pro facto

Verkennend onderzoek

De verwerking van politiegegevens in vijf Europese landen

Groningen, 20 november 2020

www.pro-facto.nl

Ossenmarkt 5
9712 NZ Groningen

profacto@pro-facto.nl
050 313 98 53

rijksuniversiteit groningen

Colofon

Het onderzoek is – in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) – uitgevoerd door Pro Facto, bureau voor bestuurskundig en juridisch onderzoek, advies en onderwijs, en de vakgroep Staatsrecht, Bestuursrecht en Bestuurskunde van de Rijksuniversiteit Groningen.

Projectleider:	prof. dr. Heinrich Winter
Onderzoekers:	Joachim Bekkering (LLB; onderzoeksassistent), mr. Tinka Floor, dr.ir. Bieuwe Geertsema, mr. Stef Roest en dr. John Smits
Met medewerking van:	prof. dr. Jeanne Mifsud Bonnici
Begeleidingscommissie:	prof. mr. G.K. Sluiter (voorzitter), dr. C.H.M. Geuijen, dr. B. Van der Sloot, mr. C.A.N. Huisman, dr. L.M. van der Knaap

Samenvatting

Doel en verantwoording
Dit verkennende onderzoek is in opdracht van het WODC uitgevoerd en behelst een inventarisatie van de verschillende mogelijkheden om de verwerking van politiegegevens in wetgeving te regelen. Het doel van het onderzoek is inzichtelijk te maken hoe het juridisch kader voor de verwerking van politiegegevens in een vijftal andere Europese landen is vormgegeven en hoe dat kader zich verhoudt tot de Europese basisprincipes. De bevindingen uit dit onderzoek kunnen als input dienen voor de herziening van de Wet politie gegevens (Wpg). In dit onderzoek staan de volgende twee hoofdvragen centraal:

1. *Wat is de huidige stand van zaken in Nederland wat betreft de wet- en regelgeving voor het verwerken van politiegegevens, in hoeverre zijn de eerder geconstateerde knelpunten hierbij opgelost en welke knelpunten bestaan nog? Hoe heeft Nederland invulling gegeven aan het Europese kader voor de verwerking van gegevens door de politie?*
2. *Wat is geregeld in de wet- en regelgeving voor het verwerken van politiegegevens in andere Europese landen, hoe hebben deze landen de in Nederland bestaande en eventuele andere knelpunten ondervangen in wet- en regelgeving en hoe is hierin invulling gegeven aan het Europese kader voor de verwerking van gegevens door de politie?*

Dit leidde tot de volgende deelvragen:
1. Wat is de huidige stand van zaken in Nederland wat betreft de wet- en regelgeving met betrekking tot het verwerken van politiegegevens, in hoeverre zijn de eerder geconstateerde knelpunten hierbij opgelost en welke knelpunten bestaan nog?
2. Op basis van welke grondslagen worden in andere Europese landen politiegegevens verkregen?
3. Welke kaders zijn er in andere Europese landen met betrekking tot het bewerken van politiegegevens? In hoeverre wordt in wet- en regelgeving aandacht besteed aan nieuwe technologische ontwikkelingen, bijvoorbeeld op het gebied van het koppelen van bestanden en de inzet van methoden en technieken voor het analyseren van big data?
4. Welke kaders zijn er in andere Europese landen met betrekking tot het verstrekken van politiegegevens aan derden en wordt daarbij onderscheid gemaakt tussen verschillende partijen?
5. Welke bewaartermijnen en vernietigingsvoorwaarden gelden er in andere Europese landen? Wordt hierbij onderscheid gemaakt naar soorten gegevens of verschillende doeleinden?
6. Hoe is in andere Europese landen in de wet het toezicht vormgegeven op de verwerking van politiegegevens?
7. Worden politiegegevens in andere Europese landen ‘gelabeld’ of ‘gecategoriseerd’ en zo ja, welke labels worden gehanteerd (bijvoorbeeld feitelijke gegevens, zachte gegevens, gevoelige gegevens, et cetera)?
8. Hoe verhouden de antwoorden op bovenstaande vragen zich tot het Europeesrechtelijke kader voor verwerking van politiegegevens, met name de Richtlijn gegevensbescherming opsporing en vervolging (Richtlijn 2016/680)?

Om antwoord te kunnen geven op hoofdvraag 1 en relevante vragen te kunnen stellen in de te onderzoeken landen, was het van belang om het huidige juridisch kader in Nederland voor

het verwerken van politiegegevens duidelijk in beeld te hebben. De daarvoor benodigde data zijn verzameld door middel van deskresearch en vier interviews met sleutelinformanten van de politie, de Koninklijke Marechaussee en het Ministerie van Justitie en Veiligheid en een expert uit de universitaire wereld.

