor dat autorisaties niet worden ingetrokken, terwijl het onderzoek waarvoor de autorisatie is verleend al is afgesloten. Een rechercheur geeft aan dat als een onderzoek is afgesloten en de autorisaties zijn ingetrokken, het soms meer dan een week duurt om in het kader van hernieuwde verwerking toegang tot de gegevens te krijgen. Dat lijkt een zekere frustratie op te roepen: "*Over sommige zaken zijn complete boeken geschreven, die voor het hele publiek toegankelijk zijn, maar ik moet meer dan een week wachten voor ik bij de politie informatie mag. De zingeving achter de politie-organisatie wordt aangetast door al de autorisaties. Op deze manier is er geen 'free flow of information'.*".

Onvoldoende koppeling en ondersteuning ICT-systemen

Het autoriseren en de-autoriseren is volgens geïnterviewden tijdrovend, mede doordat de autorisatiematrices niet gekoppeld kunnen worden aan de personeelssystemen. Dat

[85] Landelijke rapportage hercontrole Wpg, 2013.
[86] Landelijk ging het naar schatting om 16.000 functieomschrijvingen die terug moeten worden gebracht tot 92 functieniveaus.

betekent dat alle mutaties in autorisaties handmatig moeten worden doorgevoerd. Het aantal mutaties in autorisaties dat dagelijks zou moeten worden uitgevoerd is zeer hoog door veranderingen in taken/functies en zaken waar een geautoriseerde bij betrokken is.

Capaciteitsprobleem

Het beheer van de autorisatiematrix is (veelal) bij de privacyfunctionaris belegd. Hiervoor is in de praktijk meestal niet meer dan 1 fte vrijgemaakt. Binnen deze beschikbare capaciteit is het volgens privacyfunctionarissen ook niet mogelijk om een autorisatiematrix actueel te houden. Dit nog los van de complexiteit die in het voorgaande is genoemd.

4.5 Geheimhoudingsverplichting

In art. 7 Wpg is een geheimhoudingsplicht neergelegd die geldt voor politieambtenaren en degenen aan wie politiegegevens zijn verstrekt[87].

Knelpunten uit de audits

In 2011 had volgens de audits bijna 90% van de korpsen de geheimhouding geborgd in de organisatie. De auditoren stelden wel vast dat diegenen aan wie politiegegevens werden verstrekt, niet altijd op die geheimhouding werd gewezen. Bovendien was niet bij alle korpsen het melden van de geheimhoudingsplicht richting ontvanger in een werkinstructie opgenomen[88].

In de rapportage van de hercontrole in 2013 wordt niets vermeld over dit onderwerp.

Knelpunten uit de interviews

Hanteerbaarheid van de uitleg van het begrip 'geheimhoudingsplicht' in de Wpg

De exacte interpretatie van het begrip 'geheimhouding' wordt door een aantal geïnterviewden als lastig ervaren. Op grond van de Wpg zijn politiegegevens geheim, tenzij het in bijzondere gevallen noodzakelijk is de geheimhoudingsplicht te doorbreken. Verschillende geïnterviewden vinden dat deze uitzondering in de memorie van toelichting van de Wpg erg beperkt wordt uitgelegd. Als voorbeeld van een bijzonder geval wordt in de MvT genoemd het tonen van een foto tijdens een buurtonderzoek. Hierbij gaat het volgens geïnterviewden echter niet om bijzondere gevallen nu een dergelijke situatie vaak voorkomt. Geïnterviewden geven aan dat het lastig is dit artikel te interpreteren.

[87] Artikel 7 Wpg.
[88] DAD audits, 2012.

Bewustzijn geheimhouding bij ontvanger politiegegevens

Het is volgens geïnterviewden de vraag of bij verstrekkingen op de geheimhoudingsplicht wordt gewezen. Ontvangers van politiegegevens zijn zich niet bewust van deze geheimhoudingsplicht en zorgen daarom niet voor borging van deze plicht.

4.6 Samenvattende bevindingen

Paragraaf 1 van de Wpg schetst in de artikelen 1 tot en met 7 de belangrijkste uitgangspunten die gelden voor het verwerken van politiegegevens. Onder meer als het gaat om verantwoordelijkheid, de noodzakelijkheid, rechtmatigheid en doelbinding van verwerking, de volledigheid, juistheid en beveiliging van gegevens, de autorisaties en geheimhouding.

Weinig sturing op algemene uitgangspunten

Op papier zijn leidinggevenden door de verantwoordelijke gemandateerd voor de uitvoering van de Wpg. Geïnterviewden geven aan dat in de dagelijkse leiding echter weinig wordt gestuurd op werken conform de Wpg. Dit wordt onder meer geweten aan onvoldoende kennis en daarmee bewustzijn en prioriteit. Eén van de oorzaken daarvan kan zijn de wijze waarop de communicatie naar leidinggevenden bij de invoering van de Wpg is verlopen.

Borging noodzaak en doelbinding verwerking begripsmatig en technisch lastig

Uit de audits uit 2011 bleek dat de noodzakelijkheid en doelbinding van verwerking en de beveiliging van gegevens bij veel korpsen niet systematisch en bedrijfsmatig was geborgd. Uitzondering hierop was de verwerking van CIE- en RID-gegevens. Zowel in de audits als de interviews komt daarbij het niet ondersteunen van de Wpg door de aanwezige ICT als belangrijk knelpunt voren. Uit de interviews komt daarnaast de interpretatie van begrippen als 'noodzakelijkheid' en 'doelbinding' als knelpunt naar voren. De politiepraktijk vraagt om een zekere flexibiliteit en daar sluiten de open normen bij aan. Het maakt het echter lastig om te beoordelen en (achteraf) te toetsen óf ook sprake is van respectievelijk noodzaak of doelbinding.

Autorisaties nog problematisch door dynamisch karakter en administratie

Ook de borging van het beheer van de autorisaties was bij de meting van de audits in 2011 beperkt. Er waren in 2011 wel autorisatiematrices en ook was het proces om tot autorisatie te komen beschreven. Dit geldt echter niet voor het beheer van de mutaties. In de interviews wordt naar voren gebracht dat het idee van een statische autorisatiematrix (autorisatieprofiel gekoppeld aan functieprofiel) niet goed aansluit bij de politiepraktijk. Enerzijds kan een medewerker meerdere rollen hebben of in meerdere zaken zijn betrokken. Dat betekent dat in principe verschillende autorisatieniveaus van toepassing (kunnen) zijn op een medewerker. Anderzijds is ook sprake van veel administratie door de

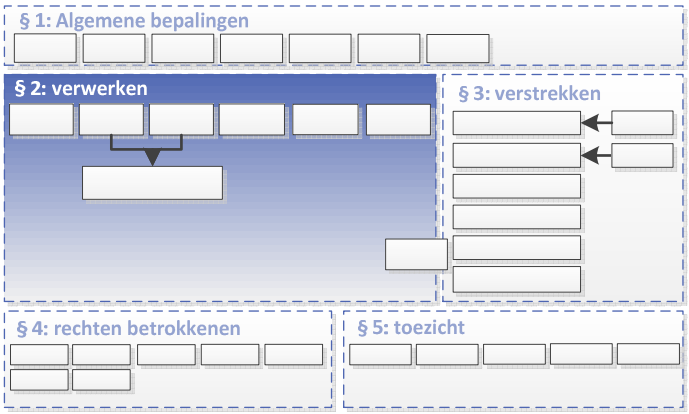
grote hoeveelheid mutaties in autorisaties. Te specifieke autorisatieprofielen kunnen bovendien de uitvoering van politietaken in de weg staan.

Geheimhouding op papier geregeld maar in de praktijk nog zoeken naar modus

Volgens de audits is de geheimhouding (art. 7 Wpg) op papier geregeld. De interviews laten op dit punt nog wel enkele knelpunten zien. Belangrijkste is of degene aan wie politiegegevens worden verstrekt, wel op de hoogte is van deze geheimhouding en/of daar door degene die verstrekt, op wordt gewezen. Daarnaast worden bij de uitvoering van politiektaken knelpunten ervaren bij de interpretatie van het begrip 'bijzondere gevallen' waarin geheimhouding kan komen te vervallen. Betrokkenen geven aan dat zich meer situaties voordoen dan de wet ogenschijnlijk toelaat.

5 Verwerking van politiegegevens

5.1 Inleiding



Paragraaf 2 van de Wpg gaat in op het centrale begrip 'verwerken'. Dit is ruim gedefinieerd, dat wil zeggen dat alle handelingen met politiegegevens hieronder worden verstaan.[89] In dit hoofdstuk schetsen we hoe de praktijk van het verwerken eruit ziet. Meer specifiek in welke mate deze conform de Wpg is en welke knelpunten in de praktijk worden ervaren. Het ter beschikking stellen en verstrekken van gegevens, dat wil zeggen daar waar politiegegevens de organisatie verlaten, wordt apart beschreven in hoofdstuk 6.

We gaan achtereenvolgens in op:

- De verwerking bij de uitvoering van de dagelijkse politietaak, art. 8 Wpg (paragraaf 5.2)
- De verwerking bij onderzoek in het kader van handhaving van de rechtsorde in een bepaald geval, art. 9 Wpg (paragraaf 5.3)
- Het onderscheid tussen artikel 8 en 9 (paragraaf 5.4)
- De verwerking bij het krijgen van inzicht in de betrokkenheid van personen bij ernstige bedreigingen van de rechtsorde, art. 10 Wpg (paragraaf 5.5)
- Geautomatiseerd vergelijken en in combinatie zoeken, art. 11 Wpg (paragraaf 5.6)
- Bewaartermijnen, art. 14 Wpg (paragraaf 5.7)
- Ontwikkelingen rond digitalisering en ICT (paragraaf 5.8)
- Overige zaken (paragraaf 5.9)

We sluiten af met de samenvattende bevindingen (paragraaf 5.10).

[89] Art. 1 onder c Wpg.

5.2 Artikel 8: uitvoering van de dagelijkse politietaak

Artikel 8 Wpg bepaalt de condities voor het verwerken van politiegegevens bij de uitvoering van de dagelijkse politietaak. Gegevens die betrekking hebben op de dagelijkse politietaak (artikel 8) mogen één jaar ongericht en nog vier jaar gericht verwerkt worden, alvorens ze moeten worden verwijderd. De gegevens worden nog wel vijf jaar bewaard alvorens tot vernietiging of archivering wordt overgegaan.

Knelpunten uit de audits

In de audits werd geconstateerd dat eind 2011 meer dan 80% van de korpsen wat betreft artikel 8 onvoldoende bedrijfsmatig had geborgd dat verwerking en vernietiging van politiegegevens conform de eisen van de Wpg plaatsvindt. Zo waren er niet altijd procesbeschrijvingen of instructies voor verwijdering en vernietiging en waren niet alle medewerkers zich voldoende bewust van de bewaartermijnen van de verschillende regiems. Vernietigen van de gegevens vond meestal niet plaats, maar was wettelijk gezien over het algemeen ook nog niet aan de orde. Zoals in hoofdstuk 4 is aangegeven bleek uit de audits dat in 2011 slechts een kwart van de korpsen (aantoonbaar) voldeed aan de eisen van noodzakelijkheid, rechtmatigheid en doelbinding bij de verwerking van artikel 8 gegevens[90].

Als verklaring voor het niet voldoen aan de eisen van de Wpg werd onder meer het uitstel van de implementatie van BVH genoemd[91]. Hierdoor werd de uitvoering van de Wpg onvoldoende door de ICT ondersteund. Zo is een afscherming van de gegevens na één jaar technisch niet mogelijk en kunnen gegevens onvoldoende worden gelabeld en gecodeerd om vervolgens automatisch tot verwijdering over te gaan. Handmatige verwijdering vergt veel tijd. Daarbij bleek ook dat de verschillende regiems in verschillende systemen door elkaar worden gebruikt.

Deze situatie was in 2013 – bij de hercontrole – niet wezenlijk verbeterd. Wel waren op dat moment de nieuwe systemen in ontwikkeling[92].

Knelpunten uit de interviews

Onduidelijkheid interpretatie verwerkingstermijn, bewaartermijn en vernietiging

Bij de organisaties waarvan medewerkers zijn geïnterviewd zijn de termijnen voor verwerking, verwijdering en vernietiging verschillend ingevuld. Een privacyfunctionaris geeft aan dat in de organisatie de begrenzing van de verwerkingstermijn van één jaar niet

[90] DAD audits, 2012.
[91] In de interviews wordt daarnaast aangegeven dat het wel geïmplementeerde BHV functioneel niet voldoet aan de eisen van de Wpg, bijvoorbeeld als het gaat om de ondersteuning bij de protocollering en de autorisaties.
[92] Landelijke rapportage hercontrole Wpg, 2013.

wordt gehanteerd. De gegevens worden vijf jaar na eerste verwerking achter een schot gezet. Een privacyfunctionaris in een andere case geeft aan dat wel de termijnen van de Wpg worden aangehouden voor zover het digitale gegevens betreft. Bij de papieren dossiers gebeurt dat volgens deze privacyfunctionaris en andere geïnterviewden niet, of in ieder geval niet systematisch. In hoeverre dat knelpunten kan opleveren in verband met bijvoorbeeld cold-cases overziet men niet. In praktische zin is dat ook nog niet aan de orde omdat de vernietigingstermijn volgens de geïnterviewde pas in 2018 ingaat.

Twijfels bij nut en noodzaak van verwerkingstermijn van één jaar

De wenselijkheid en nut en noodzaak van de verwerkingstermijn van één jaar worden betwijfeld door verschillende geïnterviewden. Een leidinggevende geeft aan dat de termijn van één jaar vooral verwarrend is. Je mag één jaar ongericht zoeken, maar tot vijf jaar gericht. In zijn ervaring komt ongericht zoeken in de praktijk niet of nauwelijks voor. Het kan wel eens handig zijn voor een agent om bijvoorbeeld na een vakantie een beeld te krijgen van wat er is gebeurd. De termijn van één jaar heeft in zijn ogen vooral bijgedragen aan het beeld dat er na één jaar bepaalde informatie niet meer mag worden opgevraagd. Daarbij wordt aangetekend dat de Wpg toch al door de eis van doelbinding 'dwingt' tot gericht zoeken. In die zin is de termijn van één jaar volgens hem niet nodig en niet praktisch.

Een ander voorbeeld dat wordt genoemd is het toezicht op vreemdelingen. Geïnterviewden geven aan dat geen zicht op de historie van een vreemdeling kan worden verkregen als gegevens na één jaar achter schot moeten. Het wordt daarbij vreemd gevonden dat instanties waaraan dezelfde informatie is verstrekt, bijvoorbeeld de IND, vaak wel gewoon directe toegang hebben tot die historie.

Onvoldoende aansluiting Wpg en BVH

Rechercheurs en leidinggevenden geven aan dat er knelpunten zijn in de 'match' tussen artikel 8 en BVH. In de praktijk wordt BVH gezien als de applicatie waarin de politiegegevens voor de uitvoering van dagelijkse politietaken worden verwerkt. Het systeem is in 2008 ingevoerd, maar niet 'Wpg-proof'. Enerzijds is het technisch niet mogelijk om een scheiding aan te brengen in toegankelijkheid van gegevens tot één jaar en tussen de één en de vijf jaar. Anderzijds komen ook in BVH artikel 9-gegevens voor. Óf omdat zij ook relevant zijn voor de uitvoering van dagelijkse politietaken, óf omdat overheveling naar BVO lastig is. In één case geven de geïnterviewden aan dat de gegevens in BVH na vijf jaar automatisch achter een schot komen en ze alleen nog via een zogenaamde 'poortwachter' toegankelijk zijn. Omdat BVH pas in oktober 2008 is geïmplementeerd zitten er in beginsel nog geen gegevens in die ouder zijn dan vijf jaar.

Verlies aan informatie voor cold-case onderzoek

Er worden ook knelpunten gezien bij het oplossen van cold-cases. In meerdere gesprekken is aangegeven dat bijna per definitie geldt dat gegevens ex artikel 8 Wpg die relevant kunnen zijn voor een cold-case onderzoek, ouder zijn dan tien jaar. Als voorbeeld wordt genoemd een vrouw die begin deze eeuw, vermoedelijk door een misdrijf, om het leven is gekomen. Na meer dan tien jaar wordt haar identiteit vastgesteld. De politiegegevens die destijds onder artikel 8 zijn verwerkt kunnen inzicht geven in haar toenmalige woonomgeving en in het milieu waarin ze destijds verkeerde. Deze gegevens zijn echter vernietigd. Daardoor konden ze niet mee worden genomen in het onderzoek.

Persoon niet of moeilijker kunnen aanmerken als verdachte

Om een persoon als verdachte te kunnen aanmerken is een overzicht van relevante mutaties in BVH en/of processen-verbaal volgens verschillende geïnterviewden soms noodzakelijk. Zo kan het feit dat iemand al jarenlang aanwezig is op de Wallen zeer relevant zijn in de opbouw van een verdenking van mensenhandel. In bijlage 3 van de Aanwijzing Mensenhandel staat vermeld dat één van de indicatoren van mensenhandel een relatie met personen met relevante antecedenten is of met locaties die geassocieerd worden met mensenhandel. Om in dit voorbeeld een jarenlange aanwezigheid op de Wallen te kunnen aannemen, is het soms noodzakelijk informatie op grond van artikel 8 Wp te gebruiken. Na vijf jaar kunnen de artikel 8-gegevens echter niet meer verwerkt worden en volgens de geïnterviewden beperkt dat de opsporingsmogelijkheden.

Toestemming bevoegd gezag

Op grond van artikel 14 Wpg is voor de hernieuwde verwerking van verwijderde gegevens toestemming van het bevoegd gezag noodzakelijk. Hernieuwd verwerken kan alleen in bijzondere gevallen. Aangegeven is dat dit in de praktijk tot een knelpunt kan leiden: de matchingsautoriteit[93] (hierna: MA) beheert identiteitsgegevens en zorgt voor het matchen van identificerende persoonsgegevens. Als sprake is van een 'mismatch' of als verdachten zich in het verleden voor een ander hebben uitgegeven, wordt nader onderzoek verricht. Omdat het veelal gaat om recidivisten die bij aanhouding vaak verschillende valse namen of namen van anderen gebruikten, worden ook gegevens uit BVH verwerkt die ouder zijn dan vijf jaar. Bij de geschetste casus is over het algemeen geen sprake van bijzondere gevallen waarbij hernieuwde verwerking is toegestaan. Het gaat vaak om kleine feiten in het kader van de dagelijkse politietaak. Op grond van artikel 13 Wpg kunnen politiegegevens die worden verwerkt overeenkomstig artikel 8, 9 en 10 verder worden verwerkt ten behoeve van de ondersteuning van de politietaak. Omdat de bewaartermijn van artikel 8 korter is dan die van artikel 13 kun je uiteindelijk echter niet meer bij de brongegevens.

[93] Zie http://www.justid.nl/matchingsautoriteit/

Belang van behoud brongegevens voor bijvoorbeeld trendanalyses

Een specifiek knelpunt van de termijn van vijf jaar waarin artikel 8-gegevens verwerkt mogen worden betreft grootschalige data-analyses. Om te kunnen voorzien in de informatiebehoefte van de politie en haar ketenpartners worden gegevens uit verschillende bronsystemen gecombineerd. Dit betekent dat gegevens worden gebundeld, gesynchroniseerd en verwerkt tot nieuwe (politie)gegevens. Het behoud van de brongegevens is daarbij van belang. Een voorbeeld is een analyse van een trend rond straatroven. Door de aanpassing van geografische eenheden binnen de politie (bijvoorbeeld als gevolg van de inrichting van de Nationale politie) lopen de grenzen niet meer zoals voorheen. Korpsen zijn bijvoorbeeld samengevoegd tot Eenheden. Een historische analyse op het niveau van bijvoorbeeld een wijkteam is niet meer te maken als de brongegevens op grond van de Wpg niet meer kunnen worden verwerkt of vernietigd zijn.

Doordat overhevelen van gegevens niet altijd plaatsvindt, gaan gegevens verloren

De te onderscheiden verwerkingsdoeleinden zijn aan verschillende bewaartermijnen gekoppeld. Geïnterviewden van de politie en het OM hebben aangegeven dat met de daadwerkelijke implementatie van de Wpg en de intentie tot naleving van deze wet, politiegegevens in toenemende mate zullen worden verwijderd en vernietigd. Door het verwijderen van gegevens verslechtert de informatiepositie. Deze verslechtering kan worden ondervangen door gegevens tijdig doel-afwijkend te verwerken. In de praktijk vindt deze 'overheveling' niet altijd plaats. De geïnterviewden van het OM geven aan dat dit verschillende oorzaken heeft. De kennis van de mogelijkheden van de Wpg is bij zowel de politie als het OM niet altijd aanwezig. Verder is het overhevelen van gegevens volgens hen zeer arbeidsintensief en wordt het overhevelen niet goed door de ICT ondersteund. Omdat vele gegevens worden verzameld, zou bepaald moeten worden welke gegevens relevant zijn voor verdere verwerking. Wat 'relevant' is, is volgens de geïnterviewden echter moeilijk te bepalen.

Risico's van gegevensverlies

Het verwijderen van gegevens uit BVH gebeurt in sommige regionale eenheden automatisch: volgens geïnterviewden worden elke nacht gegevens ouder dan vijf jaar door middel van een query uit BVH verwijderd. BVH kan echter ook artikel 9-informatie bevatten. De gesprekspartners geven aan dat het niet mogelijk is artikel 8-gegevens te labelen als artikel 9-gegevens. Als knelpunt van het automatisch verwijderen van gegevens wordt dan ook genoemd dat ook gegevens worden verwijderd die van status zijn veranderd, oftewel persoonsgegevens die gebruikt worden in een opsporingsonderzoek. Dat betekent volgens de geïnterviewden een onbedoeld verlies van informatie. Eigenlijk zouden de gegevens handmatig verwijderd moeten worden, maar dat is te arbeidsintensief.

5.3 Artikel 9: onderzoek in kader handhaving rechtsorde

Artikel 9 bepaalt de condities waaronder politiegegevens gericht kunnen worden verwerkt in het kader van onderzoek naar de handhaving van de rechtsorde in een bepaald geval. Als artikel 9-gegevens worden verwerkt moet het doel van deze verwerking worden vastgelegd. Gegevens mogen worden verwerkt zolang het onderzoek niet is afgesloten. Na afsluiting moeten ze na maximaal een half jaar worden verwijderd en worden ze nog maximaal vijf jaar bewaard alvorens te worden vernietigd of gearchiveerd.

Knelpunten uit de audits

Uit de audits blijkt dat ruim 90% van de korpsen eind 2011 niet voldeed aan de eisen van verwijdering en vernietiging van artikel 9-gegevens. Behalve vertraging in de implementatie van de ICT (BVO) werd het niet ontvangen van afloopberichten van het OM hiervoor als oorzaak genoemd. De helft van de korpsen voldeed eind 2011 (aantoonbaar) aan de eisen van doelbinding, noodzakelijkheid en rechtmatigheid bij de verwerking van artikel 9 gegevens[94]. Het beeld in 2013 is vergelijkbaar, zo blijkt uit de hercontrole. De politie ontvangt (nagenoeg) geen afloopberichten, waardoor verwijdering binnen de termijn lastig is. Bij de vernietiging heeft men met dezelfde problemen te maken als bij artikel 8[95].

Knelpunten uit de interviews

Formele verwijderingsmoment moeilijk te bepalen

Het correct toepassen van de verwijderingstermijn van artikel 9 is volgens diverse rechercheurs en privacyfunctionarissen een knelpunt. Van belang is dat op sommige gegevens niet de Wpg van toepassing is, omdat in het wetboek van Strafvordering een bijzondere regeling is getroffen (zie paragraaf 9.2). Het verwijderen dient handmatig te gebeuren, omdat de termijn niet van tevoren te bepalen is. Een half jaar nadat het voor het doel van het onderzoek niet langer noodzakelijk is om gegevens te bewaren dienen deze verwijderd worden, hetgeen in de praktijk wordt geïnterpreteerd als een half jaar nadat een opsporingsonderzoek is afgesloten. Er bestaat echter, zo blijkt uit interviews, onduidelijkheid over de definitie van het beëindigen van een onderzoek. Gaat het om het totale onderzoek dat meerdere zaken kan behelzen of de zaak met betrekking tot een individu? Bij geïnterviewden is onduidelijk hoe het zit bij een strafzaak met meerdere verdachten, waarbij er niet voor allen een onherroepelijke uitspraak is. Het is dan volgens de geïnterviewden onduidelijk wat er met de persoonsgegevens van de andere mogelijke verdachten in het onderzoek dient te gebeuren. In de MvT is aangegeven dat in geval van een opsporingsonderzoek dat heeft geleid tot een vervolging de gegevens niet langer noodzakelijk zijn op het moment dat de rechter ten aanzien van de zaak onherroepelijk

[94] DAD audits, 2012.
[95] Landelijke rapportage hercontrole Wpg, 2013.

heeft beslist.[96] Geïnterviewden geven aan dat het onduidelijk is wanneer hiervan sprake is. Is dat na het hoger beroep, na cassatie of na een rechtsgang na het Europees hof?

Een ander voorbeeld dat wordt genoemd is de in Nederland inbeslaggenomen cocaïne. Deze is uiteindelijk afkomstig uit Zuid Amerika. Wanneer is het onderzoeksdoel dan echt gerealiseerd: als de bezitter is veroordeeld, de betrokkenen bij de import, export, vervoer, de tussenpersonen, de producenten, de opdrachtgevers, de faciliteerders, degenen die de opbrengsten hebben wit gewassen? Alleen in Nederland?

Geïnterviewden noemen het een praktisch probleem dat politie en OM een verschillend 'zaakbegrip' hanteren. Als voorbeeld is door een leidinggevende genoemd een moordzaak met drie verdachten. Voor het OM zijn dat drie zaken. Voor de politie is dat één zaak. De vraag is dan welk deel van het politiedossier moet worden verwijderd nadat een verdachte veroordeeld is of zijn/haar straf heeft uitgezeten?

Risico op vervuiling in bestanden

Omdat voor artikel 9 gegevens geen standaard verwerkingstermijn geldt, moet handmatig worden aangegeven of en zo ja welke gegevens moeten worden verwijderd. Dat vergt volgens een rechercheur – ook in het licht van het vorige punt – veel discipline, aandacht en tijd. Die tijd ontbreekt volgens de betrokkenen vaak waardoor er geen prioriteit wordt gegeven aan opschoning. Het ontvangen van een afloopbericht van het OM wordt dan vaak als signaal gebruikt om alsnog tot schoning over te gaan. Volgens betrokken worden deze berichten echter niet altijd ontvangen en vindt er dus ook geen schoning plaats. Dit heeft het risico in zich dat gegevens – op basis van de regels van de Wpg – ten onrechte worden gebruikt in een ander onderzoek. De betreffende rechercheur had nog geen zaak meegemaakt die daarop is stukgelopen, maar advocaten hebben volgens hem daar wel aandacht voor. In de praktijk is het moment dat een collega informatie opvraagt over een eerdere zaak een natuurlijk 'schoningsmoment'.

Delen van artikel 9 informatie bij noodhulp

Het kan zijn dat artikel 9 gegevens van belang zijn voor noodhulp. Bijvoorbeeld bij een brandmelding over een pand waar een sterk vermoeden van criminele activiteiten is. Verschillende agenten en het OM geven aan dat het gelet op de hulpverlening of de veiligheid van politiemensen of hulpverleners wenselijk is deze artikel 9 gegevens door te geven. Artikel 9 lid 3 Wpg biedt hiertoe ook de mogelijkheid, maar dit is blijkbaar niet altijd bekend en bovendien moeten de medewerkers van de meldkamer hiertoe ook geautoriseerd zijn.

[96] MvT, p. 43.

5.4 Onderscheid artikel 8 en 9

De Wpg maakt een onderscheid in politietaken wat betreft het verwerkingsregime dat van toepassing is. Dat impliceert dat dit onderscheid ook in de praktijk aanwezig moet zijn, bijvoorbeeld in de autorisaties, systemen, bewaartermijnen en het doel van de verwerking.

Knelpunten uit de audits

Uit de audits bleek dat eind 2011 meer dan de helft van de korpsen voldeed aan de eisen voor het onderscheid in verwerking van politiegegevens in het kader van de uitvoering van de dagelijkse politietaak (artikel 8) en gericht onderzoek bij de handhaving van de rechtsorde (artikel 9)[97]. Bij de hercontrole bleek dit onderscheid goed bekend te zijn bij specialistische afdelingen. Bij enkele eenheden die met BVH werken was men zich nog onvoldoende bewust van het onderscheid[98].

Knelpunten uit de interviews

Gegevens kunnen voor meerdere doeleinden relevant zijn

Uit onderstaand voorbeeld blijkt dat gegevens voor meerdere doeleinden relevant kunnen zijn:

Bij een toevallige constatering bij een verkeerscontrole bevinden zich twee bekende criminelen bij elkaar in een auto en worden enkele vuurwapens aangetroffen. Dit leidt in eerste instantie tot een verwerking met een art. 8 Wpg doel. Deze politiegegevens kunnen bij relevantie direct doel-afwijkend worden verwerkt:

- voor een art. 9 Wpg verwerkingsdoel, te weten het onderzoek van het Boven Regionaal Team (BRT) dat liep "op" één van beide verdachten;
- voor een art. 10 lid 1 onder a Wpg verwerkingsdoel, te weten als één van beide "CIE-subject" (de betrokkene is in beeld bij de CIE) is;
- voor een art. 13 Wpg verwerkingsdoel, te weten de vermelding in het Herkenningsdienstsysteem (HKS)[99] dat deze verdachten vuurwapengevaarlijk zijn.

Scheidslijn tussen artikel 8 en artikel 9 gegevens niet altijd scherp te trekken

Geïnterviewden geven aan dat het in de praktijk niet eenvoudig is te bepalen of een politiegegeven op grond van artikel 8 of 9 moet worden verwerkt. In de Memorie van Toelichting[100] wordt aangegeven dat de grens tussen de artikelen 8 en 9 ligt bij de inzet van bijzondere opsporingsmiddelen en de inzet van een opsporingsteam. In de praktijk wordt de scheidslijn als minder eenduidig gezien. Ook recherchewerkzaamheden waarvoor geen

[97] DAD audits, 2012.
[98] Landelijke rapportage hercontrole Wpg, 2013.
[99] HKS bevat informatie over verdachten en processen verbaal; HKS wordt ook wel aangeduid als het 'verdachtenbestand' van de politie.
[100] Wpg, Memorie van Toelichting, p. 71-72.

bijzondere opsporingsmethoden of een opsporingsteam zijn ingezet, kunnen onder artikel 9 vallen. Hoe een persoonsgegeven uiteindelijk 'gelabeld' wordt, is van belang voor de verwerkingstermijn en de vraag of de herkomst en wijze van verkrijging vastgelegd moeten worden en de doelen van de verwerking geprotocolleerd moeten worden. De administratieve verplichtingen van artikel 9 zijn zwaarder dan die van artikel 8.

Een rechercheur noemt als voorbeeld van een niet heel scherpe cesuur tussen artikel 8 en 9 een straatroof. Vaak wordt in zulke gevallen een pragmatische keuze gemaakt. Artikel 8 is dan aantrekkelijker omdat het minder administratie met zich meebrengt én gegevens minimaal vijf jaar mogen worden verwerkt.

Ook een leidinggevende van een Regionale Informatieorganisatie (RIO) geeft aan dat grens niet altijd scherp is en altijd een interpretatie en afweging vereist is. De politie is op zich wel gewend met open normen te werken, bijvoorbeeld wanneer die voortvloeien uit Sv. Bij de Wpg is dat nog niet zo; daar hebben agenten nog weinig gevoel bij. Er wordt getracht om met praktijkvoorbeelden tastbaarder te maken wat de afwegingen zijn die je kunt/moet maken.

Daarnaast wordt aangegeven dat de status van gegevens nogal eens verandert en gegevens moeten worden overgeheveld. De typen die de Wpg onderscheidt (in het bijzonder tussen artikel 8 en artikel 9/10) worden als enigszins kunstmatig ervaren. Er zijn wel verschillende politietaken, maar politiegegevens hangen daar niet star aan vast. Door onderscheid te maken, wordt er volgens verschillende geïnterviewden impliciet van uitgegaan dat persoonsgegevens statisch zijn: eenmaal verwerkt ten behoeve van de dagelijkse politietaak blijft de informatie gericht op dat doel en geldt het regime van artikel 8 Wpg. Persoonsgegevens die verwerkt zijn in het kader van de dagelijkse politietaak kunnen volgens verschillende geïnterviewden (agenten, leidinggevenden, rechercheurs) van belang worden voor opsporingsonderzoeken, waarmee ze onder het regime van artikel 9 Wpg komen te vallen. Informatie over een persoon kan bijvoorbeeld input bieden voor de analyse van een (crimineel) netwerk waarin iemand zich bevindt. Het feit dat twee personen gezamenlijk betrapt zijn bij een winkeldiefstal kan een stelling van een advocaat weerleggen dat de twee personen elkaar niet zouden kennen. In algemene zin geldt dat informatie van BVH (artikel 8) inzicht kan bieden in de handel en wandel van een eventuele verdachte in een opsporingsonderzoek.

Een analist geeft aan dat het bij gecombineerde gegevens moeilijk is om te bepalen welk verwerkingsregime van toepassing is. Een deel van dezelfde informatie uit een artikel 9 kan ook van belang zijn voor de uitvoering van de dagelijkse politietaak. Vanuit een oogpunt van beheer is dat volgens enkele privacyfunctionarissen en projectleiders 'een crime'.

Technische tekortkomingen systemen

Uit de verschillende gesprekken is opgemaakt dat er naar schatting 1.900 verschillende applicaties met persoonsgegevens gebruikt worden door de politie. De belangrijkste hiervan zijn BVH en BVO, waarin mutaties worden opgenomen en persoonsgegevens verwerkt. Daarbij wordt in de praktijk grosso modo de stelregel gehanteerd dat op BVH het regime van artikel 8 van toepassing is en op BVO dat van artikel 9. Helemaal zuiver is dit onderscheid overigens niet, zo staat de aanleiding voor (zware) rechercheonderzoeken vaak in BVH.[101]

Belangrijker is volgens een leidinggevende en projectleider Wpg dat gegevens in BVH in principe automatisch worden verwijderd na vijf jaar. BVH bevat echter ook artikel 9-gegevens. Het is niet mogelijk deze gegevens als zodanig te markeren en daarmee automatisch verwijderen te voorkomen.

5.5 Artikel 10: verwerking bij ernstige bedreigingen rechtsorde

Artikel 10 bevat drie gerichte verwerkingen met het oog op het krijgen van inzicht in de betrokkenheid van personen bij:

1. het beramen of plegen van bepaalde misdrijven;
2. bepaalde thematische verwerkingen;
3. ernstige schendingen van de openbare orde.

De verwerkingen van artikel 10 lid 1 onder a worden wel CIE-verwerkingen genoemd. Deze verwerking is bedoeld voor het opbouwen van een informatiepositie over de betrokkenheid van personen bij bepaalde ernstige misdrijven. De wetgever gaat er in de toelichting op de Wpg en het BPG vanuit dat: *"De kring van te autoriseren personen… beperkt moet zijn tot de politieambtenaren die taken of werkzaamheden verrichten op het gebied van de criminele inlichtingeneenheid of regionale inlichtingendienst"*.[102]

Knelpunten uit de audits

Uit de audits uit 2011 bleek dat ongeveer de helft van alle organisaties voldeed wat betreft de eisen van de Wpg inzake artikel 10[103]. Het beeld in 2013 is vergelijkbaar. Hoewel BVO beschikt over een instrument voor het opschonen en vervolgens verwijderen van deze gegevens, wordt dit in de praktijk niet altijd juist uitgevoerd. Net als bij artikel 8 en 9 wordt tegen technische problemen opgelopen bij de vernietiging van artikel 10 gegevens[104].

[101] De Kmar werkt niet met BVH en BVO, maar met het Recherche Basis Systeem (RBS), Vreemdelingen Basis Systeem (VBS) en Bedrijfs Processen Systeem (BPS). Op termijn zal bij de Kmar worden gewerkt met SummIT. Ook de BOD-en gebruiken dat systeem.
[102] Nota van toelichting Bpg, p. 39.
[103] DAD audits, 2012.
[104] Landelijke rapportage hercontrole Wpg, 2013.

Knelpunten uit de interviews

Informatiepositie aanpak ZwaCri problematisch door bewaartermijnen en voorzieningen

Volgens het OM ligt het zwaartepunt van de verwerkingen met als doel het krijgen van zicht op betrokkenheid van bepaalde personen bij zware criminaliteit, op informatie van informanten. Overige gegevens worden daarbij ter aanvulling, verificatie of falsificatie gebruikt. Daarbij kan volgens het OM een probleem zijn dat artikel 8- en 9-gegevens al zijn verwijderd of vernietigd. Daarnaast is het volgens het OM ook in meer praktische zin niet mogelijk om dergelijke gegevens te gebruiken: de capaciteit en ICT ondersteuning die nodig zijn voor een vergaande analyse en veredeling van dergelijke gegevens ontbreken volgens het OM. Daardoor is het volgens het OM niet goed mogelijk om (meer structureel) geconcretiseerde netwerk- en dreigingsanalyses te maken en daarmee operationele sturingsinformatie te genereren, bijvoorbeeld voor het opstarten van een onderzoek.

Noodzakelijkheid verwerking CIE-gegevens moeilijk aan te geven

Een van de kritiekpunten uit de audits was dat de noodzakelijkheid van het verwerken van CIE-gegevens onvoldoende gecontroleerd wordt. Dat wordt door het OM onderkend, maar tevens wordt aangegeven dat niet duidelijk is waaraan je dan moet toetsen. Bij het krijgen van zicht en grip op zware criminaliteit is volgens het OM eerder sprake van een permanent proces van analyse van personen en relaties dan van een concreet verwerkingsdoel. Het algemene inzicht kan leiden tot het opstarten van een operationeel opsporingsonderzoek waarbij dan wel sprake is van een concreet verwerkingsdoel. Een specifiek doel is derhalve niet altijd meteen te geven.

Onduidelijkheid over wie artikel 10 verwerkingen mag doen

Leidinggevenden van zowel regionale als landelijke eenheden geven aan de indruk te hebben dat artikel 10 specifiek is bedoeld voor de CIE en RID[105]. Het doen van de in artikel 10 bedoelde analyses kan echter ook buiten de CIE/RID toepassing vinden. Bijvoorbeeld als het gaat om het krijgen van zicht op netwerken en het volgen van ontwikkelingen in netwerken. Dergelijke gegevensverwerkingen vinden in sommige (regionale) eenheden plaats door decentrale informatiemedewerkers (ten behoeve van rechercheonderdelen). Bij diverse geïnterviewden is het beeld dat indien de opbouw van een informatiepositie door decentrale informatiemedewerkers niet onder 'werkzaamheden op het gebied van de criminele inlichtingeneenheid' valt, dat mogelijk geen wettelijke basis heeft.

[105] Deze veronderstelling is niet juist. De Wpg en het Bpg sluiten art. 10 verwerkingen door anderen dan de CIE/RID niet uit. In hoofdstuk 10 komt het kennisaspect over de Wpg als één van de verklarende factoren voor de knelpunten terug.

5.6 Artikel 11: geautomatiseerd vergelijken en in combinatie zoeken

De Wpg kent (limitatief) twee verschillende vormen van doorzoeken van politiegegevens: geautomatiseerd vergelijken (art. 8 lid 2, 11 lid 1, 11 lid 2 en 12 lid 4 Wpg) en in combinatie verwerken (art. 8 lid 3 en 11 lid 4).

