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

Inhoud

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.

Summary

Purpose and accountability
This exploratory study was carried out on behalf of the WODC (Research and Documentation Centre of the Dutch Ministry of Justice and Security), and comprises an inventory of the various options for regulating the processing of police data in legislation. The aim of the study is to provide insight into how the legal framework for the processing of police data is designed in five other European countries and how that framework relates to the European basic principles. The findings from this study can serve as input for the revision of the Police Data Act (Wet politiegegevens, Wpg). The following two main questions are central to this research:

- *What is the current state of affairs in the Netherlands with regard to the legislation for processing police data, to what extent have the previously identified problems been resolved and what problems remain? How has the Netherlands implemented the European framework for the processing of data by the police?*
- *What is regulated in the legislation for the processing of police data in other European countries, how have these countries overcome the problems that exist in the Netherlands and any other problems through legislation, and how has the European framework for the processing of data by the police been implemented?*

This leads us to the following subquestions:

1. What is the current state of affairs in the Netherlands with regard to the legislation on the processing of police data, to what extent have the previously identified problems been resolved and what problems remain?
2. On what grounds are police data obtained in other European countries?
3. What frameworks are there in other European countries for the processing of police data? To what extent does legislation focus on new technological developments, for example in the field of linking files and the use of methods and techniques for analysing big data?
4. What frameworks are in place in other European countries for providing police data to third parties, and is a distinction made between different parties?
5. What retention periods and destruction conditions apply in other European countries? Is a distinction made between types of data or different purposes?
6. How, in other European countries, is the supervision of the processing of police data arranged by law.
7. Are police data in other European countries 'labeled' or 'categorized' and if so, which labels are used (e.g. factual data, soft data, sensitive data, etc.)?
8. How do the answers to the above questions relate to the European legal framework for processing police data, in particular the Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution (Directive 2016/680)?

In order to answer main question 1 and ask relevant questions in the countries to be studied, it was important to have a clear picture of the current legal framework in the Netherlands for processing police data. The data required for this were collected by means of desk research and four interviews with key informants from the police, the Royal Netherlands

Marechaussee (Kmar) and the Ministry of Justice and Security and an expert from the academic world.
Five European countries were selected by means of a quick scan and predefined criteria. The selected countries are Belgium, Denmark, Germany, Finland and Ireland. Desk research was carried out in each country to look at the legislation in each reference country. The information obtained was then examined in more detail, tested and supplemented with (practical) information from interviews with people from the police, supervisors, policy officers from the responsible department and independent academic experts. Only in Denmark has it not been possible to speak to all the intended parties. It is important to note that due to the short duration and limited aim (mainly studying the legislation) of this study, it was not possible to form a complete picture of the implementation practice in each reference country.

Problems in the Netherlands
The sub-study in the Netherlands shows that the Wpg has hardly changed, in a rapidly developing digitized world, since its entry into force in 2008. Developments such as the transition to a single National Police Force, digitization, technology and the implementation of the Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution have not resulted in a (radical) revision of the Wpg. It is therefore not surprising that some problems identified during the evaluation of the Wpg in 2013 remain. In addition, new problems have also arisen. The main problems are:

Legislative system: compliance with the Wpg and the extent to which the Wpg lends itself to compliance

The Wpg is difficult to comply with because it contains many open standards, is perhaps too detailed on other points and is not very aligned with implementation practice and organization/ICT. Additionally, the Wpg was originally written for the processing of data by and the exchange of data between regional police forces within the Netherlands. Neither has the implementation of EU Directive 2016/680 improved compliance with the Wpg. The Directive applies to the *prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (including the safeguarding against and the prevention of threats to public security*) by competent authorities. The Wpg defines police data, just as in the time prior to the Directive, as *any personal data that are processed in the context of the performance of the police task.* However, there are exceptions to this. For example, with the entry into force of the European framework, a number of tasks now fall under the GDPR. Art 2 Wpg declares the Wpg applicable to the processing of police data by a competent authority, whereby a 'competent authority' is defined based on the police tasks referred to in the Police Act 2012 and art. 1 sub a Wpg, rather than using the definition set out in the Directive. This creates confusion and demarcation problems.

Legislative system and data processing: the categorization of police data

Police data are categorized by police task on the basis of the Wpg (art. 8-13 Wpg). Each category has a processing regime with a retention period that, in practice, creates 'surplus'. This is not practical for police work because data can fall into several categories and the role of the data subject can differ per case, making it unclear which regime should be applied.

Legislative system: concurrence with other legal regimes for data processing

The Wpg overlaps and has interfaces with various other laws and regimes for data processing. This creates a lack of clarity, for example when providing data to parties that fall under the GDPR.

Acquiring data: basis for acquiring data is too restrictive for police work

Art. 3 of the Police Act 2012 (description of the police task) is often the basis for acquiring data collected with new techniques to maintain public order. An example of this is the use of the bodycam. However, this general article only acts as a legal basis if there is a minor breach of privacy; more serious breaches require a specific legal basis.

Digitization and technology

There are more and more data available from more and more different sources. For example, the internet, drones and bodycams. There are also more and more possibilities to analyse data (on a large scale). On the other hand, according to (European) privacy legislation, a specific legal regulation is required for every breach of privacy. The question is, how can Dutch legislation comply with this and at the same time last for a longer period of time without becoming outdated with every new technological development?

Retention of data: multiple dilemmas with retention periods

Data can fall under different processing regimes, which means that multiple retention periods apply to the same data. In addition, retention periods have been included in various laws, so it is not always clear how long data may be retained. The police also experience tension between the importance of privacy and concern about losing information valuable for police work. As a result, data are retained for too long.

Provision and sharing of data: semi-closed provision regime of the Wpg incompatible with the need for cooperation

Sharing police data outside the Wpg domain is only possible in exceptional cases due to the semi-closed regime of the Wpg. This regime is not (any longer) in line with the level of cooperation between the police and other parties in the Netherlands. On the other hand, police data often consists of sensitive and sometimes soft information, and it is sometimes difficult to distinguish between fact and opinion.