Door middel van een quickscan en vooraf opgestelde criteria zijn vijf Europese landen geselecteerd. De geselecteerde landen zijn België, Denemarken, Duitsland, Finland en Ierland. In elk land is een deskresearch uitgevoerd waarmee de regelgeving in elk vergelijkingsland in kaart is gebracht. De verkregen informatie is vervolgens verdiept, getoetst en aangevuld met (praktijk)informatie uit interviews met mensen van de politie, toezichthouder(s), beleidsmedewerkers van het verantwoordelijke departement en onafhankelijke academische experts. Alleen in Denemarken is het niet gelukt om alle beoogde gesprekspartners te spreken. Het is belangrijk om te melden dat door de korte looptijd en het beperkte doel (het in kaart brengen van de regelgeving) van dit onderzoek, er geen compleet beeld kon worden gevormd van de uitvoeringspraktijk in elk vergelijkingsland.

Knelpunten Nederland

Uit het deelonderzoek Nederland komt het beeld naar voren van een sinds de inwerkintreding in 2008 nauwelijks veranderde Wpg in een sterk veranderde, gedigitaliseerde wereld. Ontwikkelingen als de overgang naar één Nationale Politie, digitalisering, technologisering en de implementatie van de Richtlijn gegevensbescherming opsporing en vervolging (Richtlijn) hebben niet tot een (ingrijpende) herziening van de Wpg geleid. Gezien dit feit is het dan ook niet verrassend dat enkele knelpunten die tijdens de evaluatie van de Wpg 2013 zijn geconstateerd, zich nog steeds voordoen. Daarnaast zijn er ook nieuwe knelpunten ontstaan. De belangrijkste knelpunten zijn:

Wetssystematiek: de naleving en 'naleefbaarheid' van de Wpg

De Wpg is moeilijk na te leven omdat deze veel open normen bevat, op andere punten wellicht juist te gedetailleerd is en niet goed aansluit op uitvoeringspraktijk en organisatie/ICT. Ook is de Wpg oorspronkelijk geschreven voor de verwerking van gegevens door en uitwisseling tussen regionale korpsen binnen Nederland. Daarnaast heeft de implementatie van de Richtlijn de naleefbaarheid van de Wpg ook niet verbeterd. De Richtlijn is van toepassing op *de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen (met inbegrip van de afweer van gevaren voor de openbare orde en veiligheid)* door (daartoe) *bevoegde autoriteiten*. De Wpg definieert een *politiegegeven* net als in de tijd voorafgaand aan de Richtlijn als *elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak.*[1] Hierop zijn echter wel uitzonderingen. Zo is met de inwerkingtreding van het Europese kader een aantal taken onder de AVG komen te vallen.[2] Art 2 Wpg verklaart de Wpg vervolgens van toepassing op de verwerking van politiegegevens door een bevoegde autoriteit, waarbij voor de definitie van 'bevoegde autoriteit' weer wordt aangesloten bij de politietaken in de zin van de Politiewet 2012 en art. 1 sub a Wpg, in plaats van de definitie van de Richtlijn over te nemen. Dit zorgt voor verwarring en afbakeningsproblematiek.

Wetssystematiek en bewerken van gegevens: de categorisering van politiegegevens

Politiegegevens worden op grond van de Wpg gecategoriseerd naar politietaak (art. 8-13 Wpg). Bij elke categorie hoort een verwerkingsregime met bewaartermijn dat in de praktijk

[1] Zoals omschreven in art. 3 en 4 Politiewet 2012.
[2] Zoals die op grond van de Vreemdelingenwet 2000.

voor 'verschotting' zorgt. Dit is niet praktisch voor het politiewerk omdat gegevens in meerdere categorieën kunnen vallen en de rol van de betrokkene per dossier kan verschillen, waardoor het onduidelijk is welk regime moet worden toegepast.

Wetssystematiek: samenloop met andere wettelijke regimes voor gegevensverwerking

De Wpg overlapt en heeft raakvlakken met diverse andere wetten en regimes voor gegevensverwerking. Dit zorgt voor onduidelijkheid, bijvoorbeeld bij het verstrekken van gegevens aan partijen die onder de AVG vallen.