Knelpunten uit de audits

Uit de audits in 2011 kwam naar voren dat ongeveer twee derde van de korpsen niet beschikte over duidelijke definities, instructies, regelingen e.d. voor geautomatiseerd vergelijken en gecombineerd zoeken. Bij bijna een kwart van de korpsen was de verantwoordelijkheid niet duidelijk geregeld[106]. In 2013 voldoen de eenheden nog niet volledig aan de eisen van artikel 11. Er zijn landelijk definities vastgesteld, maar deze zijn niet nader uitgelegd, geïmplementeerd en toepasbaar. Ook wordt in een aantal eenheden niet voldaan aan de eisen tot het verkrijgen van een opdracht van het OM en protocollering. Het proces van aanwijzing van functionarissen is wel geborgd.

Knelpunten uit de interviews

Onduidelijkheid over verschil geautomatiseerd vergelijken en in combinatie verwerken

In de Wpg en de parlementaire geschiedenis is geen scherp verschil aangegeven tussen geautomatiseerd vergelijken en gecombineerd verwerken. Evenmin is aangegeven wat de gevolgen zijn voor de politiepraktijk. Geïnterviewden geven aan dat de Wpg op dit punt moeilijk te interpreteren is en dit in de praktijk voor knelpunten zorgt. Bijvoorbeeld omdat onduidelijk is wanneer aan vereisten zoals instemming van de OvJ moet worden voldaan.

Definities OM[107]

Geautomatiseerd vergelijken: het met een binaire zoeksleutel van (een) trefwoord(en) zoeken van bepaalde politiegegevens. Het resultaat van deze gerichte zoekslag is een uitkomst van hit / no hit.

Gecombineerd verwerken: zonder binaire zoeksleutel binnen (een selectie van) beschikbare politiegegevens zoeken naar verbanden. Het resultaat van deze vrije zoekslag is een verzameling van gegevens die voldoen aan bepaalde gemeenschappelijke kenmerken. Deze gemeenschappelijke kenmerken kunnen een profiel van indicatoren of bepaalde kenmerken (trefwoorden) inhouden.

Onduidelijk wat onder geautomatiseerd vergelijken wordt verstaan

De term 'geautomatiseerd vergelijken' wordt lastig gevonden. Een privacyfunctionaris vraagt zich af of bijvoorbeeld een zoekopdracht in feite ook geautomatiseerd vergelijken is. Het systeem vergelijkt immers de zoekterm met de database. Of automatische kentekenregistratie? Een informatiemanager stelt een vergelijkbare vraag ten aanzien van het gebruik van BlueView.

[106] DAD audits, 2012.
[107] Uit de Aanwijzing Wet politiegegevens, (2013A013) die op 1 september 2013 in werking is getreden.

Lacune voor ondersteunende taken

Geïnterviewden van de landelijke eenheid stellen vast dat er een lacune is wat betreft het geautomatiseerd mogen verwerken van politiegegevens in het kader van ondersteunende taken. Bijvoorbeeld als het gaat om rechtshulpverzoeken of gegevens die afkomstig zijn van inspectiediensten, gemeenten of de RDW zonder dat die worden verwerkt in het kader van artikel 8, 9 of 10. Bij de totstandkoming van de Wpg is ervan uitgegaan dat de gegevensverwerking rond rechtshulp plaatsvindt op grond van artikel 8 Wpg. Het vergelijken van deze gegevens met die van de artikelen 9 en 10 is niet mogelijk, vanwege de beperking in de artikelen 8 en 11.

Vervaging scheidslijnen verwerkingsregime door geautomatiseerde verwerking

Een teamleider en een analist van een landelijke eenheid geven aan dat om netwerken in kaart te brengen, moet worden geput uit vele bestanden en systemen. Zowel binnen de politie als daarbuiten (bijvoorbeeld gemeenten, kamer van koophandel, RDW etc.). Doordat wordt geput uit verschillende bronnen en vanuit de analyse van netwerken gerichte verwerkingen kunnen voortvloeien, vinden zij het zeer moeilijk te bepalen binnen welk regime van de Wpg de verwerking uiteindelijk thuishoort.

Waar liggen de grenzen, mede door nieuwe technieken?

Analisten geven aan dat onduidelijk is of en zo ja in welke mate datawarehousing en geautomatiseerd vergelijken zijn toegestaan op grond van de Wpg. Dit geldt met name voor het gebruik van gegevens ouder dan 5 jaar (artikel 8) of gegevens die niet meer worden verwerkt (artikel 9, 10 e.v.). Toch kunnen die gegevens van belang zijn om bijvoorbeeld recidive-risico's bij (groepen) jongeren de onderzoeken of het bij het opstellen van profielen van overlastveroorzakers. Ze erkennen wel dat nieuwe technieken waarbij grote hoeveelheden data (kunnen) worden verwerkt nog in een experimentele fase zitten, maar juist daarom wordt voldoende 'speelruimte' nodig geacht om nieuwe (ondersteunende) onderzoekstechnieken te ontwikkelen.

5.7 Artikel 14: bewaartermijnen

Het omgaan met de bewaartermijnen wordt in brede kring als lastig ervaren. In verschillende organisaties (landelijk en territoriaal) vragen leidinggevenden, rechercheurs en analisten zich af of je überhaupt tot vernietiging zou moeten overgaan.

Knelpunten uit de audits

In 2011 voldeed volgens de audits 80% van de korpsen niet aan de bewaartermijnen voor artikel 8 gegevens. Zo ontbraken procesbeschrijvingen of instructies voor verwijdering en vernietiging en waren volgens de auditoren niet alle medewerkers zich voldoende bewust van de bewaartermijnen. Vernietiging van de gegevens vond nog niet plaats (was wettelijk

gezien ook nog niet aan de orde in 2011). Ruim 90% van de korpsen voldeed niet aan de bewaartermijnen voor artikel 9 gegevens.

Verwijdering en vernietiging van artikel 10 gegevens verliep in meer dan de helft van de organisaties wel volgens de norm. Voor wat betreft informantgegevens (artikel 12) voldeed in 2011 ruim 90% aan de norm van verwijderen en ruim 75% aan de norm van controleren en vernietigen.

Het beeld is in 2013 niet wezenlijk anders. Als belangrijke verklaring wordt het niet goed aansluiten van de ICT bij de Wpg genoemd. Zo bevat BVH niet alleen artikel 8 maar ook artikel 9 gegevens. Het systeem kan echter geen onderscheid maken in de status van gegevens.

Knelpunten uit de interviews

Bewaartermijnen veroordeelden

Een leidinggevende ziet een knelpunt bij veroordeelden die een langere straf uitzitten. Na de vrijlating zijn de antecenten mogelijk vernietigd. Die kunnen volgens hem van belang zijn als iemand zijn of haar criminele carrière weer oppakt. Bij vernietiging moet je dan je informatiepositie opnieuw gaan opbouwen. De suggestie is gedaan om bij veroordeling de bewaartermijn te verlengen met de periode dat iemand vast zit (en effectief pas begint te lopen als iemand weer vrij komt).

Informatie over netwerken

Ook het vernietigen van politiegegevens in dossiers over grootschalig onderzoek naar netwerken rond hennepteelt of (motor)bendes wordt als problematisch omschreven. Verschillende geïnterviewden geven aan dat veel specifieke en algemene kennis over netwerken verloren kan gaan. Een teamleider en analist relativeren het belang van langere bewaartermijnen voor het analyseren van netwerken. Je kijkt toch vooral naar wat er actueel gebeurt in een netwerk. Netwerken zijn fluïde dus informatie van meer dan twee tot drie jaar geleden is waarschijnlijk vaak verouderd.

Een privacyfunctionaris stelt daar tegenover dat dat erg afhangt van de aard van het netwerk. Als voorbeeld wordt genoemd een dadergroep met hechte familiebanden en vriendschappen. Zo'n netwerk, ook al zit de 'harde kern' bijvoorbeeld vast, kan lange tijd vrij stabiel zijn. Wat in elk geval van belang is, is het inzicht in hoe netwerken zich in algemene zin ontwikkelen, welke patronen zie je etc. Technisch en organisatorisch gezien is dat nog niet goed mogelijk (kost veel tijd), maar dat kan veranderen.

Discrepantie met Wjsg

Rechercheurs zien een discrepantie met het OM dat op basis van de Wet justitiële en strafvorderlijke gegevens strafdossiers twintig tot dertig jaar kan bewaren (art. 4 Wjsg) terwijl het onderzoeksdossier waarin de betreffende personen voorkomen, moet worden vernietigd zodra de rechterlijke uitspraak onherroepelijk is.

Beperking uitvoering dagelijkse politietaak door bewaartermijn van vijf jaar?

Een wijkagent wijst op het belang van het zicht houden op ontwikkelingen en eventuele risico´s in de buurten, wijken en dorpen waar de agent werkzaam is. Als voorbeeld wordt genoemd de verhuizing van iemand met een verleden in geweld, drugsscene etc. van gemeente A naar B. Eén zo'n persoon kan grote invloed hebben op hoe een groep (hang) jongeren in gemeente B zich ontwikkelt als hij met hen in contact komt. Als wijkagent wil je ook zicht hebben op iemands verleden. De basis voor crimineel gedrag wordt volgens hem vaak al gelegd rond het 12^{e}/13^{e} jaar.

Een ander voorbeeld dat hij geeft betreft de situatie dat er een melding binnenkomt van huiselijk geweld. In hoeverre is dan nog traceerbaar wat de historie is van de mogelijke verdachte van het geweld en of daar risico's aan zitten voor de surveillanten? Ook bijvoorbeeld de dossieropbouw kan bij huiselijk geweld belemmerd worden indien geen gegevens ouder dan vijf jaar gebruikt kunnen worden.

Een privacyfunctionaris vraagt zich in relatie tot het voorgaande af of de bewaartermijnen echt een knelpunt zijn. Het gaat erom dat je selectief bent in wat je (langer) wilt bewaren. Het is mogelijk gegevens om te zetten naar artikel 10 of 13 als je gegevens langer wilt bewaren, maar dat krijgt de politie niet goed georganiseerd. Knelpunt is dat een 'na-analyse' van informatie (wat is/lijkt van belang om te bewaren en wat niet?) veel tijd en ook specifieke deskundigheid vraagt. Die is er vaak niet.

Verjaringstermijn geen alternatief als maatstaf voor bewaartermijn

Koppeling van de bewaartermijn aan de verjaringstermijn is niet voor alle organisaties een optie. Een geïnterviewde geeft als voorbeeld een melding van de vermissing of mogelijke diefstal van een vuurwapen binnen de dienst. Dat is een schending van het dienstvoorschrift. Het feit verjaart na drie jaar. Maar wat als het betreffende wapen tien of vijftien jaar later opduikt in een moordzaak? Dan is volgens de geïnterviewde niet meer te traceren onder welke omstandigheden het wapen is zoekgeraakt.

Geen vernietiging maar gegevens achter slot en grendel?

In de praktijk worden er 'to be on the save side' kopieën gemaakt van de dossiers in BVH/BPS en BVO/RBS. Diverse geïnterviewden van politie, OM en KMar suggereren een

systeem waarin gegevens na een bepaalde periode achter slot en grendel komen en alleen nog mogen worden verwerkt na toestemming van bijvoorbeeld het OM of de rechter.

Daarbij wordt onder meer gewezen op het oplossen van cold-cases en witwasonderzoeken (waarbij herkomst van crimineel vermogen een belangrijk aandachtspunt is). Oude onderzoeken kunnen informatie bevatten over verklaringen van verdachten waaruit kan worden opgemaakt of mensen elkaar (al langer) kennen of niet. Door vernietiging is die informatie niet meer beschikbaar (en de OM-dossiers zijn vaak beperkter qua informatie). Bij cold-cases kan op het oog 'triviale' informatie (zoals verkeerovertredingen) aanwijzingen geven of een verdachte bijvoorbeeld in de buurt van het plaats delict was.

5.8 Ontwikkelingen digitalisering en ICT

Digitalisering werkveld en werkwijze politie

Diverse leidinggevenden en analisten wijzen op de veranderingen in de wereld als het gaat om ICT, netwerkvorming, internationalisering en de rol van social media. Dat geldt zowel voor de samenleving in het algemeen en het karakter van criminaliteit en de opsporing in het bijzonder. Daar is de Wpg volgens de geïnterviewden niet op berekend.

De afhankelijkheid van de politie van ICT en digitale analyses neemt volgens geïnterviewden alleen maar toe. Bijvoorbeeld als het gaat om de aanpak van hightech-criminaliteit, cyberaanvallen of phishing. Voor de bestrijding daarvan heb je specialisten nodig die de politie niet altijd zelf in huis heeft of kan hebben. Dat betekent dat je veel moet samenwerken met andere partijen waarmee informatie wordt gedeeld. Dat kan gaan om andere overheidsdiensten zoals als het NFI of de AIVD maar ook om marktpartijen zoals FOX IT. Inhoudelijk gaat dit om zeer grote datastromen en persoonsgegevens waarin naar patronen wordt gezocht.

In onderzoeken worden ook in toenemende mate grote digitale bestanden in beslag genomen, bijvoorbeeld in het kader van kinderporno of creditcardfraude. Deze bestanden kunnen relevante informatie bevatten over structuren, achterliggende netwerken of relaties naar andere criminele activiteiten. Analyse kost veel tijd en vereist de inzet van geavanceerde technieken en specialistische kennis. Probleem daarbij is dat het verwerkingsdoel vooraf vaak niet specifiek te beschrijven is. Daarnaast kan het onderzoek naar structuren en netwerken (veel) langer duren dan bijvoorbeeld het strafrechtelijk onderzoek naar een specifieke verdachte. Als die veroordeeld is, mogen de in beslag genomen bestanden dan nog worden verwerkt?

Efficiëntere verwerking beeldmateriaal?

Een rechercheur ziet knelpunten in de verwerking van onder meer beeldmateriaal. Bijvoorbeeld als er een overval is geweest. Er hangen op veel plekken camera's en het beeldmateriaal moet dan worden gevorderd en achteraf worden geanalyseerd. Dat wordt als een weinig efficiënt wijze van verwerken ervaren. Veel materiaal blijkt achteraf van slechte kwaliteit of maar ten dele relevant. In de huidige situatie mogen politiemensen niet zelf vragen om ter plekke het beeld materiaal te verwerken, dat wil zeggen bekijken en te beoordelen (dat mag alleen als dit bijvoorbeeld door de betreffende winkelier wordt aangeboden). In termen van verwerking en de uitvoering van politietaken is dat volgens betrokkenen niet efficiënt en effectief: in één werkproces zijn zowel het Sv als de Wpg van toepassing en dat is juridisch nu gescheiden. Als oplossing werd in één casus een 'preventief' rondje langs alle winkeliers in het centrum gemaakt. Daarbij werd de winkeliers gevraagd om bij een overval zelf het initiatief te nemen om de camerabeelden aan de politie aan te bieden. Dan hoeven volgens de geïnterviewden de opnames niet te worden gevorderd en kunnen die dan wel ter plekke worden verwerkt. De verwerking is volgens hen dan veel efficiënter.

5.9 Overige zaken

Rechtshulpverzoeken en internationale vormen van criminaliteit

De landelijke eenheid krijgt veel informatie vanuit het buitenland. De privacyfunctionaris geeft aan dat artikel 13 als grondslag wordt beschouwd voor het verwerken van deze informatie. Dit artikel kan formeel echter alleen worden toegepast als het gaat om politiegegevens die zijn verwerkt in het kader van artikel 8, 9 en 10. Artikel 11 Wpg biedt bovendien niet de mogelijkheid over te gaan tot geautomatiseerd vergelijken en in combinatie zoeken met artikel 13 gegevens.

Daarnaast worden de bewaartermijnen in relatie tot internationale vormen van criminaliteit als problematisch ervaren. Een voorbeeld is een onderzoek naar verdovende middelen na een rechtshulpverzoek van land A. Dat onderzoek leidt tot vervolging van een Nederlandse verdachte. Zes jaar na het onherroepelijk worden van het vonnis doet land B een rechtshulpverzoek. Daarbij worden onder meer de processen-verbaal opgevraagd van het Nederlandse onderzoek. Doordat gegevens waren vernietigd, kon niet aan het verzoek worden voldaan. Daardoor mist het opsporingsonderzoek in land B mogelijk relevante onderzoeksinformatie.

Een ander voorbeeld is oorlogsmisdaden. Er wordt vaak gestart met een breed oriënterend feitenonderzoek. Dat kan praktisch en juridisch gezien een langdurig proces zijn omdat er vaak meerdere rechtshulpverzoeken moeten worden gedaan. Het onderzoek zal zich

toespitsen op enkele personen maar een breder netwerk in beeld brengen. Als de strafzaak tegen de primaire verdachten is afgerond, moeten de gegevens worden verwijderd tenzij een nieuw onderzoek wordt gestart naar een andere verdachte. De (moeizaam) opgebouwde informatiepositie kan van belang zijn voor buitenlandse opsporingsinstanties. Door de verwijderings/vernietigingstermijnen gaan gegevens echter verloren.

Aanpak zware criminaliteit

Bij de aanpak van zware criminaliteit speelt het gebruik van oude onderzoeken vaak een belangrijke rol. Bijvoorbeeld bij een onderzoek naar de samenhang tussen een reeks van liquidaties over een langere periode, het terug rechercheren om te achterhalen of er criminele contacten bestaan/bestonden (en mensen die ontkennen elkaar te kennen, elkaar toch blijken te kennen), het in beeld brengen van opdrachtgevers achter bijvoorbeeld drugstransporten of een moord of het achterhalen van het motief voor een liquidatie. Het vernietigen van onderzoeksdossiers beperkt de informatiepositie.

5.10 Samenvattende bevindingen

Uit de audits en hercontrole is gebleken dat aan de eisen van de artikelen 8 en volgende van de Wpg nog niet voldaan wordt.

De geïnterviewden ervaren vooral knelpunten met betrekking tot het onderscheid tussen de artikelen 8 en 9 Wpg en de bewaartermijnen. Het onderscheid tussen genoemde artikelen wordt als niet praktisch en zinvol ervaren. De scheidslijn tussen beide soorten verwerkingen is niet altijd eenduidig te trekken en de status van politiegegevens kan veranderen. De systemen sluiten niet aan bij het gemaakte onderscheid.

De bewaartermijnen knellen volgens geïnterviewden. Opgebouwde informatieposities gaan verloren, het is moeilijk te bepalen wanneer termijnen gaan lopen en het handmatig moeten verwijderen van artikel 9 gegevens zorgt voor hoge administratieve lasten.

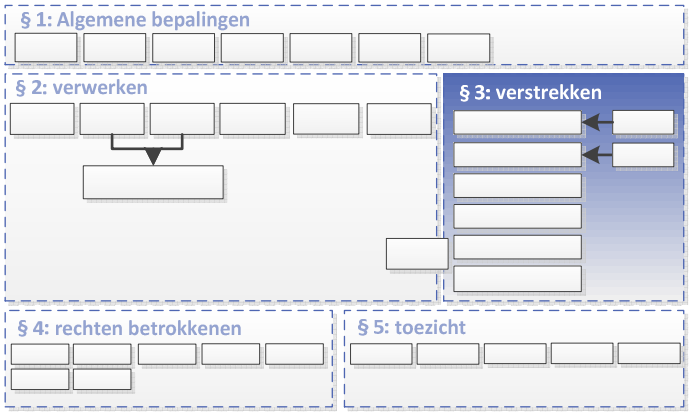
De Wpg is volgens geïnterviewden niet goed toegesneden op het verkrijgen van een strategische informatiepositie, data-warehousing, en nieuwe technieken en toepassingen. Het is moeilijk te bepalen op grond van welk artikel de verwerkingen plaatsvinden en vooraf is niet altijd een concreet doel te benoemen. Ook is de wet niet goed toegesneden op informatie die wordt verkregen vanuit het buitenland.

Ten aanzien van artikel 9 zijn de belangrijkste knelpunten dat het onderzoeksdoel niet altijd vooraf is aan te geven en dat niet altijd is aan te geven wanneer een doel is bereikt.

6 Verstrekking en ter beschikking stelling

6.1 Inleiding

Dit hoofdstuk gaat in op het verstrekken en ter beschikking stellen van politiegegevens. Als gegevens worden gedeeld binnen of tussen de politie, Kmar of BOD- en spreekt de Wpg van 'ter beschikking stellen' ('Free-flow-of-information'). Bij het doorgeven van gegevens aan bijvoorbeeld gemeenten (burgemeesters) of samenwerkingsverbanden (zoals RIEC's) spreekt de Wpg van 'verstrekken'. Het accent ligt in dit hoofdstuk op verstrekkingen. De wijze van verstrekking is in de Wpg vastgelegd in de artikelen 16 tot en met 24. In paragraaf 6.2 wordt kort samengevat wat het landelijke beeld is rond verstrekkingen op basis van de audits. Vervolgens gaan we in op het beeld vanuit de interviews:



- De mate waarin het mogen verstrekken helder is (paragraaf 6.3)
- De knelpunten bij verstrekkingen in samenwerkingsverbanden (paragraaf 6.4)
- De risico's van verstrekkingen die worden gezien (paragraaf 6.5)
- Verstrekkingen en social media (paragraaf 6.6)
- Ter beschikking stelling (paragraaf 6.7)
- Overige knelpunten (paragraaf 6.8)

We sluiten af met de samenvattende bevindingen (paragraaf 6.8).

6.2 Beeld uit de audits

In de audits van eind 2011 is beoordeeld in hoeverre de korpsen voldoen aan de vereisten in paragraaf 3 van de Wpg. Meer specifiek is gekeken naar de mate waarin korpsen een verstrekkingenwijzer[108] hanteren, of op een juiste wijze met convenanten inzake informatie-uitwisseling wordt omgegaan en hoe wordt omgegaan met geautomatiseerde verstrekking. Het beeld was samengevat als volgt.

De landelijke verstrekkingenwijzer was bij 85% van de korpsen ingevoerd. Afwijkingen waren vooral het niet bekend zijn met de wijzer. Naast de landelijke verstrekkingenwijzer is

[108] Een handreiking voor de medewerkers waarin is aangegeven aan wie welke gegevens met wel doel mogen worden verstrekt, opgesteld in het kader van het Project implementatie Wpg, 2009.

in de audits ook gekeken of een regionaal verstrekkingenschema was opgesteld en werd gehanteerd. Bijna 40% bleek daar niet aan te voldoen. Vaak ontbrak het schema of was niet duidelijk wie wat aan wie verstrekt[109]. In de landelijke rapportage hercontrole Wpg is aangegeven dat inmiddels is voldaan aan dit onderdeel[110].

Ruim 60% van de korpsen voldeed in 2011 niet aan de regels over convenanten. In de meeste gevallen waren de processen wel omschreven, maar bleken niet alle bestaande convenanten getoetst te zijn aan de Wpg. In sommige gevallen was er geen borging op de naleving van het proces en geen sturing op de noodzaak en inhoud van de convenanten. Ook was soms onduidelijk hoe intern werd omgegaan met verstrekkingen op basis van convenanten. Wat betreft het proces voor artikel 20 besluiten bleek ruim 65% wel te voldoen aan de norm. In de gevallen dat men niet voldeed, bleek dat niet altijd getoetst werd aan de doeleinden geformuleerd in art. 20 Wpg, een enkeling had geen gedocumenteerd proces hiervoor en er was soms geen borging op naleving van het proces. Bij de hercontrole is aangegeven dat het proces van convenanten en artikel 20 besluiten begin 2013 goed is opgezet en dat de eenheden bezig zijn met de implementatie daarvan.

Op het gebied van geautomatiseerde verstrekkingen bleek meer dan de helft van de korpsen niet te voldoen aan de norm. De reden hiervoor was met name het feit dat het proces niet omschreven was of dat niet goed inzichtelijk was welke gegevens automatisch werden verstrekt, waardoor periodieke controle niet mogelijk is. Ook was deze verstrekking in een aantal gevallen overgelaten aan het OM, waardoor toetsing aan de kwaliteitsaspecten vooraf niet mogelijk was. Overigens bleken de korpsen niet altijd gebruik te maken van deze vorm van verstrekking. In de rapportage hercontrole Wpg is aangegeven dat het proces van geautomatiseerde verstrekking landelijk is gerealiseerd en dat een (latere) audit daarvan hierover uitsluitsel moet geven.

6.3 Mag ik verstrekken?

Geïnterviewden geven aan dat het voor mensen op de werkvloer vaak moeilijk is om af te wegen of informatie verstrekt mag worden of niet.

Basishouding: als er een convenant is, mag het (waarschijnlijk)

Om op zeker te spelen was en is er een neiging om niet te verstrekken als er geen convenant is afgesloten met een samenwerkingspartij. Bij twijfel geldt volgens een geïnterviewde vaak het ‘better safe then sorry’-principe. Het wordt echter niet uitgesloten dat bij de mondelinge verstrekkingen medewerkers zich weinig gelegen laten aan de Wpg. Het hangt erg van de persoon af. Het heeft volgens geïnterviewden ook veel te maken met

[109] DAD audits, 2012.
[110] Landelijke rapportage hercontrole Wpg, 2013.

kennis en op zijn minst het gevoel dat het mag. Een convenant heeft wat dat laatste betreft ook een duidelijke functie, maar kan volgens enkele geïnterviewden ook tot de gedachte leiden dat bij een convenant je alles mag verstrekken. Blijkbaar is er onduidelijkheid of onvoldoende kennis over de condities waaronder wat aan wie mag worden verstrekt en wordt het convenant gezien als het instrument om die duidelijkheid te bieden.

Ook onzekerheid binnen gestructureerd samenwerkingsoverleg

Maar er is ook onzekerheid of verstrekt mag worden binnen een meer gestructureerd samenwerkingsoverleg. Di speelt niet zozeer bij specifieke functionarissen maar bij meerdere partners. Een voorbeeld is de verkennende fase met mondeling overleg in RIEC-verband (Regionaal Informatie en Expertise Centrum), of andere samenwerkingsverbanden, voordat een formeel onderzoek wordt gestart. Waar liggen de grenzen op het moment dat je met elkaar aan het verkennen bent of één of meerdere personen mogelijk als verdachten moeten worden aangemerkt? Soms wordt een blok/buurt of straat doorgelicht om daar zicht op te krijgen. Of de gemeente komt met signalen van burgers over een bepaalde persoon. Je moet volgens de geïnterviewden dan in voldoende heldere taal met elkaar van gedachte kunnen wisselen en op basis daarvan bijvoorbeeld beslissen of iemand als verdachte wordt aangemerkt. In de praktijk zien geïnterviewden vaak nog terughoudendheid en de neiging om in bedekte termen te spreken (‘subject A’). Dat maakt het volgens hen moeilijk om tot een goede analyse te komen[111].

Bewustzijn, professionaliteit en vertrouwensrelatie cruciaal

Volgens de geïnterviewden is het convenant vooral een algemeen kader en geen harde instructie. Dat kan ook niet, omdat in elke situatie een nieuwe inschatting moet worden gemaakt. Het genoemde bewustzijn en de professionaliteit zijn dan ook net zo belangrijk als het convenant.

Dat betekent dat bij verstrekkingen, zeker als het gaat om de dagelijkse politietaken, volgens een leidinggevende de vraag altijd is ‘waarvoor heeft de partner de gevraagde informatie nodig, wat weet hij of zij zelf al of wat had hij of zij (op andere wijze) kunnen weten en welke informatie kan de politie daarbij nog invullen’. Daarbij is onder meer getraind aan de hand van praktijkvoorbeelden.

Een informatiemanager en wijkagent in één case geven daarbij aan dat je in de praktijk ook wel móet delen omdat je in toenemende mate gezamenlijk optrekt met partners. Bijvoorbeeld als het gaat om (ontspoorde) jongeren. Dat kan alleen als er ook een zekere

[111] Zie ook eerdere opmerkingen: dit staat los van de vraag of de Wpg ook feitelijk beperkingen oplegt aan de mogelijkheden van verstrekken. De kennis en interpretatie van de wet spelen hierbij een rol. Zie ook hoofdstuk 10.

vertrouwensrelatie is. Het goed daarmee omgaan moet een deel van de professionaliteit van de medewerker zijn.

Een voorbeeld hiervan is de samenwerking tussen KMar en Douane. Dat gebeurt nu in zogenaamde flex-teams. Dat betekent bijvoorbeeld dat ze ook samen op pad gaan en bij elkaar in de auto zitten. Daarbij is het onvermijdelijk dat de douanier bepaalde informatie meekrijgt. Dat geldt ook tijdens het werkoverleg waar een douanier aanwezig is. Het is niet werkbaar om in die situaties telkens een stop te maken of te verzoeken de kamer te verlaten. Vertrouwelijkheid, professionaliteit en geheimhoudingsplicht moeten dan de informationele privacy borgen.

6.4 Verstrekking in het kader van samenwerkingsverbanden

Knelpunten bij de verstrekking van politiegegevens worden verder met name ervaren in samenwerkingsverbanden. Te denken valt aan het Veiligheidshuis en het RIEC. De samenwerking kan een zeer breed palet van partners bestrijken. Behalve gemeenten en het OM gaat het bijvoorbeeld om woningcorporaties, de belastingdienst, Centrum voor Jeugd en Gezin (CJG), Bureau Jeugdzorg (BJZ), Consultatiebureau, Welzijnsorganisaties, Leerplichtambtenaren, Scholen, Schuldhulpverlening en GGD. De belangrijkste knelpunten zijn volgens de geïnterviewden onduidelijkheid over wanneer verstrekken begint, wat je mag verstrekken, de soms tegenstrijdige wettelijke kaders, de plaats en positie van convenanten en hoe het staat met de informationele privacy nadat verstrekt is.

Welke informatie mag je en welke zou je moeten delen in RIEC-verband?

Een specifiek knelpunt met betrekking tot de RIEC's vormde artikel 4:5 Bpg. Op grond van het eerste lid van dit artikel worden geen artikel 9- of 10-gegevens ten behoeve van een samenwerkingsverband verstrekt, behoudens indien dringend noodzakelijk voor een goede uitvoering van de politietaak. Deze uitzondering wordt in de nota van toelichting beperkt uitgelegd. Deze gegevens zijn echter ook van belang voor de geïntegreerde aanpak van georganiseerde criminaliteit. Om dit knelpunt op te lossen heeft de minister van Veiligheid en Justitie recent een besluit genomen op grond van artikel 18, tweede lid, Wpg (het Wpg-machtigingsbesluit RIEC's/werkproces integrale casusanalyse).

Verschillende en soms strijdige verstrekkingsregimes

In de praktijk lopen politie, KMar en OM tegen een aantal knelpunten aan die te maken hebben met tegenstrijdigheden in wettelijke kaders, onduidelijkheid over welk wettelijke regime van toepassing is en het werken met convenanten. In hoofdstuk 9 wordt dieper ingegaan op de relatie met andere wetgeving. Kort samengevat komen uit de interviews de volgende knelpunten voren bij de uitvoering van politietaken:

- Informatie die door partner A wordt verwerkt maar niet meer relevant is voor hem, kan nog wel relevant zijn voor partner B, maar mag of kan niet meer altijd worden verstrekt.
- Het kunnen verstrekken van gegevens aan de ene partner, betekent niet dat de andere partner de gegevens ook mag ontvangen.
- Het niet hoeven of mogen verstrekken en het moeten verstrekken op basis van andere wetgeving (zoals de Zorgverzekeringswet)
- Als informatie wordt uitgewisseld en gedeeld, of gezamenlijk een gegevensbestand wordt opgebouwd is niet altijd duidelijk wie op basis van welke wetgeving verantwoordelijk is.

Stapeling van convenanten

Als knelpunt is ook genoemd dat sommige structurele samenwerkingspartners niet in de Wpg en het Bpg als zodanig zijn benoemd. Dat betekent dat steeds aparte convenanten moeten worden afgesloten. De geïnterviewden van één van de organisaties spreken over in het kader van de Wpg meer dan honderd afgesloten convenanten, deels met dezelfde samenwerkingspartners maar voor andere doelen van de gegevensverstrekking. Als voorbeeld is onder meer genoemd de GGD, waarmee voor elk doel waarvoor samengewerkt wordt een convenant moet worden afgesloten. Het opstellen en toetsen van convenanten legt een zwaar beslag op de juridische capaciteit bij de politie. Het is voor medewerkers ook moeilijk te overzien welke gegevens aan welke partners rond welke thema's mag worden verstrekt. De geïnterviewden zien dus niet zozeer een juridisch obstakel in de Wpg voor het afsluiten van convenanten, maar wel knelpunten in de beheersbaarheid van het werken met convenanten zoals mogelijk gemaakt door de Wpg.

Een leidinggevende suggereert om landelijk thema's aan te wijzen waarbij wordt aangegeven welke informatie met wie mag worden gedeeld. Dat is bijvoorbeeld al gebeurd met mensenhandel en terrorisme. Dat zou volgens hem veel breder kunnen. Dan voorkom je een wirwar van convenanten en borg je enige uniformiteit. Vanwege de flexibiliteit zou dit volgens hem echter niet in de Wpg zelf moeten worden vastgelegd maar bijvoorbeeld via een aanwijzing moeten worden geregeld.

6.5 Risico's van verstrekking

In de gesprekken is ook een aantal uiteenlopende risico's van verstrekkingen genoemd.

Wie gaat verstrekte gegevens gebruiken?

Een privacyfunctionaris aanschouwt de uitwisseling in RIEC-verband met enige verwondering. Het palet van partners is sterk gestegen. Daarbij ontbreekt het zicht erop wat er precies met verstrekte gegevens gebeurt en wie deze gegevens feitelijk verder

verwerkt. Ook een privacyfunctionaris van de KMar ziet hier een knelpunt, bijvoorbeeld bij de verstrekking van gegevens aan de IND. Dat gebeurt in de regel via een algemene mailbox bij de IND. De KMar heeft echter geen zicht op wie is geautoriseerd voor die mailbox. Zijn dat bijvoorbeeld ook administratieve ondersteuners of systeem/applicatiebeheerders? Vanuit de BOD-en bestaat ook enige aarzeling bij het breed verstrekken van politiegegevens. Met name richting partners die geen toezichthoudende of handhavende taken hebben.

Shoppen naar informatie?

Verschillende geïnterviewden geven aan dat de advocatuur ook in de gaten krijgt dat er meer wordt gedeeld. Dat betekent dat dezelfde informatie op meerdere plekken aanwezig kan zijn, bijvoorbeeld bij het OM (strafdossier), politie (onderzoeksdossier) en gemeente (bestuurlijke rapportage) én gehaald kan worden. Het is ook voor de geïnterviewden niet duidelijk of daar in voldoende mate eenzelfde beleidslijn wordt gehanteerd[112].

Veiligheid van degene over wie gegevens worden verstrekt?

Binnen de EU geldt vrije uitwisseling en de verplichting tot verstrekken aan opsporingsinstanties in andere lidstaten. In wat er precies wordt verstrekt is wel enige ruimte. Dat kan volgens rechercheurs bijvoorbeeld van belang zijn als er twijfels zijn over de mogelijke gevolgen voor de persoon waar het om gaat. Of als er een risico van een 'lek' is bij buitenlandse opsporingsinstanties richting criminele organisaties. Voor landen buiten de EU geldt dat er een verdrag moet zijn. Ook beleidsmatig kan de uitwisseling volgens geïnterviewden dan soms wat gecompliceerder zijn. Bijvoorbeeld bij landen die de doodstraf kennen. Dan kijkt het ministerie van Veiligheid en Justitie mee bij de afweging wat wordt verstrekt[113]. Geïnterviewden vragen zich wel af hoe informatie die via een rechtshulpverzoek is verkregen en hoe verstrekte informatie wordt gebruikt. Is er bijvoorbeeld een risico van verhoormethoden die in Nederland strafbaar zijn of een risico van marteling? Onduidelijk is in hoeverre buitenlandse opsporingsinstanties gegevens die Nederland heeft verstrekt, weer doorverstrekken[114].

6.6 Verstrekkingen en social media

Verstrekken wordt volgens een wijkagent in de Wpg vooral geassocieerd met klassieke communicatiekanalen: mondeling, schriftelijk of via de email. Met de komst van social media zie je de grenzen verschuiven. Mensen zetten veel op internet. Ook de

[112] Daar staat tegenover dat geen van de geïnterviewden een concrete zaak heeft meegemaakt waar de Wpg in een strafzaak de hefboom was om (een deel van) het procesdossier van tafel te krijgen. In meerdere gesprekken is wel aangegeven dat het signaal dat de advocatuur belangstellend is wat betreft de privacywetgeving, rechercheurs en blauw bewuster heeft gemaakt van het politie-belang van privacy.

[113] Op basis van art. 552k t/m m Sv.

[114] Strikt genomen vallen rechtshulpverzoeken buiten het bestek van de Wpg. Geïnterviewden ervaren hier echter wel een knelpunt vanuit de doelstellingen van de Wpg: waarborgen van de privacy/persoonlijke levenssfeer, lichamelijke integriteit etc.; Ook als relativering van de aandacht voor kleinere administratieve schendingen van de Wpg versus informatie die mogelijk is verkregen door of wordt gebruikt voor schending van mensenrechten.

omloopsnelheid van informatie is enorm toegenomen. Volgens de wijkagent is de maatschappelijke informatiepositie van de politie daarmee veranderd: je hebt niet meer het monopolie over bepaalde informatie én over het moment dat informatie publiekelijk wordt gemaakt. Als voorbeeld noemt hij de identiteit van een slachtoffer van een verkeersongeval of zelfdoding. Het komt voor dat ouders eerder via de social media vernemen wat hun kind is overkomen dan dat de politie dit kan melden. Dat betekent dat de dynamiek rond verstrekken verandert (snelheid, foute berichtgeving media corrigeren, etc.).

De vraag is dan ook: waar liggen de grenzen van informationele privacy(schendingen)? De politie is op dit moment zoekende. En dat gaat wel eens fout. De wijkagent geeft als voorbeeld het innemen van een rijbewijs van een chauffeur die 140 km/u reed op een weg waar 50 km/u is toegestaan. Het ging om een berucht stuk weg waar al veel (bijna) ongelukken zijn gebeurd. De aanhouding werd getwitterd om een signaal af te geven: "we proberen bij te dragen aan uw veiligheid". In de tweet werd echter ook de Poolse afkomst van de chauffeur gemeld. Daarover ontstond discussie. Volgens de wijkagent had achteraf gezien de afkomst van de chauffeur niet vermeld mogen worden. Het betekent dat je als politie niet alleen goed voor ogen moet houden wat het doel is van een verstrekking maar ook wat het mogelijke (onbedoelde) effect daarvan kan zijn. De betreffende wijkagent realiseert zich ook dat als de politie iets twittert, de impact daarvan groter kan zijn als wanneer een willekeurige burger hetzelfde bericht de wereld instuurt.

6.7 Ter beschikking stellen

Volgens artikel 15 Wpg stelt de verantwoordelijke politiegegevens ter beschikking aan personen die door hemzelf dan wel door een andere verantwoordelijke overeenkomstig artikel 6, tweede lid, zijn geautoriseerd voor de verwerking van politiegegevens, voor zover zij deze behoeven voor de uitvoering van hun taak. Van belang hierbij is dat met de vorming van de Nationale politie sprake is van één organisatie en één verantwoordelijke. Zoals in paragraaf 4.4 al is aangegeven is volgens sommige gesprekspartners door de wijze van autoriseren geen sprake van een 'free flow of information'. Gesprekspartners geven aan dat de technische mogelijkheden om gegevens uit te wisselen nog beperkt zijn zolang er geen sprake is van één landelijk (samenhangend) ICT-systeem. Het is niet zo dat medewerkers van verschillende eenheden of bij de KMar of BOD-en geautoriseerd zijn tot toegang in elkaars systemen.

6.8 Overige zaken

Signalerende rol en verstrekkingen?