Provision and sharing of data: checking safeguards when disclosing to third countries is cumbersome

Provision to third countries on the basis of art. 17a Wpg can be a problem. The BES islands (Bonaire, Saint Eustatius and Saba) also fall under these third countries. If it has not previously been established that the third country/international organization falls under art. 17a paragraph 2, the controller must each time weigh up the need for disclosure and the infringement of the rights of the data subject. This system can cause problems in practice, especially when cooperation with a country is required on the basis of a certain security problem, but the country in question does not offer the appropriate privacy safeguards.

Supervision: external supervision still has open ends

The Personal Data Authority (AP) does not have the authority to stop processing or to delete unlawfully processed data. The question is whether the powers of the AP are sufficient. In addition, discussion partners say that the AP has insufficient manpower and means to supervise.

The Dutch problems in the reference countries

Legal system

The legal system in the reference countries differs. Some countries have opted to convert/implement both the GDPR and the Directive into a national privacy law. Other countries have implemented the Directive through a separate transposition law, with some countries opting

for additional legislation per competent authority. Germany had already included a section on data processing in each police act (at least at Federal level and in North Rhine-Westphalia).

The legislation in all reference countries is based on the protection of personal data, as defined in European law, by the police and other competent authorities. The term ‘police data’ and the legal system opted for in the Netherlands does not seem to be used elsewhere. The term 'competent authorities' in the Directive is interpreted differently in the reference countries: Belgium, Denmark and North Rhine-Westphalia explicitly name the competent authorities, while other countries follow the definition of the Directive literally and do not specify it further. In Ireland, for example, whether the action falls under the Directive has to be determined on a case-by-case basis.

The collection, use or sharing of data is only lawful under European and national regulations if there is a legal basis for this and it is necessary for the purpose. Such a purpose and legal basis may be the performance of a police task described by law. In the reference countries, data are not categorized ‘statically’ according to the police task and the corresponding purpose (‘daily police task’, investigation in a specific case, etc.), as in the Netherlands on the basis of art. 8-13 Wpg, but the police task is used as a basis when assessing the purpose limitation, necessity and proportionality of the processing of personal data. Personal data can therefore be used for purposes other than those for which they were collected, provided this fits within the task field of the police; the reference countries are less affected by surpluses due to the categorization of data.

Acquisition

The bases for obtaining police data in the reference countries largely correspond with the Dutch bases. The general conditions and safeguards are based on the European principles of data protection. The reference countries have many different specific legal bases for police action in special laws (in addition to the general basis in privacy law, police law and the criminal procedure code) to justify a breach of privacy. The emphasis that the countries place in this respect differs: one country puts more emphasis on the information position of the police, the other country more on the protection of personal data.

Digitization

When it comes to digitization and technology and the acquisition of personal data, all countries experience the same problem as the Netherlands. Each country tries to take into account the rapid technological developments by formulating the legislation as ‘technology-neutral’ as possible, while at the same time the legislation must be as specific as possible from a fundamental rights perspective.

In the reference countries, we also investigated what powers authorities have once data are in their possession (options for processing police data). Given the Dutch problems, the focus was on (technical) use and analysis options, including use for purposes other than those for which the data were obtained. Most of the countries have adopted the Directive almost literally on this point. The countries choose not to give further substance to the technological possibilities. The reference countries do, however, have general guidelines for the use of new techniques. These guidelines often concern necessity, proportionality, purpose limitation and appropriate technical and organizational security measures. In practice, this leads to restraint and caution in the use of new technological possibilities in the processing of personal data.

Editing

In the Netherlands, police data are categorized by police task. This makes editing data (in this study defined as: using data for a purpose other than that for which it was collected) difficult. With the exception of Germany, the reference countries set less stringent requirements for this. For instance, the editing of data is possible when the new purpose fits within the task field of the police and the judiciary. In Germany, strict conditions apply to processing data for a purpose other than that for which they were obtained. At the very least, there must be an equally serious criminal offence or an equally important interest or legal claim ('principle of hypothetical re-collection of data').

When editing police data, it is important that data are clearly categorized and labeled. The reference countries have adopted the mandatory categorization of personal data from the Directive into their legislation and have often added categories to it. In practice, however, the same problems still arise as in the Netherlands: the distinction between fact and opinion is sometimes difficult to make, and the role of the data subject may differ per case. In addition, large datasets do not lend themselves to categorization because the requirements for categorization are more tailored to individual cases.

Retention and destruction

The rules on the deadlines for retaining and deleting/archiving/destroying data differ in the reference countries. In Belgium and Finland, rules have been laid down by law with regard to retention periods and grounds for destruction. In Germany, Denmark and Ireland this is mainly laid down in protocols of competent authorities and left to the discretion of the professional in the individual case. Germany lays down certain maximum periods (for checking whether data should/may be kept longer) in legislation.

Provision and sharing

In all reference countries, three types of disclosures of police data within the country can be distinguished: disclosures to other authorities within the regime of the Directive, disclosures to authorities with a public and legal task for which data sharing is appropriate, and disclosures to other organizations and persons. The Directive applies to the first group and the conditions are set at a low level. The conditions and requirements for the other two groups differ in the reference countries. However, a certain form of regulation has always been drawn up in the form of agreements for the provision to and/or sharing with these two groups.

In the case of disclosure in the international sphere, the Directive is leading, with the result that the same debate as in the Netherlands is going on in each country with regard to disclosure to third countries. The Danish situation is particularly interesting for the Netherlands in this case, because Denmark, like the Netherlands, has overseas territories outside European territory. These areas are regarded as third countries, which means that data cannot be automatically shared. Denmark is therefore working on the implementation of sufficient data protection rules in those areas to get an adequacy decision from the European Commission. It is also important to point out that, following up case law of the Federal Constitutional Court (Bundesverfassungsgericht), Germany has included in the legislation an additional test of the rule of law and human rights that must be carried out before sharing data with (parties in) third countries.