Verkrijgen van gegevens: grondslag voor verkrijgen gegevens te beperkend voor politiewerk

Art. 3 Politiewet 2012 (omschrijving van de politietaak) is veelal de grondslag voor de verkrijging van gegevens die zijn verzameld met nieuwe technieken om de openbare orde te handhaven. Een voorbeeld hiervan is het inzetten van de bodycam. Dit algemene artikel voldoet echter alleen als wettelijke grondslag als sprake is van een geringe inbreuk op de persoonlijke levenssfeer; voor ingrijpender inbreuken is een specifieke wettelijke basis nodig.

Digitalisering en technologisering

Er zijn steeds meer gegevens beschikbaar uit steeds meer verschillende bronnen. Voorbeelden zijn het internet, drones en bodycams. Ook zijn er steeds meer mogelijkheden om (grootschalige) data te analyseren. Voor elke inbreuk op de persoonlijke levenssfeer is daarentegen volgens (Europese) privacywetgeving een specifieke wettelijke regeling vereist. De vraag is hoe de Nederlandse wetgeving hieraan kan voldoen en tegelijkertijd voor langere tijd mee kan zonder bij elke nieuwe technologische ontwikkeling achterhaald te zijn.

Bewaren van gegevens: meerdere dilemma's met bewaartermijnen

Gegevens kunnen in verschillende verwerkingsregimes vallen, waardoor er meerdere bewaartermijnen gelden ten opzichte van dezelfde gegevens. Daarnaast zijn bewaartermijnen opgenomen in verschillende wetten, waardoor het niet altijd duidelijk is hoe lang gegevens mogen worden bewaard. Ook wordt bij de politie een spanningsveld ervaren tussen het belang van privacy en de vrees voor het verlies van voor het politiewerk waardevolle informatie. Dit heeft als gevolg dat gegevens te lang bewaard worden.

Verstrekken en delen van gegevens: semi-gesloten verstrekkingsregime Wpg wringt met behoefte aan samenwerking

Delen van politiegegevens buiten het Wpg-domein is slechts bij uitzondering mogelijk vanwege het semi-gesloten regime van de Wpg. Dit regime past niet (meer) bij het niveau van samenwerking tussen de politie en andere partijen binnen Nederland. Aan de andere kant bestaan politiegegevens vaak uit gevoelige en soms zachte informatie en is het onderscheid tussen feit en mening soms lastig te maken.

Verstrekken en delen van gegevens: controle op waarborgen bij verstrekking aan derde landen omslachtig

Verstrekking aan derde landen op grond van art. 17a Wpg kan een knelpunt vormen. Ook de BES-eilanden vallen onder deze derde landen. Wanneer niet eerder is vastgesteld dat het derde land/de internationale organisatie onder art. 17a lid 2 valt, moet de verwerkingsverantwoordelijke elke keer zelf de afweging maken tussen noodzaak van verstrekking en inbreuk op rechten van de betrokkene. Dit systeem kan in de praktijk problemen opleveren, vooral wanneer vanuit een bepaald veiligheidsprobleem met een land moet worden samengewerkt, maar het desbetreffende land niet de passende privacywaarborgen biedt.

Toezicht: extern toezicht heeft nog open eindjes

De autoriteit persoonsgegevens (AP) heeft niet de bevoegdheid om verwerkingen stil te leggen of onrechtmatig verwerkte gegevens zelf te verwijderen. De vraag is of de bevoegdheden van de AP toereikend zijn. Daarnaast geven gesprekspartners aan dat de AP onvoldoende menskracht en middelen heeft om toezicht te houden.

De Nederlandse knelpunten in de vergelijkingslanden

Wetssystematiek

De wetssystematiek in de vergelijkingslanden verschilt. Enkele landen hebben ervoor gekozen zowel de AVG als de Richtlijn om te zetten/uit te werken in een nationale privacywet. Andere landen hebben de Richtlijn geïmplementeerd door middel van een aparte omzettingswet, waarbij sommige landen kiezen voor aanvullende wetgeving per bevoegde autoriteit. Duitsland had al langer in elke politiewet (in elk geval op Bondsniveau en in Nordrhein-Westfalen) een hoofdstuk over gegevensverwerking opgenomen.

De wetgeving in alle vergelijkingslanden gaat uit van de bescherming van persoonsgegevens in Europeesrechtelijke zin door de politie en andere bevoegde autoriteiten. Het begrip 'politiegegevens' en de in ons land gekozen wetssystematiek lijkt elders niet te worden gehanteerd. Het begrip 'bevoegde autoriteiten' uit de Richtlijn wordt verschillend ingevuld in de vergelijkingslanden: België, Denemarken en Nordrhein-Westfalen benoemen expliciet de bevoegde autoriteiten, terwijl andere landen letterlijk de definitie van de Richtlijn volgen en deze niet nader specificeren. Zo moet in Ierland bijvoorbeeld per geval worden bepaald of het handelen onder de Richtlijn valt.