De politie heeft ook een signalerende functie. Bijvoorbeeld in de persoon van een wijkagent richting hulpverleningsinstanties (over vereenzaming, verwaarlozing, potentieel huishoudelijk geweld). Maar ook richting scholen als het gaat om het vroeg signaleren van

een risico van ontsporen van leerlingen. Een wijkagent noemt als voorbeeld kinderen die op de basisschool gedragsproblemen vertonen en bijvoorbeeld gewelddadig zijn richting klasgenootjes of vernielingen aanrichten. Dat krijgt volgens hem op de basisschool vaak wel aandacht, maar het gaat meestal pas echt mis op de middelbare school. Hij vraagt zich af hoe ver kun je gaan als politie daar ook middelbare scholen in te kennen zodat zij daar naar kunnen handelen?

Een ander voorbeeld dat een wijkagent noemt: een school stelt vast dat een kind steeds meer leerproblemen heeft. Gesprekken met kind en ouders geven geen specifiek uitsluitsel (tijdelijke dip? puberen?) en er wordt gekozen voor bijles om de leerling bij te spijkeren. Maar wat als je als schooldirecteur weet dat de moeder van de betreffende leerling regelmatig slachtoffer is van huiselijk geweld? Zou je dan anders omgaan met zo'n leerling? Mag je als politie die informatie delen?

Rechtsbescherming politiemedewerker

Een ander aandachtspunt is de rechtsbescherming van bijvoorbeeld een agent die (mondeling) informatie deelt met hulpverleners over iemand die overlast veroorzaakt en (vermoedelijk) kampt met psychische problemen. Als degene waarover informatie wordt gedeeld – of diens familie - daarover klaagt kan een disciplinaire straf volgen. Dit kan leiden tot terughoudendheid in verstrekkingen waar het delen van informatie juist wel in het belang kan zijn van de betrokkene en/of zijn omgeving[115].

Is verstrekking effectief?

Een privacyfunctionaris vraagt zich af of algemene verstrekkingen wel effectief zijn. Zowel in preventieve zin (kun je op basis daarvan beter barrières opwerpen tegen georganiseerde criminaliteit?) als in repressieve zin (helpt het om bijvoorbeeld jeugdbendes beter aan te pakken?). De effectiviteit van verstrekkingen zou volgens de betreffende privacyfunctionaris een graadmeter moeten zijn voor je verstrekkingenregime.

6.9 Samenvattende bevindingen

Eind 2011 hadden de korpsen in algemene zin een verstrekkingenwijzer ingevoerd om invulling te geven aan de open normen van de Wpg, maar de meeste korpsen hadden die nog niet vertaald naar de eigen organisatie. Aan de eisen die aan convenanten worden gesteld, werd door een groot deel van de korpsen niet voldaan evenals aan de eisen van geautomatiseerd verstrekken.

[115] Het gaat weliswaar niet om een knelpunt in de Wpg zelf maar een ander knelpunt dat gevolgen heeft voor het gedrag dat de Wpg beoogt, namelijk het delen van informatie.

In de dagelijkse praktijk is het voor politiemedewerkers nog vaak onduidelijk of en zo ja wat ze mogen verstrekken. Het hebben afgesloten van een convenant is daarbij meestal het ijkpunt. Uit de interviews komt naar voren dat een combinatie van voldoende bewustzijn van het privacy-aspect bij de uitvoering van politietaken, het professionele vermogen om een eigen afweging te kunnen maken binnen de kaders van bijvoorbeeld een convenant en een vertrouwensrelatie met degene aan wie wordt verstrekt, belangrijke succesfactoren zijn.

De verstrekking van politiegegevens in samenwerkingsverbanden is in zekere zin nog een zoektocht. Het wordt in de praktijk niet altijd helder gevonden wanneer je wat mag verstrekken en wanneer verstrekken begint. Zodra een onderzoek is gestart, is dat voor de meesten wel helder, maar de verkenningsfase daarvoor is nog erg aftasten. Aan de ene kant willen politie en OM redelijk open met de partners van gedachten kunnen wisselen over de vraag of een onderzoek moet worden opgestart. Een specifiek knelpunt wordt ervaren bij het verstrekken van artikel 9 en 10-gegevens in relatie tot de aanpak van georganiseerde criminaliteit. De wettelijke marges lijken daar beperkter dan voor de aanpak nodig is.

Juridisch wordt het vooral als een knelpunt ervaren dat de verschillende wettelijke kaders deels tegenstrijdig zijn en dat niet altijd helder is welk wettelijk kader van toepassing is op bijvoorbeeld gezamenlijk aangelegd bestanden. De constructie van convenanten wordt enerzijds noodzakelijk geacht maar ook ondoorzichtig.

Voorts is er enige zorg over de borging van de informationele privacy zodra gegevens zijn verstrekt. Het is niet altijd duidelijk wie bijvoorbeeld geautoriseerd is om verstrekte gegevens te verwerken. Bij verstrekkingen in internationaal verband komt daarbij dat er soms ook risico’s zijn in relatie tot de veiligheid van degene waarvan gegevens zijn verstrekt en het onrechtmatig doorverstrekken.

Er vinden ook in toenemende mate verstrekkingen plaats aan private partijen. Bijvoorbeeld advocaten, makelaars en verzekeraars. Dat geeft aan dat het speelveld van strekkingen steeds breder wordt. Daarbij loopt de politie soms ook weer tegen tegenstrijdigheid in wetgeving aan (niet mogen of hoeven verstrekken volgens de Wpg, moeten verstrekken volgens andere wetgeving).

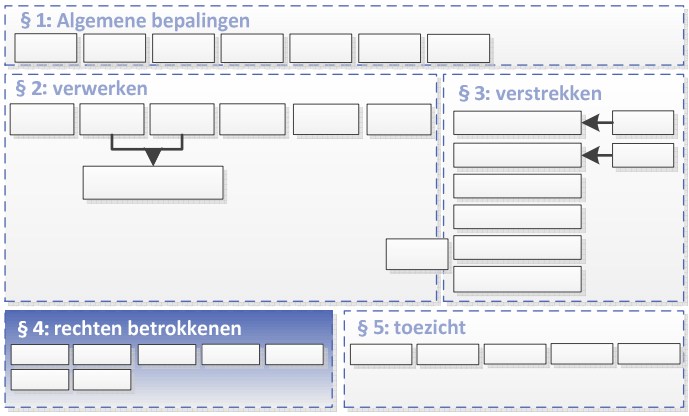
De opkomst van social media en het nog steeds toenemende internetgebruik heeft ook gevolgen voor de informatiepositie van de politie en verstrekkingen. Hoe die (kunnen) uitpakken is nog niet duidelijk. Het verstrekken van politiegegevens bijvoorbeeld via

Twitter levert zowel positieve als negatieve ervaringen op. De politie is op dat punt zoekende.

In de interviews wordt als een belangrijk knelpunt genoemd de administratieve last die verstrekkingen met zich mee brengen. Dit geldt met name voor de (toenemende) mondelinge verstrekkingen in het kader van de samenwerking. Protocollering daarvan gebeurt dan ook maar beperkt.

7 Kennisneming

7.1 Inleiding



In dit hoofdstuk wordt de uitvoeringspraktijk geschetst rond de rechten van betrokkenen[116]. De betrokkene kan een kennisnemingsverzoek over de eigen gegevens indienen en eventueel verzoeken tot verbetering, aanvulling of afscherming (markeren van gegevens om doel van verwerking te beperken) van de gegevens. Het recht op kennisneming en correctie is beperkter dan dat van de Wbp, vanwege het bijzondere karakter van politiegegevens.[117]

7.2 Algemene context

Een verzoek tot kennisneming moet schriftelijk worden ingediend. De website van de politie is hier summier over. Het accent ligt op informatie over het indienen van een Wob-verzoek.[118] Het CBP heeft op de website www.mijnprivacy.nl een voorbeeldbrief gepubliceerd voor een kennisnemingsverzoek. Eveneens is een voorbeeldbrief voor een verzoek tot verbetering, aanvulling, verwijdering of afscherming van gegevens beschikbaar.[119] Flitsfoto's kunnen via de website www.mijnpolitie.nl worden opgevraagd.

Ten tijde van het opstellen van de Wpg bestond geen duidelijk inzicht in de uitoefening van het recht op kennisneming (aard en complexiteit van de verzoeken en de werkbelasting die daar voor de politie uit voortvloeit). Wel werd in de Memorie van Toelichting opgemerkt dat het aantal verzoeken aanzienlijk was gestegen.[120]

Gegevens over het aantal verzoeken om kennisneming en correctie zijn te achterhalen via de jaarverslagen van privacyfunctionarissen. Aan de privacyfunctionaris is door de wetgever een rol toegedacht bij het recht op kennisneming en correctie van politiegegevens.[121] Omdat de jaarverslagen niet openbaar toegankelijk zijn gemaakt, niet altijd aan de verslagplicht wordt voldaan en onduidelijk is of altijd informatie is opgenomen

[116] Art. 25 t/m 31 Wpg.
[117] MvT, p. 3,
[118] http://www.politie.nl/onderwerpen/wet-openbaarheid-van-bestuur.html.
[119] http://www.mijnprivacy.nl/Voorbeeldbrieven/Pages/Voorbeeldbrieven.aspx
[120] MvT, p. 83.
[121] MvT, p. 91. Op welke wijze precies invulling aan die rol zou moeten worden gegeven, is niet aangegeven.

over de uitoefening van de rechten van betrokkenen, zijn gegevens over de totale aantallen kennisnemingsverzoeken etc. onbekend.

Tegen een besluit op een verzoek om kennisneming of correctie kan beroep bij de rechter worden ingesteld. Voorafgaand daaraan kan het CBP worden gevraagd te bemiddelen. Een rechter kan het CBP eveneens om advies vragen. Het percentage gevallen waarin tegen een besluit op een verzoek om kennisneming/correctie beroep is ingesteld is onbekend.

In het jaarverslag van het CBP over 2011 is aangegeven dat in 2011 96 bemiddelingsverzoeken zijn ontvangen. Het betreft hier zowel verzoeken op grond van de Wpg als de Wbp. Hoeveel verzoeken op de Wpg betrekking hadden is niet exact aan te geven. In 2010 waren er 154 bemiddelingsverzoeken en in 2009 189. Er lijkt dus sprake van een daling van het aantal bemiddelingsverzoeken. De reden daarvoor is niet duidelijk. Het merendeel van de verzoeken is niet ingewilligd; belanghebbenden zijn in die gevallen doorverwezen naar andere instanties.[122] Hoeveel verzoeken wel zijn ingewilligd, is onduidelijk. In het jaarverslag 2012 is eveneens aangegeven dat het merendeel van de verzoeken om bemiddeling is afgewezen. Cijfers zijn in dit verslag niet opgenomen.[123]

Rechten betrokkenen moeilijk te effectueren

In de literatuur wordt door sommigen aangegeven dat het recht op kennisneming bijna geen waarborgen biedt. "Op dit moment is het zo dat de eerste de beste boze buurman via de Stichting M (Meld Misdaad Anoniem) of via een tip aan de CIE eraan kan bijdragen dat aantekening wordt gemaakt van een verdenking van kindermisbruik of hennepkweek of terrorisme. Zelfs als zulks onjuist blijkt, is niet gezegd dat deze aantekeningen worden verwijderd".124 Buruma haalt jurisprudentie aan waarbij na vrijspraken van ontucht, stalking en openlijke geweldpleging pas na een uitspraak van de rechter werd overgegaan tot verwijdering van de politiegegevens.125

7.3 Knelpunten uit de audits

Ruim 75% van de korpsen had ten tijde van de audits een procesbeschrijving, werkinstructie, stroomschema e.d. voor het afhandelen van verzoeken om kennisneming. Geconstateerd werd dat in een aantal gevallen verzoeken niet binnen de gestelde termijn werden afgehandeld. Daarnaast is in de audits aangegeven dat het afhandelen van kennisnemingsverzoeken door de privacyfunctionaris, zoals dit bij sommige korpsen plaatsvond, niet wenselijk is gelet op de toezichthoudende rol van de privacyfunctionaris. In gevallen waarin de privacyfunctionarissen alleen de complexe verzoeken afhandelden, was dat volgens de auditors wel in overeenstemming met de Wpg.

Bij de afhandeling van correctieverzoeken werden bij meer dan de helft van de korpsen tekortkomingen geconstateerd. Niet alle korpsen hadden een procesbeschrijving waarin

[122] Jaarverslag 2011 Cbp, p. 45.
[123] Jaarverslag 2012 Cbp, p. 43.
[124] Buruma 2010 Delikt en Delinkwent, Opvragen, bewerken en kennisnemen van gegevens voor de opsporing (DD 2010, 57).
[125] Idem.

was bepaald hoe correctieverzoeken moesten worden afgedaan. Ook was soms wel een procesbeschrijving aanwezig, maar ontbrak daarin hoe derden (organisaties aan wie de informatie verstrekt was) van de correctie op de hoogte zouden worden gesteld. Overigens kwamen correctieverzoeken in de praktijk niet veel voor[126].

Uit de rapportage over de hercontrole in 2013 blijkt dat inmiddels een landelijke werkwijze is opgesteld. Deze werkwijze was bij twee eenheden nog niet vastgesteld en geïmplementeerd. Uit de hercontrole bleek dat een aantal eenheden de procedure voor afhandeling van correctieverzoeken nog niet goed had geïmplementeerd en dat nog niet in alle eenheden conform de landelijke procedure werd gewerkt.[127]

7.4 Knelpunten uit de interviews

Het algemene beeld van de geïnterviewden van politie en KMar is dat zich bij de afwikkeling van verzoeken om kennisnemingen geen grote knelpunten voordoen. Het aantal verzoeken om kennisnemingen varieert van enkele tientallen (KMar, eenheid Limburg) tot honderden (landelijke eenheid). 70 tot 80% van de verzoeken wordt (bij de organisaties die zijn geïnterviewd) ontvankelijk verklaard. De geïnterviewden geven aan dat dit zeer incidenteel leidt tot een verzoek tot correctie van gegevens. Bij de landelijke eenheid betrof in 2012 ruim 10% een verzoek tot verwijdering van gegevens (waarvan ongeveer de helft is ingewilligd). In een klein aantal gevallen wordt beroep ingesteld tegen een weigering tot kennisneming, correctie of verwijdering. Dit kunnen langlopende zaken zijn.

Verzoeken om kennisnemingen Kmar

In 2012 zijn 28 verzoeken om kennisneming ingediend, waarvan 22 ingewilligd. Er zijn twee correctieverzoeken ingediend, die beide zijn ingewilligd. Er is tweemaal beroep ingesteld bij de rechter. In 2011 waren bij de Kmar nog 50 verzoeken om kennisneming ingediend. Een klein deel daarvan heeft verzocht om correctie, waarbij in een nog kleiner percentage van de gevallen aanleiding was om tot aanpassing of verwijdering over te gaan. In 2011 is bij de Kmar één verzoek om bemiddeling bij het CBP ingediend. Dat verzoek is afgewezen, waarna beroep bij de rechtbank aanhangig is gemaakt.

Verzoeken om kennisnemingen Dienst Landelijke Informatie Organisatie

Bij de dienst Landelijke Informatie Organisatie zijn in 2012 meer dan 300 verzoeken om kennisneming en verwijdering ontvangen. Van de 43 verzoeken tot verwijdering zijn er in ieder geval 19 ingewilligd.[128] De privacyfunctionaris van de LIO: "In al de jaren (ruim 17) dat ik mij bezig houd met behandelen van verzoeken, heb ik nog nooit een verzoek om correctie ontvangen."

Verzoeken om kennisnemingen politie Limburg

De politie Limburg heeft over de periode 2010-2012 gemiddeld circa 20 verzoeken om kennisneming per jaar ontvangen. Daarbij wordt in enkele gevallen per jaar een verzoek om correctie ingediend.

[126] DAD audits, 2012.
[127] Landelijke rapportage hercontrole Wpg, 2013.
[128] In ieder geval 19 verzoeken zijn ingewilligd. Het aantal kan hoger zijn volgens de privacyfunctionaris. Hij ontvangt niet altijd gegevens over de afhandeling van de verzoeken.

De Nationale Ombudsman geeft aan jaarlijks enkele (tientallen) klachten te ontvangen over verzoeken tot kennisneming. Meestal gaan deze over de wijze van kennisgeving (wordt kopie gegevens verstrekt? Wordt alleen mondeling informatie verstrekt? Mag betrokkene gegevens alleen inzien maar geen kopie maken?) of de onjuistheid van gegevens. De klachten over de Wpg zijn slechts een klein deel van het totaal aan klachten dat de Nationale Ombudsman over de politie ontvangt[129].

Door de Nederlandse Orde van Advocaten is aangegeven dat de politie vaak nog (te) passief omgaat met correctieverzoeken. Daarbij signaleren ze ook als (potentieel) knelpunt dat de politie bij een kennisgevingsverzoek niet altijd kan aangeven of (onjuiste) gegevens op meerdere plekken zijn opgeslagen (binnen de eigen organisatie of verstrekt aan derden). Correctie of verwijdering op de plek waar kennisnemingsverzoek is ingediend, is daarmee nog geen garantie dat alle onjuiste gegevens worden gecorrigeerd of verwijderd.

Indruk dat vaker verzoeken worden ingediend en voor andere doelen

Geïnterviewden geven aan dat het aantal kennisnemingsverzoeken toeneemt en dat de afhandeling hiervan veel tijd vergt. Het doel van de kennisnemingsverzoeken verandert, zo geeft een geïnterviewde aan. In sommige gevallen worden verzoeken gedaan om informatie te verkrijgen over lopende onderzoeken of de buurt. Ook komt het steeds vaker voor dat betrokkenen in het kader van rouwverwerking een verzoek tot kennisneming indienen, bijvoorbeeld als een naaste is omgekomen door een misdrijf. Het is de geïnterviewden niet altijd duidelijk in hoeverre dat ook mogelijk is conform de Wpg dan wel of het de bedoeling is geweest van de wetgever dat politiegegevens daarvoor kunnen worden gebruikt.

Verzoeken om kennisnemingen CIE- en informantgegevens

In de praktijk worden kennisnemingsverzoeken om CIE-gegevens[130] en informantgegevens[131] vrijwel standaard afgewezen op grond van artikel 27 in welk artikel is bepaald dat een verzoek wordt afgewezen in het belang van de goede uitvoering van de politietaak, de bescherming van de rechten van de betrokkene of van de rechten en vrijheden van derden of de veiligheid van de staat. Kielman heeft eerder al de vraag gesteld of dit recht ten aanzien van deze categorie gegevens niet moet worden afgeschaft.[132] Geïnterviewden geven aan dat de administratieve lasten aanzienlijk zouden kunnen worden verlaagd als in de Wpg zou worden bepaald dat betrokkenen geen rechten kunnen uitoefenen ten aanzien van dergelijke gegevens.

---

[129] In 2012 heeft de Nationale Ombudsman circa 1350 klachten over de politie ontvangen. Minder dan 5% betrof de verwerking van politiegegevens; bron: politiejaarbrief 2012, 19 maart 2013

[130] Gegevens die worden verwerkt op grond van artikel 10 lid 1 onder a Wpg.

[131] Artikel 12 Wpg.

[132] Kielman 2010, p. 170-171.

Mondelinge verstrekkingen vormen een probleem

Volgens een privacyfunctionaris bij een voormalig korps worden in de praktijk vaak alleen mondeling gegevens verstrekt. Dit levert een knelpunt op wanneer om kennisneming wordt verzocht. De verzoeker kan dan niet worden meegedeeld aan wie de op hem betrekking hebbende politiegegevens zijn meegedeeld. Bij correctie kan dan evenmin bericht aan derden worden gegeven.

Samenloop met Wob en Sv

In het kader van het onderzoek hebben verschillende geïnterviewden aangegeven dat bij het kennisnemingsrecht sprake is van samenloop tussen de Wpg en de Wet openbaarheid van bestuur. Ook is sprake van samenloop met Sv wanneer het OM een strafdossier samenstelt. Op deze samenloop wordt in hoofdstuk 9 ingegaan.

7.5 Samenvattende bevindingen

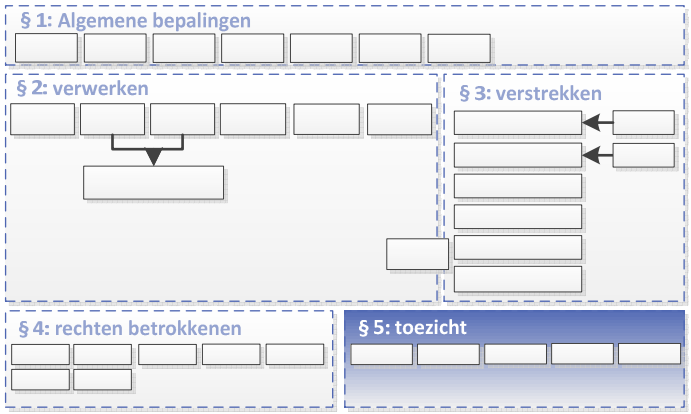
Naar aanleiding van de audits van 2011 is een landelijke procedure vastgesteld met betrekking tot de rechten van betrokkenen. Niet alle eenheden werken al conform deze procedure.

Het kennisnemingsrecht is een belangrijke waarborg voor de informationele privacy. Gegevens over de aantallen verzoeken die landelijk gezien worden ingediend zijn onbekend. Het is de vraag of betrokkenen altijd op de hoogte zijn van hun rechten en het verwijderen van gegevens is niet altijd eenvoudig.

Bij de uitoefening van rechten door betrokkenen doen zich vanuit het oogpunt van de politie knelpunten voor in de samenloop met de Wob (zie verder hoofdstuk 9), de administratieve lasten die met de afhandeling van verzoeken gepaard gaan en veranderende, volgens geïnterviewden soms onterechte doelen van kennisname.

8 Toezicht

8.1 Inleiding



De Wpg wijdt een aparte paragraaf aan het toezicht op de wijze waarop politiegegevens worden verwerkt. Het begrip 'toezicht' wordt daarbij ruim opgevat en omvat niet alleen formeel toezicht (met sanctiemogelijkheden) maar ook enkele instrumenten die een rol (kunnen) spelen bij de borging van de informationele privacy rond politiegegevens in het algemeen. Meer specifiek noemt de Wpg de volgende toezichtinstrumenten en toezichtfiguren:

- Protocollering
- Uitvoering privacy-audits
- Intern toezicht (privacyfunctionaris/functionaris gegevensbescherming)
- Extern toezicht (CBP)

8.2 Protocollering

Artikel 32 Wpg verplicht tot schriftelijke vastlegging van verschillende zaken, zoals het doel van het onderzoek bij art. 9 verwerking, hernieuwde verwerking, geautomatiseerd vergelijken, in combinatie met elkaar verwerken van gegevens, toekennen van autorisaties, onrechtmatige handeling en bepaalde verstrekkingen[133]. De protocolplicht is enerzijds bedoeld om intern en extern toezicht mogelijk te maken. Anderzijds moet protocollering ook ondersteuning bieden bij het informeren van betrokkenen waarvan gegevens zijn gecorrigeerd.

Knelpunten uit de audits

Protocollering verwerking artikel 9 gegevens grotendeels vastgelegd

In 2011 voldeed volgens de audits ruim 75% van de korpsen aan de eisen voor het vastleggen van protocollering bij de verwerking van artikel 9 gegevens[134]. Bij de hercontrole in 2013 voldeden alle eenheden[135]. Het bewaren van de protocolgegevens was in 2011 bij ruim 90% van de korpsen vastgelegd. Afwijkingen zaten vooral in het niet structureel protocolleren van (kleine) onderzoeken, in (te) summiere doelomschrijvingen of het (bij de

[133] Artikel 32 Wpg.
[134] DAD audits, 2012.
[135] Bij twee eenheden was de protocollering wel vastgelegd, maar voldeed deze nog niet helemaal aan de wettelijke eisen.

privacyfunctionaris) ontbreken van een actueel overzicht van lopende en beëindigde onderzoeken of de bewaarplaats van protocolgegevens. De daadwerkelijke protocollering is niet onderzocht in de audits[136].

Protocollering verwerking politiegegevens art. 11 in afwachting van landelijke richtlijn

De protocollering van artikel 11 gegevens was in 2011 bij minder dan 40% van de korpsen vastgelegd. Deze verliep volgens de auditors in ruim 60% van de gevallen niet volgens de eisen van de Wpg. Bijna 40% van de korpsen voldeed aan de norm met betrekking tot het bewaren van de protocolgegevens. Afwijkingen zaten met name in het niet (structureel) of inhoudelijk afdoende vastleggen van verwerkingen, onduidelijke omschrijving van de protocollering in werkinstructies/procesbeschrijvingen en/of het ontbreken van actief toezicht op de protocollering. In 2013 zijn op dit punt de meeste eenheden in afwachting van een landelijke richtlijn voor de protocollering van deze gegevens.

Protocollering verwerking politiegegevens art. 13 nog niet goed geregeld

Wat betreft de verwerking van politiegegevens in het kader van ondersteunende taken (artikel 13 Wpg) had in 2011 bijna de helft van de korpsen de wijze van protocollering daarvoor vastgelegd. Ruim 60% van de korpsen voldeed aan de norm voor bewaring van deze protocolgegevens. De afwijkingen zaten vooral in het ontbreken van een (inhoudelijk afdoende) verslaglegging, het ontbreken of onvolledig zijn van procesbeschrijvingen of het ontbreken van inzicht in de protocolleringen (door de privacyfunctionaris). Het beeld was in 2013 niet wezenlijk gewijzigd.

Protocollering onrechtmatige handelingen

Iets meer dan de helft van de korpsen had in 2012 de protocollering van een onrechtmatige handeling (zoals onterechte verstrekking) niet vastgelegd. Voor zover er wel geprotocolleerd werd, werden de gegevens door 60% van de korpsen correct bewaard. Afwijkingen van de wettelijke eisen bestonden vooral uit het ontbreken van werkinstructies en procedureomschrijvingen, het niet bijhouden van onrechtmatige handelingen of het ontbreken van overzichten de overzichten daarvan. De protocollering van een onrechtmatige handeling is in het kader van de hercontrole niet onderzocht[137].

Protocollering verstrekkingen vindt selectief plaats

Protocollering van verstrekkingen gebeurde volgens de auditors in 2011 in ruim 25% van de gevallen volgens norm. Voor zover werd geprotocolleerd, werden de protocolgegevens

[136] Landelijke rapportage hercontrole Wpg, 2013.

[137] Voor wat betreft de protocollering van gemeenschappelijke verwerking verliep dat altijd volgens de eisen uit de Wpg, voor zover van belang, gezien het feit dat er weinig gemeenschappelijke verwerking plaats vond binnen de korpsen. Bij de hercontrole werd geconcludeerd dat door de vorming van een korps, met één verantwoordelijke, er binnen de politie onderling geen gemeenschappelijke verwerkingen meer plaats vinden.

bij 85% van de organisaties correct bewaard. De afwijkingen waren met name het ontbreken van structurele en/of juiste protocollering. Dit gold met name voor protocollering van art. 8 gegevens (aan de hand van het zogenaamde I90-formulier). De protocollering van de verstrekking van art.10 gegevens (CIE-gegevens) en verstrekkingen via de Info-desk verliepen vaak wel conform de eisen van de Wpg. Verder bleken medewerkers vaak onbekend met de protocolleringsprocedure en verschilden de wijze van protocollering waardoor controle achteraf moeilijk is[138]. In de hercontrole van 2013 wordt gesproken van een verbetering op dit punt (meer protocollering op basis van I90 en meer uniformiteit). Er is nog geen sprake van een volledige conformiteit met de Wpg, vooral omdat de eenheden in afwachting zijn van nadere landelijke richtlijnen en hulpmiddelen[139].

Knelpunten uit de interviews

Administratieve druk

Diverse geïnterviewden geven aan dat protocollering bij de verstrekking van gegevens in het kader van de uitvoering van dagelijkse politietaken niet systematisch plaatsvindt. Een wijkagent geeft aan dat het om zeer veel meldingen, verstrekkingen of vormen van uitwisseling per dag kan gaan, vaak ook mondeling. In de eenheid waarvan hij onderdeel uitmaakt, gaat het om circa 30.000 geregistreerde verstrekkingen per jaar. Daarbij is volgens hem een extra barrière dat de systemen de protocollering onvoldoende (gebruikersvriendelijk) ondersteunen. Een deel van de gegevens (wat, wie, waar) moet zowel in BVH als op het I90-formulier worden ingevuld. Daarbij is het mogelijk om gegevens over te zetten of te 'knippen en plakken'. Dat levert volgens hem veel dubbel werk op.

Ook een medewerker van een BOD geeft aan dat de ICT-systemen waar de primaire informatie in wordt opgeslagen de protocollering niet ondersteunen. Dat betekent extra administratie in andere systemen of voorzieningen.

Medewerkers van de Kmar geven aan dat ongeacht hoe vaak een bepaald type verstrekking voorkomt of dat verstrekking wettelijk verplicht is, er toch geprotocolleerd moet worden. Een enkele handeling kost volgens de betrokkenen maar een paar minuten, maar omdat het om vele verstrekkingen per dag gaat, kost het administreren in totaal toch veel tijd.

[138] DAD audits, 2012.
[139] Landelijke rapportage hercontrole Wpg, 2013.

Dubbelingen in administratie

Een rechercheur vraagt zich ook af waar nut en noodzaak liggen van een dubbele registratie. Als voorbeeld wordt genoemd een bestuurlijke rapportage. Daarin is vastgelegd wat waarom aan wie wordt verstrekt. Waarom moet dat nogmaals apart worden geregistreerd? Een andere rechercheur stelt daar tegenover dat het in het kader van het onderzoek van belang kan zijn om niet alle informatie in het onderzoeksdossier te hebben zitten. Een betrokkene kan immers een verzoek om kennisneming doen. Je wilt volgens hem niet altijd dat een betrokkene weet aan wie gegevens zijn verstrekt. Een ander voorbeeld wordt genoemd door een wijkagent: als je gegevens verstrekt of uitwisselt via de mail, en deze mailwisseling wordt opgeslagen, dan is daarmee ook vastgelegd wat aan wie is verstrekt.

Tegenstrijdigheid en nut ter discussie

Soms wordt protocollering als zinloos dan wel ongewenst ervaren, bijvoorbeeld als andere wetgeving verplicht tot het verstrekken van politiegegevens[140].

Een privacyfunctionaris merkt op dat de huidige wijze van protocolleren het krijgen van overzicht lastig maakt. De protocollering is een 'vrije tekst invoer'. Bij grote aantallen protocolleringen is daar moeilijk inhoudelijke management- of sturingsinformatie uit te halen.

Balans protocollaire en professionele borging

Een geïnterviewde geeft aan dat meer vertrouwd zou moeten worden op de professionele afweging van de medewerker. Naar zijn zeggen is binnen de eigen dienst (BOD) sprake van een sterk besef dat wordt omgegaan met vertrouwelijke informatie. Het staat op zich ook niet ter discussie dat een deel van de verstrekkingen moet worden geprotocolleerd. De balans tussen professionele en protocollaire borging ontbreekt op dit moment volgens hem echter. De protocolplicht zou volgens verschillende geïnterviewden meer moeten afhangen van gevoeligheid en context van de informatie en de risico's van de verstrekking.

Wanneer protocolleren?

Zoals in hoofdstuk 6 is aangegeven vinden betrokkenen het niet altijd duidelijk wanneer sprake is van een verstrekking. Een medewerker van de Kmar geeft als voorbeeld de verstrekkingen aan de IND in het kader van de vreemdelingenwetgeving. Dit zijn (verplichte) verstrekkingen in het kader van het uitvoeren van een wettelijke taken, derhalve is volgens hem protocolleren niet aan de orde.

[140] Zie ook eerdere opmerkingen. Dit staat los van de vraag of dit beeld van protocolplicht ook overeenstemt met de eisen van de Wpg. In hoofdstuk 10 komt dit terug.

8.3 Privacy-audits

Artikel 33 Wpg voorziet in het periodiek door een onafhankelijke auditor laten uitvoeren van privacy audits naar de naleving van de Wpg. De verantwoordelijke laat dit twee jaar na de inwerkingtreding en vervolgens elke vier jaar uitvoeren. Bij onvoldoende naleving zal er binnen een jaar een hercontrole moeten worden uitgevoerd[141]. Daarnaast dient de verantwoordelijke (minstens éénmaal per jaar) zorg te dragen voor het uitvoeren van interne audits[142].

Op grond van de Wpg hadden alle (voormalige) regionale politiekorpsen en BOD-en in 2010 (twee jaar na de inwerkingtreding van de Wpg) de eerste privacy audit moeten laten uitvoeren.

Knelpunten uit de audits

In 2010 bleek dat geen van de korpsen of opsporingsdiensten aan de auditverplichting had voldaan[143]. Na een interventie van het CBP is in 2011 bij alle korpsen eind 2011 een audit uitgevoerd[144]. Het algemene beeld daaruit was dat slechts een klein deel van de korpsen op hoofdlijnen voldeed aan de Wpg.

De interne auditfunctie was bij circa 40% van de korpsen structureel aanwezig. Circa 25% van de korpsen had een (adequaat) auditplan en circa 35% van de korpsen rapporteerde op de juiste wijze. Vaak was er geen plan of rapport aanwezig of werd dit niet structureel opgeleverd[145]. Bij de hercontrole in 2013 bleek op één eenheid na de auditfunctie wel structureel ingevuld te zijn met één of meer interne auditors. Ook hebben alle eenheden een hercontrole laten uitvoeren als onderdeel van het interne auditproces. Nog niet alle eenheden hebben een intern auditplan, dit in afwachting van een landelijk (model) auditplan[146].

Knelpunten uit de interviews

Aanjaagfunctie audits

De privacyfunctionaris stelt dat de audits mede een aanjager zijn geweest om de Wpg beter op de agenda te krijgen. Volgens hem gaan de audits wel voorbij aan de meer onderliggende oorzaken waarom de Wpg niet goed is geïmplementeerd. Belangrijk(st)e

[141] Artikel 33 Wpg en artikel 6:5 Bpg.
[142] Artikel 3 Regeling periodieke audit politiegegevens.
[143] CPB, 2011.
[144] Uitgezonderd het korps Zeeland en de FIOD die na een eerste interventie van het CBP wel een privacy-audit hadden uitgevoerd. De overige korpsen bleven ook na de eerste interventie van het CPB in gebreke.
[145] DAD audits, 2012.
[146] Landelijke rapportage hercontrole Wpg, 2013.

factor daarbij is volgens hem het niet aansluiten van de ICT. Zowel qua protocollering, qua mutaties van de status van gegevens als qua autorisatie en beveiliging.

Een andere privacyfunctionaris onderschrijft dat de audits hebben bijgedragen aan het meer op de agenda zetten van de Wpg. Het heeft er volgens hem ook wel toe geleid dat de focus erg ligt op 'het voldoen aan de audits'. Daarbij moet de politie zich volgens hem realiseren dat ook de auditoren een interpretatie hebben gemaakt van de wet in het algemeen en de invulling van de open normen in het bijzonder.

Audits (te) sterk gericht op de administratieve en procedurele kant

Een leidinggevende en een projectleider Wpg erkennen enerzijds het nut van audits, maar vragen zich anderzijds af of de vorm waarin deze (moeten) worden gegoten veel toevoegen aan het beter beschermen van de informationele privacy. De audits richten zich volgens hen vooral op de administratieve organisatie en kosten relatief veel tijd.

Een andere leidinggevende sluit daarbij aan. Volgens hem is de toetsing in de audits vooral de 'geïnterpreteerde letter van de wet'. Het is volgens hem van belang dat de focus (zeker in eerste instantie) bij de geest van de wet ligt. Anders dreigt een bureaucratisering en is het maar de vraag of er voldoende draagvlak komt. Nut en noodzaak van de Wpg zijn volgens hem nog geen gemeengoed binnen de politie.

Meerdere geïnterviewden geven aan dat in de audits voornamelijk is gekeken naar procedures en administratieve organisatie rond de Wpg (aanwezigheid rapportages, overzichten, etc.) en niet naar uitvoering zelf en de gevolgen daarvan. Verder geven ze aan dat het doorvoeren van de verbeteracties veel tijd en geld kost, terwijl het maar de vraag is of het verbeteren van de administratieve organisatie feitelijk voor verbetering van de privacybescherming zorgt.

Normenkader voldoende eenduidig?

De naleving van de Wpg is bij de BOD-en onderzocht door de Auditdienst Rijk (ADR, voorheen de RAD Rijksauditdienst) en bureau Mazars. De audits zijn volgens de medewerkers van de BOD-en gedetailleerder dan de audits die de Departementale Auditdienst (DAD) bij de verschillende politiekorpsen heeft uitgevoerd…. Geïnterviewden vragen zich in dat verband af in hoeverre de verschillende audits wel vanuit een zelfde normenkader zijn uitgevoerd en de uitkomsten derhalve vergelijkbaar zijn. Verder wordt de vraag gesteld wat dan de hardheid van de uitkomsten is. Het gaat volgens verschillende geïnterviewden immers om een (vooral proceduregerichte) interpretatie van de wet waaraan wordt getoetst.

8.4 Privacyfunctionaris/functionaris gegevensbescherming en intern toezicht

De Wpg voorziet in intern toezicht door het verplicht aanstellen van een privacyfunctionaris en de mogelijkheid van een functionaris gegevensbescherming. De privacyfunctionaris heeft tot taak toe te zien op de verwerking van politiegegevens overeenkomt het bij of krachtens de wet bepaalde en de verantwoordelijke daarover van advies te dienen. In het kader van die taak monitort de privacyfunctionaris onder meer onderzoeken, verstrekkingen en protocolleringen. Daarnaast houdt de privacyfunctionaris een overzicht bij van de autorisaties. De privacyfunctionaris kan daarnaast ondersteuning in de vorm van voorlichting en advies geven over de naleving van de Wpg. De privacyfunctionaris is geen toezichthouder in de zin van art. 5.11 Awb, is in die zin niet onafhankelijk en heeft ook geen toezichthoudende bevoegdheden. Dit in tegenstelling tot een functionaris gegevensbescherming (art. 36 Wpg).

Knelpunten uit de audits

Privacyfunctionaris overal benoemd, maar komt nauwelijks aan toezicht toe

In 2011 beschikte ruim 95% van de korpsen over een privacyfunctionaris. De auditors stellen vast dat deze in de praktijk wat de Wpg betreft vooral een adviserende en aanjagende rol heeft. De toezichtrol komt volgens de auditors in 2011 nog niet van de grond[147]. Als verklaring wordt onder meer gegeven de discrepantie tussen de beschikbare capaciteit en de feitelijk benodigde capaciteit om 'de Wpg organisatie-breed tussen de oren te krijgen'. In 2013 zijn in alle eenheden één of meer privacyfunctionarissen benoemd en aangemeld. Nog steeds is niet in alle eenheden een overzicht van protocolleringen aanwezig. Als argument wordt aangevoerd dat een landelijk format in de maak is waar men op wacht. Wel zijn in nagenoeg alle eenheden jaarverslagen opgemaakt[148].

Weinig managementinzicht in protocollering

Minder dan een kwart van de korpsen kon in 2011 een overzicht van de protocollering overleggen en ongeveer een derde had een jaarverslag. Volgens de auditors kwam dat onder andere doordat privacyfunctionarissen geen inzage hadden in alle protocolleringen[149]. Bij ruim 25% van de korpsen bleek er onvoldoende toezicht te zijn op (de protocollering van) verstrekkingen[150]. De hercontrole in 2013 laat op dit punt geen wezenlijke verbeteringen zien[151].

[147] DAD audits, 2012.
[148] Landelijke rapportage hercontrole Wpg, 2013.
[149] DAD audits, 2012.
[150] DAD audits, 2012.
[151] Landelijke rapportage hercontrole Wpg, 2013.