Supervision

In the reference countries, external supervision is often entrusted to a general authority that supervises both the GDPR and the Directive. Only Belgium deviates here: it has an external supervisor specifically for the implementation of the Directive. This supervisor already existed

in a slightly different form before the implementation of the Directive and was established because a special supervisor could deploy more expertise with regard to the work of competent authorities. In all reference countries, it appears that the supervisor often uses soft means when it has to act against the processing of personal data. In contrast to the AP, the external regulator does have the option in many countries to intervene sharply, for example by having the processing operations stopped. In practice, however, this remedy is hardly used because it is considered to be too drastic.

With regard to the access of data subjects to the data collected and processed about them, all countries except Belgium follow the Directive. Belgium uses the system of 'indirect access'. This means that the supervisory authority processes the request for access, passes it on if necessary and only provides limited information about the processing of data to the data subject. Whether this interpretation of the Directive is tenable is very questionable.

Follow up

This exploratory study provides the Dutch legislator with starting points for adapting Dutch legislation and a possible starting point for further research into the described developments that are taking place in other countries and choices that are made elsewhere. This study could be expanded by including the implementation practice in the reference countries to a larger extent.

1

Inleiding

1.1 Achtergrond

De Wet politiegegevens (Wpg) vormt in Nederland het kader voor (een deel van) de verwerking van persoonsgegevens door de politie, KMar, Rijksrecherche, bijzondere opsporingsdiensten[3] en buitengewoon opsporingsambtenaren (boa's).[4] Deze persoonsgegevens worden aangeduid met de term politiegegevens. De Algemene Verordening Gegevensbescherming (AVG) is niet van toepassing op de verwerking van politiegegevens. Op 1 januari 2008 is de Wpg in werking getreden. In 2013 hebben Arena Consulting en Pro Facto de Wpg geëvalueerd in opdracht van het Wetenschappelijk Onderzoeks- en Documentatiecentrum (WODC) van het Ministerie van Veiligheid en Justitie. De belangrijkste bevinding van het onderzoek was dat de uitvoering van de Wpg werd omschreven als "een worstelende praktijk": organisaties ervaarden de wet als moeilijk te lezen en lastig te interpreteren.[5]

Sinds de evaluatie hebben zich enkele veranderingen voorgedaan. In 2018 is ter bevordering van de samenwerking op het terrein van politie en justitie de Europese Richtlijn gegevensbescherming opsporing en vervolging aangenomen (Richtlijn).[6] De Richtlijn is in Nederland geïmplementeerd met de Wijzigingswet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen. Hierbij was het uitgangspunt minimumimplementatie.[7]

[3] De vier bijzondere opsporingsdiensten (BOD'en) zijn de Inspectie Sociale Zaken en Werkgelegenheid, de Fiscale Inlichtingen- en OpsporingsDienst (FIOD), de Nederlandse Voedsel- en Warenautoriteit (NVWA) en de Inspectie Leefomgeving en Transport (ILT).
[4] De taken van de bijzondere opsporingsdiensten en buitengewoon opsporingsambtenaren die onder de Wpg vallen zien op hun opsporingsbevoegdheden (strafrechtelijke handhaving) en nadrukkelijk niet op de toezichtstaken (bestuursrechtelijke handhaving).
[5] Smits e.a. 2013.
[6] Richtlijn (EU) 2016/680.
[7] *Kamerstukken II* 2018/19, 34889, 3.

Daarnaast hebben zich verschillende maatschappelijke ontwikkelingen voorgedaan die van invloed zijn op het werk van de politie. Hiervan zijn de belangrijkste voorbeelden digitalisering, technologisering en de toenemende mate waarin de politie samenwerkt met andere partijen die ook betrokken zijn bij handhaving en bevordering van de veiligheid in Nederland. Deze ontwikkelingen zorgen ervoor dat de politie bij uitvoering van de politietaken tegen de grenzen van de Wpg aanloopt; de wet is aan herziening toe.

Op 10 september 2019 gaf de Minister van Justitie en Veiligheid in een brief aan de kamer aan bezig te zijn met de voorbereidingen van de herziening van de Wpg.[8]

1.2 Doel- en vraagstelling

Het doel van dit vergelijkende onderzoek is om inzichtelijk te maken hoe het (juridisch) kader voor de verwerking van politiegegevens in een vijftal andere Europese landen is vormgegeven en hoe dat zich verhoudt tot de Europese basisprincipes. De bevindingen uit dit onderzoek kunnen als input dienen voor de herziening van de Nederlandse Wpg.

Vooraf dient een belangrijk voorbehoud te worden gemaakt. Dit onderzoek is een verkennend onderzoek en behelst een inventarisatie van de verschillende mogelijkheden om de verwerking van politiegegevens in wet en praktijk vorm te geven. Door de korte looptijd en het beperkte doel (het onderzoek richt zich op het in kaart brengen van wet- en regelgeving) van dit onderzoek, kan er geen compleet beeld worden gevormd van de uitvoeringspraktijk in elk casestudyland. De studie geeft dus een globaal overzicht van de wetgeving en de omgang daarmee in de bestudeerde landen, maar voor verdere verdieping is nader onderzoek nodig.

In dit onderzoek staan de volgende twee hoofdvragen centraal:

3. 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?

4. 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?

Om de centrale onderzoeksvragen te kunnen beantwoorden zijn de volgende deelvragen opgesteld:

9. 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?

10. Op basis van welke grondslagen worden in andere Europese landen politiegegevens verkregen?

[8] *Kamerstukken II* 2019/20, 29268, 859.

11. 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?

12. 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?

13. Welke bewaartermijnen en vernietigingsvoorwaarden gelden er in andere Europese landen? Wordt hierbij onderscheid gemaakt naar soorten gegevens of verschillende doeleinden?

