Samenvatting

Projectnummer 2236
Titel Glazen privacy – Knelpuntenonderzoek uitvoering 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 websites 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

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:

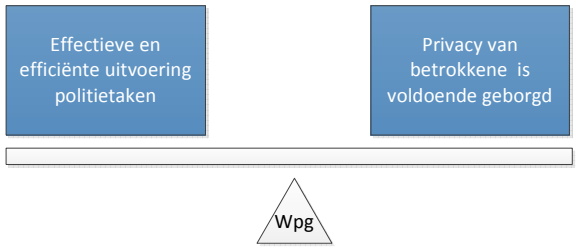
1. Wat heeft de wetgever beoogd met de Wet politiegegevens (wat is de beleidstheorie)?
2. Hoe wordt de Wet politiegegevens in de praktijk uitgevoerd; is dit volgens de doelstellingen en de verwachtingen van de wetgever en wat zijn de resultaten en knelpunten?

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 in plaats van 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 en bedrijfsmatige borging binnen Nationale politie

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.