Functionaris gegevensbescherming nauwelijks in beeld

In 2011 hebben twee regionale korpsen een functionaris gegevensbescherming. Bij één van deze korpsen was volgens de auditoren geen sprake van onafhankelijk toezicht omdat deze de taken van de privacyfunctionaris had overgenomen. Bij het tweede korps was de functionaris net benoemd[152]. Andere korpsen gaven in 2011 aan te wachten op de vorming van de Nationale politie en dan te bezien of een functionaris gegevensbescherming wordt aangesteld[153]. In de landelijke rapportage hercontrole is niet ingegaan op de functionaris gegevensbescherming.

Knelpunten uit de interviews

De privacyfunctionaris lijkt volgens de geïnterviewden degene te zijn waaraan de naleving van de Wpg vrijwel volledig wordt opgehangen. Van deze functionaris zou verwacht worden de hele organisatie op sleeptouw te nemen bij het naleven van de Wpg.

Meerdere privacyfunctionarissen geven aan (daardoor) niet of nauwelijks aan de toezichthoudende taken toe te komen. Het accent ligt vooral op het geven van voorlichting en advies aan medewerkers (en leiding) over hoe bijvoorbeeld kan worden omgegaan met de open normen. Daar komt volgens hen bij dat privacyfunctionarissen vaak ook andere taken hebben, zoals het behandelen van verzoeken tot kennisneming, Wob-verzoeken of het toetsen van convenanten en samenwerkingsovereenkomsten.

Verschillende geïnterviewden geven aan dat de advies- en toezichtrol niet goed verenigbaar zijn, omdat dan de eigen adviezen worden getoetst. Een privacyfunctionaris geeft aan in een spagaat te komen: enerzijds moet deze onafhankelijk en buiten de lijn kunnen opereren (bijvoorbeeld toetsen of de verwerking, verstrekking en protocollering conform de Wpg plaatsvindt). Anderzijds moet deze verantwoording afleggen aan de verantwoordelijke[154]. Deze staat volgens een privacyfunctionaris echter vaak ver af van de Wpg.

De capaciteit die voor privacyfunctionarissen is vrijgemaakt, verschilt volgens de geïnterviewden zeer sterk. Daarbij lijkt er geen directe relatie te bestaan tussen bijvoorbeeld de omvang van een organisatie en deze capaciteit. Zo geeft een privacyfunctionaris aan 0,5 fte beschikbaar te hebben voor een organisatie met 900 medewerkers en een andere privacyfunctionaris 1,0 fte voor een organisatie met 6000 medewerkers. Ze geven aan dat de capaciteit voor (de taken van) privacyfunctionarissen

[152] Mazars Management Consultants, 2011.
[153] DAD audits, 2012.
[154] De privacyfunctionaris werkt weliswaar onder verantwoordelijkheid van de leidinggevende (verantwoordelijke) maar moet wat betreft de inhoudelijke beoordeling van de naleving van de Wpg onafhankelijk kunnen toetsen. Een vergelijkbare spagaat is er bijvoorbeeld ook voor een concerncontroller of kwaliteitsfunctionaris. Belangrijk verschil is dat de privacyfunctionaris wettelijk is vastgelegd.

de afgelopen jaren is afgenomen. Als voorbeeld noemt een privacyfunctionaris dat bij het in werking treden van de Wpg er twee privacyfunctionarissen waren en nu nog één.

Verschillende geïnterviewden vragen zich af hoe een en ander zich zal ontwikkelen na de vorming van de Nationale politie. Wetstechnisch gezien zou volgens hen kunnen worden volstaan met één privacyfunctionaris voor de hele Nationale politie.

Een leidinggevende is sceptisch over de vraag of intern toezicht kan werken. In zijn ogen bevat de Wpg veel (ook verborgen) toezichtfiguren. Dit leidt volgens hem in de praktijk vooral tot bureaucratisering en daarmee blijft de weerstand tegen de Wpg.

8.5 Extern toezicht

Het externe toezicht op de verwerking van politiegegevens is belegd bij het CBP. Als niet conform de wet wordt gehandeld kan het CBP een boete opleggen[155].

Knelpunten uit de audits

In de audits en de hercontrole is het externe toezicht niet onderzocht.

Knelpunten uit de interviews

De meeste geïnterviewden geven aan weinig te merken van het externe toezicht door het CBP. Dit behoudens de interventie in 2011 die heeft geleid tot het uitvoeren van de audits.

Het CBP bevestigt dit beeld door aan te geven vooral marginaal en selectief te willen toetsen of de Wpg wordt nageleefd. Bijvoorbeeld als het gaat om specifieke onderwerpen zoals de CIE-verwerkingen en bij signalen dat op systeemniveau de Wpg niet geborgd is (zoals de interventie in 2011 die heeft geleid tot het uitvoeren van privacy-audits).

Ten aanzien van de handhavende actie van het CBP op de CIE-verwerkingen geven gesprekspartners aan dat de Wpg inderdaad een periodieke noodzakelijkheidstoets moet worden uitgevoerd (artikel 10 lid 6 Wpg) maar dat het daadwerkelijk invulling geven aan deze toets ondoenlijk is en in de dagelijkse praktijk nagenoeg onmogelijk. Volgens de gesprekspartners vergt een controle een onevenredig grote inzet van capaciteit.

Het CBP geeft zelf aan niet zoveel instrumenten te hebben om naleving van de Wpg af te dwingen. In theorie kan een bestuurlijke boete worden opgelegd. De bedragen zijn volgens de betrokkenen echter te laag (€4.500) om effect te hebben. Eventueel kan ook een last onder dwangsom worden toegepast. Maar daar was tot nu toe nog geen aanleiding voor. Daarbij wordt aangetekend dat ook de capaciteit daartoe ontbreekt. Als belangrijkste

[155] Artikel 35 Wpg.

instrumenten zien de medewerkers van het CBP publiciteit (naming and shaming), het geven van voorlichting en het waar mogelijk direct aanspreken van de leiding.

Medewerkers van de BOD-en geven aan dat het CBP zich met name richt op de artikel 10 en 12 verwerkingen. Dat is volgens hen echter maar een klein deel van alle verwerkingen. Dat zijn bovendien de verwerkingen waar het bewustzijn van het belang van het goed omgaan met de informationele privacy relatief hoog is. Volgens hen laat het CBP 95% van de relevante verwerkingen, namelijk die op basis van artikel 9, liggen.

De opvattingen van geïnterviewden over de rol van het CBP verschillen. Enerzijds wordt aangegeven dat het CBP een adviserende rol moet aannemen. Anderzijds schuilt daarin een gevaar volgens geïnterviewden, omdat verantwoordelijken zich niet altijd bewust blijven van de risico's. "Als het CBP het goed vindt, dan mag het".

8.6 Overig

In zijn algemeenheid merken meerdere geïnterviewden op dat de Wpg en stapeling van toezichtfiguren kent. Naast de formele toezichtfiguren van protocollering, audits en de algemene toezichtrol van de privacyfunctionaris/functionaris gegevensbescherming en het CBP zijn er volgens hen ook meer onzichtbare toezichtfiguren zoals de autorisaties, het recht op kennisneming of toetsing vanuit het OM (CIE-OvJ). Dat leidt volgens verschillende geïnterviewden tot een stapeling van toezicht met het risico van bureaucratisering zonder dat dat toezicht effectief bijdraagt aan de verhoging van de privacybescherming.

Een privacyfunctionaris vraagt zich af op het toezicht zich wel op de juiste zaken richt. Het gaat vooral over de protocollen en de administratie. Volgens hem heeft de organisatie niet of nauwelijks inzicht in wat het resultaat of het effect is van alle maatregelen: is de informationele privacy afdoende beschermd? En: leidt in een inbreuk op de informationele privacy ook tot aantasting van de persoonlijke levenssfeer?

8.7 Samenvattende bevindingen

De Wpg kent een reeks toezichtfiguren die moeten bijdragen aan het borgen van de informationele privacy bij het verwerken van politiegegevens.

Protocollering houdt in het vastleggen van onder meer het doel van bijvoorbeeld verstrekkingen of bepaalde verwerkingen. Daarmee kan achteraf worden getraceerd of bijvoorbeeld een verwerking rechtmatig was. Daarnaast heeft protocollering een functie bij de kwaliteitsborging van gegevens, bijvoorbeeld om te traceren of incorrecte gegevens zijn verstrekt. Het algemene beeld is dat het protocolleren van artikel 9 gegevens redelijk tot goed is geborgd en de verwerking van artikel 11 en 13 gegevens beperkt is geborgd. Bij

verstrekkingen vindt protocollering selectief plaats. Vooral de protocollering van de verstrekking van artikel 8 gegevens voldoet niet aan de wettelijke eisen.

In de uitvoeringspraktijk wordt de administratieve druk als een groot knelpunt genoemd. Deze hangt volgens de geïnterviewden aan de grote hoeveelheden verstrekkingen bij de uitvoering van dagelijkse politietaken en de onvoldoende ondersteuning door de ICT. Door het laatste is er volgens de betrokkenen soms sprake van een dubbele administratie. Verder wordt de vraag gesteld in hoeverre de balans tussen een bedrijfsmatige borging (verslaglegging, controles etc.) en professionele borging (bewustzijn en eigen afwegingsruimte en verantwoordelijkheid medewerker) in evenwicht is.

Organisaties die onder de Wpg vallen moeten periodiek privacy-audits uitvoeren. Dit is voor het eerst in 2011/2012 gebeurd, mede onder druk van het CBP. De constatering daarbij was dat maar 40% van de (toenmalige) korpsen een structurele auditfunctie had. Eind 2013 hadden (op één na) alle eenheden de auditfunctie wel ingevuld. Een knelpunt dat in de praktijk wordt ervaren is dat de audits voorbij gaan aan de onderliggende oorzaken van knelpunten bij de invoering van de Wpg, met name op het vlak van de ICT. Bovendien wordt gesteld dat de auditoren een interpretatieslag hebben moeten maken om van de wet tot een normenkader te komen. Dat is daarbij niet geheel eenduidig bleken. De gevolgde 'rule-based' benadering draagt volgens geïnterviewden bovendien niet bij aan het draagvlak voor de Wpg. De audits zeggen volgens hen weinig over de eventuele feitelijke inbreuk op de informationele privacy en de aantasting van de persoonlijke levenssfeer. Het zijn vooral formele schendingen van de Wpg. Bovendien gaan de audits volgens geïnterviewden voorbij aan verschillende ontwikkelingen die de verwerking van politiegegevens in een ander perspectief kunnen plaatsen. Het imago van een ingewikkelde en bureaucratische wet, wordt volgens hen door de audits eerder bevestigd dan doorbroken.

Alle eenheden beschikken over een privacyfunctionaris die is belast met het interne toezicht op de verwerking van politiegegevens en het adviseren van de organisatie. In de praktijk komen de privacyfunctionarissen maar beperkt aan hun toezichtrol toe. Enerzijds door andere taken die ze moeten uitvoeren. Anderzijds omdat er veel tijd gaat zitten in advisering en voorlichting. Daar komt bij dat volgens geïnterviewden de capaciteit de afgelopen jaren eerder is afgenomen dan toegenomen. Het gevolg daarvan is ook dat er maar weinig (bruikbare) managementinformatie is over bijvoorbeeld vertrekkingen.

Van de mogelijkheid om een functionaris gegevensbescherming aan te stellen is zeer beperkt gebruik gemaakt. Bij verschillende geïnterviewden bestaat er de nodige scepsis over de vraag of intern toezicht kan functioneren.

Het externe toezicht is belegd bij het CBP. De betrokkenen geven in de gesprekken aan hier in de praktijk weinig van te merken. Wel erkennen betrokkenen de aanjagende rol die het CBP heeft gehad bij het uitvoeren van audits in 2011/2012.

De stapeling van toezichtfiguren heeft volgens diverse geïnterviewden het risico van bureaucratisering in zich, zonder dat dat aantoonbaar heeft bijgedragen / bijdraagt aan een betere bescherming van de informationele privacy. Daarnaast wordt de vraag opgeworpen of het toezicht (intern en extern) zich wel op de juiste zaken richt. De focus ligt volgens de geïnterviewden nu vooral op de organisatie-eisen (protocollering, beschrijving werkprocessen etc.) en niet op de vraag in hoeverre de informationele privacy ook feitelijk wordt geschaad of de persoonlijke levenssfeer wordt aangetast en/of de effectiviteit en efficiëntie van de betrokken organisaties worden verhoogd.

9 Verhouding tot andere wetten

9.1 Inleiding

Onderzoeksvraag 5 richt zich op de verhouding van de Wpg tot aanpalende wet- en regelgeving. Naast de Wpg gelden er verschillende andere wetten waarin de verwerking van persoonsgegevens c.q. de bescherming van informationele privacy wordt geregeld. Te denken valt aan de Wet justitiële en strafvorderlijke gegevens (Wjsg), het Wetboek van Strafvordering (Sv), de Wet op de jeugdzorg (Wjz), afdeling 7.5 van het Burgerlijk Wetboek (de Wet inzake de geneeskundige behandelingsovereenkomst, Wgbo) en de Wet op de Beroepen in de Individuele Gezondheidszorg (Wet BIG). Als specifieke wetgeving ontbreekt is de Wet bescherming persoonsgegevens (Wbp) van toepassing. In paragraaf 9.2 worden de geconstateerde knelpunten besproken. Paragraaf 9.3 gaat in op de specifieke knelpunten in de samenloop met de Wob.

9.2 Ervaren knelpunten

Bij samenwerken onduidelijkheid over wettelijk regime dat van toepassing is

In de praktijk worden met name bij samenwerkingsverbanden knelpunten ervaren bij de samenloop van de Wpg met andere wetgeving. Te denken valt aan verbanden als het Veiligheidshuis en het Regionaal Informatie en Expertise Centrum (RIEC), waarin met diverse partners wordt samengewerkt. Voorbeelden van partners zijn gemeenten, het OM, woningbouwcorporaties, de belastingdienst, het Centrum voor Jeugd en Gezin (CJG), Bureau Jeugdzorg (BJZ), welzijnsorganisaties, de leerplichtambtenaren, scholen, schuldhulpverlening en de GGD. Deze partners hebben te maken met bijzondere wetten waarin specifieke regels zijn opgenomen over gegevensuitwisseling en geheimhouding.

Het is voor samenwerkingspartners niet altijd duidelijk welk regime op bepaalde gegevens van toepassing is; daarnaast wordt de interpretatie van de verschillende wetten in de praktijk lastig bevonden. Verschillende gesprekspartners van diverse instanties geven aan het opstellen van een convenant erg arbeidsintensief te vinden doordat voor elke partner moet worden nagegaan welke regels gelden en wanneer wel en niet gegevens mogen worden verstrekt. Het ontbreken van een actuele, overkoepelende handleiding wordt als een gemis ervaren.[156] Aangegeven is dat een adviserende rol van het CBP in dit kader erg op prijs zou worden gesteld.

[156] Er zijn wel voorbeeldconvenanten of privacyreglementen beschikbaar voor sommige samenwerkingsverbanden, bijvoorbeeld voor het veiligheidshuis. De handreiking over privacyaspecten bij criminaliteitspreventie is opgesteld voor gemeenten en dateert van 2003 (auteur: Sauerwein).

Botsende regimes

Volgens gesprekspartners lijken de privacyregels soms met elkaar in tegenspraak te zijn. Een voorbeeld dat genoemd is, is dat van verzekeraars die met enige regelmaat om gegevens verzoeken in verband met schadeclaims of ziektekosten. Het verzoek betreft dan niet alleen persoonsgegevens, maar ook bijvoorbeeld het proces-verbaal, getuigenverklaringen, een forensisch rapport, e.d. De verzekeraar wil vanwege vertrouwelijkheid over het algemeen geen informatie geven over het belang en het gebruiksdoel van de gevraagde informatie. De Wpg verbiedt het verstrekken van informatie als het doel en de noodzaak niet duidelijk zijn, maar zij vragen zich af of artikel 88 Zorgverzekeringswet niet verplicht tot verstrekken[157].

Onduidelijkheid over verantwoordelijkheid voor gegevens

Door het delen van politiegegevens is dezelfde informatie soms bij meerdere instanties aanwezig, bijvoorbeeld bij het OM (strafdossier), de politie (onderzoeksdossier) en de gemeente (bestuurlijke rapportage). Soms wordt ook een gegevensbestand aangelegd speciaal voor het samenwerkingsverband. Naast de onduidelijkheid over welk wettelijk regime van toepassing is, ervaren geïnterviewden eveneens problemen bij het bepalen van de verantwoordelijke voor de gegevens.

Politiegegevens komen in het kader van samenwerken bij een andere instantie terecht en worden daar door bijvoorbeeld advocaten opgevraagd. Het is voor de gesprekspartners van de politie onduidelijk hoe met deze verzoeken wordt omgegaan en of de handelwijze overeenkomt met die van de Wpg. In de praktijk is een goede afstemming derhalve gewenst.

Op dezelfde gegevens kunnen meerdere wettelijke regimes van toepassing zijn

Het zich bij verschillende partijen bevinden van gegevens komt ook voor in de strafrechtketen. Gesprekspartners bij de politie en het OM ervaren het als knelpunt dat ten aanzien van dezelfde gegevens verschillende wettelijke regimes van toepassing kunnen zijn, een en ander afhankelijk van waar in het proces en bij wie de gegevens zich bevinden.

Politiegegevens kunnen zich zowel bij de politie en andere opsporingsinstanties bevinden als bij het OM. In het eerste geval is de Wpg van toepassing. Op gegevens die deel uitmaken van een lopend onderzoek of die in een strafdossier of langs geautomatiseerde weg door het OM worden verwerkt, zijn de bepalingen van Sv en de Wjsg van toepassing. De regels die de Wpg, Sv en de Wjsg stellen ten aanzien van het verwerken van gegevens verschillen van elkaar.

---

[157] Ook hier speelt mogelijk weer de kennis van de wet- en regelgeving parten. Artikel 88 van de Zorgverzekeringswet verwijst naar de Wbp maar niet naar de Wpg. Dergelijke algemene verstrekkingsplichten (de belastingwetgeving kent ze ook), doorbreken niet het gesloten verstrekkingenregime van de Wpg

Voor gegevens die onder het regime van artikel 125n[158] en 126dd[159] Sv vallen is in Sv een speciale regeling getroffen. De verstrekkingsregels van de Wpg zijn op die gegevens niet van toepassing.[160] De officier van justitie moet ten aanzien van de politiegegevens die zijn verkregen met behulp van de opsporingsbevoegdheden vermeld in art. 125n lid 1 Sv of art. 126cc lid 1 Sv bepalen of deze gegevens verwerkt mogen worden in een ander strafrechtelijk onderzoek dan waartoe de bevoegdheid is uitgeoefend, dan wel mogen worden verwerkt voor een doel als genoemd in art. 10 lid 1, onder a en b Wpg.[161] Ook is de regeling ten aanzien van bewaren en verwijderen van de Wpg niet van toepassing. In de betreffende artikelen is geregeld dat de gegevens na afronding van de zaak moeten worden vernietigd.[162] Gesprekspartners van het OM ervaren de afwijkende regeling in Sv als een knelpunt. De regeling over het vernietigen van gegevens is te rigide, omdat de betreffende politiegegevens ook van belang kunnen zijn voor toekomstige onderzoeken.

Samenloop met Archiefwet

Ook als het gaat om de samenloop van de Wpg met de Archiefwet worden problemen ervaren met betrekking tot de bewaartermijn. Volgens artikel 14, lid 4, Wpg wordt van de vernietiging van politiegegevens afgezien voor zover de waarde van de archiefbescheiden als bestanddeel van het cultureel erfgoed of voor historisch onderzoek zich daartegen verzet. Het is volgens betrokkenen moeilijk te beoordelen of een situatie als bedoeld in genoemd artikel aan de orde is. Duidelijke beleidsregels ontbreken op dit punt.

9.3 Wet openbaarheid van bestuur

De Wet openbaarheid van bestuur regelt het recht van burgers op informatie van de overheid. De Wob zorgt ervoor dat de burger inzage heeft in het overheidshandelen en kan deelnemen aan de democratie en overheidsbesluitvorming. Uitgangspunt van de Wob is dat overheidsinformatie openbaar is. Uitzonderingen gelden alleen als de Wob of andere wetten bepalen dat de gevraagde informatie niet geschikt is om openbaar te maken. In de Wob is bepaald dat geen informatie wordt verstrekt als het belang daarvan niet opweegt tegen het belang van de opsporing en vervolging van strafbare feiten.[163] Gesprekspartners voeren desalniettemin aan dat zij vrezen dat inwilliging van een Wob-verzoek ertoe kan leiden dat lopende onderzoeken kunnen worden geschaad.

[158] Gegevens die zijn verkregen tijdens een doorzoeking
[159] Gegevens die zijn verkregen door observatie met behulp van een technisch hulpmiddel dat signalen registreert, het opnemen van vertrouwelijke communicatie, het opnemen van telecommunicatie of het vorderen van gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker.
[160] MvT, p. 16 en 69.
[161] Art. 126dd lid 1 Sv.
[162] Artikel 125n, eerste lid en artikel 126cc, tweede lid Sv.
[163] Artikel 10 lid 2 Wob.

Verhouding Wob en Wpg

Tot 2006 werd ervan uitgegaan dat op grond van het beginsel dat de Wob wijkt voor specifieke verstrekkingsregelingen bij een verzoek om stukken uit politieregisters, de integrale stukken aan de Wpolr getoetst moesten worden.[164] Eind 2006 oordeelde de Afdeling bestuursrechtspraak van de Raad van State dat de Wpolr weliswaar een uitputtende regeling vormt ten opzichte van de Wob, maar dat de Wpolr alleen van toepassing is op persoonsgegevens. Als het om andere gegevens gaat, is de Wob van toepassing. Als documenten niet alleen politiegegevens c.q. persoonsgegevens in de zin van de Wet politieregisters bevatten, kunnen ze niet integraal onder de werking van die wet worden gebracht. Ook de Wob is dan van toepassing. Per document moet de aard van de informatie worden onderzocht.[165] [166] Hoewel de uitspraak voorafgaand aan de invoering van de Wpg is gedaan, is in de parlementaire geschiedenis niet gerept over de verhouding tussen de Wob en de Wpg.

Administratieve lasten

In de literatuur wordt door sommigen aangegeven dat de verhouding tussen beide wetten onnodig complex is.[167] Gesprekspartners bij de politie erkennen de belangrijke functie van de Wob voor het handelen van de politie, maar geven eveneens aan dat zij veel administratieve lasten ervaren bij de afhandeling van de, soms vele, Wob-verzoeken. Aangegeven is dat veel verzoeken om kennisneming tevens worden gebaseerd op de Wob. Dit komt met name voor bij verkeersovertredingen. Als een verzoek op grond van art. 25 Wpg wordt ingediend over een verkeersovertreding die de verzoeker zou hebben begaan, ontvangt deze wel de foto (politiegegeven) maar niet het ijkrapport van het meetinstrument (geen politiegegeven).

De gesprekspartners van de politie wijzen op onderzoek waaruit is gebleken dat politiekorpsen verreweg de meeste Wob-verzoeken ontvangen (gemiddeld 964 per korps) en dat korpsen in vergelijking tot andere bestuursorganen met afstand de meeste verzoeken ontvangen waarvan vermoed wordt dat zij gericht zijn op *verdienen* (gemiddeld 187 verzoeken per korps). Ook zijn bij politiekorpsen de meeste verzoeken ontvangen waarvan wordt vermoed dat zij gericht zijn op *frustreren en/of vertragen* (gemiddeld 210 per korps). De aantallen van de overige bestuursorganen vallen volgens de onderzoekers hierbij in het niet. Bestuursorganen hebben gemiddeld 1 verzoek ontvangen waarvan zij vermoeden dat het voortkomt uit *een obsessief streven tot openbaarmaking*. Politiekorpsen hebben gemiddeld de meeste van deze verzoeken ontvangen. Bijna een derde van de

[164] ABRvS 4 maart 1999, AB 2002, 39 m.nt. SZ.
[165] ABRvS 29 november 2006, JB 2007, 13 en AB AB 2007, 24 m.nt. P.J. Stolk. Zie ook J.A.M. Berkvens, Wob-verzoek om inzage in politieregister, P&I 2007, 6.
[166] Zie ook Overkleeft-Verburg, Openbaarheid van bestuur, privacywetgeving en gegevensverwerking door de politie, in P&I 2007, nr. 5, te raadplegen op: http://www.overkleeft-verburg.nl/PDFs/Wob%20en%20politieregisters.pdf.
[167] Zie bv: http://www.overkleeft-verburg.nl/PDFs/ABRvS%205%20september%202012%20Wpg%20Wob%20en%20Archiefwet.pdf.

politiekorpsen heeft sinds de inwerkingtreding van de Wet dwangsom en beroep bij niet tijdig beslissen op 1 oktober 2009 één of meerdere keren een dwangsom uitgekeerd vanwege overschrijding van de termijn. Korpsen hebben vaker te maken met bezwaar en beroep en een veroordeling in de vergoeding van proceskosten dan andere bestuursorganen.[168]

Open en controleerbaar functioneren van de politie, maar geen onbeperkte inzet

In 2011 gaf de toenmalige minister van Binnenlandse Zaken en Koninkrijksrelaties aan dat een bestuursorgaan als de politie, dat in onze samenleving samen met het leger een monopolie bezit op het gebruik van geweldsmiddelen, open en controleerbaar hoort te functioneren.[169] Hierbij is eveneens opgemerkt dat de politiecapaciteit niet ongelimiteerd kan worden ingezet voor de afhandeling van Wob-verzoeken. In het kader van het plan 'Minder regels, meer op straat' worden verschillende maatregelen aangekondigd om de administratieve lasten bij de politie te verminderen.[170] In het kader van het terugdringen van de administratieve lasten, is de politie overgegaan tot actieve openbaarmaking van bepaalde informatie. Een aantal eenheden publiceren inmiddels informatie op www.mijnpolitie.nl. Onder andere burgers kunnen op deze site gegevens over verkeersovertredingen zelf inzien via de zogenaamde boetevolgservice (BVS) en hoeven zij daarvoor geen Wob-verzoek meer in te dienen.[171]

9.4 Samenvattende bevindingen

Als de politie samenwerkt met andere partners, gelden verschillende bijzondere wetten waarin specifieke regels zijn opgenomen over gegevensuitwisseling en geheimhouding. Samenwerkingspartners geven aan dat het interpreteren van de verschillende regelingen lastig is en dat knelpunten bestaan bij het bepalen welk regime op welke gegevens van toepassing is. Er kunnen knelpunten ontstaan in bijvoorbeeld bewaartermijnen doordat op dezelfde gegevens meerdere wettelijke regelingen van toepassing kunnen zijn.

De politie ervaart administratieve lasten bij de afhandeling van Wob-verzoeken en geeft aan dat lopende onderzoeken kunnen worden geschaad door inwilliging van Wob-verzoeken. Om de lasten te verlagen wordt informatie actief openbaar gemaakt. Daarnaast achten gesprekspartners een wetswijziging geboden.

---

[168] Haeften, Wils en Grimmius 2010, *Omvangrijke en oneigenlijke Wob-verzoeken. Aantallen, kenmerken en wijze van afhandeling*, Zoetermeer: Research voor Beleid, oktober 2010, p. 6, 8 en 9.
[169] Brief van 31 mei 2011, kenmerk 2011-2000224719.
[170] http://www.rijksoverheid.nl/onderwerpen/politie/minder-regels-meer-op-straat.
[171] In de eerste voortgangsrapportage is aangegeven dat deze maatregel heeft geleid tot minder administratieve lasten. http://www.rijksoverheid.nl/onderwerpen/politie/minder-regels-meer-op-straat.

Deel III: Nadere analyses en conclusies

10 Verklaringen knelpunten

10.1 Inleiding

In de vorige hoofdstukken is de praktijk van de uitvoering van de Wpg geschetst. Daarbij is op basis van de audits de (borging van de) naleving van de Wpg geschetst en zijn op basis van interviews de de door betrokkenen ervaren Wpg-gerelateerde knelpunten bij de uitvoering van politietaken in beeld gebracht.

In dit hoofdstuk vatten we het totaalbeeld aan knelpunten rond de naleving van de Wpg kort samen (paragraaf 10.2) en gaan we in op de factoren die deze knelpunten kunnen verklaren. We maken daarbij een onderscheid in vier clusters van factoren:

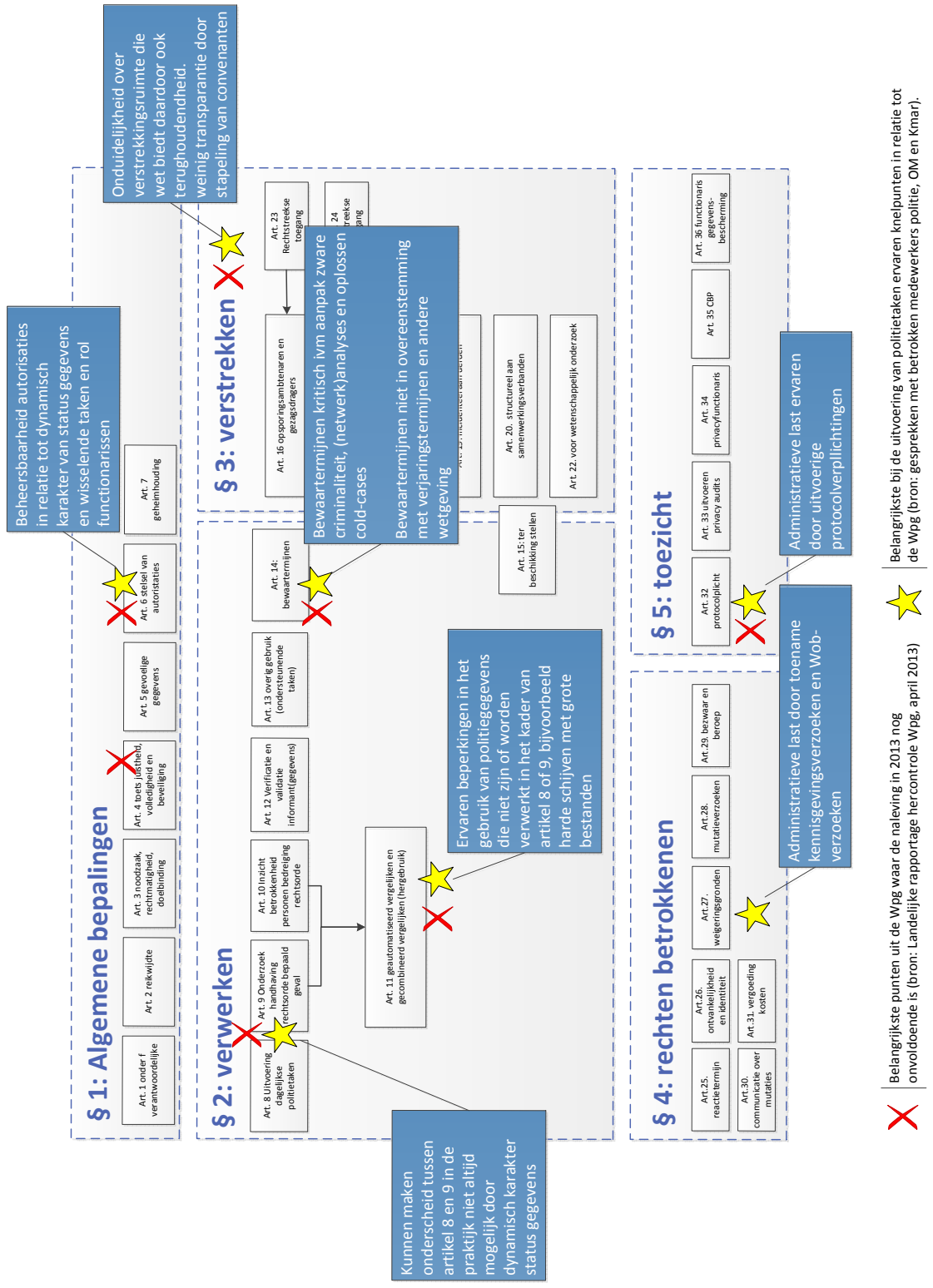
- Vertreksituatie politieorganisatie in 2008 (paragraaf 10.2)
- De gevolgde implementatiestrategie (paragraaf 10.3)
- De wettelijke kaders (paragraaf 10.4)
- Omgevingsfactoren (paragraaf 10.5)

In paragraaf 10.6 wordt het geheel aan mogelijke verklaringen samengevat.

10.2 Samengevat beeld knelpunten

In de vorige hoofdstukken is de praktijk van de uitvoering van de Wpg geschetst. Daarbij is zowel ingegaan op de vraag of de naleving (op papier) voldoende is geborgd als op de knelpunten die door de betrokken organisaties zelf worden ervaren. Het algemene beeld is er een van een worstelende praktijk. Samengevat hebben de audtis laten zien dat de naleving eind 2011, bijna vier jaar na het in werking treden van de wet, vooral hiaten vertoonde bij het onderscheiden van de verschillende verwerkingsregimes, het hanteren van de juiste bewaartermijnen, de beveiliging van gegevens, het regelen van de autorisaties en het in de wet geformuleerde toezicht (toezichtrol privacyfunctionaris, protocollering en uitvoeren privacy-audits). Daarbij waren er wel aanzienlijke verschillen tussen de (voormalige) korpsen. Begin 2013 blijkt uit de volgende ronde audits dat er over de hele linie sprake is van verbetering en van een meer gestroomlijnde aanpak bij het borgen van de naleving. Toch zijn ook dan zaken als de beveiliging, de protocollering, het onderscheid in verwerking tussen artikel 8 en 9, de kaders voor verstrekkingen en het hanteren van de juiste bewaartermijnen nog niet volledig conform de eisen van de Wpg geborgd. Daarbij moet overigens wel in acht worden genomen dat gedurende het onderzoek steeds meer verbeteringen zijn doorgevoerd en ook nog doorliepen op het moment van afronding van deze rapportage.

Figuur 10.1: Belangrijkste knelpunten in naleving van de Wpg en de belangrijkste ervaren knelpunten bij de uitvoering van politietaken in relatie tot de Wpg.



In grote lijnen blijken de onderdelen van de Wpg waar de naleving ook in 2013 nog onvoldoende is, tevens de onderdelen te zijn waar de praktijk knelpunten ervaart als het gaat om een effectieve en efficiënte uitvoering van de politietaken. De belangrijkste ervaren knelpunten zijn:

- De complexiteit van de (interpretatie van de) wet.
- Het niet goed aansluiten van de (statische) structuur van de wet (zoals onderscheid artikel 8 en 9) bij de uitvoeringsprocessen en de dynamische status van gegevens.
- De administratieve last rond protocollering, statusverandering van gegevens, het beheer van autorisaties en de afwikkeling van verzoeken om kennisnemingen.
- De vaak nog heersende onduidelijkheid over de mate waarin en de condities waaronder gegevens mogen worden verstrekt aan derden, vooral bij de uitvoering van dagelijkse politietaken en in samenwerkingsverbanden.
- Het door de bewaartermijnen (dreigend) verlies aan informatiepositie bij de aanpak van zware criminaliteit en tot op zekere hoogte het oplossen van cold-cases.
- De onvoldoende aansluiting tussen Wpg en andere wettelijke regelingen en het in één of samenhangende werkprocessen te maken hebben met meerdere wetten.

In de volgende paragrafen gaan we nader in op de verklaringen voor de knelpunten bij de implementatie en naleving van de Wpg. Bij de analyse van verklarende factoren is gebruik gemaakt van de interviews en de expertmeeting met betrokkenen (zie bijlagen 2 en 3). Daarnaast is bestaande literatuur geraadpleegd.

10.3 Vertreksituatie politieorganisatie 2008

Gevoelde noodzaak: van 'moetje' naar eigenbelang

Een eerste verklaring voor de gesignaleerde knelpunten is aanvankelijk het bij de politie grotendeels ontbreken van een gevoelde noodzaak voor invoering van de Wpg.

'Moetje'

Ook vóór de inwerkingtreding van de Wpg in 2008 golden er op basis van de Wpolr regels voor het gebruik van politiegegevens. In de politiepraktijk speelde de Wpolr echter slechts een beperkte rol; er werd nauwelijks naar gehandeld. Alhoewel feitelijk niet juist, was (en deels is) het algemene beeld van de Wpg dat van een wet die in vergelijking met de Wpolr vooral (extra) beperkingen oplegt. Vanuit het perspectief van de politieorganisatie (medewerkers en korpsleidingen) waren nut en noodzaak voor de (implementatie van de) wet zeer beperkt. Door de autonomie van de korpsen en het ontbreken van externe druk (politiek, organisatorisch, maatschappelijk, bijvoorbeeld als gevolg van incidenten) werd de wet gezien als een 'moetje' en waren er voor de politie geen duidelijke prikkels om tot systematische invoering en uitvoering van de wet over te gaan. Die houding was niet

zozeer gericht tegen het belang van de bescherming van informationele privacy, maar tegen de wijze waarop die (meer bedrijfsmatig) geborgd zou moeten worden.

Strategisch belang

Dit veranderde met de uitvoering van de externe audits in 2011 en de publiciteit die er ontstond, mede doordat de rapportages via een Wob-procedure openbaar werden. Hieruit ontstond het beeld dat de politie de privacywetgeving niet naleeft en leken integriteit en geloofwaardigheid van de politie onder druk te komen. Dit speelde ten tijde dat de organisatie van de Nationale politie in de steigers werd gezet.

In de aanloop naar die Nationale politie per 1 januari 2013 kregen de politiekorpsen de opdracht alle zeilen bij te zetten om ervoor te zorgen dat in de loop van 2013 wel zou worden voldaan aan de eisen van de wet, oftewel dat de (nieuwe) politie-eenheden met goed gevolg uit de (vervolg)audits zouden komen. Van een 'bureaucratisch moetje' wordt het naleven van de Wpg van strategisch belang voor het imago van de politie.

Tactisch en operationeel belang

Parallel aan het proces van verbetering van de naleving van de Wpg neemt binnen de politie ook het bewustzijn van het inhoudelijke en bedrijfsmatige belang voor de organisatie toe.[172] Inhoudelijk ziet de politie dat het niet goed in acht nemen van de privacyregels een probleem kan vormen in de procesgang : een zaak zou kunnen stuklopen bij de rechter omdat er onrechtmatig verkregen gegevens zijn gebruikt. Het bedrijfsmatige belang zit erin dat het niet goed organiseren van de privacyregels veel extra werk met zich mee kan brengen, bijvoorbeeld omdat uit verzoeken om kennisneming blijkt dat gegevens niet kloppen en gecorrigeerd moeten worden. Ook wordt het belang van het zorgvuldig omgaan met politiegegevens duidelijker met de intensivering van de samenwerking met andere instanties (bestuur, fiscus, RIEC's etc.).

Privacycultuur: 'dat regelen we zelf wel'

Onder de Wpolr was grotendeels sprake van een praktijk van verstrekken naar eigen inzicht.[173] Daarbij werd erop vertrouwd dat de mores van de organisatie en medewerkers (geheimhoudingsplicht, 'lekken is vertrekken' en professionaliteit) voldoende waarborgen boden voor de informationele privacy van de burger. Er was weinig behoefte aan toezicht op de politieorganisatie (door bijvoorbeeld het CBP). Het uitgangspunt was 'dat lossen we zelf wel op' (op korpsniveau). Dat gold zowel voor de medewerkers als voor de leiding.

---

[172] Nationale Politie (2013), Landelijk projectplan 2.0, Implementatie Wet Politiegegevens 2013/2015, p.5 e.v.