14. Hoe is in andere Europese landen in de wet het toezicht vormgegeven op de verwerking van politiegegevens?

15. 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)?

16. 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)?

Deelvraag 1 moet antwoord geven op hoofdvraag 1 van het onderzoek en is het vertrekpunt voor dit onderzoek. Dit deel van het onderzoek dient als een soort voorfase en richt zich op het beschrijven van de Nederlandse situatie.

Deelvraag 2 tot en met deelvraag 7 richten zich op de andere Europese landen en maken deel uit van de landenvergelijking. Hierbij is het de vraag of de knelpunten die zich in Nederlandse voordoen ook in de andere Europese landen spelen en op welke wijze hiermee wordt omgegaan. Bij het opstellen van deelvragen 2 tot en met 7 is aansluiting gezocht bij de startnotitie van het WODC.

Deelvraag 8 is een uitwerking van het tweede deel van hoofdvragen 1 en 2. Hierbij wordt gekeken op welke wijze de nationale wetten en regelgeving invulling geven aan het Europese kader.

1.3 Onderzoeksmethoden

Voor de beantwoording van de onderzoeksvragen zijn verschillende onderzoeksmethoden toegepast. In deze paragraaf worden deze onderzoeksactiviteiten kort toegelicht.

1.3.1 Voorfase

Dit deel van het onderzoek richt zich op het in kaart brengen van de Nederlandse situatie en het selecteren van de casestudylanden. Gezien het feit dat dit onderzoek een vergelijkend karakter heeft en de opzet was om vijf andere landen te onderzoeken, is ervoor gekozen het onderzoek naar de Nederlandse situatie enigszins beperkt te houden.

Deskresearch

Er is deskresearch verricht naar de Nederlandse situatie. Hierbij zijn de Wpg, de evaluatie van de Wpg uit 2013 en achterliggende stukken uit de parlementaire geschiedenis bestudeerd. Op basis hiervan zijn doel en systematiek van de Wpg omschreven. Ook is in deze fase de verhouding tussen de Nederlandse wetgeving en relevante Europese wetgeving bestudeerd.

Oriënterende interviews

Om de juiste vragen te kunnen stellen in het vervolg van het onderzoek, was het essentieel dat de Nederlandse situatie eerst goed in kaart werd gebracht. In de offerte was neergelegd dat hiervoor drie oriënterende gesprekken zouden worden gevoerd. Tijdens het onderzoek is besloten een extra oriënterend interview te houden. Er is gesproken met de politie, de Koninklijke Marechaussee, de universitaire wereld en het Ministerie van Justitie en Veiligheid. Een lijst van de geïnterviewde personen is opgenomen in bijlage 6.

Tijdens de interviews is de gesprekspartners gevraagd welke knelpunten, grenzen en uitdagingen zij zien of tegenkomen bij de huidige Wpg. Daarnaast is aan de gesprekspartners gevraagd welke inzichten de landenvergelijking zou moeten opleveren op het gebied van digitalisering en uitwisseling van gegevens met derden. Door de opbrengst uit deze interviews te gebruiken bij het opstellen van itemlijsten voor de gesprekken die in de casestudylanden zijn gevoerd, kan voorzien worden aan de informatiebehoefte. Daarnaast is de gesprekspartners ook gevraagd of zij suggesties hadden voor de selectie van landen voor het vergelijkende onderzoek.

Quickscan

Met een quickscan is de wet- en regelgeving over de verwerking van politiegegevens van EU-lidstaten onderzocht. In de quickscan is rekening gehouden met een aantal selectiecriteria die tijdens de voorbereiding van het onderzoek zijn opgesteld. Volgens de belangrijkste selectiecriteria zijn we op zoek gegaan naar landen met verschillen in wet- en regelgeving, een uiteenlopende traditie van digitalisering, een verschillende cultuur(historie) op het gebied van gegevensbescherming/privacy en een verschillende mate van decentralisatie. Ook vonden we het van belang enkele buurlanden waarmee politionele samenwerking bestaat te selecteren. Op basis van deze selectiecriteria en de gevoerde interviews zijn vervolgens vijf Europese landen gekozen. Hieronder volgt per gekozen land een korte toelichting waarom de keuze op dat specifieke land is gevallen.

België

België is een buurland van Nederland waarmee veel wordt samengewerkt. Daarnaast vormt de taal geen barrière in België, omdat de wet- en regelgeving in het Nederlands beschikbaar is. Ook is België qua omvang vergelijkbaar met Nederland. Tot slot is België geselecteerd als casestudyland omdat de zaak Dutroux een herstructurering van de politie tot gevolg heeft gehad. Het werd interessant bevonden om te onderzoeken of dit effect heeft gehad op de omgang met verwerking van persoonsgegevens.

Denemarken

Denemarken vertoont veel overeenkomsten met Nederland. De organisatie van de politie in Denemarken komt voor een groot deel overeen met de Nederlandse politieorganisatie en het Deense staatsbestel lijkt op het Nederlandse. Ook is Denemarken interessant omdat het koninkrijk Denemarken naast het land Denemarken overzeese gebieden heeft die niet behoren tot de Europese Unie. Dit is vergelijkbaar met de Nederlandse situatie.

Duitsland

Een praktische reden om Duitsland te selecteren als casestudyland is omdat dit land voldoet aan de randvoorwaarden van taal en eenvoudige toegankelijkheid. Daarnaast is Duitsland een buurland van Nederland, waardoor er veel (politionele) samenwerking is. Ook acht Duitsland privacy van groot belang vanwege het nazi- en Stasiverleden. Om het onderzoek behapbaar te houden hebben we de casestudy gericht op het *Land* Nordrhein-Westfalen, omdat dit grenst aan Nederland en ongeveer evenveel inwoners heeft als Nederland.