Het verzamelen, gebruiken of delen van gegevens is op grond van de Europese en nationale regelgeving alleen rechtmatig als daarvoor een wettelijke grondslag bestaat en noodzakelijk is met het oog op het doel. Zo'n doel en wettelijke grondslag kan zijn het uitvoeren van een in de wet omschreven politietaak. In de vergelijkingslanden worden gegevens niet 'statisch' gecategoriseerd naar onderdeel van de politietaak en het bijpassende doel ('dagelijkse politietaak', onderzoek in een bepaald geval, etc.), zoals in Nederland op grond van art. 8-13 Wpg, maar wordt de politietaak gebruikt bij het beoordelen van de doelbinding, noodzakelijkheid en proportionaliteit van de verwerking van persoonsgegevens. Persoonsgegevens kunnen dus eerder voor andere doelen worden gebruikt dan waarvoor ze zijn verzameld, mits dit past binnen het taakveld van de politie; de vergelijkingslanden hebben minder last van verschotting door de categorisering van gegevens.

Verkrijgen

De verkrijgingsgrondslagen voor politiegegevens in de vergelijkingslanden komen grotendeels overeen met de Nederlandse grondslagen. De algemene voorwaarden en waarborgen komen namelijk voort uit de Europese beginselen van gegevensbescherming. De vergelijkingslanden hebben veel verschillende specifieke wettelijke grondslagen voor politiehandelen in bijzondere wetten (naast de algemene basis in de privacywetgeving, politiewetgeving en het wetboek van strafvordering) om een inbreuk op de persoonlijke levenssfeer te rechtvaardigen. De nadruk die de landen hierbij leggen verschilt: het ene land legt de nadruk meer op de informatiepositie van de politie, het andere land meer op de bescherming van persoonsgegevens.

Digitalisering

Als het gaat om digitalisering en technologisering en het verkrijgen van persoonsgegevens ervaren alle landen hetzelfde knelpunt als Nederland. Elk land probeert rekening te houden

met de snelle technologische ontwikkelingen door de wetgeving zo 'technologieneutraal' mogelijk te formuleren terwijl de wetgeving tegelijkertijd vanuit het perspectief van grondrechten zo specifiek mogelijk dient te zijn.

In de vergelijkingslanden hebben wij ook onderzocht welke bevoegdheden autoriteiten hebben wanneer gegevens eenmaal in hun bezit zijn (mogelijkheden tot het bewerken van politiegegevens). Gezien de Nederlandse knelpunten lag hierbij de focus op (technische) gebruiks- en analysemogelijkheden, waaronder het gebruik voor andere doelen dan waarvoor de data zijn verkregen. Het merendeel van de landen heeft de Richtlijn op dit punt vrijwel één op één overgenomen. De landen kiezen ervoor geen nadere invulling te geven aan de technologische mogelijkheden. Wel kennen de vergelijkingslanden algemene richtlijnen voor het gebruik van nieuwe technieken. Deze richtlijnen zien veelal op noodzakelijkheid, proportionaliteit, doelbinding en passende technische en organisatorische beveiligingsmaatregelen. In de praktijk leidt dit tot terughoudendheid en voorzichtigheid bij de inzet van nieuwe technologische mogelijkheden bij de verwerking van persoonsgegevens.

Bewerken

In Nederland worden politiegegevens gecategoriseerd naar politietaak. Dit maakt het bewerken van gegevens (het gebruiken van gegevens voor een ander doel dan waarvoor zij verzameld zijn) lastig. Op Duitsland na stellen de vergelijkingslanden hier minder hoge eisen aan. Bewerken van gegevens is bijvoorbeeld al mogelijk wanneer het nieuwe doel past binnen het taakveld van politie en justitie. In Duitsland zijn zware voorwaarden verbonden aan verwerking voor een ander doel dan waarvoor verkregen. Er moet minstens sprake zijn van een net zo ernstig strafbaar feit of een net zo zwaarwegend belang of rechtsgoed ('beginsel van hypothetische nieuwe gegevensverkrijging').

Voor het bewerken van politiegegevens is het van belang dat gegevens duidelijk worden gecategoriseerd en gelabeld. De vergelijkingslanden hebben de verplichte categorisering van persoonsgegevens uit de Richtlijn overgenomen in hun wetgeving en hebben hier vaak categorieën aan toegevoegd. In de praktijk doen zich echter nog steeds dezelfde problemen voor als in Nederland: het onderscheid tussen feit en mening is soms lastig te maken, en de rol van de betrokkene kan per dossier verschillen. Daarnaast lenen grote datasets zich niet voor categorisering omdat de eisen aan categorisering meer op individuele gevallen toegesneden zijn.