[173] Daarbij geldt een zeker onderscheid tussen de privacy van de burger in het algemeen en die van de verdachte/veroordeelde: 'het recht op privacy is verspeeld door de privacy van anderen (ernstig) te schaden'. In de organisatie zijn er twee 'subculturen' als het gaat om het verstrekken van informatie. Enerzijds een relatieve geslotenheid bij de recherche (zo min mogelijk informatie delen, ook intern) en anderzijds een relatieve openheid bij het blauw, in het bijzonder de wijkagenten (in vertrouwen breed delen van informatie met collega's en partners).

Naast een kanteling in het denken en gebruiken van politiegegevens (van register naar verwerking) vraagt de Wpg in vergelijking met de Wpolr om een meer transparante en meer systematische borging van informationele privacy. Vooral door agenten die belast zijn met de uitvoering van dagelijkse politietaken werd een omschakeling gevraagd van 'professionele borging van informationele privacy' (kennis, competenties en vaardigheden medewerkers) naar 'bedrijfsmatige borging (planning & control in de organisatie) van informationele privacy'.

Met de Wpg werd de professionele ruimte van de politiemedewerker gestructureerd in termen van autorisaties (welke gegevens mag je verwerken?) en protocolplicht (registreren wat je doet). Dit staat in zekere zin haaks op de - in 2008 nog gangbare - cultuur waarbij de politiefunctionaris een grote professionele bewegings- en afwegingsruimte had als het gaat om het gebruik van politiegegevens. De Wpg vraagt dus van de politieorganisatie niet alleen een meer bedrijfsmatige benadering maar ook een cultuurverandering. Dat de Wpg ook een aantal (interne) organisatie-eisen voor de politie bevat (protocollering, autorisaties, audits, privacyfunctionarissen, etc.) doet vermoeden dat de wetgever er niet helemaal gerust op was dat dat vanzelf van de grond zou komen.

Organisatiestructuur: 'archipel-organisatie'

De politieorganisatie bestond bij de inwerkingtreding van de Wpg in 2008 uit 26 hiërarchisch en functioneel min of meer autonome organisaties. De verantwoordelijkheid voor de (wijze van) implementatie van de Wpg lag bij de afzonderlijke korpsbeheerders en korpschefs. De korpsen verschilden in organisatiekenmerken en fase van organisatieontwikkeling. Daarbij ging het onder meer om:

- Grootte (formatie)
- Opbouw (functies, specialismen, taakaccenten etc.)
- Beschrijving werkprocessen (zijn deze beschreven? Hoe ingericht?)
- Wijze van aansturing (besturingsmodel, besturingsstijl)
- Interne organisatiestructuur
- ICT en (technische) hulpmiddelen
- Werkwijzen bij samenwerking met partners
- Personeelsopbouw en functieboeken
- Wijze van kwaliteitsborging, ook in relatie tot informationele privacy

Dit betekent dat in 2008 sprake was van (zeer) uiteenlopende startcondities voor de Wpg, zowel wat betreft de stappen die moesten worden gezet om 'Wpg-proof' te worden als in de vorm waarin de invoering van de Wpg (redelijkerwijs) kon worden gegoten. Door de feitelijke autonomie van de korpsen ontbrak het in deze structuur aan mogelijkheden en instrumenten om naleving van de wet af te kunnen afdwingen.

Zeker zo belangrijk is dat de relatieve autonomie ook heeft geleid tot uiteenlopende interpretaties van de wet, bijvoorbeeld als het gaat om 'geautomatiseerd vergelijken' (is zoeken ook geautomatiseerd vergelijken?) of 'verstrekken' (wanneer valt casusgerichte bespreking met derden in kader pré-onderzoeksfase daaronder?).

Met de vorming van de Nationale politie wilde de wetgever de slagkracht en doelmatigheid van de politie vergroten. Daar hoort in de opvatting van het Kabinet ook een sterke centrale aansturing bij. Voor de Wpg betekende dat in elk geval dat er centrale doorzettingsmacht aanwezig zou zijn én dat meegelift zou worden op de algehele stroomlijning van onder meer werkprocessen en ICT. Een aantal barrières waarmee de invoering van de Wpg te maken had, werden met de vorming van de Nationale politie (in elk geval op papier) weggenomen door een meer centrale aansturing en doorzettingsmacht en een algehele harmonisatie van organisatiecondities. Het laatste houdt wel in dat de kaders en uitvoering van de Wpg moesten aansluiten bij de verdere inrichting van de Nationale politie, bijvoorbeeld als het gaat om het regelen van autorisaties (aansluiting nieuwe functie/taakprofielen, ICT), verstrekkingen en protocollering (inrichting werkprocessen).

ICT: gefragmenteerd, te laat en niet toegesneden op Wpg

Bij de voorbereiding en invoering van de Wpg was het aanvankelijke uitgangspunt dat de politie (spoedig) zou beschikken over één (nieuw) ICT-systeem (Politie Suite). De wetgever erkende dat dit bij het in werking treden van de Wpg nog niet gerealiseerd zou zijn en er nog enige tijdelijke voorzieningen nodig zouden zijn.

Het ene ICT-systeem is er tot op heden niet gekomen. Op zichzelf staat de Wpg los van de technische voorzieningen. Toch is de operationele inrichting van de ICT een belangrijke barrière geweest voor de naleving van de Wpg. Meer specifiek gaat het om de volgende punten.

- Er was en is sprake van een gefragmenteerde en deels verouderde ICT. Er zijn hulpstructuren en applicaties nodig om politiegegevens te verwerken, bijvoorbeeld om beeld- en geluidsmateriaal te verwerken. Bij de verwerking van politiegegevens en protocollering moeten er meerdere systemen/applicaties worden opgestart (basisregistratie in BVH/BVO, protocollering i90, zaakinformatie op server en/of overige applicaties). Daarbij moet informatie soms meermaals worden ingevoerd omdat kopieermogelijkheden beperkt zijn. Dit compliceert zowel technisch, organisatorisch als intrinsiek de invoering.
- Belangrijke ICT-systemen bij de politie zijn BVH (Basisvoorziening Handhaving) en BVO (Basisvoorziening Opsporing). In de praktijk wordt vaak het onderscheid gehanteerd dat artikel 8 van de Wpg betrekking heeft op BVH en artikel 9 op BVO.

Dit onderscheid is echter niet altijd scherp te maken (BVH kan gegevens bevatten die in het kader van artikel-9 worden verwerkt en BVO gegevens die relevant zijn voor de uitvoering van dagelijkse politietaken). Bovendien is informatie niet statisch: het kan van handhavingsinformatie veranderen in opsporingsinformatie. De labeling van gegevens conform de Wpg is echter niet mogelijk, waardoor er bijvoorbeeld problemen kunnen ontstaan met het hanteren van de bewaartermijnen.

- De toegankelijkheid van de systemen (gebruiksgemak) werd (en wordt) als verre van optimaal ervaren.

Het naleven van de Wpg moet niet onmogelijk worden geacht in deze omstandigheden, maar is desondanks een barrière. Los van de fricties in tijdbesteding en mogelijk optimaal gebruik van politiegegevens, was (en is) de ICT en de inrichting daarvan (mede in relatie tot de vastgelegde werkprocessen) wel een extra voedingsbodem voor weerstand tegen de Wpg. Dat staat echter los van de Wpg zelf.

10.4 De gevolgde implementatiestrategie

De verantwoordelijkheid voor de implementatie van de Wpg lag in 2008 bij de korpsbeheerders en korpschefs. Voor de ondersteuning van de implementatie van de Wpg is een landelijke projectorganisatie opgezet die de invoering moest faciliteren door het opstellen van handreikingen en kaders voor de invoering en het verzorgen van (algemene) voorlichting. De organisatie van de implementatie per korps was aan de korpschefs.

De implementatie van de Wpg in de korpsen is vanuit de landelijke projectorganisatie en (voor zover aanwezig) de privacyfunctionarissen stevig aangezet. Daarvoor was –ceen unicum bij het invoeren van nieuwe wetgeving gericht op de politie – een landelijk projectbudget beschikbaar gesteld door het ministerie van Binnenlandse Zaken (€ 6,8 miljoen voor een periode van drie jaar, gemiddeld ongeveer € 250.000 per korps). Dit is onder meer ingezet voor onderzoek, communicatie, systeemontwikkeling (tijdelijke voorzieningen), opleiding (waaronder e-learning) en modelontwikkeling. Feitelijk werd een deel van de landelijke projectcapaciteit ook ingezet om de implementatie bij de korpsen direct te ondersteunen.

Hiermee leek te zijn voldaan aan belangrijke voorwaarden om tot een succesvolle implementatie te komen. Dat deze toch maar moeizaam van de grond is gekomen, kan worden teruggevoerd op de volgende factoren.

Wpg als vertrekpunt, niet de primaire processen en professionals

Bij de landelijke aanpak is gekozen voor een min of meer centrale interpretatie van de Wpg en een technisch-organisatorische vertaling naar de implementatie in de vorm van handreikingen en quickscans. Alhoewel de uitwerking inhoudelijk recht deed aan de Wpg en in zichzelf efficiënt was, heeft deze benadering onvoldoende oog gehad voor de benodigde cultuurverandering en de daarvoor essentiële steun van en focus bij de leiding. Door te kiezen voor een vertaling van de Wpg naar te nemen operationele maatregelen werd ook voor de leiding (korpsen, basiseenheden) de complexiteit van de Wpg mogelijk eerder vergroot dan dat de kern transparant werd gemaakt. Dit werd versterkt doordat het accent van de implementatie lag op de inrichting van de ondersteunende processen en organisatiecondities (registraties, protocollering, audits, autorisaties etc.) en niet of veel minder op de primaire processen en de rol van de professionals daarin: hoe voer je politietaken uit conform de Wpg? Hierdoor werd – ook bij de leiding – het beeld van een 'bureaucratieverhogende wet' versterkt. De actieve steun van de leiding voor de (implementatie van de) Wpg was en bleef daardoor beperkt.

Beperkt gezag en aanzien implementatieteams en privacyfunctionarissen

De invoering van de Wpg werd bij de meeste korpsen ondergebracht bij een implementatieteam (projectgroep) buiten de lijn, onder verantwoordelijkheid van bijvoorbeeld de regionale informatieorganisatie (RIO) en met een centrale rol van de privacyfunctionaris. De doorvertaling naar de werkvloer vond plaats op basis van instructie en voorlichting en niet op basis van inbedding in - en sturing op - de primaire processen.

De centrale rol die de privacyfunctionaris had, kon vaak maar ten dele worden waargemaakt. Deze had niet alleen de taak voorlichting te geven en te adviseren over de Wpg, maar ook erop toe te zien dat de uitvoering goed plaatsvindt. Daarnaast was (en is) de privacyfunctionaris vaak ook nog 'gewoon' korpsjurist. Dit betekent dat hij/zij ook andere taken heeft, zoals de behandeling van Wob-verzoeken, waardoor de effectieve tijd voor de implementatie beperkt was.

Eigen keuzes bij vertaling naar werkprocessen en ICT

Een belangrijk deel van de knelpunten bij de uitvoering is terug te voeren op de administratieve last die de Wpg met zich mee zou brengen. Dit geldt in het bijzonder voor het gebruik van de zogenaamde i90 formulieren. Ook het beheer van gegevens (zoals het verwijderen ervan) zorgt voor praktische en administratieve knelpunten. Dergelijke knelpunten vloeien echter niet zozeer voort uit de Wpg zelf, maar zijn een gevolg van de wijze waarop de politie haar werkprocessen en ICT heeft ingericht.

Kennis en draagvlak werkvloer onderbelicht

Gelet op de vertreksituatie (informationele privacy geen 'hot item', organisatiestructuur, ontbreken eigen motief, ICT nog groot knelpunt) was er weerstand tegen de invoering van de Wpg te verwachten. Ook de wetgever wijst hier (indirect) op door in de Memorie van Toelichting aan te geven dat scholing nodig is vanwege de andere manier van denken en werken en dat een fasering bij de invoering aannemelijk is vanwege de (nieuwe) complexiteit[174].

Onze indruk is dat deze gemankeerde uitgangssituatie (veel) te weinig aandacht heeft gekregen bij de implementatie. Daarbij kunnen, zo blijkt uit interviews, vraagtekens worden geplaatst of de kennis van bijvoorbeeld de wet- en regelgeving (zoals de Wpg en het Bpg) op peil is binnen een brede laag van de politie. De Wpg leeft niet op de werkvloer en wordt ingewikkeld geacht, zo blijkt uit vrijwel alle interviews. Daar blijkt ook uit dat de finesses van de wet bij slechts een relatief beperkte kring gebruikers bekend zijn. Uit interviews is gebleken dat een toets op de beheersing van de kennis en vaardigheden ook nu niet of nauwelijks plaatsvindt.

In het implementatietraject is er weinig tot geen aandacht geweest voor kennis en draagvlak op de werkvloer. De omslag in het denken die de wetgever veronderstelde is niet van de grond gekomen. Zonder steun van de leiding en inbedding in een bredere cultuurverandering, moest dit waarschijnlijk ook een lastig te realiseren ambitie worden geacht.

Risico's van focus op rule based audits

Het referentiekader voor een goede uitvoering van de Wpg wordt nu gevormd door de externe audits. De focus daarvan is 'conformiteit met de wet' (rule based). De operationalisering van de wettelijke bepalingen en het invulling geven 'wanneer het goed is' zijn echter ook interpretaties. Bovendien richten de audits zich vooral op meer formele en procedurele elementen van de wet (zijn de voorgeschreven organisatorische voorzieningen getroffen?) en minder op de naleving van de wet in de primaire werkprocessen. De audits zijn wel zeer sturend voor de wijze van implementatie van de politie op dit moment. Dit is enerzijds begrijpelijk, maar anderzijds vindt de implementatie derhalve nog steeds plaats vanuit een 'moeten' en wordt geen rekening gehouden met de meer brede en ingrijpende veranderingen door de vorming van de Nationale politie.

10.5 De wettelijke kaders

De basis voor de Wpg is gelegen in de Privacyrichtlijn, het data-protectieverdrag en in het standpunt van de wetgever dat de politie voor het gebruik van persoonsgegevens een

[174] TK 2005-2006, 30 327, nr. 3, MvT p.19

eigen wettelijk regime nodig heeft. Dat kan suggereren dat de opzet, inhoud en positionering van de Wpg de enig denkbare wijze is om informationele privacy bij gebruik van politiegegevens te borgen (en de uitvoering van de politietaken mogelijk te maken als het gaat om verwerking en verstrekking van politiegegevens). EU-lidstaten verschillen in insteek in bijvoorbeeld de grondslag (al dan niet een aparte wet gericht op de politie) en de lengte van bewaartermijnen, het verstrekkingenregime en de mate waarin wettelijk is vastgelegd hoe de interne organisatie moet worden ingericht.

De vraag is of de Wpg zelf heeft bijgedragen aan de moeizame implementatie en oorzaak is van knelpunten waar de praktijk tegenaan loopt, dus afgezien van de implementatie van de Wpg, ICT en werkprocessen bij de politie. Op basis van de interviews zien we de volgende verklaringen in de Wpg zelf.

Begrippen

De wetgever hanteert in de Wpg zogenaamde open normen, normen met een globaal geformuleerde doelstelling of globaal geformuleerde gedragsvoorschriften die de normadressaat, degene tot wie een wettelijk voorschrift zich richt, ruimte laat om zelf te bepalen op welke wijze het doel wordt gerealiseerd en of aan de gedragsvoorschriften wordt voldaan.[175] Naast het bepaalde in artikel 3 lid 1, op grond waarvan politiegegevens alleen mogen worden verwerkt als dat *noodzakelijk* is voor de bij of krachtens de Wpg geformuleerde doeleinden, gaat het bijvoorbeeld om de bepaling dat politiegegevens *toereikend, terzake dienend* en *niet bovenmatig* mogen zijn. Ook kan gewezen worden op artikel 20 Wpg waarin wordt gesproken van een *zwaarwegend algemeen belang*. Deze normen blijken in de praktijk soms moeilijk hanteerbaar te zijn.[176] De geïnterviewden geven aan dat het lastig is de normen in concrete situaties in te vullen.

In de Wpg staat daarnaast een aantal begrippen centraal die nader moesten worden ingevuld bij de toepassing van de wet. Het gaat onder meer om begrippen als 'verwerking', 'geautomatiseerd vergelijken', 'doel onderzoek bereikt'. Dit levert nog steeds interpretatieproblemen en –verschillen op. Ook de memorie van toelichting is op punten als de bovenstaande niet steeds helder en toegespitst geformuleerd.

Overlap en frictie met andere wetten: wat voegt de Wpg toe?

De keuze voor een aparte privacywet voor de politie met een eigen normenkader leidt er onvermijdelijk toe dat er overlap en mogelijk frictie ontstaat met andere wetgeving. Dit geldt in het bijzonder voor het Wetboek van Strafvordering, de Archiefwet, de Wet justitiële en strafvorderlijke gegevens (allen bewaartermijnen), de Wet openbaarheid bestuur (recht

[175] Dorbeck-Jung e.a. 2005, p. 20
[176] Vergelijk ook het evaluatieonderzoek naar de Wbp.

op kennisneming), de Wet bescherming persoonsgegevens (regels voor verwerking en verstrekking) en de Politiewet 2012 (geheimhouding, verwerking gegevens, bescherming gegevens).

Focus op aantal organisatie-interne zaken

De Wpg regelt in feite drie domeinen als het gaat om politiegegevens:

- het 'interne gebruik'/free-flow: opslag, beheer, bewerken, inzien etc. binnen en tussen politie, Kmar, BOD-en en OM;
- de verstrekking aan derden (zoals gemeenten, zorginstellingen, RIEC's etc.);
- het toezicht.

Met het opnemen van organisatie-interne gedragsregels inzake autorisaties, protocollering, audits en toezicht lijkt de wetgever ook te hebben willen sturen op enige 'disciplinering' van de politieorganisatie. De vraag kan worden gesteld in hoeverre het vanuit de rol van de wetgever wenselijk is dat organisatie-interne eisen zijn geformuleerd in de Wpg. Om te beginnen straalt de Wpg daarmee – in elk geval in de ogen van politiemensen –een zeker wantrouwen uit naar de politie. Dit heeft bijgedragen aan het versterken van het beeld dat de Wpg voor de politie beperkender is dan de Wpolr. Verder ontneemt de Wpg in zekere zin de politie de eigen verantwoordelijkheid om de bescherming van persoonsgegevens voldoende te waarborgen in de eigen inrichting van de werkprocessen en organisatie: de wetgever schrijft niet alleen het resultaat (bescherming persoonsgegevens) maar ook de middelen voor. Door bijvoorbeeld wel expliciet de protocollering te noemen maar niet de rol en het belang van de eigen professionaliteit van de politie 'dwingt' de Wpg de organisatie in een besturingsmodel dat niet aansluit bij bijvoorbeeld het inrichtingsplan van de Nationale politie dat een duidelijk accent legt op de professionele afwegingsruimte. Het expliciet vastleggen van dergelijke inrichtingseisen sluit niet aan bij een organisatie die zich (periodiek) moet aanpassen aan veranderende omstandigheden.

Onderdelen structuur wet gaan uit van een geordende wereld

De de wet is gestructureerd aan de hand van verschillende politietaken: dagelijkse politietaken, gericht onderzoek, onderzoek bedreiging rechtsorde, etc. Hieraan zijn doelen, verwerking, autorisaties, protocollering, bewaar-/vernietigingstermijnen en verstrekkingenregimes (indirect) gekoppeld. Dit veronderstelt een redelijk 'geordende wereld' waarin het karakter, de context en betekenis van informatie en daarmee de status bij de uitvoering van politietaken een constante is. Bovendien wordt verondersteld dat bij de politie, KMar of BOD-en verwerkte gegevens exclusief aanwezig zijn bij deze organisaties.

In de praktijk verandert informatie (continu) van karakter, context, status en betekenis ('triviale' kentekenregistratie kan de sleutel zijn tot de oplossing van een complexe zaak). Bovendien kunnen inhoud en relevantie van gegevens van een persoon (of uit een dossier) van belang zijn voor de uitvoering van dagelijkse politietaken en weer andere gegevens van deze persoon in het kader van een onderzoek. Politiegegevens zijn daarmee niet eenduidig te plaatsen in artikel 8, 9 of 10. (Politie)gegevens zijn bovendien in toenemende mate van belang in de pre-onderzoeksfase: het opbouwen en behouden van een tactische informatiepositie, of het nu gaat om de wijkagent of de landelijke recherche en of het nu gaat om de politie (of Kmar of BOD) als zodanig of om de gezamenlijke informatiepositie in het kader van de samenwerking in RIEC-verband.

De structuur van de wet sluit daarmee niet altijd voldoende aan bij de feitelijke inhoud van het politiewerk, het netwerkkarakter van de politie en de samenwerking met partners.

Toepasselijkheid alle organisaties

De Wpg lijkt vooral voor de landelijke organisaties als de Kmar en de landelijke eenheid (recherche, DLIO) minder goed te passen. Het zwaartepunt op artikel 8 en 9-verwerkingen biedt in de praktijk te weinig ruimte voor terug-rechercheren, complexere netwerkanalyses en verwerking van informatie die uit het buitenland wordt verkregen.

Hoge (indirecte) toezichtdichtheid in wet

De Wpg kent op papier een hoge toezichtdichtheid, zowel intern (privacyfunctionaris, interne audits) als extern (CBP, DAD-audits). Enerzijds heeft dit bijgedragen aan het negatieve imago van de wet onder politiemensen en de bevestiging van een zekere 'afrekencultuur', anderzijds is het de vraag of een dergelijke stapeling effectief (draagt het bij tot een betere bescherming van de informationele privacy?) en doelmatig is (werkt het kostenverhogend zonder dat dit leidt tot meer bescherming?).

Het toezicht in de praktijk is daarentegen beperkt. Het interne toezicht komt nauwelijks van de grond. De privacyfunctionarissen komen er niet aan toe, onder meer omdat ze het al druk genoeg hebben met de adviserende rol die ze ook vervullen. Interne audits zijn vaak een 'moetje', waarbij vooral gelet wordt op de formele vereisten waaraan het korps (tegenwoordig eenheid) moet voldoen en niet op de feitelijke naleving van de wet op de werkvloer. Het externe toezicht door het CBP is ook vrij beperkt. Alleen de DAD-audits hebben wat teweeg gebracht wat betreft het toezicht, onder meer doordat deze na een Wob-verzoek openbaar zijn geraakt.

10.6 Omgevingsfactoren

De context waarbinnen politietaken worden uitgevoerd en politiegegevens worden verwerkt, is de afgelopen vijf tot tien jaar veranderd. Zowel maatschappelijk, technologisch als politiek/bestuurlijk. De eisen die worden gesteld aan de uitvoering van politietaken en de mogelijkheden die er zijn om (politie)gegevens te verwerken, zijn mee veranderd. Deze omgevingsfactoren verklaren mede de knelpunten waar de uitvoeringspraktijk tegenaan loopt en waarom de implementatie op een aantal onderdelen afwijkt van de wet.

Ontwikkelingen (aanpak) criminaliteit en openbare orde

Het karakter en het schaalniveau van criminaliteit veranderen, bijvoorbeeld door het openstellen van grenzen, door internationalisering en door technologische ontwikkelingen. Ook is er sprake van een zekere 'vermaatschappelijking' van criminaliteit: op zichzelf niet criminele burgers of ondernemers zijn (onbewust) verbonden met criminele organisaties of netwerken, bijvoorbeeld als het gaat om hennepteelt, mensenhandel of milieucriminaliteit.

Mede door de technologische ontwikkelingen nemen de aard en organisatie van criminaliteit andere vormen aan (meer netwerken dan hiërarchische structuren) en worden schaal en moment opgerekt. Dit stelt ook andere eisen aan de informatiepositie van politie en justitie bij de bestrijding van deze vormen van criminaliteit. Het biedt aan de andere kant ook nieuwe mogelijkheden. Bijvoorbeeld bij de verwerking en koppeling van grote hoeveelheden digitale informatie.

Dat betekent dat ook nieuwe technieken worden ingezet om bijvoorbeeld inzicht te krijgen in criminele netwerken en patronen. Daarbij is niet altijd sprake van een zeer gerichte verwerking maar van een continu proces (van monitoring). Met name het minder specifiek doelgerichte karakter van dit type verwerkingen én het feit dat het gaat om zeer grote hoeveelheden gegevens, staan mogelijk op gespannen voet met een werkbare uitvoering van de Wpg. De politie en het OM zijn op dit punt zoekende.

Social media en veranderende opvattingen over informationele privacy

In de samenleving heeft het gebruik van internet, smartphones en social media een enorme vlucht genomen. Persoonsgegevens worden 'met enig gemak' (vrijwillig) aan Facebook, Twitter of internetbedrijven toevertrouwd. De schatting is dat de gemiddelde Nederlander al snel in enkele honderden zo niet duizenden bestanden is geregistreerd[177].Het denken over (informationele) privacy is daarbij in beweging en de discussie rond het gebruik van internet en social media in zekere zin ambigu. Enerzijds wordt vrij internetverkeer (zonder controle of restricties van de overheid) geëist. Anderzijds wordt van de overheid een vergaande borging van de informationele privacy gevraagd.

[177] Consideratie, 2009, Onze digitale schaouw, Een verkennend onderzoek naar het aantal databeses waarin de gemiddelde Nederlander geregistreerd staat (in opdracht van het CBP).

De politie probeert in meerdere opzichten hierin mee te bewegen. Bijvoorbeeld door informatie van social media te gebruiken voor het 'veredelen' van politiegegevens of om netwerkanalyses te maken. Daarbij krijgen gegevens wel een andere status (politiegegeven) en worden eisen gesteld aan bijvoorbeeld protocollering bij doorverstrekking, ook al komen deze gegevens uit publieke bronnen.

De politie tast daarnaast zelf de mogelijkheden van een actief gebruik van social media af. Bijvoorbeeld door het verzenden van een Amber Alert of het twitteren van een foto van een geweldpleger. Het verspreiden (verstrekken) van (foto)materiaal door de politie is daarbij altijd extra gevoelig omdat dit maatschappelijk een blijvende annotatie van 'verdachte' met zich mee kan brengen voor de betrokkene, ook al blijkt hij of zij achteraf onschuldig .

De politie is zoekende naar de maatschappelijk en juridisch grenzen van het gebruik van social media en persoonsgegevens uit publieke bronnen, naar een antwoord op de vraag wat nut en noodzaak zijn én wat de bijbehorende etiquette is[178].

10.7 Samenvattende bevindingen

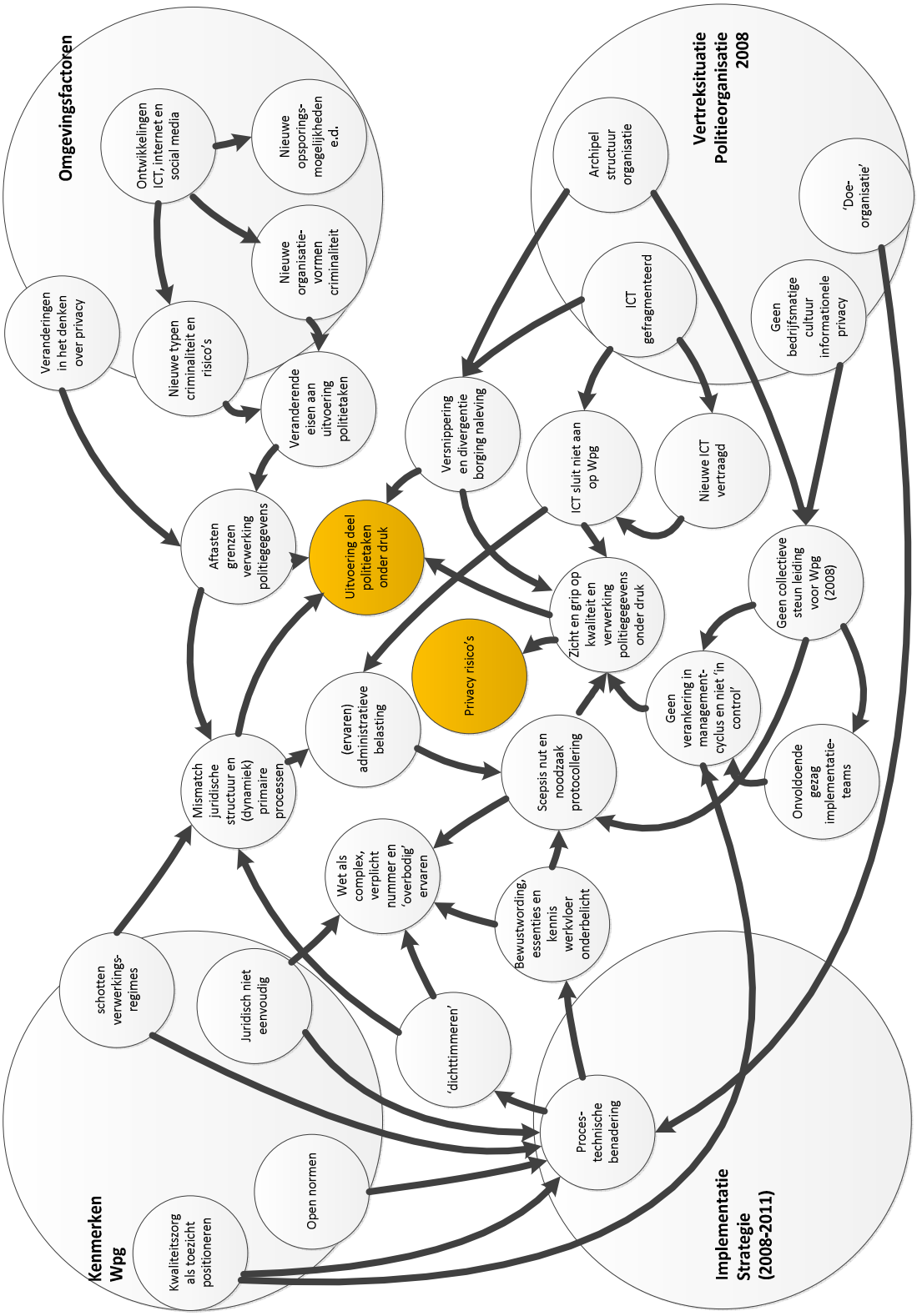
De implementatie van de Wpg is moeizaam van de grond gekomen. Alhoewel de naleving van de Wpg sinds 2011 is verbeterd, zijn er nog steeds knelpunten. De onderdelen van de Wpg waar de naleving het meeste problemen oplevert, zijn in grote lijnen ook onderdelen waar de praktijk in relatie tot de Wpg de meeste knelpunten ervaart bij de uitvoering van politietaken. Problemen met voldoende uitvoering en uitvoerbaarheid van de Wpg concentreren zich blijkbaar rond dezelfde zaken.

De belangrijkste verklaringen voor het moeizaam van de grond komen van de implementatie zijn deels gelegen in de Wpg zelf, deels in de organisatie van de politie als zodanig en deels in de wijze waarop de politie de implementatie heeft opgepakt.

Een belangrijke faalfactor was het ontbreken van een duidelijke (als zodanig door de politie ervaren) noodzaak om tot nieuwe privacywetgeving te komen toen de Wpg werd ontworpen en ingevoerd. Onder het regime van de Wpolr was (informationele) privacy in belangrijke mate een intern issue bij zowel de leiding als agenten en rechercheurs. Met de Wpg werd informationele privacy voor het eerst 'afrekenbaar' gemaakt door te sturen op borging in de organisatie en de bedrijfsprocessen.

[178] Zie bijvoorbeeld Steven de Smet, 2013, De Nieuwe Politie

Figuur 10.2: Indicatieve mindmap samenhang verklarende factoren knelpunten uitvoering Wpg



De implementatiestrategie sloot niet goed aan bij de startcondities waarmee de Wpg in de 26 korpsen te maken kreeg: het ontbreken van steun van de leiding, de heersende cultuur (in het bijzonder in het omgaan met informationele privacy) en de variëteit in inrichting van de afzonderlijke (min of meer autonome) korpsen. Er was wel een technische invoeringsstrategie maar geen duidelijke veranderstrategie. Dat de ICT versnipperd en nog weinig toegesneden was op de nieuwe wet heeft de invoering bemoeilijkt: er moesten hulpstructuren worden ontwikkeld die in combinatie met de interpretatie van de protocolplicht een zweem van bureaucratie opriepen, vooral bij de uitvoering van de dagelijkse politietaken. Vanuit de (landelijke) projectorganisatie en aansturing (korpsleiding) is het accent vooral gelegd op specifiek de invoering van de Wpg en niet op de bredere context van de benodigde cultuur- en organisatieverandering: een wet als de Wpg was (en is) alleen succesvol in te voeren als deze wordt ondersteund door een algehele stroomlijning en herinrichting van de werkprocessen (en de ICT) én aandacht voor het veranderingsproces. De politieorganisatie was wel doordrongen van het belang van (informationele) privacy maar onvoldoende van het belang van een meer bedrijfsmatige borging daarvan.

De inhoud van de Wpg heeft het proces daarbij op een aantal punten niet geholpen. De juridische structuur van de wet sluit niet overal goed aan bij (de dynamiek in) de werkprocessen bij de uitvoering van politietaken. Dit geldt vooral voor de inrichtingseisen bij verwerkingsregimes en op onderdelen de bewaartermijnen en de beheersbaarheid van bijvoorbeeld autorisaties en protocolleringen. Het plaatsen van (de instrumenten van) kwaliteitszorg onder de wettelijke titel van toezicht heeft in zekere zin het beeld van ‘verplicht nummer’ versterkt en deze instrumenten buiten de managementcyclus gehouden.

Een ander cluster van factoren dat de knelpunten kan verklaren betreft veranderingen in de context van de uitvoering van politietaken en informationele privacy. Het karakter van criminaliteit en de aanpak daarvan veranderen ook, zowel wat betreft de aard (zoals cybercrime), de verschijningsvorm (netwerken) als de schaal (internationalisering). Technologische ontwikkelingen spelen daarbij een grote rol. Diezelfde ICT maakt nieuwe opsporingsmethoden mogelijk waarvan de grenzen van wat kan, noodzakelijk en effectief is en maatschappelijke en juridisch acceptabel, op voorhand niet altijd bij voorbaat duidelijk zijn. Dit moet mede worden gezien in het licht van verschuivende panelen in de rol van en het omgaan met persoonsgegevens in de samenleving als geheel.

11 Beantwoording onderzoeksvragen

11.1 Inleiding

In de voorgaande hoofdstukken is beschreven wat de aannames zijn rond de (werking van de) Wpg, in welk mate de Wpg wordt nageleefd, waar de uitvoeringspraktijk tegenaan loopt en welke verklaringen er zijn voor de knelpunten. Daarnaast is specifiek stilgestaan bij de relatie tussen de Wpg en de Wob. In dit hoofdstuk geven we antwoord op de centrale onderzoeksvragen.

11.2 Onderzoeksvraag 1: Wat heeft de wetgever in 2008 beoogd met de Wpg?

1. Wat heeft de wetgever beoogd met de Wet politiegegevens (hoe ziet de beleidstheorie eruit)?

De eerste onderzoeksvraag behelst de reconstructie van de beleidstheorie van de Wpg, meer specifiek het geheel aan vooronderstellingen over de werking van de wet in de praktijk. De reconstructie heeft plaatsgevonden aan de hand van de (concept)wetteksten en besluiten, de memorie van toelichting, correspondentie rond de totstandkoming van de wet en enkele interviews met bij de totstandkoming van de wet betrokken personen.

a. Wat zijn de doelstellingen van de Wpg?

De Wpg heeft in de kern een tweeledige doelstelling. Enerzijds moet de wet voldoende ruimte scheppen voor de verwerking van persoonsgegevens met het oog op een effectieve en efficiënte uitvoering van politietaken. Anderzijds moet de wet de informationele privacy borgen van degenen waarvan gegevens worden verwerkt. Het uitgangspunt van de Wpg is een voldoende balans tussen deze twee hoofddoelstellingen. De wet probeert dat langs drie wegen te bereiken:

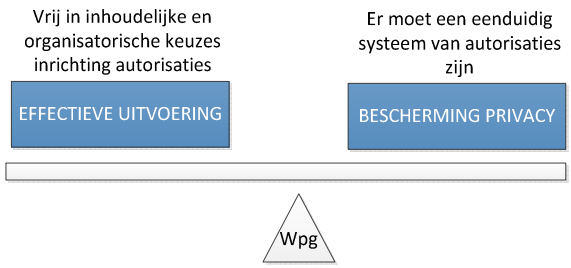
1. Een geconditioneerde verruiming ten opzichte van de Wpolr. Dat houdt in dat er meer mogelijk is maar dat er een qua verwerkings- en bewaartermijnen een onderscheid is gemaakt tussen de verschillende doelen binnen de politietaak.
2. Het stellen van organisatie-eisen qua autorisaties, protocollering en het uitvoeren van evaluaties en onderzoek, waarbij de organisatie in grote mate wordt vrij gelaten in de wijze hoe dit organisatorisch wordt ingevuld.
3. Het verplicht stellen van intern toezicht waarbij het externe toezicht terughoudender kan zijn naarmate de organisatie het interne toezicht beter heeft geregeld.

Daarnaast beoogt de Wpg harmonisatie van de privacyregelgeving te bewerkstelligen die geldt bij de uitvoering van politietaken met de algemene privacywetgeving, in het bijzonder de Wet bescherming persoonsgegevens. Een nevendoelstelling van de Wpg is het verminderen van de administratieve lasten die werden ervaren bij de Wet politieregisters.

b. Hoe zijn de doelstellingen en verwachtingen geformuleerd voor de volgende onderdelen:

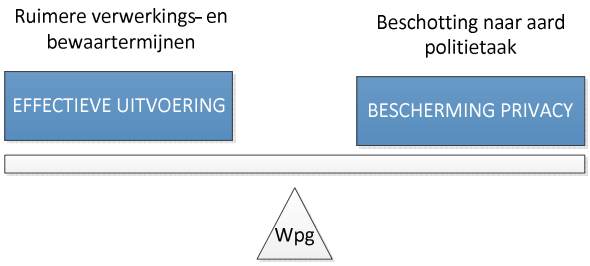
- *Autorisatie*
- *Verwerkings- en bewaartermijnen*
- *Verstrekkingen*
- *Kennisneming*
- *Toezicht*
- *Organisatorische waarborgen?*

Autorisaties verplicht, met ruimte voor wijze inrichting



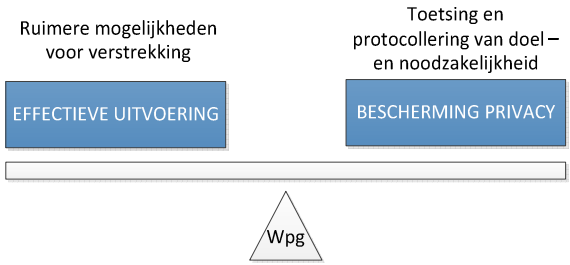
De autorisatieplicht heeft tot doel te waarborgen dat politiegegevens alleen worden verwerkt voor zover dat noodzakelijk is voor de uitvoering van de politietaak. Een systeem van autorisaties geeft de verantwoordelijke de mogelijkheid om deze noodzakelijkheid van bijvoorbeeld het raadplegen, wijzigen of verstrekken op persoonsniveau (taak/functieniveau) in goede banen te leiden (helderheid voor medewerker, inrichting ICT, aanknopingspunt voor toezicht). In de wijze waarop de verantwoordelijke de autorisaties inricht wordt deze grotendeels vrijgelaten.