Finland

Finland is geselecteerd als casestudyland omdat uit de QuickScan naar voren kwam dat er bij overheidsorganisaties in Finland sprake is van een hoge mate van digitalisering. Een belangrijke aanleiding voor dit onderzoek is het digitaliseringsknelpunt dat zich voordoet bij de huidige Wpg. Met betrekking tot dit knelpunt kon naar alle waarschijnlijkheid veel geleerd worden in Finland. Daarnaast is Finland qua bevolkingsomvang vergelijkbaar met Nederland.

Ierland

Ierland is gekozen als casestudyland omdat het voldoet aan de randvoorwaarde taal/toegankelijkheid. Daarnaast zijn de Europese hoofdkantoren van grote technologiebedrijven gevestigd in Dublin. Het is interessant om te onderzoeken hoe door de politie persoonsgegevens met deze bedrijven worden uitgewisseld. Tot slot werd verondersteld dat in Ierland regelgeving in verschillende opzichten aan lagere overheden is overgelaten.

Van elk van deze landen is een casestudyverslag opgesteld. Die verslagen hebben we als bijlage bij het hoofdrapport opgenomen. Over de belangrijkste bevindingen wordt in hoofdstuk 4 van het hoofdrapport gerapporteerd.

1.3.2 Landenvergelijking

Gezien het feit dat dit onderzoek een verkennend karakter heeft met als doel een inventarisatie op te leveren van de verschillende mogelijkheden om de verwerking van politiegegevens, is ervoor gekozen om in elk casestudyland een deskresearch uit te voeren en verschillende interviews te houden. Op deze manier kan de wet- en regelgeving uitvoerig worden onderzocht. Ook kan de praktijkervaring met de wet- en regelgeving worden onderzocht, zij het in beperkte mate gezien de korte looptijd en het beperkte doel van dit onderzoek.

Deskresearch

Door middel van deskresearch is de wet- en regelgeving van elk casestudyland in kaart gebracht. Hiervoor is gebruik gemaakt van nationale wet- en regelgeving, achterliggende (parlementaire) stukken en kritische bronnen van privacywaakhonden en/of toezichtsorganen. Ook is in elk land gezocht naar relevante wetenschappelijke publicaties, (wetenschappelijke) artikelen en onderzoeksrapporten. Voor alle landen (en ook Nederland) geldt dat de verwerking van politiegegevens en dan met name EU-Richtlijn 2016/680 wetenschappelijk relatief onontgonnen terrein is; er is nog weinig over geschreven en weinig onderzoek naar verricht. De Richtlijn is tegelijk met de AVG in werking getreden en de aandacht is tot nu toe vooral naar die laatste regeling uitgegaan. De volgende punten zijn aan de hand van deskresearch verhelderd:

- het doel van de wet- en regelgeving;
- de structuur van de wet- en regelgeving;
- de reikwijdte van de wet- en regelgeving;
- een globaal idee van de in het land gemaakte keuzes waar het de specifieke knelpunten betreft die in Nederland worden ervaren.

Interviews in de casestudylanden

De informatie die is verkregen door middel van deskresearch is getoetst en verdiept tijdens een aantal interviews. Het doel van deze interviews was na te gaan welke knelpunten door de geïnterviewden in de praktijk worden ervaren, of de Nederlandse knelpunten ook in het casestudyland worden ervaren en zo ja, hoe met deze knelpunten wordt omgegaan. In elk land is geprobeerd om interviews te houden met:

- wetgevingsjuristen en/of beleidsmedewerkers bij het verantwoordelijke departement;
- sleutelinformanten bij de politie;
- sleutelinformanten bij een toezichthouder/andere (politie)medewerkers die meer kunnen vertellen over het toezicht op de verwerking van politiegegevens;
- onafhankelijke academische experts die kunnen reflecteren op de praktijk.

In België, Ierland, Finland en Duitsland is het gelukt om met alle bovengenoemde gesprekspartners een interview te houden. Wel werd onze vraag naar gesprekspartners een enkele keer anders opgevat dan wij voor ogen hadden, waardoor we vanuit toezicht bijvoorbeeld in Duitsland/Nordrhein-Westfalen niet de toezichthoudende autoriteit zelf hebben gesproken, maar alleen functionarissen gegevensbescherming bij de politie.[9] Voor alle onderzochte landen moet het voorbehoud worden gemaakt dat het beperkte aantal afgenomen interviews niet representatief is voor de hele praktijk bij alle bevoegde autoriteiten. Dit geldt vooral voor Denemarken: het is in Denemarken niet gelukt interviews te houden met een wetgevingsjurist en een toezichthouder. De drukte ten gevolge van Covid-19 werd hiervoor als reden aangedragen.

We merken op dat tijdens de uitvoering van de landenvergelijking duidelijk werd dat (rechts)systemen niet zonder meer vergelijkbaar waren. Zo is het begrip 'politiegegevens' niet bekend in de vergelijkingslanden. Ze gaan in de wetgeving uit van de verwerking en bescherming van persoonsgegevens (door de politie en andere bevoegde autoriteiten). Besloten is om zoveel mogelijk aansluiting te zoeken bij de scope van de Nederlandse Wet politiegegevens. Dit had als gevolg dat buitenlandse termen zijn geïnterpreteerd in het licht van de terminologie uit de Wpg. Ook heeft de reikwijdte van de Nederlandse Wpg bepaalt welke onderwerpen onderzocht zijn en welke gesprekspartners zijn geselecteerd.

1.3.3 Analysefase

Expertbijeenkomst

De bevindingen van de voorfase en de landenvergelijking zijn bij elkaar gebracht in een conceptrapportage. De voorlopige bevindingen en conclusies zijn getoetst in een expertbijeenkomst. Bij de expertbijeenkomst zijn personen uitgenodigd met expertise op het gebied van het beleid en de praktijk in Nederland. Een overzicht van de deelnemers is opgenomen in bijlage 5.