Bewaren en vernietigen

De regels over de termijnen voor het bewaren en verwijderen/archiveren/vernietigen van gegevens zijn in de vergelijkingslanden verschillend. In België en Finland zijn bij wet regels gesteld met betrekking tot de bewaartermijnen en vernietigingsgronden. In Duitsland, Denemarken en Ierland is dit voornamelijk vastgelegd in protocollen van bevoegde autoriteiten en overgelaten aan de beoordeling van de professional in het individuele geval, waarbij Duitsland bepaalde maximumtermijnen (voor controle of gegevens langer moeten/mogen worden bewaard) vervolgens wel weer opneemt in wetgeving.

Verstrekken en delen

In alle vergelijkingslanden kunnen drie soorten verstrekkingen van politiegegevens aan nationale autoriteiten worden onderscheiden: verstrekkingen aan andere autoriteiten binnen het regime van de Richtlijn, verstrekkingen aan instanties met een publieke en wettelijke taak waarvoor gegevensdeling passend is, en verstrekkingen aan organisaties en personen die daarbuiten vallen. Voor de eerste groep is de Richtlijn van toepassing en zijn de voorwaarden laagdrempelig. In de vergelijkingslanden verschillen de voorwaarden en eisen voor de andere

twee groepen. Wel is het zo dat in alle vergelijkingslanden voor het verstrekken en/of delen aan deze twee groepen altijd een bepaalde vorm van regulering is opgesteld in de vorm van overeenkomsten.

Bij verstrekking aan buitenlandse instanties is de Richtlijn leidend, met als gevolg dat ten aanzien van verstrekking aan derde landen in elk land dezelfde discussie speelt als in Nederland. Met name de Deense situatie is in dit geval interessant voor Nederland, omdat Denemarken net als Nederland overzeese gebieden buiten het Europees grondgebied heeft. Deze gebieden gelden als derde landen, waardoor niet zonder meer gegevens gedeeld kunnen worden. Denemarken werkt daarom aan de implementatie van voldoende gegevensbeschermingsregels in die gebieden om een adequaatheidsbesluit van de Europese Commissie te krijgen. Ook is het van belang om te benoemen dat Duitsland naar aanleiding van rechtspraak van het Bundesverfassungsgericht een extra toets aan rechtsstatelijkheid en mensenrechten in de wet heeft opgenomen die moet worden uitgevoerd voordat tot delen van gegevens aan derde landen wordt overgegaan.

Toezicht

Het externe toezicht is in de vergelijkingslanden vaak belegd bij een algemene autoriteit die toeziet op zowel de AVG als op de Richtlijn. Alleen België wijkt hier af: er is een externe toezichthouder specifiek voor de uitvoering van de Richtlijn. Deze toezichthouder bestond voor de implementatie van de Richtlijn al in iets andere vorm en is opgericht omdat een speciale toezichthouder meer expertise zou kunnen inzetten ten aanzien van het werk van bevoegde autoriteiten. In alle vergelijkingslanden blijkt dat de toezichthouder veelal zachte middelen inzet wanneer die moet optreden tegen een verwerking van persoonsgegevens. De externe toezichthouder heeft, in tegenstelling tot de AP, in veel landen wel de mogelijkheid om hard in te grijpen door bijvoorbeeld het verwerkingsprocessen te laten stopzetten. In de praktijk wordt dit middel echter vrijwel niet gebruikt omdat het te ingrijpend wordt geacht.

Met betrekking tot de toegang van betrokkenen tot de over hen verzamelde en verwerkte gegevens volgen op België na alle landen de Richtlijn. België hanteert het systeem van ‘onrechtstreekse toegang’. Dit houdt in dat de toezichthoudende autoriteit het verzoek om toegang behandelt, zo nodig doorspeelt en slechts beperkte informatie over de verwerking van gegevens aan de betrokkene terugkoppelt. Het is zeer de vraag of deze interpretatie van de Richtlijn houdbaar is.

Vervolg

Dit verkennende onderzoek biedt de Nederlandse wetgever aanknopingspunten voor de aanpassing van de Nederlandse regelgeving en een mogelijk vertrekpunt voor nader onderzoek van de omschreven ontwikkelingen die in andere landen spelen en keuzes die elders worden gemaakt. Een verdieping van dat onderzoek zou kunnen worden gevonden door ook de uitvoeringspraktijk in vergelijkingslanden daarbij in sterkere mate te betrekken.

pro facto