Verwerkings- en bewaartermijnen afhankelijk van doel



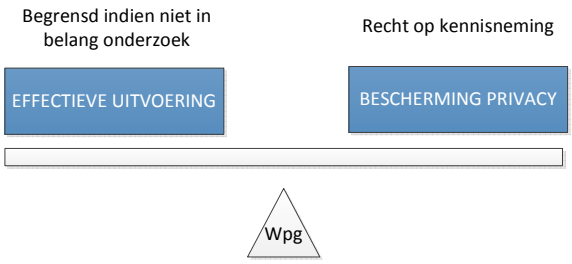
Met (gedifferentieerde) eisen aan verwerkingsdoeleinden en verwerkings- en bewaartermijnen beoogt de wetgever een werkbare balans tussen een voldoende lange termijn om politiegegevens (in)direct te kunnen verwerken en de borging van de informationele privacy. De Wpg stelt de periode waarbinnen gegevens mogen worden verwerkt en operationeel direct beschikbaar zijn afhankelijk van het doel van de verwerking.

Verstrekkingen verruimd onder conditie specificatie doel en protocollering



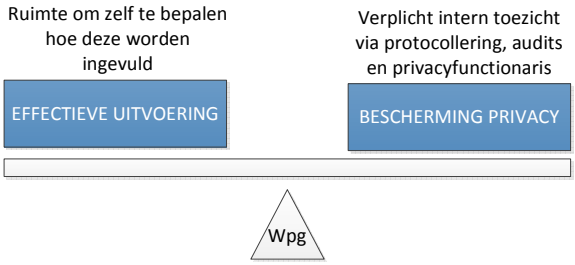
De mogelijkheden om politiegegevens aan derden te verstrekken zijn verruimd ten opzichte van de Wpolr. Dit geldt generiek voor verstrekkingen aan het OM, BOD-en, burgemeesters, inlichtingendiensten en politie en gezagsdragers op de BES-eilanden. Daarnaast biedt de wet de mogelijkheid om in het kader van samenwerking of specifieke omstandigheden tot verstrekking over te gaan. Daarbij moet door de verantwoordelijke specifiek worden vastgelegd wat doel en noodzaak van de verstrekking is. De feitelijke verstrekking moet daaraan worden getoetst en de verstrekking zelf moet worden geprotocolleerd.

Recht op kennisneming



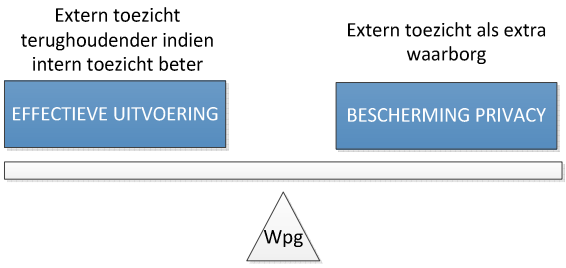
Het recht op kennisneming (op grond waarvan iemand inzicht kan krijgen in zijn eigen gegevens die door de politie verwerkt zijn) is enerzijds een belangrijk aspect van de rechtsbescherming omdat voor politiegegevens geen actieve informatieplicht geldt. Anderzijds verwacht de wetgever dat dit recht een prikkel voor de politieorganisatie is om zorgvuldig met politiegegevens om te gaan. Het recht op kennisneming is begrensd, namelijk daar waar kennisgeving strijdig is met de in artikel 27 Wpg opgesomde belangen.

Toezicht: preventieve prikkel en handvat voor correctie



De Wpg onderscheidt intern en extern toezicht. Dit is enerzijds gericht op toetsing of de organisatie conform de privacyregels werkt en anderzijds moet het toezicht de organisatie stimuleren tot meer bewustzijn en verbetering. Qua intern toezicht onderscheidt de Wpg twee instrumenten, te weten protocollering en monitoring/evaluatie en audits. Protocollering houdt in dat van bepaalde verwerkingen onder meer het doel en de noodzaak ervan worden vastgelegd. De functie van protocollering is controle op correcte verwerking, het kunnen traceren en corrigeren van gegevens die achteraf onjuist bleken te zijn en het bewustmaken van de organisatie en medewerkers. Monitoren/evalueren en auditen sluiten volgens de wetgever aan bij de (toen geldende) doelstelling van de politie om de kwaliteit

van de organisatie als geheel te borgen. In de wijze waarop de protocollering, monitoring, evaluatie en audits worden ingevuld, is de organisatie grotendeels vrij. Voor de privacy-audits geldt wel dat deze door een onafhankelijke auditor moeten worden uitgevoerd.



Het externe toezicht is belegd bij het CBP. Het CBP kan op grond van de Awb sanctiemiddelen (bestuursdwang, dwangsom, boete) inzet als de Wpg onvoldoende wordt nageleefd. De gedachte is dat het CBP terughoudender invulling geeft aan haar toezichtrol naarmate de politie beter invulling geeft aan het interne toezicht. Daarmee worden de administratieve lasten verlicht.

Organisatorische waarborg door kennis en capaciteit privacyfunctionaris

Om ervoor te zorgen dat er in de organisatie expliciet tijd en deskundigheid beschikbaar is voor de borging van de informationele privacy bij de verwerking en verstrekking van politiegegevens, moet de verantwoordelijke een privacyfunctionaris benoemen. Deze heeft de rol van adviseur van de verantwoordelijke. Dat gebeurt enerzijds door ondersteuning in het doorlopen van de managementcyclus als het gaat om monitoren, rapporteren en adviseren over de mate waarin de verwerking en verstrekking aan de kwaliteitseisen voldoet en anderzijds door het geven van voorlichting binnen de organisatie.

c. Welke verwachtingen waren er over de uitvoerbaarheid en mogelijke neveneffecten?

De wetgever heeft bij de uitwerking van de Wpg aansluiting gezocht bij de politiepraktijk. Daarmee werd beoogd dat de invoering van de wet zo weinig mogelijk belasting voor de politie met zich mee zou brengen. Daartoe maakt de wet onderscheid tussen de dagelijkse politietaak (‘blauw’) in artikel 8 en onderzoek (‘recherche’) in de artikelen 9, 10 en 11. Voorts was een aanname dat er (binnen afzienbare tijd na het in werking treden van de wet) één informatiesysteem zou komen voor de verwerking van politiegegevens.

Voor zover we dat hebben kunnen nagaan werden er geen specifieke neveneffecten verwacht. In een ex ante onderzoek dat in opdracht van het (toenmalige) ministerie van Justitie en het ministerie van BZK is uitgevoerd, werd geconstateerd dat de wet prima paste binnen de (te verwachten) ontwikkelingen op het vlak van ICT en de werkwijze van de politie, bijvoorbeeld als het gaat om informatie-gestuurde opsporing en datamining of specifieke vormen van criminaliteit (jeugdcriminaliteit, winkelcriminaliteit)[179].

[179] Rietveld c.s. 2004

11.3 Onderzoeksvraag 2: Hoe ziet de praktijk van de Wpg er uit?

2. *Hoe wordt de Wet politiegegevens in de praktijk uitgevoerd, is dit volgens de doelstellingen en de verwachtingen van de wetgever en wat zijn de resultaten en knelpunten?*

De tweede onderzoeksvraag richt zich op de praktijk, meer specifiek in hoeverre de Wpg wordt nageleefd en en tegen welke knelpunten in de praktijk wordt aangelopen (uitvoerbaarheid van de wet). Voor de beantwoording van het eerste deel van deze vraag is gebruik gemaakt van de audits die in 2011 (met een hercontrole in 2012/2013) zijn uitgevoerd door de Departementale Audit Dienst van het ministerie van Veiligheid en Justitie. Voor de beantwoording van de tweede vraag zijn gesprekken gevoerd met leidinggevenden, projectleiders, privacyfunctionarissen, agenten, rechercheurs, informatiebeheerders, analyses en overige medewerkers van twee territoriale eenheden van de politie, een landelijke eenheid van de Nationale politie en de KMar. Daarnaast zijn er (groeps)gesprekken gevoerd met diverse betrokkenen binnen en buiten de politie (zie bijlage 2).

a. In welke mate is de uitvoering van de Wpg conform de wettelijke kaders?
De korpsen zijn in 2011 geaudit. Op basis daarvan hebben de korpsen verbetertrajecten opgestart en heeft er eind 2012/begin 2013 een hercontrole plaatsgevonden. Uit de audits en hercontroles komt samengevat het volgende beeld naar voren over de stand van naleving van de Wpg.

Algemene bepalingen

In 2011 was volgens de auditoren sprake van een geringe borging van de beginselen zoals geformuleerd in de artikelen 3 (noodzaak, rechtmatigheid en doelbinding) en 4 (juistheid, volledigheid en beveiliging). Deze borging was wel beter geregeld naarmate de verwerking specifieker is. Als een van de verklaringen geven de auditoren dat de ICT-systemen de Wpg onvoldoende ondersteunen.

De autorisaties waren in 2011 niet goed geregeld. In 2013 is sprake van enige verbetering, onder meer door de ontwikkeling van landelijke standaarden en formats.

Volgens de auditoren voldeden de meeste korpsen in 2011 aan de eisen van de geheimhoudingsplicht, maar was de digitale en fysieke beveiliging van gegevens onvoldoende geborgd.

Verwerking

Eind 2011 voldeed een kleine 20% van de korpsen aan de in artikel 8 genoemde termijnen. Voor de beperkte naleving werd onder meer als verklaring gegeven het uitstel van de implementatie van BVH. Bij de hercontrole in 2013 was deze situatie niet wezenlijk veranderd. Zo is een afscherming van de gegevens na één jaar technisch niet mogelijk en kunnen gegevens onvoldoende worden gelabeld en gecodeerd om vervolgens automatisch tot verwijdering over te gaan. Zo bevat BVH ook artikel 9 gegevens, maar kunnen deze niet als zodanig worden gemarkeerd. Handmatige vernietiging gebeurt niet (systematisch) omdat dat veel tijd vergt.

Circa 10% van de korpsen voldeed eind 2011 aan de eisen van verwijdering en vernietiging van artikel 9 gegevens. Behalve vertraging in de implementatie van de ICT (BVO) werd veelal ook het niet ontvangen van afloopberichten van het OM genoemd. De helft van de korpsen voldeed wel (aantoonbaar) aan de eisen van doelbinding, noodzakelijkheid en rechtmatigheid bij de verwerking van artikel 9 gegevens[180]. Het beeld in 2013 is vergelijkbaar.

Meer dan de helft van de korpsen voldeed in 2011 aan de eisen voor het onderscheid tussen artikel 8 en artikel 9 bij de verwerking van politiegegevens[181]. Bij de hercontrole in 2013 was hierin enige verbetering[182].

De helft van de organisaties voldeed in 2011 aan de eisen van artikel 10[183]. Het beeld in 2013 is vergelijkbaar. Net als bij artikel 8 en 9 lopen de organisaties tegen technische problemen aan bij de vernietiging van artikel 10 gegevens[184].

Ongeveer twee derde van de korpsen beschikte in 2011 niet over duidelijke definities, instructies, regelingen e.d. voor geautomatiseerd vergelijken. Bij bijna een kwart van de korpsen was niet duidelijk wie verantwoordelijk was voor het geautomatiseerd vergelijken[185]. In 2013 is er enige verbetering. Er zijn landelijk definities vastgesteld maar deze zijn nog niet geïmplementeerd. Niet alle eenheden voldoen aan de eisen van protocollering.

[180] DAD audits, 2012.
[181] DAD audits, 2012.
[182] Landelijke rapportage hercontrole Wpg, 2013.
[183] DAD audits, 2012.
[184] Landelijke rapportage hercontrole Wpg, 2013.
[185] DAD audits, 2012.

Verstrekking

De landelijke verstrekkingenwijzer was in 2011 bij 85% van de korpsen ingevoerd. Afwijkingen waren er vooral door onbekendheid met deze verstrekkingenwijzer[186]. Ruim 60% van de korpsen beschikte ook over een regionaal verstrekkingenschema. In 2013 geldt dat voor alle eenheden[187].

Bijna 40% van de korpsen voldeed in 2011 aan de eisen die gelden voor het afsluiten van convenanten met het oog op verstrekkingen. In de meeste gevallen waren de processen wel omschreven, maar bleken niet alle bestaande convenanten getoetst te zijn aan de Wpg. Bij de hercontrole in 2013 bleek dat het proces voor afsluiten van convenanten en artikel 20 besluiten is beschreven bij de eenheden en dat wordt gewerkt aan de implementatie daarvan[188].

In 2011 voldeed bijna de helft van de korpsen niet aan de eisen die gelden voor geautomatiseerde verstrekkingen. Met name omdat de processen niet beschreven waren of dat niet inzichtelijk was welke gegevens automatisch werden verstrekt. In 2013 is het proces van geautomatiseerde verstrekking vastgelegd bij het Politiedienstencentrum (voorheen VtsPN).

Recht op kennisneming

In 2011 voldeed het merendeel van de korpsen aan de eisen voor het afwikkelen van verzoeken tot kennisname. Dit gold en geldt nog niet voor het afhandelen van (verzoeken om) correcties.

Toezicht

Bijna alle eenheden hebben de procedure voor de protocollering van het doel van het onderzoek van artikel 9 gegevens vastgesteld. Of die protocollering ook feitelijk gebeurt hebben de auditoren niet onderzocht. Voor de protocollering van artikel 11 gegevens en verstrekkingen zijn de eenheden in afwachting van een landelijk product. Voor de protocollering van artikel 13 verwerking gelden landelijke reglementen die nog niet bij alle eenheden zijn geïmplementeerd.

De interne auditfunctie (art. 33) was in 2011 niet (structureel) ingevuld. In 2013 is dit wel het geval. Ook hebben alle eenheden een privacyfunctionaris ingesteld en hebben deze functionarissen een jaarverslag opgeleverd. Een overzicht van protocolleringen is niet altijd aanwezig, ook in afwachting van het landelijk product. Het toezicht van leidinggevenden op de protocollering en autorisaties vindt volgens de auditoren nog niet voldoende plaats.

---

[186] (landelijke) handreiking bij afweging, aan wie en onder welke condities politiegegevens mogen worden verstrekt.
[187] Landelijke rapportage hercontrole Wpg, 2013.
[188] Landelijke rapportage hercontrole Wpg, 2013.

b. Welke knelpunten worden in de praktijk ervaren? Met name als het gaat om autorisaties, verwerking, bewaartermijnen, verstrekkingen, kennisneming, toezicht en organisatorische waarborgen?

Algemeen

De wet wordt als moeilijk te lezen en te interpreteren ervaren en daardoor ook als moeilijk te hanteren. Dit geldt onder meer voor het centrale begrip 'verwerken' (de wet gebruikt dit begrip zowel voor het beheer als het gebruik van politiegegevens) of bijvoorbeeld 'geautomatiseerd vergelijken' (is zoeken met query's of het geheel geautomatiseerd verwerken van bijvoorbeeld kentekenregistraties bij trajectcontroles ook geautomatiseerd vergelijken?). Hetzelfde geldt voor de verwerkings-, bewaar- en vernietigingstermijnen en wat wel en wat niet mag onder deze verwerkingsregimes. Ook is niet altijd duidelijk welke wet van toepassing is, onder meer als het gaat om het recht op kennisneming en de Wob of de bewaartermijnen uit de Wpg versus de eisen van de Archiefwet.

Verwerking

In zijn algemeenheid roept het begrip 'verwerken' nog de nodige vragen op, vooral wat betreft de afbakening. In artikel 1 van de Wpg wordt ook 'verzamelen' aangeduid als verwerken, maar dat is verder niet uitgewerkt in de wet. Ook het begrip 'verstrekken' valt onder 'verwerken', echter wordt dat nu juist weer afzonderlijk benoemd in de wet. Daarbij is in de uitvoering van politietaken de grens tussen 'verwerken' in de zin van 'gebruiken' niet altijd scherp te onderscheiden van 'verstrekken'.

Het onderscheid tussen artikel 8 en 9 wordt in de praktijk weinig praktisch en ook weinig zinvol gevonden. Het is niet altijd helder of een politietaak die wordt uitgevoerd in artikel 8 of 9 te plaatsen is. Bijvoorbeeld een straatroof. Gaat het om een 'heterdaad' dan valt dit onder artikel 8. Gaat het om een onderzoek terwijl de verdachte nog voortvluchtig is, gaat het om artikel 9. Bovendien kan de status van informatie veranderen, bijvoorbeeld als een slachtoffer van een verkeersongeluk een gezocht persoon blijkt te zijn. Het veranderen van de status van gegevens komt veel voor en is technisch gezien nog een knelpunt omdat de status van informatie niet in termen van de Wpg in de systemen te labelen is.

Een ander knelpunt zijn de verwerkings-, bewaar- en vernietigingstermijnen. Om te beginnen is er nog veel onduidelijkheid en spraakverwarring, en daardoor ook verschillend ingevulde praktijken rond deze termijnen. Dit is een van de punten van kritiek op de begrijpelijkheid van de wet.

Als belangrijkste inhoudelijke knelpunt wordt gezien het verlies aan informatiepositie door de (bij artikel 8 systematische) vernietiging van gegevens. Dat geldt zowel voor de

uitvoering van dagelijkse politietaken als voor cold-cases en grootschalig onderzoek/terug-rechercheren.

Verder is een inhoudelijk en organisatorisch knelpunt het bepalen van het moment waarop gegevens moeten worden verwijderd en wat de grondslag is voor het bepalen of gegevens niet vernietigd mogen worden. Dat is maatwerk en kost dus veel tijd en specifieke deskundigheid. Die is vaak niet voorhanden.
De systemen zijn niet goed ingericht op de Wpg. Dat kan betekenen dat artikel 9-gegevens in BVH automatisch worden verwijderd of vernietigd.

Het niet meer beschikbaar zijn van de onderliggende artikel 8 en 9-gegevens[189] kan een knelpunt zijn bij de artikel 10-verwerkingen. De onderliggende gegevens kunnen bijvoorbeeld nodig zijn om een informant te toetsen. Daarbij komt dat de capaciteit en ICT-ondersteuning ontbreekt om tot veredeling van deze gegevens te komen. Dit bemoeilijkt bijvoorbeeld het maken van netwerkanalyses. Een vermeend knelpunt is dat artikel 10-verwerkingen alleen door de CIE/RID mogen plaatsvinden. Dat is echter een onjuiste aanname en duidt op onvoldoende kennis van de Wpg.

Wat betreft het geautomatiseerd vergelijken en in combinatie verwerken is in de praktijk niet altijd duidelijk wat hieronder wordt verstaan casu quo wat het verschil tussen deze twee is. Door de digitalisering van informatievergaring, beheer en analyse, valt een handeling al snel onder geautomatiseerd vergelijken. Daarnaast worden er enkele lacunes ervaren. Specifiek geldt dat voor artikel 13 (bij grootschalig onderzoek, verwerken informatie van buitenlandse opsporingsinstanties, datamining, in beeld brengen van netwerken etc.).

Ook wordt de vraag opgeworpen of de Wpg wel voldoende is toegesneden op ontwikkelingen op het vlak van dataverwerking, analysemethoden en nieuwe vormen van criminaliteit. Er zijn soms grote hoeveelheden data (bijvoorbeeld door in beslag genomen harde schijven) beschikbaar op basis waarvan een gericht onderzoek wordt opgezet. Maar mogen de overige gegevens worden verwerkt als het onderzoek is afgesloten maar er nog onvoldoende zicht is op nut en haalbaarheid van het opstarten van een ander onderzoek aan de hand van de data? Ook hiervoor geldt dat het doel niet altijd is te benoemen.

Verstrekken

De verstrekking van politiegegevens in samenwerkingsverbanden is in zekere zin nog een zoektocht. Het wordt in de praktijk niet altijd helder gevonden wanneer je wat mag verstrekken en wanneer verstrekken begint. Zodra een onderzoek is gestart, is dat voor de

[189] Bijvoorbeeld doordat deze door het verstrijken van de bewaartermijn zijn vernietigd.

meesten wel helder, maar de verkenningsfase daarvoor is nog erg aftasten. De protocolleringseisen worden vooral in die fase als een administratieve last gezien.

Het hebben afgesloten van een convenant is bij verstrekkingen in samenwerkingsverbanden meestal het ijkpunt, maar biedt niet altijd soelaas. Bovendien is de praktijk door een stapeling van convenanten ook niet altijd transparant.

Juridisch wordt het vooral als een knelpunt ervaren dat de verschillende wettelijke kaders deels tegenstrijdig zijn en dat niet altijd helder is welk wettelijk kader van toepassing is op bijvoorbeeld gezamenlijk aangelegde bestanden. Dat geldt ook voor het toenemend aantal verstrekkingen aan private partijen als makelaars, (zorg)verzekeraars of advocaten.

De opkomst van social media en het nog steeds toenemende internetgebruik heeft ook gevolgen voor de informatiepositie van de politie en voor verstrekkingen. Hoe die (kunnen) uitpakken is nog niet duidelijk. Het verstrekken van politiegegevens, bijvoorbeeld via Twitter, levert zowel positieve als negatieve ervaringen op. De politie is op dat punt zoekende.

Uit de interviews komt naar voren dat een combinatie van voldoende bewustzijn van informationele privacy bij de uitvoering van politietaken, het professionele vermogen om een eigen afweging te kunnen maken binnen de kaders van bijvoorbeeld een convenant én een vertrouwensrelatie met degene aan wie wordt verstrekt, belangrijke succesfactoren zijn.

Kennisnemingen

De belangrijkste knelpunten die in de interviews naar voren worden gebracht rond kennisneming hebben vooral te maken met de samenloop met de Wob (zie onderzoeksvraag 4), de verzoeken om kennisneming als het gaat om CIE-gegevens en de bewerkelijkheid van het verwerken van verzoeken om kennisneming en de verschuivingen in motieven voor een verzoek om kennisneming (zoals rouwverwerking, verzekeringskwesties, advocatuur, makelaardij). Bij het laatste is de grens tussen kennisnemingsverzoek en verstrekkingsverzoek niet altijd even scherp en draagt het toenemend gebruik van het recht tot kennisneming tot een groot tijdsbeslag. Bij de verwerking van CIE-gegevens wordt het verzoek in het belang van de goede uitvoering van de politietaak in vrijwel alle gevallen afgewezen. Het toch moeten beoordelen en verwerken van deze verzoeken kost volgens de betrokkenen dus onnodig tijd.

Toezicht

In de interviews worden vooral de administratieve lasten en de focus van het toezicht als knelpunten ervaren. Het eerste vloeit vooral voort uit de eisen aan protocollering, vooral bij

verstrekkingen. Als oorzaken worden genoemd de toename van verstrekkingen (vooral in samenwerkingsverbanden), het niet inhoudelijk aansluiten van de (inrichting van de) werkprocessen en de ICT bij de eisen van de Wpg en het niet gebruiksvriendelijk zijn van de ICT. Ook is niet altijd duidelijk wanneer men precies moet protocolleren en wanneer het precies om een verstrekking gaat, als bedoeld in de Wpg.

De focus van de toezichtinstrumenten (protocollering, audits) wordt als zeer administratief ervaren en als een zeer letterlijke vertaling van de Wpg zonder dat de vraag wordt gesteld of dat nog bijdraagt aan meer informationele privacy en of dat past in de praktijk van de uitvoering van politietaken. In dat licht wordt het doorvoeren van de verbeterpunten naar aanleiding van de audits als tijdrovend ervaren zonder dat er de overtuiging is dat het veel bijdraagt aan de borging van de informationele privacy en/of een betere uitvoering van de politietaken.

Qua organisatie van het interne toezicht blijken privacyfunctionarissen maar beperkt aan toetsing van de uitvoering in de vorm van monitoring en evaluatie toe te komen. Advisering, zowel in het kader van de Wpg als meer algemene juridische advisering, neemt in de praktijk veel tijd in beslag. In vergelijkbare zin hebben de geïnterviewden aangegeven in de praktijk weinig te merken van toezicht door het CBP, anders dan de interventie in 2011 die heeft geleid tot het uitvoeren van privacy-audits.

Over het geheel wordt wel een stapeling van toezicht ervaren, deels in verhulde vorm. Alhoewel aan protocollering door de wetgever meerdere functies worden toegekend, domineert het beeld van controlemiddel. Dat geldt ook voor de audits (zijn eigenlijk managementinstrument om tot verbetering te komen) en het recht op kennisneming (is een vorm van toezicht door de betrokkene). Dit naast de meer traditionele toezichtvormen via het CBP of de eventuele functionaris gegevensbescherming.

c. Welke (onvoorziene) neveneffecten worden ervaren bij de uitvoering van politietaken?
De wetgever had mede op basis van onderzoek naar de uitvoerbaarheid van de wet en de (beperkte) reacties vanuit de politieorganisatie op de uiteindelijke concept-wet niet de verwachting dat de invoering bijzondere neveneffecten zou hebben. Wel realiseerde de wetgever zich dat er nog wel een 'kennis- en cultuuromslag' bij de politie nodig was, de veronderstelde landelijke informatievoorziening er bij het in werking treden van de wet niet zou zijn en dat de financiële implicaties bij het inwerking treden nog niet helemaal duidelijk waren. De wetgever gaf echter niet aan welk effect hij verwachtte als de omslag er niet zou komen en de financiële implicaties niet in beeld zouden worden gebracht.

Negatief imago Wpg terwijl doelen worden onderschreven

De wetgever heeft het negatieve imago van de Wpg zoals dat uit de interviews naar voren komt, niet voorzien. Dit kwam mogelijk doordat de achterliggende doelstellingen van de wet, verruiming van de mogelijkheden tot verwerking van politiegegevens en borging van de informationele privacy, breed onderschreven leken te zijn. Temeer daar de politie in de voorbereiding van de Wpg, behoudens de wens om het gebruik van persoonsgegevens door de politie in één wet te regelen, geen blijk heeft gegeven van grote kritiekpunten.

De wetgever heeft in de opzet van de wet een accent gelegd op de bedrijfsmatige borging van informationele privacy in de politieorganisatie. Dit gebeurde vanuit de veronderstelling dat dit paste bij de filosofie over management en kwaliteitszorg bij de politie. De wetgever heeft zich waarschijnlijk onvoldoende gerealiseerd dat de kloof tussen de bedrijfsmatige insteek van de Wpg en de politiepraktijk, zeker bij blauw, bij het in werking treden van de Wpg zeer groot was: het maken van individuele afwegingen binnen een algemene professionele mores (‘wie lekt vertrekt’) versus een borging van informationele privacy op basis van planning en control. Deze kloof was er niet alleen op de werkvloer maar ook bij het management. In de communicatie naar de organisatie en de inrichting van het implementatieproces is weinig aandacht besteed aan het overbruggen van deze kloof. In combinatie met een (zeer) gebrekkige kennis van de wet binnen de politieorganisatie en het voor de gemiddelde diender ondoorgrondelijke inhoud van de wet (ook experts binnen de politie kwalificeren de wet als moeilijk te begrijpen) ontstond al snel het beeld van een overbodige en bureaucratische wet. Daar komt bij dat de voorganger van de Wpg, de Wpolr, in de praktijk nauwelijks nageleefd werd. Waar de Wpg op papier ruimere mogelijkheden voor het verwerken van gegevens biedt, werd de wet in de praktijk gezien als meer belemmerend dan de Wpolr.

Groei samenwerkingsverbanden en hanteerbaar maken wet

De Wpg geeft nadrukkelijk meer ruimte voor het verstrekken van politiegegevens in het kader van de samenwerking met (bestuurlijke) partners. Artikel 18 en verder van de Wpg bieden daarvoor de grondslagen. Wat de wetgever niet heeft voorzien is dat het aantal samenwerkingsverbanden sterk zou toenemen, zeker als het gaat om de bestuurlijke partners bij de aanpak van georganiseerde criminaliteit (maar ook andere politietaken). Als de contacten intensief zijn, kan het aantal verstrekkingen groot zijn. Om te voorkomen dat er een ‘overload’ aan protocolleringen en daarmee administratieve lasten ontstaat, worden in de praktijk convenanten afgesloten waarin in algemene zin het doel en de noodzaak van verstrekkingen worden vastgelegd. Er geldt dan nog steeds een protocolleringsplicht, maar die kan dan eenvoudiger worden ingevuld onder verwijzing naar het convenant. Het aantal (incidentele) samenwerkingsverbanden is echter dusdanig groot dat ook dan nog sprake is van een stapeling van convenanten. De oplossing in de praktijk – het creëren van een

raamwerk in de vorm van een convenant - garandeert vooral meer professionele borging en niet zozeer een protocollaire borging.

Motieven bij gebruik van recht op kennisneming en administratieve lasten

De wetgever heeft niet voorzien dat het recht op kennisneming (en Wob-verzoeken) zou leiden tot een verhoging van de administratieve lasten.

Van het recht op kennisneming wordt in toenemende mate gebruik gemaakt. Ook het aantal Wob-verzoeken neemt toe. Dit houdt enerzijds een hogere administratieve last in. Dat verklaart bijvoorbeeld dat privacyfunctionarissen niet altijd aan hun eigenlijke taken (zoals toezicht), toekomen. Anderzijds wordt geconstateerd dat de indieners van een verzoek om kennisneming andere motieven hebben dan bedoeld in de Wpg, namelijk het bieden van rechtsbescherming tegen onjuiste of onrechtmatige (verwerking van) politiegegevens. Als afwijkende motieven zijn genoemd rouwverwerking, inzicht in lopende onderzoeken in de buurt en verlichting van een procesdossier.

11.4 Onderzoeksvraag 3: Welke verklaringen zijn er voor de knelpunten?

3. Wat zijn de verklaringen voor de uitvoerings- en uitvoerbaarheidsproblemen?

In deze paragraaf worden de belangrijkste verklaringen voor de onvoldoende naleving van de Wpg én de oorzaken van de knelpunten waar de praktijk tegenaan loopt, samengevat. We onderscheiden daarin vier clusters verklarende factoren:

- Verklaringen uit de vertreksituatie van de politieorganisatie in 2008
- Verklaringen uit de gevolgde implementatiestrategie
- Verklaringen uit de wettelijke kaders
- Verklaringen uit omgevingsfactoren

Verklaringen uit de organisatie van de politie

Het moeizaam van de grond komen van de implementatie en de uitvoeringsknelpunten die in de praktijk nog naar voren komen, zijn om te beginnen te verklaren uit een aantal kenmerken van de politieorganisatie. Samengevat zijn deze als volgt:

- *Geen gevoelde noodzaak:* Ook onder de Wpolr golden regels voor bijvoorbeeld protocollering en doelgerichte verwerking. In de praktijk was de borging daarvan vooral professioneel, dat wil zeggen aan de beoordeling van de betrokken medewerker. Voor de politieorganisatie en de uitvoering van politietaken verliep deze praktijk naar tevredenheid. De politieorganisatie was wel doordrongen van het belang van (informationele) privacy maar onvoldoende van het belang van een meer bedrijfsmatige borging daarvan. Met de Wpg werd informationele privacy voor

het eerst 'afrekenbaar' gemaakt door te sturen op borging in de organisatie en de bedrijfsprocessen. Mogelijk heeft de politie zich de implicaties van de Wpg onvoldoende gerealiseerd. Dit mede gelet op de beperkte kritiek op het (uiteindelijke) wetsontwerp. De noodzaak daarvan werd echter niet gevoeld en de Wpg werd daardoor al snel gezien als 'een moetje'. Mogelijk heeft de politie zich bij de totstandkoming van de wet ook onvoldoende gerealiseerd wat de implicaties zouden kunnen zijn van de Wpg voor de eigen organisatie. Dit mede gelet op de beperkte kritiek op het uiteindelijke wetsontwerp[190].

- *ICT-als barrière:* Bij de voorbereiding en invoering van de Wpg was het uitgangspunt dat de politie binnen afzienbare tijd zou kunnen beschikken over één ICT-systeem. Op zichzelf staat de Wpg los van de technische voorzieningen. Toch is de operationele inrichting van de ICT een belangrijke barrière geweest voor naleving van de Wpg. Meer specifiek gaat het om:
    - De fragmentatie en het verouderde karakter (zoals geen beeldmateriaal kunnen opslaan) waardoor veel hulpstructuren worden gebruikt.
    - Het niet als één datawarehouse kunnen functioneren van de Basisvoorziening Handhaving (BVH) en de Basisvoorziening Opsporing (BVO) waardoor het dynamisch karakter van de status van politiegegevens in technische zin beperkt werd (wordt).
    - De gebruikersvriendelijkheid stimuleert (in de ogen van medewerkers) het verrichten van administratieve handelingen zoals het protocolleren niet.

  Los van de fricties in tijdbesteding en mogelijk optimaal gebruik van politiegegevens, was (en is) de ICT en de inrichting daarvan (mede in relatie tot de vastgelegde werkprocessen) wel een extra voedingsbodem voor weerstand tegen de Wpg.

- *'Archipel-organisatie':* De politieorganisatie bestond bij de inwerkingtreding van de Wpg in 2008 uit 26 hiërarchisch en functioneel min of meer autonome organisaties. De korpsen verschilden in organisatiekenmerken (grootte, opbouw, wijze aansturing, ICT, etc.) en fase van organisatieontwikkeling. Dit betekent dat in 2008 sprake was van (zeer) uiteenlopende startcondities voor de Wpg, zowel wat betreft de stappen die moesten worden gezet om 'Wpg-proof' te worden als in de vorm waarin de invoering van de Wpg (redelijkerwijs) kon worden gegoten. Door de autonomie van de korpsen ontbrak het in deze structuur ook aan mogelijkheden en instrumenten om naleving van de wet te kunnen afdwingen. De relatieve

[190] De belangrijkste kritiek vanuit de politieorganisatie stamt uit 2004. Daarin werd een pleidooi gehouden voor één integrale wet voor het omgaan met persoonsgegevens door de politie.

autonomie heeft ook geleid tot uiteenlopende interpretaties van de wet, bijvoorbeeld als het gaat om 'geautomatiseerd vergelijken' (is zoeken ook geautomatiseerd vergelijken?) of 'verstrekken' (wanneer valt casusgerichte bespreking met derden in kader pré-onderzoeksfase daaronder?).

Verklaringen uit de wijze van implementatie

De implementatie van de Wpg werd stevig aangezet. Er was een landelijke projectorganisatie, regionale implementatieteams, een implementatiebudget, een uitvoerige impact-analyse van de wet voor de politie en op basis daarvan opgestelde formats, protocollen en instructievoorzieningen. De gekozen strategie heeft op de volgende punten bijgedragen aan het niet slagen van de implementatie:

- *Geen duidelijke veranderstrategie.* De focus van de implementatie lag vooral op de bedrijfstechnische vertaling van Wpg naar de werkprocessen en organisatie. Er was weinig oog voor kennis van de essentie van de Wpg, bewustwording (politiebelang) en draagvlak voor het omgaan met informationele privacy. Dit had tot gevolg dat het beeld van de Wpg als een 'bureaucratische en complexe wet' werd versterkt.

- *Focus op voldoen aan de wet, niet op inhoudelijk belang voor politie.* Door het negatieve imago wat de wet, het gebrek aan steun bij de leiding en de technische benadering kwam de implementatie niet van de grond. Externe druk (CBP, audits, Bits of Freedom) om tot adequate uitvoering te komen is daarvan het gevolg. De externe druk richt zich echter vooral op de formele naleving van de wet. Met een focus daarop bij de doorstart van de implementatie blijft de invoering van de wet voor de meeste medewerkers 'een moetje' en blijft de steun uit.

Verklaringen uit de Wpg

Uit de interviews komen de volgende zaken naar voren die knelpunten in de uitvoering met zich meebrachten:

- *Begrippen.* De interpretatie van begrippen als 'verwerking', 'geautomatiseerd vergelijken', 'doel onderzoek bereikt' levert nog steeds discussie of op zijn minst interpretatieverschillen op.

- *Overlap met andere wetgeving.* De keuze voor een aparte privacywet voor de politie met een eigen normenkader leidt er onvermijdelijk toe dat er overlap en mogelijk frictie ontstaat met andere wetgeving. Dit geldt in het bijzonder voor de Archiefwet (bewaartermijnen), de Wet strafvorderlijke justitiële gegevens (bewaartermijnen), de Wet openbaarheid bestuur (recht op kennisneming), de Wet

bescherming persoonsgegevens (regels voor verwerking/verstrekking) en de Politiewet (geheimhouding, verwerking gegevens, bescherming gegevens).

- *Zwaar accent op organisatie-eisen*. Met het opnemen van organisatie-interne eisen in de Wpg inzake autorisaties, protocollering, audits en toezicht lijkt de wetgever ook te hebben willen sturen op enige 'disciplinering' van de politieorganisatie. De Wpg straalt daarmee – in elk geval in de ogen van politiemensen – een zeker wantrouwen uit. Verder ontneemt de Wpg in zekere zin de politie de eigen verantwoordelijkheid om de informationele privacy voldoende te waarborgen door vooral te letten op 'conformiteit met de wet' zonder dat dit gepaard gaat met bewustwording. Het expliciet vastleggen van organisatie-eisen in de wet is boven niet praktisch met het oog op veranderende interne en externe omstandigheden.

- *Wpg gaat teveel uit van geordende wereld.* De wet is gestructureerd aan de hand van de verschillende politietaken: dagelijkse politietaken, gericht onderzoek, onderzoek bedreiging rechtsorde etc. Hieraan zijn doelen, verwerking, autorisaties, protocollering, bewaar/vernietigingstermijnen en verstrekkingenregimes (indirect) gekoppeld. Dit veronderstelt een redelijk 'geordende wereld' qua status en gebruik van informatie. In de praktijk verandert informatie (continu) van karakter, context, status en betekenis. Het onderscheid in artikel 8 en 9 is in de praktijk zowel op zaak, taak/functie als informatieniveau minder scherp te maken en minder statisch dan de Wpg veronderstelt.

- *Hoge toezichtdichtheid.* De Wpg kent op papier een hoge toezichtdichtheid, zowel intern (privacyfunctionaris, interne audits) als extern (CBP, DAD-audits). Enerzijds heeft dit bijgedragen aan het negatieve imago van de wet onder politiemensen en de bevestiging van een zekere 'afrekencultuur', anderzijds is het de vraag of een dergelijke stapeling effectief (draagt het bij tot een betere bescherming van de informationele privacy?) en doelmatig is (werkt het kostenverhogend zonder dat dit leidt tot meer bescherming?). Het bijzondere is bovendien dat instrumenten als protocollering, monitoring/evaluatie en audits in de noemer 'toezicht' in de wet zijn ondergebracht. De vraag is of dat de juiste adressering is van dergelijke managementinstrumenten en of je deze als managementinstrument in de wet moet opnemen. Neem als voorbeeld de protocollering: deze heeft een drieledig doel, namelijk achteraf kunnen controleren of verwerking juist heeft plaatsgevonden, basis om eventueel onjuiste verstrekte gegevens te kunnen traceren en meer bewustwording bij de medewerker. In de praktijk wordt protocollering vooral ervaren als toezicht en draagt de protocollering niet bij aan bewustwording.

Deze kenmerken van de Wpg verklaren mede waarom ook organisaties die wel actief hebben geïnvesteerd in de implementatie van de Wpg, tegen uitvoeringsproblemen aanlopen. Dit naast factoren die samenhangen met de algemene kenmerken van de organisatie en een aantal omgevingsfactoren (zie ook hieronder).

Verklaringen uit omgevingsfactoren

De context waarbinnen politietaken worden uitgevoerd en politiegegevens worden verwerkt, is de afgelopen vijf tot tien jaar veranderd, zowel maatschappelijk, technologisch als politiek/bestuurlijk. Dit leidt ertoe dat de eisen die worden gesteld aan de uitvoering van politietaken en de mogelijkheden die er zijn om (politie)gegevens te verwerken, ook veranderen.

- *Informatieaanbod creëert nieuwe vraag.* De informatiepositie die de politie opbouwt roept ook nieuwe informatie-vraag op: van burgers (diverse redenen voor kennisneming of Wob-verzoeken), de advocatuur, gemeenten (in het kader van de bestuurlijke aanpak) maar ook bedrijven (verzekeringsmaatschappijen, deurwaarders, etc.). Dit leidt in tot een hogere (administratieve) belasting.