1.4 Leeswijzer

In hoofdstuk 2 van deze rapportage wordt het Europese kader voor de verwerking van politiegegevens uiteengezet. Vervolgens komt in hoofdstuk 3 de Nederlandse wet- en regelgeving met betrekking tot politiegegevens aan de orde. In dat hoofdstuk geven we aandacht aan de

[9] Die wel zicht hebben op de werkwijze van de toezichthoudende autoriteit; ze werken daar immers intensief mee samen.

knelpunten die zich in de praktijk voordoen. In hoofdstuk 4 geven we een vergelijkende analyse van de bevindingen uit de landenstudies. Hoofdstuk 5 bevat de slotbeschouwing en de conclusies van dit onderzoek.

2

Het Europese kader

2.1 Inleiding

In dit hoofdstuk bespreken we het Europese juridisch kader dat relevant is voor de landenvergelijkende verkenning van de verwerking van politiegegevens. In Europees verband wordt dit kader gevormd door de Richtlijn gegevensbescherming, opsporing en vervolging (de Richtlijn). Deze regelt de bescherming van natuurlijke personen in verband met de verwerking van hun persoonsgegevens, binnen het domein van politie, justitie en aanverwante instanties bij uitoefening van specifieke taken. In paragraaf 2.2 bespreken we hoe deze domeinen zijn opgedeeld en gedefinieerd. Paragraaf 2.3 geeft vervolgens een beschrijving van de aard en inhoud van de Richtlijn.

2.2 Verhouding met de AVG

2.2.1 De AVG

In de AVG is het grondrecht op bescherming van persoonsgegevens, zoals vastgelegd in het Handvest van de grondrechten van de Europese Unie en het Verdrag betreffende de werking van de Europese Unie, in een Europese wet geregeld. De verordening is een Europese regeling die in Nederland op 25 mei 2018 de Wet bescherming persoonsgegevens heeft vervangen. Het feit dat de bescherming van persoonsgegevens is geregeld in een Europese verordening die in alle lidstaten geldt, zorgt voor een harmonisatie van de wet- en regelgeving in de gehele Europese Unie.

Dit onderzoek betreft de verwerking van politiegegevens, die juist niet geregeld is in de AVG. Omdat de Richtlijn gegevensbescherming, opsporing en vervolging op zeer veel vlakken overeenkomsten kent met de AVG is het toch goed om de inhoud van de AVG op hoofdlijnen door te nemen.

De AVG legt onder andere het volgende vast:

- De beginselen waar de verwerking van persoonsgegevens aan moet voldoen, de rechtvaardigingsgronden voor het verwerken van persoonsgegevens en de voorwaarden waaraan toestemming voor het verwerken van persoonsgegevens moet voldoen;

- de rechten van de betrokkene (onder meer recht op informatie, toegang, rectificatie, verwijdering, overdraagbaarheid, bezwaar en beperking) en de mogelijke uitzonderingen en beperkingen daarop;
- de eisen waaraan een behoorlijke verwerking van persoonsgegevens moet voldoen, zoals het aanstellen van een functionaris voor gegevensbescherming, het verplicht registreren van alle verwerkingen en het beveiligen van persoonsgegevens;
- de verhouding tussen de verwerkingsverantwoordelijke en de verwerker.

2.2.2 Toepassingsbereik AVG en Richtlijn

De AVG en de Richtlijn hebben verschillende toepassingsdomeinen. De AVG is breed van toepassing wanneer er sprake is van een geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, of wanneer er sprake is van handmatige verwerking van persoonsgegevens die in een bestand zijn of zullen worden opgenomen. Overheden, bedrijven, verenigingen en andere instanties die zich met dergelijke gegevensverwerking bezig houden moeten voldoen aan de AVG.

Het toepassingsgebied van de Richtlijn is veel nauwer gedefinieerd, in artikel 1, eerste lid van diezelfde Richtlijn:

> Bij deze Richtlijn worden de regels vastgesteld 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 of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

Daarin ligt besloten dat de Richtlijn van toepassing is als voldaan wordt aan de volgende vereisten:[10]

1. Het **doeleinde** van de verwerking van persoonsgegevens betreft de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten en de tenuitvoerlegging van straffen, inclusief bescherming tegen en voorkoming van gevaren voor de openbare veiligheid.
2. De verwerking van persoonsgegevens wordt gedaan door **bevoegde autoriteiten**.

De bevoegde autoriteiten worden in artikel 3, zevende lid gedefinieerd als a) een overheidsinstantie die bevoegd is voor een van de doeleinden zoals hierboven beschreven of b) een ander orgaan of entiteit gemachtigd met uitoefening van openbaar gezag en openbare bevoegdheden met het oog op deze doeleinden. In Nederland zijn dit (onder meer) de politie, de Koninklijke marechaussee, de bijzondere opsporingsdiensten, de rijksrecherche, officieren van justitie, strafrechters, het College van procureurs-generaal, de minister van Justitie en Veiligheid en buitengewoon opsporingsambtenaren.

Uit het bovenstaande volgt dat wanneer bevoegde autoriteiten gegevens verzamelen voor doeleinden anders dan hierboven beschreven (bijvoorbeeld werving en selectie van eigen personeel), dit niet onder Richtlijn maar onder de AVG valt.

[10] Wegwijzer Richtlijn 2016/680.

2.3 De Richtlijn gegevensbescherming opsporing en vervolging (Richtlijn 2016/680)

We bespreken per hoofdstuk de inhoud van de Richtlijn en enkele belangrijke punten die hieruit volgen voor de verwerking van persoonsgegevens voor opsporing en vervolging.

In hoofdstuk I zijn algemene bepalingen opgesteld, zoals doelstelling, toepassingsgebied en gehanteerde definities.