- *Veranderende opvattingen over informationele privacy en de opkomst van social media.* Mede door de opkomst van sociale media, openbare bronnen, smartphones en de rol van de 'traditionele' media verschuiven de grenzen in denken en doen over informationele privacy. Bij de uitvoering van politietaken is nog niet duidelijk waar de grenzen liggen van bijvoorbeeld het actieve en passieve gebruik van social media en hoe zich dat verhoudt tot (de verschuivende grenzen in) het denken over informationele privacy en de wetgeving daarbij.

- *Veranderend karakter van criminaliteit en de aanpak daarvan,* zowel wat betreft de aard (zoals cybercrime), de verschijningsvorm (netwerken) als de schaal (internationalisering). Technologische ontwikkelingen spelen daarbij een grote rol. Nieuwe vormen van criminaliteit en/of inzet van ICT bij criminele activiteiten maken een goed informatiepositie van de politie steeds belangrijker. Diezelfde ICT biedt de politie ook nieuwe mogelijkheden om deze informatiepositie te bekleden. De grenzen tussen wat kan, wat nodig is en wat zou moeten mogen zijn daarbij nog niet scherp te trekken (en zullen waarschijnlijk in beweging blijven).

Deze omgevingsfactoren verklaren vooral dat de politie (en andere opsporingsdiensten) op zoek is naar de technische, maatschappelijke en juridische mogelijkheden en grenzen van de verwerking van politiegegevens. Dat betekent ook dat de vraag wordt gesteld hoe eisen die de omgeving stelt of de mogelijkheden die die omgeving biedt om politietaken uit te

voeren, zich verhouden tot de Wpg. Bijvoorbeeld als het gaat om het protocolleren van de verwerking van grote hoeveelheden data, de niet specifiek doelgerichte analyses (netwerkanalyses) of het onderscheid in verwerkingsregimes.

11.5 Onderzoeksvraag 4: Hoe verhoudt de Wpg zich tot andere wetten?

4. Hoe verhoudt de Wpg zich tot aanpalende wet- en regelgeving zoals de Wbp, de Wob en internationale wet- en regelgeving?

a. Hoe werd de Wpg in 2008 door de wetgever gepositioneerd ten opzichte van aanpalende wetten zoals de Wbp, de Wob en internationale wet- en regelgeving?

Naast de Wpg gelden er andere wetten waarin de verwerking van persoonsgegevens en de bescherming van de informationele privacy worden geregeld. Denk daarbij aan de Wet justitiële en strafvorderlijke gegevens (Wjsg), het Wetboek van strafvordering (Sv), de Wet op de Jeugdzorg (Wjz), het Burgerlijk wetboek (Bw), de Wet inzake de geneeskundige behandelingsovereenkomst (Wgbo) en de Wet Beroepen in de Individuele Gezondheidszorg (Wet BIG). Als specifieke wetgeving ontbreekt, is de Wet bescherming persoonsgegevens van toepassing. In de strafketen is er vooral samenloop tussen de Wpg, de Wjsg, de Sv en de Wbp.

De Wet openbaarheid bestuur (Wob) regelt de openbaarheid van informatie van de overheid. Het principe daarbij is dat geheimhouding uitzondering is en dat openbaarmaking een plicht is van een bestuursorgaan. Over de samenloop tussen de Wpg en de Wob is bij de totstandkoming van de Wpg niet gerept. Dit ondank een uitspraak van de Afdeling bestuursrechtsspraak van de Raad van State in 2006 dat de Wob van toepassing is op de (toenmalige) Wpolr als het niet om persoonsgegevens gaat. De wetten kennen dan ook geen samenloopbepalingen. In de Wob is in zijn algemeenheid wel vastgelegd dat geen informatie wordt verstrekt als het belang daarvan niet opweegt tegen het belang van opsporing en vervolging van strafbare feiten.

b. Hoe verhoudt de Wpg zich in de praktijk ten opzichte van andere wet- en regelgeving?

Als de politie samenwerkt met andere partners, gelden verschillende bijzondere wetten waarin specifieke regels zijn opgenomen over gegevensuitwisseling en geheimhouding. Samenwerkingspartners geven aan dat het interpreteren van de verschillende regelingen lastig is en dat knelpunten bestaan bij het bepalen welk regime op welke gegevens van toepassing is. Het feit dat op dezelfde gegevens meerdere wettelijke regelingen van

toepassing kunnen zijn, zorgt (met name bij het bepalen van de bewaartermijn) voor problemen.

De politie ervaart administratieve lasten bij de afhandeling van Wob-verzoeken en geeft aan dat lopende onderzoeken kunnen worden geschaad, door inwilliging van Wob-verzoeken. Om de lasten te verlagen wordt informatie actief openbaar gemaakt, maar daarnaast achten gesprekspartners een wetswijziging geboden.

12 Slotbeschouwing

12.1 Inleiding

In het voorgaande hoofdstuk zijn de onderzoeksvragen beantwoord. De belangrijkste conclusie is dat de knelpunten bij de uitvoering van de Wpg zijn terug te voeren op een samenstel van factoren die te maken hebben met de politieorganisatie als zodanig (structuur en privacy-cultuur in 2008, ICT), de wijze van implementatie, de structuur van de Wpg en externe ontwikkelingen. In dit hoofdstuk sluiten we het rapport af met een slotbeschouwing. We gaan daarbij achtereenvolgens in op de vraag hoe de uitkomsten moeten worden gezien in het licht van de (risico's voor de) privacy van betrokkenen (paragraaf 12.2) en de houdbaarheid van de beleidstheorie van de Wpg (paragraaf 12.3). Daarnaast gaan we in op de consequenties die uit het onderzoek kan hebben voor de wet zelf (paragraaf 12.4), de focus van de aanpak voor een betere naleving door de politie (paragraaf 12.5) en de bredere context van de naleving van de Wpg (paragraaf 12.6).

12.2 Aantasting privacy: geen structurele calamiteiten; wel incidenten en risico's

De achterliggende gedachte van de Wpg is dat de gestelde eisen een waarborg zijn tegen (risico's op) inbreuken op de informationele privacy en als mogelijk gevolg daarvan aantasting van de persoonlijke levenssfeer en schade.

Figuur 12.1: Achterliggende aannames relaties tussen onvoldoende naleving Wpg en risico's voor

Of schendingen ook daadwerkelijk hebben plaatsgevonden, was geen primair doel van het onderzoek. Er is wel indicatief gekeken of er signalen zijn dat er sprake is van schendingen en aantasting van de persoonlijke levenssfeer of schade. Daartoe is gekeken naar registraties van klachten en gesproken met de Nationale Ombudsman, het CBP en de Nederlandse Orde van Advocaten (NOVA).

Klachten privacy-schendingen politie

Om een beeld te krijgen van het aantal privacy-schendingen door de politie is van de afdeling Veiligheid, Integriteit en Klachten van de Korpsstaf cijfermateriaal ontvangen over het aantal zaken in 2011 en 2012 waarbij sprake was van het lekken van informatie e.d. In 2011 zijn 81 zaken aan de orde geweest over het lekken van informatie naar criminelen of anderen, het maken van misbruik van informatie of het informatiesysteem, het schenden van de geheimhoudingsplicht, het maken van misbruik van de positie. Uiteindelijk bleek in 10 zaken niet van plichtsverzuim. In 2012 ging het om 63 zaken, waarbij in 8 gevallen niet van plichtsverzuim is gebleken. Deze cijfers, die betrekking hebben op alle destijds bestaande regio's, moeten in perspectief worden geplaatst. Immers, bij de Nationale politie (de voormalige 25 regionale politiekorpsen, het KLPD en de VtsPN) werken ongeveer 63.000 medewerkers.

Het algemene beeld is dat er geen sprake is van systematische aantasting van de persoonlijke levenssfeer. Het aantal Wpg-gerelateerde klachten bij voorbeeld dat door de politie zelf en de Nationale Ombudsman ontvangen is, is in vergelijking met de totale hoeveelheid gegevens die worden verwerkt en in vergelijking met de overige klachten over de politie, (zeer) beperkt. De Nationale Ombudsman ontving in 2012 1350 klachten over de politie waarvan enkele tientallen betrekking hadden op politiegegevens.[191] De klachten gaan vooral over de wijze waarop de politie een kennisnemingsverzoek afwikkelt[192] en over het onjuist of onterecht aanwezig zijn van politiegegevens. Meer specifiek gaat het onder meer om:

- Onjuiste of onduidelijk gemarkeerde gegevens, bijvoorbeeld het veranderen van de status van 'verdacht' in 'niet-verdacht', het aanpassen van kenmerken als veranderde wetgeving daar aanleiding toe geeft[193].
- Gegevens die verwijderd hadden moeten worden vanwege overschrijding van de bewaartermijn.
- Onvoldoende onderbouwde gegevens, bijvoorbeeld vermelding in een systeem zonder dat onderliggende dossiers nog aanwezig zijn of een anonieme melding over een persoon waarvan de hardheid niet (meer) traceerbaar is.
- Het (ook intern) niet traceerbaar zijn of en aan wie eventueel onjuiste gegevens ter beschikking zijn gesteld of zijn verstrekt.

Dergelijke ruis heeft als risico voor betrokkenen dat onjuiste gegevens worden verstrekt aan derden of leiden tot onjuiste conclusies (en acties) van de politie. De Nationale Ombudsman, het CBP en de NOVA maken melding van patronen van incidenten waarbij sprake is van feitelijke (reputatie)schade die mensen ondervinden. Met de groeiende informatiestroom, de technieken om data te verwerken en de praktijk om gegevens te delen, is het volgens hen onvermijdelijk dat deze ruis toeneemt en daarmee de kans op een aantasting van de persoonlijke levenssfeer en schade voor betrokkenen. Daarbij hoeft geen sprake te zijn van het willens en wetens de wet (Wpg) overtreden, maar gaat het om 'collateral damage' van onvoldoende controle in het beheer van politiegegevens, zowel technisch (ICT) als bedrijfsmatig (werkprocessen en kwaliteitsborging). Daarnaast ontbreekt het volgens hen aan aandacht voor de corrigeerbaarheid van gegevens. Dat betekent dat – vanwege het veelvuldig delen van gegevens – ook traceerbaar moet zijn waar welke gegevens zijn opgeslagen en aan wie deze zijn verstrekt.

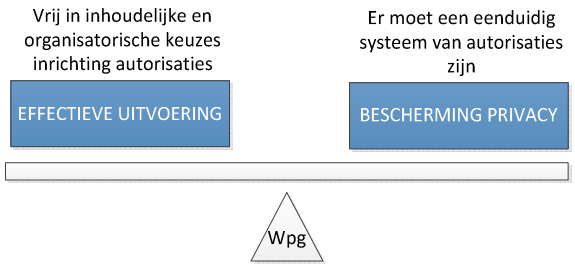
[191] Exacte aantallen kon de Nationale Ombudsman niet geven.
[192] Bijvoorbeeld over het onvolledig kennisgeven of over de vorm van kennisgeving (kopie stukken, inzage dossier, samenvatting, mondeling etc.)
[193] Bijvoorbeeld een veranderde definitie van het begrip 'verkrachting'.

12.3 Beleidstheorie in balans?

Het voorgaande roept de vraag op hoe valide de beleidstheorie van de Wpg was en in welke mate er met de wet een (voldoende) balans wordt bereikt tussen de doelstellingen van de wet. De beleidstheorie gaat ervan uit dat deze balans wordt bereikt door op de verschillende onderdelen condities te verbinden aan verruimingen van de mogelijkheden om politiegegevens te verwerken en ruimte te laten voor de invulling waar de wet direct eisen stelt aan het borgen van de informationele privacy.

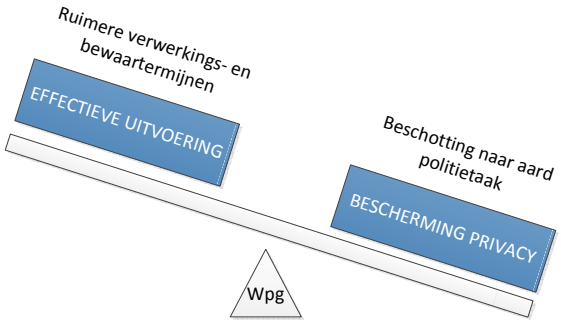
Een lastig punt bij de beoordeling hiervan is dat de Wpg in de praktijk onvolledig wordt nageleefd. Bij onvoldoende (poging tot) naleving is niet aan te geven waar de grenzen van de wet liggen. Om deze reden zijn voor de interviews organisaties gekozen die de borging van de naleving van de Wpg in 2011 al redelijk op orde hadden. Onze aanname was dat als deze organisaties nog tegen knelpunten aanlopen, dat kan worden geïnterpreteerd als mogelijke grenzen van de wet. Vanuit de analyse van de knelpunten en verklaringen daarvoor (hoofdstuk 10) komen we tot de volgende bevindingen als het gaat om balans in de Wpg.

Eisen aan autorisaties, kwaliteit en beveiliging met ruimte voor invulling



De Wpg eist borging van de kwaliteit en de (fysieke) veiligheid van politiegegevens en het vastleggen van autorisaties voor het hebben van toegang tot informatie. We zien dat de uitvoeringspraktijk op dit punt niet voldoet aan de eisen van de Wpg. Uit het onderzoek blijkt echter niet dat deze eisen belemmerend zijn voor de uitvoering van de politietaken. Op dit punt is de Wpg in balans. Het kunnen voldoen aan de eisen van autorisaties wordt wel bemoeilijkt door het onderscheid in verwerkingsregimes dat de Wpg maakt. Dit komt terug bij het volgende punt.

Ruimere maar geconditioneerde verwerking en bewaartermijnen

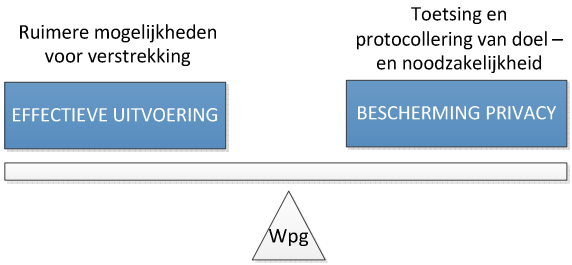


De Wpg kent ruimere verwerkings- en bewaartermijnen dan de Wpolr. Daarbij is een beschotting aangebracht in de verwerkingstermijnen, afhankelijk van het doel van de verwerking. De beschotting in de Wpg (zoals de artikelen 8 en 9 en bewaartermijnen) sluit niet goed aan bij (de ontwikkelingen in) de

werkprocessen bij de uitvoering van politietaken en het dynamische karakter van (het gebruik van) politiegegevens. De gestelde bewaartermijnen zijn in algemene zin werkbaar, maar houden voor specifieke typen zaken (met name zware criminaliteit en toepassing bij grootschalige analyses) het risico in zich dat de informatiepositie van de politie ondergraven wordt. In de Wpg zijn de eisen die worden gesteld aan de inrichting van de verschillende werkingsregimes en op enkele punten de bewaartermijnen niet in balans met de werkprocessen en dynamiek van de uitvoering van politietaken.

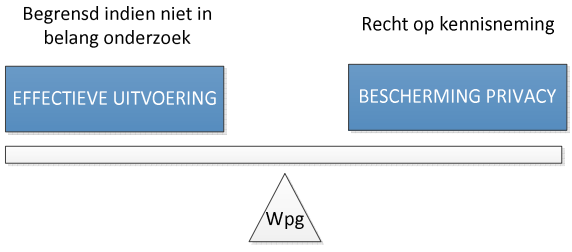
Ruimere maar geconditioneerde verstrekkingsmogelijkheden

De verstrekkingsmogelijkheden onder de Wpg zijn ruimer dan onder de Wpolr. De voorwaarde daarbij is dat doel en noodzaak van de verstrekking worden vastgelegd. In de praktijk wordt dit maar ten dele als werkbaar ervaren. Het is voor de betrokkenen niet altijd duidelijk of ze mogen verstrekken. Dat is echter geen belemmering die voortvloeit uit de Wpg zelf maar uit de wijze waarop de Wpg door de politie is geïmplementeerd (kennis/opleiding, aandacht voor essentie). Het protocolleren van verstrekkingen bij de uitvoering van dagelijkse politietaken roept volgens de betrokkenen veel (dubbele) administratie op. Ook dat lijkt echter vooral een gevolg van de wijze waarop de politie de protocollering (ook qua ICT) heeft ingericht en de interne spelregels die daarbij zijn geformuleerd. De beleidstheorie is op het punt van verstrekkingen en daaraan gestelde eisen voldoende in balans.



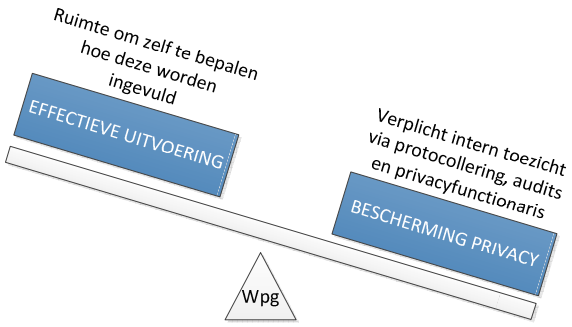
Recht op kennisneming

Betrokkenen hebben het recht om kennis te nemen van gegevens die van hen worden verwerkt en kunnen – indien aan de orde – eisen dat onjuiste gegevens worden aangepast of verwijderd. Dit recht geldt alleen als er geen strijdigheid is met het belang van een onderzoek. In de praktijk worden op dit punt geen wezenlijke knelpunten ervaren anders dan een zekere administratieve last. Deze vloeit volgens de betrokkenen deels voort uit de toename (om uiteenlopende redenen) van het aantal verzoeken om kennisnemingen. Meer specifiek wordt deze administratieve last gevoeld bij verzoeken om kennisnemingen bij art. 10-verwerkingen. Deze verzoeken worden standaard afgewezen in het belang van de goede



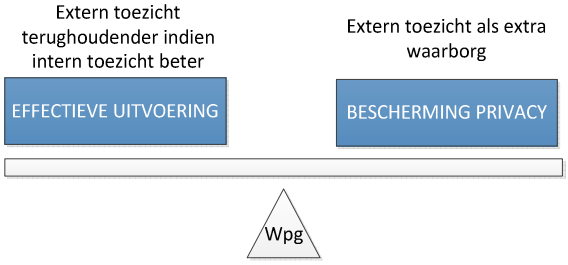
uitvoering van de politietaak maar vergen toch de nodige tijd in verband met de procedurele afwikkeling. Als geheel is de Wpg op dit onderdeel redelijk in balans.

Organiseren intern toezicht maar zelf bepalen hoe dat wordt ingericht



De Wpg heeft diverse toezichtfiguren, zijnde de protocollering, het uitvoeren van privacy-audits en een interne toezichthouder in de persoon van een privacyfunctionaris (en eventueel een functionaris gegevensbescherming). Het interne toezicht op grond van de Wpg komt in de praktijk maar gedeeltelijk van de grond. Dit heeft onder meer te maken met de prioriteitstelling bij de politie zelf. Na de uitvoering van de audits in 2011 is meer invulling gegeven aan het interne toezicht. Het interne toezicht bevindt zich in een 'ongemakkelijke' positie: het is niet onafhankelijk (of heeft de schijn tegen). Daar komt bij dat de in de Wpg genoemde instrumenten van protocollering, monitoring en het uitvoeren van audits primair instrumenten zijn voor kwaliteitsborging. Door ze in de wet te positioneren als toezichtinstrumenten raakt de primaire functie op de achtergrond. De Wpg is op dit punt niet in balans.

Bij voldoende intern toezicht terughoudend extern toezicht



Het CBP is aangewezen als externe toezichthouder voor de Wpg. Het uitgangspunt is dat het toezicht van het CBP terughoudender is als de onder de Wpg vallende organisaties hun interne toezicht (of in elk geval de daarbij genoemde instrumenten) beter hebben georganiseerd. Het externe toezicht fungeert daarbij vooral als extra waarborg. In de praktijk blijkt dit ook zo te functioneren: toen de politie en de KMar niet de verplichte privacy-audits uitvoerden, volgde een interventie van het CBP. Deze interventie was op zijn beurt weer een prikkel om de auditfunctie in te voeren. De Wpg is op dit punt in balans.

Samengevat

Samengevat is de Wpg deels in balans als het gaat om het mogelijk maken van een effectieve en efficiënte uitvoering van politietaken en de eisen aan bescherming van de informationele privacy. Dit geldt in elk geval voor de algemene eisen aan autorisaties, beveiliging etc., de mogelijkheden om politiegegevens te verstrekken, de rechtsbescherming van betrokkenen en het externe toezicht. Deels – wat betreft de

verschillende verwerkingsregimes en de insteek van het interne toezicht - slaat de balans door naar de eisen aan het borgen van de informationele privacy. Daarbij is deels niet aannemelijk dat deze beperkingen aanvullend bijdragen aan de bescherming van de informationele privacy maar bemoeilijken ze wel de naleving van de Wpg als geheel en de uitvoering van politietaken. Daarbij moet worden aangetekend dat de onbalans niet op zichzelf staat en op een aantal punten mede is veroorzaakt of versterkt door de wijze waarop de politie (zeker aanvankelijk) de implementatie van de Wpg heeft ingezet én de condities waaronder de Wpg bij de politie is ingevoerd. Daarbij kan gedacht worden aan de kwaliteit van de ICT[194].

12.4 Uitbalanceren Wpg

Onze conclusie is dat de Wpg op een aantal punten meer in balans kan worden gebracht. Hoe zich een en ander verhoudt tot de mogelijke wijzigingen in de Europese wet- en regelgeving, kunnen we niet overzien. Gelet op de verschillen die er op dit moment zijn tussen lidstaten als het gaat om de wetgeving rond politiegegevens, mag het aannemelijk worden geacht dat ook de Nederlandse wetgever daar enige speelruimte heeft. We komen dan tot de volgende punten.

Ontschotting van verwerkingsregimes

We achten het niet aannemelijk dat het onderscheid in verwerkingsregimes, in het bijzonder die van de artikelen 8 en 9, bijdraagt aan een extra bescherming van informationele privacy. Wat de schotten tussen de verschillende verwerkingsregimes trachten te borgen, wordt ook al geborgd door de algemene bepalingen die gelden voor doelbinding, noodzakelijkheid en proportionaliteit. Bovendien zijn in de wet zekerheden ingebouwd in de vorm van eisen aan autorisaties, protocollering en toezicht (waarbij wij protocollering niet expliciet als toezichtinstrument positioneren). Daar staat tegenover dat de beschotting voor inhoudelijke en bedrijfsmatige problemen zorgt bij de uitvoering van politietaken. In feite vormen ze daarmee ook een belemmering voor de free-flow-of-information binnen de politieorganisatie. Het wegnemen van deze beschotting laat de uitvoeringsorganisatie de ruimte om de borging van de informationele privacy te laten aansluiten bij de aard van de primaire werkprocessen zonder dat daarbij constructies nodig zijn om de structuur van de Wpg en deze werkprocessen op elkaar te laten aansluiten. Dit zal naar verwachting ook de administratieve belasting die nu wordt ervaren verminderen en het rechtvaardigt een stevig toezicht op de wijze waarop de organisatie hiermee omgaat.

[194] De beleidstheorie had ook geen expliciete aandacht voor de vraag of de Wpg in 2008 onder de condities binnen de politieorganisatie implementeerbaar was. Er is in 2004 wel een uitvoerbaarheidsonderzoek uitgevoerd, maar daarbij is niet specifiek gekeken naar de implicaties voor de inrichting van de organisatie van de politie. Bovendien was ook in dat onderzoek (evenals bij de wetgever in 2008) de verwachting dat de politie weldra over één ICT-systeem zou gaan beschikken.

Gekwalificeerde verlenging bewaartermijnen

Naar ons oordeel moeten de bewaartermijnen van de Wpg, dat wil zeggen tot vijf jaar na verwerking, op zichzelf werkbaar worden geacht voor een groot deel van de politietaken. Voor een klein maar belangrijk deel van de politietaken is een bewaartermijn van vijf jaar te kort. Dat is vooral het geval bij de aanpak van zware criminaliteit, het maken van algemene criminaliteits- of netwerkanalyses en het oplossen van cold cases. Het probleem zit vooral bij de politiegegevens die niet direct in een onderzoek zijn betrokken. De relevantie daarvan is niet op voorhand aan te geven. Denk daarbij aan een op zichzelf onbetekenende bekeuring voor een snelheidsovertreding die echter wel kan aantonen dat iemand op een bepaald tijdstip in de buurt van een plaats delict is geweest. Het automatisch vernietigen van gegevens na het aflopen van de bewaartermijn heeft het risico in zich dat de informatiepositie van de politie wordt ondergraven. Het bewaren van alle gegevens heeft echter grote risico's voor de (informationele) privacy vanwege de kans toenemende ruis in de kwaliteit van de gegevens. Dat geldt zeker in de huidige situatie waarin de politie zowel technisch (qua ICT) als bedrijfsmatig (kwaliteitsborging, werkprocessen) nog onvoldoende grip heeft op kwaliteit van de politiegegevens. Bovendien zal het bewaren van alle gegevens – ook bij een betere grip op de kwaliteit van de gegevens - leiden tot sterk toenemende beheerskosten.

Vanuit het oogpunt van (informationele) privacy lijkt het langer dan de huidige termijnen bewaren van alle politiegegevens niet wenselijk. Het belang van de opsporing kan in specifieke gevallen prevaleren boven het belang van privacy, maar dit mag geen algemene beleidslijn zijn. Er zal dus een modus moeten worden gevonden om te komen tot gekwalificeerde verlenging van de bewaartermijnen van niet aan een onderzoek gekoppelde politiegegevens die relevant kunnen zijn voor de aanpak van zware criminaliteit, het maken van (netwerk)analyses en het onderzoek naar cold cases. Daarbij zal extra gewicht moeten worden toegekend aan het regime voor beheer, beveiliging, kwaliteit (juistheid) en autorisatie tot verwerking. Een voorwaarde voor meer ruimte tot gekwalificeerde verlenging van bewaartermijnen is dat de politie in de bedrijfsvoering en de ICT voldoende 'in control' is wat betreft het beheer van politiegegevens. Dat is nu nog niet het geval.

Landelijke kaders voor verstrekkingen

We delen de suggestie die in enkele interviews is gedaan om landelijk eenduidige en uniforme kaders aan te reiken voor verstrekkingen in samenwerkingsverbanden. Dit ter vervanging van het brede en bonte palet van regionale convenanten, in elk geval waar het gaat om de samenwerking bij de handhaving rond de prioritaire thema's uit het nationale dreigingsbeeld. Dit is niet in de wet zelf geregeld, maar onder meer als Aanwijzing. Nu

sprake is van een Nationale politie lijkt het ook niet meer dan logisch dat één organisatie rond dezelfde thematieken en met vergelijkbare partners ook handelt binnen één kader.

Toezicht en kwaliteitsborging scheiden

De paragraaf 'toezicht' in de Wpg is een verzameling van instrumenten waarvan de vlag de lading niet helemaal dekt en die daardoor een aantal onbedoelde neveneffecten oproept. Het is om te beginnen de vraag of bij het toezicht de figuren van de privacyfunctionaris, de functionaris gegevensbescherming en het CBP naast elkaar een duidelijk te onderscheiden rol hebben. Toezicht werkt het best als dit onafhankelijk is. Intern toezicht is een instrument van kwaliteitscontrole en heeft een adviserende functie. De privacyfunctionarissen blijken in de praktijk vooral die adviserende rol te hebben.

De vraag is ook of de figuur van de functionaris gegevensbescherming een gelukkige keuze is vanwege de beeldvorming rond integriteit van de politie. Op papier is de functionaris gegevensbescherming onafhankelijk, maar deze is aangesteld door de verantwoordelijke en kan daarmee in de beeldvorming vooral 'het keuren van het eigen vlees' blijven. Het is zuiverder als het CBP haar toezichthoudende taak explicieter invult. Een aandachtspunt daarbij is ook de uiteindelijke sanctie die op het structureel schenden van de vanuit privacy-optiek gezien meest kardinale punten van wet staat. De huidige (bestuursrechtelijke) vorm biedt weinig slagkracht, zo blijkt uit gesprekken.

Het lijkt ons daarnaast verstandig om instrumenten als protocollering, monitoring en audits expliciet uit de sfeer van het toezicht te halen in casu het hoofdstuk 'Toezicht' in de wpg. Dit zijn primair instrumenten voor kwaliteitsborging en moeten onderdeel zijn van de reguliere managementcyclus. De primaire functies van deze instrumenten raken op de achtergrond door ze als toezichtinstrumenten te positioneren en werken eerder averecht op de verinnerlijking van het goed omgaan met informationele privacy, zo heeft de praktijk geleerd. Het is beter ze te positioneren onder 'kwaliteitsborging' en de externe toezichthouder er – als een vorm van systeemtoezicht - expliciet op toe te laten zien dat deze borging ook plaatsvindt.

Samenloop met andere wetten

De verschillende bewaartermijnen die gelden voor persoonsgegevens in diverse wetten (zoals Wpg, Archiefwet en Wjsg) worden als een probleem ervaren en behoeven harmonisatie. Dat geldt bijvoorbeeld ook voor de bewaartermijnen en de verjaringstermijnen van delicten.

Een tweede aandachtspunt is het in de praktijk in elkaar overlopen of in één werkproces samenkomen van het 'ophalen', opslaan en verwerken (gebruiken, verstrekken) van

gegevens. Daarbij kan gedacht worden aan het gebruik van live camerabeelden of het ter plaatse verwerken van camerabeelden na een overval. De juridische splitsing van informatie ophalen en verwerken staat daarbij soms op gespannen voet met een efficiënte bedrijfsvoering en de effectiviteit van de uitvoering van politietaken.

Wat betreft de Wob wordt vooral de administratieve belasting van de organisatie als knelpunt ervaren. Dit is echter een knelpunt dat in bredere zin voor de Wob geldt en momenteel (medio 2013) de politieke aandacht heeft.

12.5 Verbeterde borging van de naleving

De uitvoeringspraktijk bij de politie laat een ambivalent beeld zien. Enerzijds was en is er naar de letter van de wet sprake van 'selectieve naleving', anderzijds is er vergeleken met 2011 wel een duidelijke slag gemaakt, zowel in het regelen van een aantal waarborgen als in het stroomlijnen van de aandacht voor de regels van de privacywetgeving. De audits en de vorming van de Nationale politie waren daarvoor belangrijke aanjagers.

De condities voor een (verdergaande) adequate uitvoering van de Wpg , zijn verbeterd ten opzichte van 2008. Met de vorming van de Nationale politie is – in elk geval op papier - de (centrale) aansturing en verankering in de leiding beter geborgd. Ook dat is echter nog geen garantie dat de Wpg 'verinnerlijkt' en geïntegreerd en systematisch wordt nageleefd.

Focus op kwaliteit en veiligheid gegevens

Het meest essentieel is de borging van de kwaliteit van de politiegegevens, zowel wat betreft de juistheid, rechtmatigheid als de traceerbaarheid en corrigeerbaarheid. Hierin schuilen vanuit privacy-oogpunt, los van de formele afwijkingen van de Wpg, de grootste concrete risico's voor betrokkenen. Vooral wat betreft het verwerken en verstrekken van onjuiste gegevens en mogelijk daarop volgende onjuiste gevolgtrekkingen of stigmatisering.

Samenhang en balans in professionele en bedrijfsmatige borging

Voor een goede borging van de kwaliteit van politiegegevens moeten voldoende kennis van de essenties van de Wpg, het bewustzijn van het (politie)belang van het professioneel en bedrijfsmatig omgaan met informationele privacy en de basisvoorzieningen in de ICT aanwezig zijn. Essentieel is de balans tussen professionele en bedrijfsmatige borging van de Informationele privacy. Informationele privacy alleen borgen op basis van procedures en regels zal niet werken, het is ook een kwestie van 'mores'. Aandacht voor de bewustwording en het professioneel omgaan met informationele privacy is van groot belang. Dat betekent dat het spoor dat bij de eerste implementatieronde is blijven liggen, namelijk de aandacht voor kennis, bewustwording en training in het omgaan met

politiegegevens, binnen de uitvoering van de primaire processen moeten worden opgepakt. De waargenomen kanteling van het nalevingsmotief van 'moeten' naar 'belang voor mores en slagvaardigheid bij de politie' en de kanteling van een focus op 'rule based' naar 'risk-based' naleving zijn daarbij belangrijke stappen.

Integrale verankering in proces inrichting Nationale politie

De verdere invulling van de borging van de naleving kan zeker niet los worden gezien van de inrichting van de Nationale politie. Informationele privacy is in dat traject echter slechts één van de inrichtingssporen. Niet onbelangrijk, maar ook niet allesbepalend. De inrichting van de Nationale politie en de verbetering van de naleving van de privacyregelgeving zullen samen moeten gaan. Anderzijds is het actiever delen van informatie, een van de doelstellingen van de Wpg, ook een van de centrale ambities in het inrichtingsplan van de Nationale politie. De inrichtingseisen voor het borgen van de naleving van de Wpg (professionele afweging, samenwerken en delen, geïntegreerde ICT, goede bedrijfsvoering, kwaliteitsborging) sluiten dan ook naadloos aan bij de centrale doelstellingen van de Nationale politie. In die zin kan de verbeterde borging van de naleving van de Wpg ook als een speerpuntproject fungeren in het inrichtingsproces van de Nationale politie. Een stapsgewijze aanpak met focus op een aantal meest kritische processen vanuit het belang van de politietaak én de privacy, ligt daarbij voor de hand.

12.6 Politieke afweging: grenzen opgaven politie en privacy

In hoofdstuk 1 hebben we bij de begripsbepaling al aangegeven dat het begrip 'privacy' niet statisch is. De invulling en het gewicht dat eraan wordt gegeven is context- en functie-afhankelijk. De verschuivingen in het denken over informationele privacy hangen sterk samen met de maatschappelijke context (zoals veiligheidsgevoel) en ontwikkelingen in ICT, digitalisering en het gebruik van social media. Ook het karakter van criminaliteit, de verwachtingen die politiek en samenleving hebben van de politie en de (mogelijke) opsporingsmethoden veranderen. Opsporingsdiensten zoeken daarbij naar de grenzen, zowel wat technisch kan (zoals 'real time information capability'), wat werkt (levert het zinvolle informatie op?, kun je zaken meer/beter oplossen en criminaliteit of openbare-ordeverstoringen voorkomen?), wat nodig is en wat (gelet op informationele privacy) mag.

Er zal net als in de aanloop naar de Wpg in 2008 en los van de verbeterpunten in de uitvoeringspraktijk, een nieuwe balans moeten komen tussen wat van de politie wordt verwacht, welke ruimte de politie daarvoor nodig heeft bij de verwerking van politiegegevens, welke eisen daaraan vanuit privacy-optiek moeten worden gesteld én wat de organisatorische en technische (on)mogelijkheden daarbij zijn. Dit veronderstelt niet alleen een juridische afweging maar ook een politieke heroriëntatie.

BIJLAGEN

Bijlage 1 Geraadpleegde literatuur en documenten

Aardweg, M. v. (2009). De Wet politiegegevens: nieuwe perspectieven voor de privacyfunctionaris. *Privacy & Informatie. Jaargang 12*, 162-170.

Actal Adviescollege toetsing regeldruk. (2011). *Armslag voor de politieprofessional.* Den Haag: Actal.

Actieprogramma Lokale Besturing Politie. (2012). *Gezamenlijke veiligheidszorg. Volop lokale kansen in nieuw politiebestel.* Den Haag: Actieprogramma Lokale Besturing Politie.

Adviescommissie 'Veiligheid en persoonlijke levenssfeer'. (2009). *Gewoon doen, beschermen van veiligheid en persoonlijke levenssfeer.*

Algemene Rekenkamer. (2011). *ICT politie 2010.* Den Haag: Sdu Uitgevers.

Big Brother Watch. (sd). *Police databases: Over 900 Police staff abuse their access.* Opgehaald van www.bigbrotherwatch.org.uk

Bits Of Freedom. (2012). *Gegevens burgers niet veilig bij de politie. Onderzoek naar de audits Wet Politiegegevens bij de politie.*

Bovens, M., & Zouridis, S. (2002). *Van street-level bureaucratie naar systeem-level bureaucratie.* Utrechtse School voor Bestuurs- en Organisatiewetenschap.

Bron, R., Duijneveldt, I. v., Waarsing, H., Uden, A. v., Vijverberg, W., & Visser, D. (2010). *(Niet) voor de wijk. De tijdsbesteding van wijkagenten.* Den Haag/Utrecht.

Brummelkamp, G., & Linssen, M. (2006). *Inventarisatie administratieve belasting van de politie. Vooronderzoek ter identificatie van knelpunten.* EIM.

Bureau Centrale Informatie Organisatie. (2013). *BVO Korpsmonitor.* Politie Amsterdam-Amstelland.

Bureau Korpsondersteuning Politie Flevoland. (2012). *Brief aan Bits of Freedom betreffende Besluit Wob Beslisboom Wpg.* Lelystad: Politie Flevoland.

CIO Politie. (2012). *Bijstelling Aanvalsprogramma IV Politie. Tweede helft 2012 en doorkijk eerste helft 2013.*

College bescherming persoonsgegevens. (2009). *Beleidsregels CBP Handhaving Protocolplicht Wet politiegegevens.* Opgehaald van http://www.cbpweb.nl

College bescherming persoonsgegevens. (2010). *Brief aan de minister van Veiligheid en Justitie betreffende het Ontwerpbesluit tot aanpassing van het Besluit politiegegevens.* Den Haag.

College bescherming persoonsgegevens. (2010). *Onderzoek bij het KLPD naar door Nederland ingevoerde gegevens in het Europol Informatiesysteem.*

College bescherming persoonsgegevens. (2011). *Brief aan de korpsbeheerder van het Regionaal de Minister van Veiligheid en Justitie betreffende het onderzoek externe privacy audit KLPD; definitieve bevindingen.*

College bescherming persoonsgegevens. (2011). *Brief aan de korpsbeheerder van het Regionaal Politiekorps Amsterdam-Amstelland betreffende het onderzoek externe privacy audit; definitieve bevindingen.*

College bescherming persoonsgegevens. (2011). *Informatieblad: Verstrekken van persoonsgegevens.*

College bescherming persoonsgegevens. (2011). *Onderzoek CIOT-bevragingen. Onderzoek CIOT.* Den Haag.

College bescherming persoonsgegevens. (2011). *Onderzoek CIOT-bevragingen. Onderzoek Dienst Nationale Recherche.* Den Haag.

College bescherming persoonsgegevens. (2011). *Onderzoek CIOT-bevragingen. Onderzoek Regionaal Politiekorps Haaglanden.* Den Haag.

College bescherming persoonsgegevens. (2012). *Informatieblad 31a. Informatie delen in samenwerkingsverbanden.*

College bescherming persoonsgegevens. (2013). *Jaarverslag 2012.* Den Haag: College bescherming persoonsgegevens.

College bescherming persoonsgegevens. (2013). *Onderzoek naar de verwerking van persoonsgegevens in het kader van de mobiele applicatie whatsapp door WhatsApp Inc.* Den Haag.

Considerati. (2009). *Onze digitale schaduw, een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat* (in opdracht van het CBP)

Cozijn, C. (1996). *Wet en Besluit politieregisters. Een inventarisatie van knelpunten in de politiepraktijk.* Den Haag: WODC.