Hoofdstuk II beschrijft de beginselen, de uitgangspunten van de Richtlijn, onder meer ten aanzien van verwerking van persoonsgegevens en verwerking door andere instanties, categorisering van betrokkenen en typen gegevens, verwerking van bijzondere categorieën van persoonsgegevens. In dit hoofdstuk is ook een verbod op besluitvorming op basis van volledig geautomatiseerde gegevensverwerking opgenomen. Ook is vastgelegd dat lidstaten zelf passende termijnen moeten bepalen voor het opslaan en wissen[11] van gegevens.

Hoofdstuk III gaat in op de rechten van betrokkenen van wie gegevens verwerkt kunnen worden. Zo staat hierin beschreven hoe de betrokkene zijn rechten kan uitoefenen ten aanzien van inzage en controle van gegevens. In art. 14 staat beschreven dat een betrokkene informatie kan opvragen over de gegevens die over hem zijn opgeslagen, inclusief onder meer het doeleinde van verwerking, de categorieën gegevens, de (verwachte) duur van opslag van de gegevens en het recht op rectificatie of wissing. Art. 15 geeft hier beperkingen bij die vastgesteld kunnen worden, indien inzage de werkprocessen voor opsporing en vervolging zou kunnen belemmeren.

Hoofdstuk IV behandelt de rollen en verantwoordelijkheden van verwerkingsverantwoordelijke(n) en verwerkers. Ook wordt voorgeschreven hoe met een register van verwerkingsactiviteiten, logboeken en gegevensbeschermingseffectbeoordelingen moet worden gewerkt bij verwerking van gegevens en hoe de partijen om dienen te gaan met de toezichthoudende autoriteiten. Verder zijn in afdeling 2 van dit hoofdstuk voorschriften vastgelegd voor beveiliging van (verwerking van) persoonsgegevens. Hierbij is ook voorgeschreven welke maatregelen lidstaten verplicht moeten stellen in het geval van een inbreuk in verband met persoonsgegevens, zowel ten aanzien van de toezichthoudende autoriteit als de betrokkene. Afdeling 3 bevat voorschriften voor aanwijzing, positie en taken van de functionaris voor gegevensbescherming.

Hoofdstuk V betreft een regeling voor de doorgifte van persoonsgegevens aan derde landen of internationale organisaties. Deze regeling lijkt grotendeels op die van de AVG, waarbij specifieke voorzieningen worden geboden voor de gevallen waarin de belangen van opsporing en vervolging nopen tot gegevensuitwisseling ondanks het ontbreken van een adequaat niveau van gegevensbescherming. Er wordt uitgebreid ingegaan op doorgifte aan (organisaties in) derde landen op basis van adequaatheidsbesluiten, of bij het ontbreken van een dergelijk besluit op doorgifte op basis van passende waarborgen en daaraan te verbinden voorwaarden. Deze regelgeving is dus ook relevant voor gegevensuitwisseling met overzeese gebieden als Caribisch Nederland of Faeröer en Groenland.

[11] De term ‘wissen’ wordt gebruikt in de Richtlijn. In nationale wetgeving worden ook andere termen (verwijderen, vernietigen) gehanteerd.

Hoofdstuk VI beschrijft hoe onafhankelijke toezichthoudende autoriteiten moeten worden opgezet, hoe hun onafhankelijkheid geborgd wordt, welke competenties, taken en bevoegdheden toegeschreven worden aan de autoriteit, en hoe gerapporteerd dient te worden over inbreuken, alsmede hoe de autoriteit verslag doet van haar activiteiten.

Hoofdstuk VII gaat in op samenwerking tussen lidstaten en de uitwisseling van persoonsgegevens ten behoeve daarvan. Er wordt in besproken hoe wederzijdse bijstand vorm krijgt en aan welke voorwaarden verzoeken en reacties daarop bijvoorbeeld moeten voldoen. In dit hoofdstuk is ook vastgelegd welke rol het Comité voor gegevensbescherming, opgericht bij de AVG, binnen het kader van de Richtlijn is toebedeeld.

Hoofdstuk VIII beschrijft de regelingen omtrent beroep, aansprakelijkheid en straffen. Hoofdstuk IX en X bevatten respectievelijk uitvoeringshandelingen en slotbepalingen.

2.4 Samenvatting

In dit hoofdstuk hebben we op bondige wijze het Europeesrechtelijk kader geschetst dat relevant is voor de verwerking van politiegegevens. De Algemene verordening gegevensbescherming (AVG) geldt als kader voor verwerking van persoonsgegevens anders dan politiegegevens, terwijl voor politiegegevens (of gegevens die politie en justitie verwerken bij de uitoefening van hun taken bij opsporing en vervolging) de Richtlijn gegevensbescherming opsporing en vervolging (2016/680) van belang is. Welk regime van toepassing is, hangt af van welke instantie de gegevens verwerkt en welk doeleinde hierbij relevant is.

We hebben deze Richtlijn in vogelvlucht doorlopen. Hierbij zijn als belangrijkste elementen te onderscheiden:

- de beginselen en uitgangspunten van de Richtlijn;
- een uitgebreide regeling voor de verstrekking van informatie aan betrokken personen;
- een uitgebreide regeling voor de doorgifte van persoonsgegevens aan ‘derde landen’ (niet-EU-lidstaten of daarmee voor wat betreft de Richtlijn gelijkgestelde landen) en internationale organisaties;
- waarborgen rond de beveiliging van persoonsgegevens;
- diverse wettelijke voorschriften waar de verwerkingsverantwoordelijkheden aan moeten voldoen;
- de invulling van de rol van een toezichthoudende autoriteit.

3

Nederland

3.1 Inleiding

Dit hoofdstuk beschrijft 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 in wet en uitvoeringspraktijk opgelost, welke knelpunten bestaan nog en welke nieuwe knelpunten zijn er? Daarnaast bespreken we hoe Nederland invulling heeft gegeven aan het Europese kader voor de verwerking van politiegegevens. De knelpunten en vraagstukken die in dit hoofdstuk naar voren komen, bepalen de focus voor de casestudy's in de vergelijkingslanden.