Departmentale Auditdienst. (2011). *Audit Wpg politie Flevoland*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2011). *Audit Wpg politie Gooi en Vechtstreek*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2011). *Audit Wpg politie Haaglanden*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2011). *Audit Wpg politie Hollands Midden*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2011). *Audit Wpg politie IJsselland*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2011). *Audit Wpg politie Midden en West Brabant*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2011). *Audit Wpg politie Noord- en Oost-Gelderland*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2011). *Audit Wpg politie Rotterdam-Rijnmond*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2011). *Audit Wpg Rijksrecherche*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2012). *Audit Wpg politie Amsterdam-Amstelland*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2012). *Audit Wpg politie Brabant Zuid-Oost*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2012). *Audit Wpg politie Drenthe*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2012*). Audit Wpg politie Friesland*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2012). *Audit Wpg politie Gelderland-Midden*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2012). *Audit Wpg politie Gelderland-Zuid*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2012). *Audit Wpg politie Groningen*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2012). *Audit Wpg politie Kennemerland*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2012). *Audit Wpg politie KLPD*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2012). *Audit Wpg politie Limburg Noord*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2012). *Audit Wpg politie Limburg Zuid*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2012). *Audit Wpg politie Noord-Holland Noord*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2012). *Audit Wpg politie Twente*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2012). *Audit Wpg politie Utrecht*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2012). *Audit Wpg politie Zaanstreek Waterland*. Den Haag: Ministerie van Veiligheid en Justitie.

Departmentale Auditdienst. (2012). *Audit Wpg politie Zuid-Holland-Zuid*. Den Haag: Ministerie van Veiligheid en Justitie.

Der Bayerische Landesbeauftragte für den Datenschutz. (sd). *Der Bayerische Landesbeauftragte für den Datenschutz informiert zum Thema Polizei.* München.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit. (sd). *Datenschutz bei der polizei.* Opgehaald van www.datenschutz.bund.de

Derksen, T., & Klein, D. (2010). *Bestuurlijke Coalities tegen Criminaliteit. De juridische context van de onderlinge uitwisseling van informatie tussen de betrokken partners bij de bestuurlijke aanpak van georganiseerde criminaliteit.* Apeldoorn: Politieacademie.

Dienst Algemene Ondersteuning. (2012). *Wpg 2012.* Politie Amsterdam-Amstelland.

Dienst Landelijke Recherche. (2010). *WPG Status Productenlijst.*

Dommering, E. (2010). Recht op persoonsgegevens als zelfbeschikkingsrecht. In J. Prins, *16 miljoen BN'ers? Bescherming van persoonsgegevens in het digitale tijdperk* (pp. 83-99). Leiden: Stichting NJCM-Boekerij.

Duin, A. v. (2011). *Handboek Proces Opsporen Productbeschrijvingen Dienst Nationale Recherche.* Dienst Nationale Recherche.

Eenheid Oost Nederland. (2012). *Verbeterplan Wpg. Regionale Eenheid Oost Nederland.*

Egelkamp, M., & Mein, A. (2003). *Politiegegevens in Europees perspectief.* De Haag: ES&E.

Eissens, J. (2012). *Verbeterplan implementatie Wet politiegegevens in de (toekomstige) eenheid Noord-Holland.*

Essex Police. (sd). *How we use Personal Data.* Opgehaald van www.essex.police.uk

De Europese Commissie. (2012). *Voorstel voor een richtlijn van het Europees Parlement en de Raad 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.* 5833/12.

Eurotronics. (2009). *Brochure EDL Politie Suite.*

Fasten, J., Paans, R., Niemantsverdriet, P., & Brand, C. (2012). *Wet politiegegevens. Verbeterrapport 2012 naar aanleiding van de Externe Privacy Audit 2011.* Politie Rotterdam-Rijnmond & Politie Zuid-Holland-Zuid.

Flevoland, P. (2012). *Brief aan Bits of Freedom betreffende Besluit Wob verstrekkingenwijzer Wpg.* Lelystad.

Gemeente Amsterdam. (2011). *Raadsbesluit 219/848.* Amsterdam.

Gemeente Amsterdam, Bestuursdienst. (2005). *Bestuurlijke blokkades. Reactie op het rapport "Het Van Traa project" van de Vrije Universiteit.* Gemeente Amsterdam.

Gijn, H. v. (2008). *Vragen naar de onbekende weg. Een onderzoek naar de toepassing van de Wet Politiegegevens door de Criminele Inlichtingen Eenheden in de strijd tegen terrorisme.* Tilburg.

Groenewegen, P. (2010). *Prestatiecontracten bij de Nederlandse Politie. Een overzicht van de ontwikkelingen van 2003 t/m 2008.* Rotterdam.

Heijden, I. v., & Ilpenhof, D. v. (2012). *Review verbeterplan Wpg politie Amsterdam-Amstelland.* Den Haag: Departementale Auditdienst.

Heijden, I. v., & Postuma, R. (2012). *Concept Review verbeterplan WPG politie Amsterdam-Amstelland.* Den Haag: Departementale Auditdienst.

Helsloot, I., Groenendaal, J., & Warners, E. (2012). *Politie in de netwerksamenleving. De opbrengst van de politiële netwerkfunctie voor de kerntaken opsporing en handhaving openbare orde en de sturing hierop in de gebiedsgebonden politiezorg.* Apeldoorn: Politie & Wetenschap.

Henderik, T. (2012). *Verbeterplan Implementatie en Borging Wet politiegegevens in de (toekomstige) eenheid Oost-Brabant (korpsen BBN en BZO).*

Huisman, A. (2006). *Informatie Gestuurde Politie: De tijd en moeite waard?!*

Inspectie Openbare Orde en Veiligheid. (2006). *Landelijke coördinatie en uitwisseling van politie-informatie. Ontwikkelingen sinds rapportage 2004.* Den Haag.

Inspectie Openbare Orde en Veiligheid. (2008). *Informatiegestuurde Politie.* Den Haag: Inspectie Openbare Orde en Veiligheid.

Inspectie SZW. (2012). *Elektronische verstrekking van gegevens vanuit het SUWI-domein aan organisaties buiten SUWI. Nota van bevindingen.* Den Haag: Ministerie van Sociale Zaken en Werkgelegenheid.

Inspectie Veiligheid en Justitie. (2012). *CIOT-bevragingen. Proces en rechtmatigheid.* Den Haag: Ministerie van Veiligheid en Justitie.

Jensma, F. (2013, maart 23). Oom agent surft volautomatisch met u mee. *NRC*.

Kas, A. (2012, december 27). Bouman: 'Informatie over nieuwe nationale politie moet beter'. *NRC*, p. 1.

Kielman, H. (2010). *Politiële gegevensverwerking en Privacy. Naar een effectieve waarborging.* Den Haag.

Klap, H. (2006). *Invoering van de Wet Politiegegevens (WPG). Verkennend onderzoek naar het bereik van het implementatietraject.* Den Haag.

Klap, H. (2006). *Meerjarenbegroting Project implementatie WPG.* Den Haag.

KNMG. (2005). *Handreiking gegevensuitwisseling bemoeizorg.*

Koffijberg, J., Dekkers, S., Homburg, D., & Berg, B. v. (2009). *Niets te verbergen en toch bang. Nederlandse burgers over het gebruik van hun gegevens in de glazen samenleving.* Regioplan Beleidsonderzoek: Amsterdam.

Korps Landelijke Politiediensten. (2012). *Privacy-jaarverslag 2011 van de Dienst Nationale Recherche.*

Korpsbeheerdersberaad. (2012). *Brief aan het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties betreffende de nieuwe Wob.* Middelburg: Politieberaden.

Lasthuizen, K., Huberts, L., & Kaptein, M. (2004). *Integriteitsopvattingen bij de politie.* Zeist: Uitgeverij Kerckebosch.

Mac Gillavry, E. (2005). Heeft u even voor de nieuwe wet Politiegegevens. In A. Harteveld, D. d. Jong, & E. Stamhuis, *Systeem in ontwikkeling; Liber amicorum G. Knigge* (pp. 385-416). Nijmegen: Wolf Legal Publishers.

Mazar Management Consultants. (2011). *Rapport Privacy audit. Wet Politiegegevens Politie Zeeland.* Rotterdam.

Meershoek, A. (2012). *Onzichtbaar, integer, weinig gerespecteerd. Grondtrekken van de Nederlandse politietraditie.* Apeldoorn: Politie & Wetenschap.

Michels, W., & Boer, W. d. (2012). *Verbeterplan Wpg. Maatregelen ter verbetering van de in de privacy audit van januari 2012 geconstateerde tekortkomingen.* Politie Gelderland-Zuid.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. (2010). *Brief aan de voorzitter van het College bescherming persoonsgegevens betreffende vragen CBP over maatregelen EIS.*

Ministerie van Veiligheid en Justitie- Directoraat Generaal Politie. (2013). *Jaarverslag Nederlandse Politie 2012.* Den Haag: VijfKeerBlauw.

Moor-van Vugt, A. d., Engers, T. v., Groenewegen, F., Haaften, W. v., Klap, A., Nieuwenhuis, A., . . . Wessel, M. (2012). *Gegevensuitwisseling door Toezichthouders.* Amsterdam: Universiteit van Amsterdam.

Mul, V., Verloop, P., Mevis, P., Schreuders, E., & Wel, H. v. (2004). *Evaluatie wet bijzondere politiegegevens.*

Muller, E., Kummeling, H., & Bron, R. (2007). *Veiligheid en privacy. Een zoektocht naar een nieuwe balans.* Den Haag: Boom Juridische uitgevers.

National Criminal Intelligence Service. (2000). *The National Intelligence Model.* NCIS.

Nationale Ombudsman. (2009). *Openbaar rapport.* Rapportnummer: 2009/190.

Nationale Ombudsman. (2009). *Openbaar rapport.* Rapportnummer: 2009/124.

Nationale Ombudsman. (2010). *Rapport.* Rapportnummer: 2010/319.

Nationale Ombudsman. (2010). *Rapport.* Rapportnummer: 2010/319.

Nationale Ombudsman. (2011). *Gelukkig hebben we de foto's nog! Hoe gaat de politie om met het fotograferen en het opslaan van (persoons)gegevens van voetbalsupporters? Een voorzet voor verstandig politietoezicht.* Rapportnummer: 2011/239.

Nationale Ombudsman. (2011). *Rapport. Rapportnummer: 2011/228.*

Nationale Ombudsman. (2013). *Jaarbrief 2012 aan de Korpschef Nationale politie.* kenmerk 2013 0215 U.

Nationale Ombudsman. (2013). *Mijn onbegrijpelijke overheid 2012. Verslag van de Nationale Ombudsman 2012.* Den Haag: Sdu Uitgevers.

Nederlands Politie Instituut, Korpsbeheerdersberaad, Raad van Hoofdcommissarissen. (2004). *Brief aan de Minister van Justitie betreffende het conceptswetsvoorstel politiegegevens.* Den Haag.

Nederlands Politie Instituut; Korpsbeheerdersberaad; Raad van Hoofdcommissarissen. (2004). *Brief aan de Minister van Justitie betreffende het conceptwetsvoorstel politiegegevens.* Den Haag.

Nederlandse Orde van Advocaten. (2009). *Protocol voor de procedure gegevensverstrekking aan derden.*

Nederlandse Vereniging voor Burgerzaken. (sd). *Verstrekking uit en geheimhouding van persoonsgegevens in de Gemeentelijke basisadministratie persoonsgegevens.* Opgehaald van https://www.nvvb.nl.

Niemantsverdriet, P., Paans, R., & Fasten, J. (2012). *Wet Politiegegevens. Verbeterrapport Wpg 2012 naar aanleiding van de Externe Privacy Audit 2011.* Politie Zeeland & Politie Midden en West Brabant.

Overkleeft-Verburg, G. (2007). Openbaarheid van bestuur, privacywetgeving en gegevensverwerking door de politie. *Privacy & informatie*, 194-203.

Paans, R., & Fasten, J. (2011). De Wet Politiegegevens: Revival van het Bell-La Padula model. *De IT-Auditor*, 15-21.

Politie. (2011). *Concept Ontwerpplan Nationale politie.*

Politie. (2012). *Concept inrichtingsplan Nationale politie.*

Politie Amsterdam-Amstelland. (2012). *Input Wetsevaluatie Wet politiegegevens.* Amsterdam.

Politie Amsterdam-Amstelland. (2012). *Input Wetsevaluatie Wet politiegegevens.*

Politie en Openbaar Ministerie. (2011). *Bovenregionaal Recherche Overleg. Jaarverslag 2010.* Den Haag: Deltahage b.v.

Politie Limburg-Noord. (2012). *Besluit ondermandaat Wpg en Wob politieregio Limburg-Noord 2012.*

Politie Rotterdam-Rijnmond; Politie Zuid-Holland-Zuid; Politie Rotterdam-Rijnmond; Politie Zeeland. (2012). *Wet Politiegegevens. 'Content' voor Intranet:Werkinstructies, protocollen en procesbeschrijvingen.*

Politie Twente. (2012). *Verbeterplan Borging Wet politiegegevens Politie Twente.*

Politie Utrecht. (2012). *Verbeterplan implementatie Wet politiegegevens Politie Utrecht.*

Politie. (versie 0.9). *Beslisboom Wet Politiegegevens.*

Politie Zeeland, Juridische zaken. (2012). *Brief aan de Tweede Kamer der Staten Generaal betreffende de nieuwe Wob.* Middelburg: Politie Zeeland.

Politieacademie – School voor Politie Leiderschap. (2008). *Nederland is klein, denk groot. Blauwe denkers. Internationale politiesamenwerking.* Zijlstra.

Politieacademie. (2012). *Nieuwsbrief Milieu Extra.*

Politieacademie. (2013). *Training Privacyfunctionaris.*

Politieacademie en Andersson Elffers Felix. (2011). *Informatiegestuurde politie van en met blauw. Bijlage 2. Resultaten enquête politieagenten.* Utrecht.

Politievakorganisatie ACP. (2010). *Zwartboek BVH.* Leusden.

PricewaterhouseCoopers Advisory. (2012). *Externe audit Wet Politiegegevens Koninklijke Marechaussee.* Den Haag.

Prins, C. (2005). Advocaten, de GBA en privacy op z'n kop. *NJB. Aflevering 5*, 239.

Project implementatie Wet Politiegegevens. (2008). *Handreiking Verstrekkingen.* De Bilt.

Project Implementatie Wet politiegegevens. (2009). *Verstrekkingenwijzer WPG politie.*

Project Implementatie Wet politiegegevens. (2009). *Verstrekkingenwijzer WPG Kmar.*

Project Implementatie Wet Politiegegevens. (Verslag deelproject Wet- en regelgeving).

Project Implementatie WPG. (2009). *Implementatie Wet Politiegegevens. Oplevering producten.* De Bilt.

Project Implementatie WPG. (2010). *Uitkomsten wet- en regelgeving.* Leiderdorp.

Projectorganisatie Nationale Politie en landelijke redactie. (2012). *Route Nationale Politie. Gids voor medewerkers van de politie.*

Rathenau Instituut. (2007). *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw.* Den Haag: Rathenau Instituut.

Reenen, P. v. (2012). *Tot op heden is dergelijk onderzoek niet verricht. De effectiviteit van de politie en haar legitimiteit: studies tegen het licht gehouden. De stand van kennis en onderzoek, deel II.* Apeldoorn: Politie & Wetenschap.

Research voor Beleid. (2010). *Omvangrijke en oneigenlijke Wob-verzoeken.* Den Haag: Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

RGU Data Protection. (sd). *The 8 Data Protection Principles.* Opgehaald van www.dataprotectionact.org

Rietveld, M., Slump, G., & Beerepoot, A. (2004). *Toets uitvoerbaarheid Wet politiegegevens. Verslag van bevindingen.* Amsterdam: DSP-groep.

Ruiter, F. (2012). *Verbeterplan Wpg. Maatregelen ter verbetering van de in de privacy audit 2011 geconstateerde tekortkomingen.* Politie IJselland.

Ruth, A. v., & Schreuders, E. (2000). *Politiegegevens beschermd. Een toelichting op het gesloten verstrekkingenregime van de Wet politieregisters.* Den Haag: Registratiekamer.

Sauerwein, L., & Linnemann, J. (2002). *Wet bescherming persoonsgegevens. Handleiding voor verwerkers van persoonsgegevens.* Den Haag: Ministerie van Justitie.

Staffeleu, E., Hengst, M. d., & Hoorweg, E. (2011). *Inrichting Regionale InformatieOrganisaties Politiekorpsen. Beschrijvend (voor)onderzoek naar de inrichting van de RIO's in Nederland.* Apeldoorn: Politieacademie, Lectoraat Intelligence.

Smet, S. de (2013). *De nieuwe politie*

Streutjens, P. (2010). *Privacyfunctionaris verslag maart - dec 2010.* Venlo: Korps Regiopolitie Limburg - Noord.

Streutjens, P. (2012). *Jaarverslag 2011 Wet Politiegegevens.* Regiopolitie Limburg-Noord.

Struiksma, N., Vey Mestdagh, C. d., & Winter, H. (2012). *De organisatie van de opsporing van cybercrime door de Nederlandse politie.* Apeldoorn: Politie & Wetenschap.

Telengy. (2010). *Toezichtmodel Rotterdam CS 2011 - 2015.*

Torre, E. v., Gieling, M., Dozy, M., & Akgül, A. (2011). *Op de agenda: Een survey onder wijkagenten.* Politieacademie, Lectoraat Gebiedsgebonden politie: Apeldoorn.

Tweede Kamer der Staten-Generaal. (2006). *Brief van de Minister van Binnenlandse Zaken en Koninkrijksrelaties. 29 628 Politie. Vergaderjaar 2005–2006.* Nr. 31.

Vedder, A., & Koops, B. (2001). *Opsporing versus privacy: de beleving van burgers.* Den Haag: Sdu Uitgevers.

Vedder, A., & Koops, B. (sd). *Burgers over opsporing en privacy.* Opgehaald van http://arno.uvt.nl/show.cgi?fid=5071

Vermeulen, A. (2010). *Privacy en de Overheid, voortschrijdende techniek.* Utrecht University.

Vijver, C. v. (2012). *De professionaliteit van de politie. Wat moet centraal staan in toekomstig onderzoek? De stand van kennis en onderzoek, deel I.* Apeldoorn: Politie en Wetenschap.

Vlek, E., & Reenen, P. v. (2012). *Voer voor kwartiermakers. Wetenschappelijke kennis voor de inrichting van de Nationale Politie.* Apeldoorn: Politie en Wetenschap.

Vogelzang, P. (2013). *Bouwen aan vertrouwen. Rapportage Adviesopdracht, Raad van Toezicht, Politieacademie.*

Vrenken, L. (2012). *Wet politiegegevens. Verbeterplan 2012 Limburg.*

Vrije Universiteit Amsterdam. (2011). *Strategieën van lokale veiligheid. Een achtergrondstudie en drie reflecties.* Amsterdam University Press.

Vts Politie Nederland. (2008). *Scope. Hét relatiemagazine van vts Politie Nederland.*

Wassercordt, L. (2012). *Jaarverslag 2011 Wet Politiegegevens.* Regiopolitie Limburg-Zuid.

Wassercordt, L. (2013). *Jaarverslag 2012 Wet Politiegegevens.* Regiopolitie Limburg-Zuid & Regiopolitie Limburg Noord.

Werkgroep gebruik basisvoorzieningen. (2009). *Om te begrijpen moet je goed luisteren. Advies werkgroep gebruik basisvoorzieningen.*

Werkgroep Modellen voor beheer van de politie. (2005). *Beheer beheerst. Rapport van de werkgroep Modellen voor beheer van de politie. Interdepartementaal beleidsonderzoek 2004-2005 nr. 5.*

Werkgroep uit de NVVB-adviescommissie Identiteiten & Producten. (2012). *Schema voor schriftelijke verzoeken om gegevensverstrekking uit de GBA.*

Wiertsema, B. (2012). *Verbeterplan. Project: Duurzame implementatie WPG 2008.* Politie Noord-Nederland.

Winter, H., Jong, P. d., Sibma, A., Visser, F., Herweijer, M., Klingenberg, A., & Prakken, H. (2008). *Wat niet weet, wat niet deert. Een evaluatieonderzoek naar de werking van de Wet bescherming persoonsgegevens in de praktijk.* Den Haag: WODC.

WODC. (2009). Nodal governance en veiligheidszorg. *Justitiële verkenningen*, Boom Juridische Uitgevers.

Wolfs, P., & Goor, G. v. (2012). *Landelijk Projectplan Implementatie Wet Politiegegevens 2012/2013.*

Wolfs, P., Oort, D. v., & Biezen, A. v. (2013). *Landelijke rapportage hercontrole WPG n.a.v. privacy audit 2011 door Departementale Auditdienst.* Politie Nederland.

Wolfs, P., Oort, D. v., & Biezen, A. v. (2013). *Landelijke rapportage hercontrole Wpg. n.a.v. privacy audit 2011 door Departementale Auditdienst.* Politie Nederland.

Zwenne, G., & Erents, C. (2009). Reikwijdte Wbp: enige opmerkingen over de uitleg van artikel 4, eerste lid Wbp. *Privacy & informatie*, 60-67.

Wet- en regelgeving

Aanwijzing wet politiegegevens. 2008A017gp. Stscr. 2012, nr. 26877.

Besluit van 14 december 2007, houdende bepalingen ter uitvoering van de Wet politiegegevens (Besluit politiegegevens). Stb. 2007, 550.

Besluit van 3 juli 2009, houdende bepalingen inzake de overeenkomstige toepassing van de Wet politiegegevens op de verwerking van persoonsgegevens door een dienst van een publiekrechtelijk lichaam die is belast met de opsporing van strafbare feiten (Besluit politiegegevens bijzondere opsporingsdiensten). Stb. 2009, 305.

Besluit van 4 oktober 2012, houdende regels omtrent de doeleinden waarvoor de politie en de rijksrecherche, met inachtneming van de Wet politiegegevens, gegevens verwerken, de categorieën van gegevens die daartoe worden verwerkt, de terbeschikkingstelling en verstrekking van gegevens alsmede de wijze van verwerking (Besluit verplichte politiegegevens). Stb. 2012, 465.

Eerste Kamer der Staten-Generaal. (2012). *Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie. EU-voorstel Richtlijn bescherming persoonsgegevens bij gebruik door politiële en justitiële autoriteiten (COM(2012) 10) en EU-voorstel Verordening algemeen kader bescherming persoonsgegevens.* 22 112, FH.

Europese Commissie. (2012). *Voorstel voor een richtlijn van het Europees Parlement en de Raad 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.*

Europese Unie. (2010). *Verdrag tussen het Koninkrijk België, de Bondsrepubliek Duitsland, het Koninkrijk Spanje, de Republiek Frankrijk, het Groothertogdom Luxemburg, het Koninkrijk der Nederlanden en de Republiek Oostenrijk inzake de intensivering van de grensoverschrijdende samenwerking, in het bijzonder ter bestrijding van het terrorisme, de grensoverschrijdende criminaliteit en de illegale migratie.*

Invoering van de Politiewet 200. en aanpassing van overige wetten aan die wet (Invoerings- en aanpassingswet Politiewet 201X). Eerste Kamer, vergaderjaar 2011–2012, 32 822, A.

Mandaatbesluit Wet politiegegevens FIOD-ECD. Nr. DGB/2010/737M. Stcr. 2010, 2085.

Memorie van toelichting bij de Wet bescherming persoonsgegevens. Tweede Kamer, vergaderjaar 1997–1998, 25 892, nr. 3.

Memorie van toelichting bij de wet politiegegevens. Tweede Kamer, vergaderjaar 2005–2006, 30 327, nr. 3.

Memorie van Toelichting bij de Wet politieregisters. Tweede Kamer, vergaderjaar 1985-1986, 19 589, nr. 3.

Memorie van Toelichting bij Wet van 12 juli 2012 tot vaststelling van een nieuwe Politiewet. Stb 2012, 315.

Regeling van 1 februari 2008, nr. 5528485/08, houdende regels tot het aanwijzen van wetgeving, genoemd in artikel 4:2, tweede lid, van het Besluit politiegegevens. Stcr. 2008, 38.

Regeling van de Minister van Justitie, de Minister van Binnenlandse Zaken en de Minister van Defensie van 9 december 2008, nr. 5578598/08, houdende nadere regels ten aanzien van het toezicht op de naleving van de bij of krachtens de Wet politiegegevens gegevens voorschriften (Regeling periodieke audit politiegegegevens). Stcrt. 2008, 252.

Vaststelling van een nieuwe Politiewet. Nota van wijziging. Tweede Kamer, vergaderjaar 2010–2011, 30 880, nr. 11.

Wet van 12 juli 2012 tot vaststelling van een nieuwe Politiewet. Stb. 2012, 315.

Wet van 21 juni 1990, houdende regels ter bescherming van de persoonlijke levenssfeer in verband met politieregisters (Wet politieregisters). Stb. 1990, 414.

Wet van 26 januari 2012 tot wijziging van de Wet bescherming persoonsgegevens in verband met de vermindering van administratieve lasten en nalevingskosten, wijzigingen teneinde wetstechnische gebreken te herstellen en enige andere wijzigingen. Stb. 2012, 33.

Wet van 31 oktober 1991, houdende regelen betreffende de openbaarheid van bestuur. Stb. 1991, 703.

Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens). Stb 2000, 302.

Jurisprudentie

Afdeling bestuursrechtspraak Raad van State

ABRvS van 5 december 2012, ECLI:NL:RVS:2012:BY5104

ABRvS van 5 september 2012, ECLI:NL:RVS:2012:BX6514

ABRvS, 29 september 2010, ECLI:NL:RVS:2010:BN8578

ABRvS, 19 mei 2010, ECLI:NL:RVS:2010:BM4969

ABRvS 20 januari 2010, ECLI:NL:RVS:2010:BK9880

ABRvS 21 februari 2007, ECLI:NL:RVS:2007:AZ9026

ABRvS 29 november 2006, ECLI:NL:RVS:2006:AZ3237

Hoge Raad

Hoge Raad 20 april 2012, ECLI:NL:PHR:2012:BV3436Rechtbank Haarlem, 16 mei 2012, ECLI:NL:RBHAA:2012:BW7578

Rechtbanken

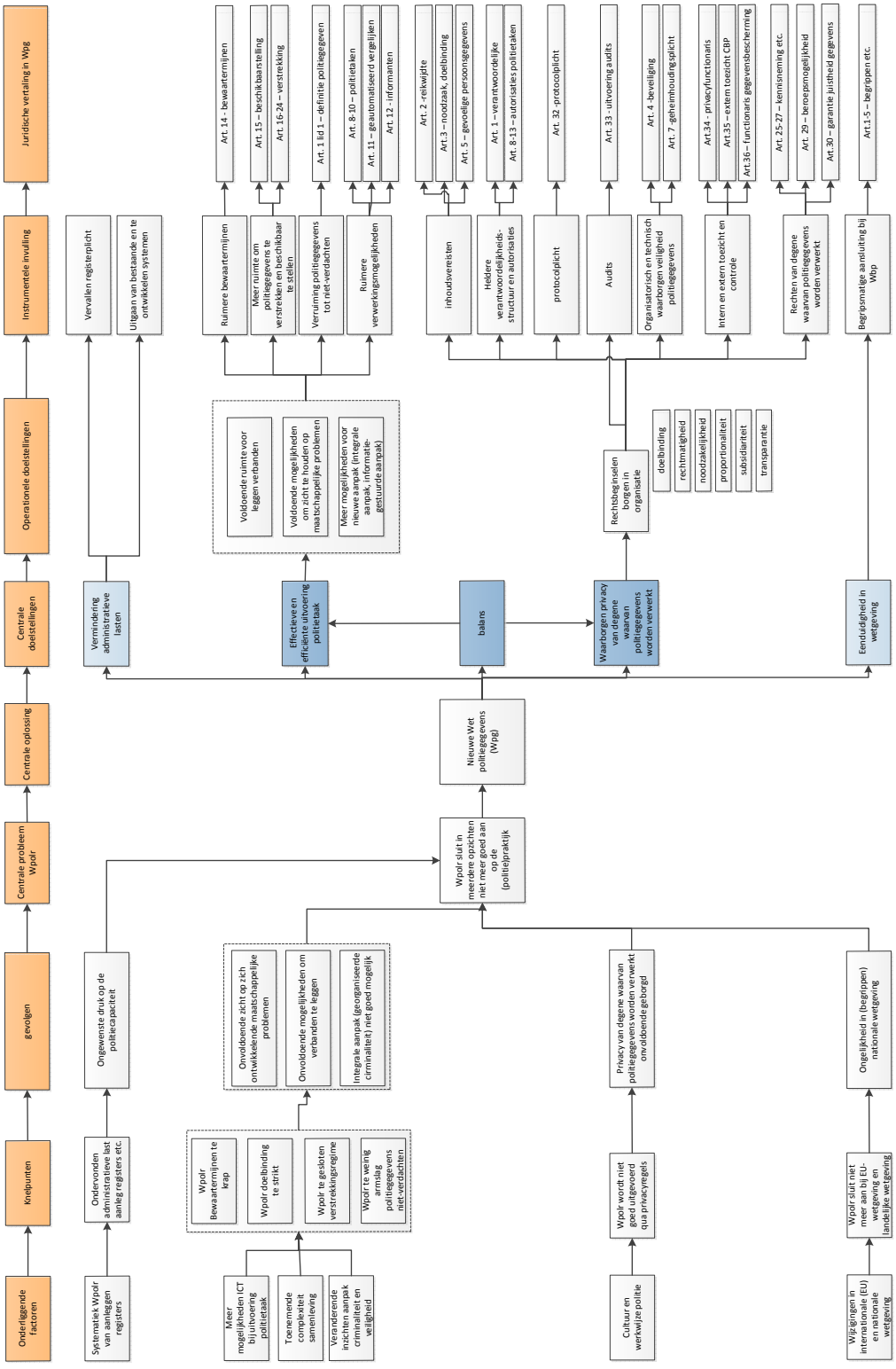
Rechtbank Noord-Nederland, 2 januari 2013, ECLI:NL:RBNNE:2013:BZ4177

Rechtbank Utrecht, 13 december 2012, ECLI:NL:RBUTR:2012:BY6261Rechtbank Arnhem, 15 november 2012, zaaknummer AWB 12/3336

Rechtbank Haarlem, 23 februari 2010, AWB 09 - 3014

Rechtbank Haarlem, 9 sptember 2008, zaaknummer AWB 08-3824

Bijlage 2 Schematische weergave transitie Wpolr naar Wpg



Bijlage 3 Geïnterviewden

Amsterdam (-Amstelland)

Bert Kok	Wijkagent Uithoorn
Birgit Vredendaal	Privacyfunctionaris
Charlotte Kuijper	Clustercoördinator Business Intelligence Competence Center
Guillian Vonk	Eenheidsprojectleider Wpg en projectenmanager
Jan Visser	Medewerker Bureau Zware criminaliteit
Jeroen Gijsen	Informatieanalist Business Intelligence Business Intelligence Competence Center
Mandy Konijn	Dossiervormer en coördinator Districtelijke recherche West
Reinder Doeleman	Chef DRR/RIO
Rinse Postuma	Interne auditor
Suzanne Franken	Wpg projectleider

Koninklijke Marechaussee

Angela Bens	Hoofd Kwaliteitsbureau
Coen Steeghs	Medewerker Kwaliteitsbureau
Dimitri Schuivens	Hoofd Sectie Intell Zuid
Floortje Scheeren	Privacyfunctionaris
Johan Burkhard	Medewerker KMar Informatie Knooppunt (KIK)
Johan Voortman	Medewerker KMar Informatie Knooppunt (KIK)
Karen van Gessel	Interne auditor
Kees Weijers	Privacyfunctionaris
Ruud Bogers	Medewerker Sectie Operaties Zuid

Landelijke Eenheid

Dirk Hoogenboezem	Chef informatie / projectleider implementatie Wpg Dienst Landelijke Recherche
Eppo Mol	Privacyfunctionaris Dienst Landelijke Informatieorganisatie
Gert van Doorn	Teamleider Dienst Landelijke Recherche
Koert Langeveld	Teamleider Dienst Landelijke Informatieorganisatie
Marijke van den Aardweg	Privacyfunctionaris Dienst Landelijke Recherche
Peter Houweling	Operationeel analist Dienst Landelijke Recherche
Tobias de Wit	Analist en Proces coördinator Dienst Landelijke Informatieorganisatie
Vincent Cillessen	Projectvoorbereider Dienst Landelijke Recherche
Wilbert Paulissen	Diensthoofd Dienst Landelijke Recherche

Limburg (Noord)

Paul Streutjens	Tactisch leidinggevende (voorheen Privacyfunctionaris Limburg Noord)
Louis Wassercordt	Privacyfunctionaris
Ard Ruiter	Jurist
Marc van Duijl	Informatiemanager
Johan Clement	Projectleider WPG en adviseur O&I
Rolf Dautzenberg	Kwartiermaker Dienst Regionale Informatieorganisatie
Peter de Vos	Waarnemend Chef Horst
Joop Crompvoets	Teamleider / Rechercheur
Arno Willemsen	Wijkagent Peel en Maas

Werksessie Limburg

Gé Timmermans	Politie Limburg
Kasper Hendrix	Gemeente Venlo
Koos Geurts	Gemeente Roermond
Mieke Engels e/v Aerts	Politie Limburg
Peter van den Heuvel	Politie Limburg
Ruud Babic	Politie Limburg
Wim van de Ven	Openbaar Ministerie
Yvonne Reijnders	Politie Limburg

Bijeenkomst juridisch panel

Pieter Liefrink	Openbaar Ministerie, Landelijk Parket Rotterdam
Robert Tuinenburg	Openbaar Ministerie, Parket Amsterdam
Dirk van der Bel	Openbaar Ministerie, Arrondissementsparket Den Haag
Gijs van der Zee	Openbaar Ministerie, Arrondissementsparket Midden-Nederland
Hanneke van der Ploeg	Openbaar Ministerie, Landelijk Parket Schiphol
Hans Pieters	Openbaar Ministerie, Ressortsparket, Arnhem-Leeuwarden

Overige interviews

Aline Klingenberg	Docent Rijksuniversiteit Groningen
Carolien Grasdijk	Voormalig beleidsadviseur Ministerie van Veiligheid en Justitie, Directoraat-generaal Politie
Wilbert Thomesen	Beleidsadviseur College bescherming persoonsgegevens
Dirk Willem Hulst	Senior operations advisor Inspectie SZW
Gerrit van Goor	Landelijk Projectleider WPG
Gery Veldhuis	Politiechef Limburg / Portefeuillehouder WPG
Alex Commandeur	Afdelingshoofd Toezicht sector Publiek plaatsvervangend directeur College bescherming persoonsgegevens
Jos Malskat	Senior adviseur beveiliging en kwaliteit, nVWA, privacyfunctionaris voor de IOD
Luut Mol Lous	Raadadviseur Ministerie van Veiligheid en Justitie, Directie Wetgeving
Nico Havenaar	Teamleider opsporing Inspectie SZW
Paul Wolfs	Landelijk Projectleider WPG
Peter Heijmans	Voormalig projectleider implementatie Wpg (PIWPG)
Bart Gossen	Korpsjurist politie
Hans Franken	Hoogleraar informatierecht en lid EK
Susan Kloppenborg	Beleidsadviseur/privacyfunctionaris FIOD
Saskia Laaper	Medewerker Landelijk Informatie en Expertise Centrum (LIEC)
Leo van den Berg	Senior bedrijfsjurist en landelijk coördinator Wob
Maarten van Dijk	Onderzoeker Nationale Ombudsman
Sandra Hoogendijk	Onderzoeker Nationale Ombudsman
Renate Croes	Advocaat FZKC-advocaten (namens NOvA)
Niels Groenhart	Advocaat Advocatenkantoor Groenhart (namens NOvA)

Bijlage 4 Deelnemers expertmeeting

Cisline Nanuruw-Basmagi	Gemeente Rotterdam
Birgit Vredendaal	Politie Amsterdam
Erik Boelaars	Gemeente Nijmegen
Peter Muijen	Openbaar Ministerie
Gijs van der Zee	Openbaar Ministerie
Floortje Scheeren	Koninklijke Marechaussee
Kees Weijers	Koninklijke Marechaussee
Henk Klap	Programmamanager Cybercrime Nationale politie; voormalig projectleider implementatie Wpg
Saskia Laaper	Landelijk Informatie en Expertise Centrum

Bijlage 5 Leden begeleidingscommissie

Prof. mr. dr. S. Zouridis (voorzitter)	Universiteit van Tilburg - Faculteit Rechtswetenschappen
Mr. L.P. Mol Lous	Ministerie van Veiligheid en Justitie, Directie Wetgeving, sectie straf- en sanctierecht
drs. F. Willemsen	Ministerie van Veiligheid en Justitie - Wetenschappelijk Onderzoeks - en Documentatiecentrum (WODC)
Mr. dr. J.B.J. van der Leij	Ministerie van Veiligheid en Justitie – Wetenschappelijk Onderzoeks - en Documentatiecentrum (WODC)
mr. dr. H.H. Kielman LL.M. Phd.	Universiteit Leiden - Faculteit der Rechtsgeleerdheid
mr. C.I. Grasdijk	Ministerie van Veiligheid en Justitie - Directoraat-generaal Politie (tot 1 januari 2013)
mr. A.D Gietema	Ministerie van Veiligheid en Justitie - Directoraat-generaal Politie (vanaf 1 januari 2013)
B. Luters	Regiopolitie Zeeland
mr. R.P. Tuinenburg	Openbaar ministerie - Arrondissementsparket Amsterdam
mr. E.E. Gillissen	Ministerie van Defensie - Directie Juridische Zaken, Afdeling Wet- en regelgeving

Bijlage 6 Lijst met afkortingen

ADR	Auditdienst Rijk
AIVD	Algemene Inlichtingen en Veiligheidsdienst
Awb	Algemene wet bestuursrecht
BJZ	Bureau Jeugdzorg
BOD	Bijzondere Opsporingsdiensten
Bpg	Besluit politiegegevens
BPS	Bedrijfsprocessen Systeem
BVH	Basisvoorziening Handhaving
BVO	Basisvoorziening Opsporing
Bw	Burgerlijk Wetboek
CBP	College Bescherming Persoonsgegevens
CIE	Criminele Inlichtingen Eenheid
CJG	Centrum voor Jeugd en Gezin
DAD	Departementale auditdienst
EU	Europese Unie
EVRM	Europees Verdrag voor de Rechten van de Mens
FIOD	Fiscale Inlichtingen- en Opsporingsdienst
GGD	Gemeenschappelijke Gezondheids Dienst
ILT-IOD	Inspectie Leefomgeving en Transport – Inlichtingen en Opsporingsdienst
IND	Immigratie- en Naturalisatiedienst
ISZW	Inspectie Sociale Zaken en Werkgelegenheid
KLPD	Korps Landelijke Politiediensten
Kmar	Koninklijke marechaussee
LIEC	Landelijk Informatie en Expertise Centrum
MvT	Memorie van toelichting
NFI	Nederlands Forensisch Instituut
NVWA-IOD	Nederlandse Voedsel en Waren Autoriteit – Inlichtingen en Opsporingsdienst
OM	Openbaar Ministerie
OvJ	Officier van Justitie
PV	Proces Verbaal
RBS	Recherche Basis Systeem
RDW	Rijksdienst Wegverkeer
RID	Regionale Inlichtingendienst
RIEC	Regionaal Informatie en Expertise Centrum
RIO	Regionale Informatieorganisatie
Sv	Wetboek van Strafvordering
Wbp	Wet bescherming persoonsgegevens
Wet BIG	Wet op de Beroepen in de Individuele Gezondheidszorg
Wgbo	Wet op de Beroepen in de Individuele Gezondheidszorg
Wjsg	Wet justitiële en strafvorderlijke gegevens

Wjz	Wet op de jeugdzorg
Wob	Wet openbaarheid van bestuur
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum
Wpg	Wet politiegegevens
Wpolr	Wet Politieregisters