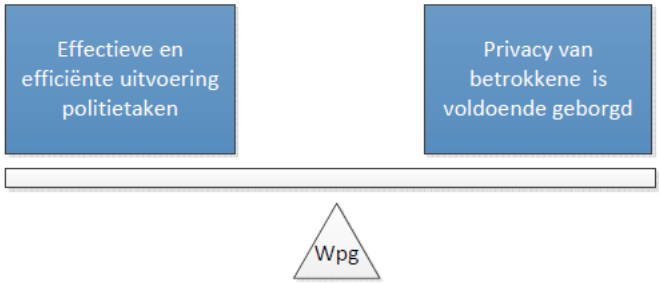
In paragraaf 3.2 schetsen we eerst het wettelijke kader. We doen dit zo beknopt mogelijk, omdat het in dit onderzoek vooral gaat om de dilemma's, knelpunten en uitdagingen die Nederland tegenkomt bij de verwerking van politiegegevens, en om voor de aanpak daarvan inspiratie op te doen uit andere landen. Vervolgens gaan we in paragraaf 3.3 in op de in 2012/2013 uitgevoerde evaluatie van de Wpg en de ervaren knelpunten (en de verklaringen daarvoor) die daaruit naar voren kwamen. Paragraaf 3.4 gaat over de periode na de evaluatie; met name de beleidsreactie op de evaluatie en de implementatie van EU-Richtlijn 2016/680. In paragraaf 3.5 inventariseren we hoe het er nu voor staat met de Wpg in Nederland: we beschrijven de knelpunten die al eerder zijn geconstateerd, maar nog steeds openstaan, en gaan in op nieuwe knelpunten en uitdagingen. In paragraaf 3.6 volgt een samenvatting.

3.2 Het wettelijke kader voor de verwerking van politiegegevens in Nederland

3.2.1 De Wpg

In 2008 trad de Wet politiegegevens (Wpg) in werking.[12] Deze wet verving de Wet politieregisters uit 1990. De Wpg beoogt een balans te vinden tussen twee hoofddoelstellingen: enerzijds meer ruimte bieden voor de verwerking van persoonsgegevens dan de Wet politieregisters, om een effectieve en efficiënte uitvoering van de politietaken mogelijk te maken; anderzijds het waarborgen van de privacy van degene van wie gegevens worden verwerkt.[13]

[12] *Stb.* 2007, 300; *Stb.* 2007, 549.
[13] Smits e.a. 2013, p. 36; *Kamerstukken II* 2005/2006, 30327, 3 (MvT), p. 1.



Figuur 3.1 Balans hoofddoelen Wpg. Bron: Smits e.a. 2013.

Over deze voorstelling als een balans/belangenafweging van 'tegengestelde' waarden/belangen kan verschillend worden gedacht; (mede) in het licht van de Europeesrechtelijke ontwikkelingen op het gebied van gegevensbescherming is wellicht meer te zeggen voor de benadering dat privacy en andere grondrechten, kortom de democratische rechtsstaat, het raamwerk en de randvoorwaarden vormen waarbinnen de uitvoering van de politietaak moet plaatsvinden.[14] Bovenstaand 'balansmodel' is echter de uitkomst van de uitgebreide beleidsreconstructie die voor de evaluatie van de Wpg is uitgevoerd, en geeft dus weer hoe de wetgever er destijds tegenaan keek.

De Wpg ziet alleen op de verwerking van politiegegevens, niet op gegevensverwerking in de rest van de strafrechtketen; daarop is de Wet justitiële en strafvorderlijke gegevens (Wjsg) van toepassing.

Reikwijdte van de Wpg (beknopt)
Artikel 1, onder a, van de Wpg definieert 'politiegegeven' als elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak, bedoeld in de artikelen 3 (daadwerkelijke handhaving van de rechtsorde en het verlenen van hulp) en 4 (taken Koninklijke Marechaussee (KMar)) van de Politiewet 2012. Art. 2 lid 1 verklaart de Wpg van toepassing op de verwerking van politiegegevens door een bevoegde autoriteit (in de zin van de EU-Richtlijn gegevensbescherming opsporing en vervolging, zie verder hoofdstuk 2 en paragraaf 3.4.2)[15] die in een bestand zijn opgenomen of die bestemd zijn daarin te worden opgenomen. In de praktijk komt dit erop neer dat (een deel van) de verwerking van persoonsgegevens door de politie, KMar, Rijksrecherche, bijzondere opsporingsdiensten[16] en buitengewoon opsporingsambtenaren (boa's) onder de Wpg valt.[17] De Wpg is niet van toepassing op de uitvoering van de Wet administratiefrechtelijke handhaving verkeersvoorschriften, de Vreemdelingenwet 2000, de grensbewakingstaak en de Wet wapens en

[14] Vergelijk de clausule in vele mensenrechtenverdragen en grondwetsteksten dat een inbreuk op een grondrecht noodzakelijk moet zijn in een democratische samenleving.
[15] Art. 1 sub l Wpg bevat de definitie van 'bevoegde autoriteit', in navolging van de Richtlijn: iedere overheidsinstantie die bevoegd is voor de politietaken genoemd in art. 1 sub a Wpg, of ieder ander orgaan dat of iedere andere entiteit die is gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen met het oog op die taken.
[16] De vier bijzondere opsporingsdiensten (BOD'en) zijn de Inspectie Sociale Zaken en Werkgelegenheid, de Fiscale Inlichtingen- en OpsporingsDienst (FIOD), de Nederlandse Voedsel- en Warenautoriteit (NVWA) en de Inspectie Leefomgeving en Transport (ILT).
[17] De taken van de bijzondere opsporingsdiensten en buitengewoon opsporingsambtenaren die onder de Wpg vallen zien op hun opsporingsbevoegdheden (strafrechtelijke handhaving) en nadrukkelijk niet op de toezichtstaken (bestuursrechtelijke handhaving).

munitie, en ook niet op de verwerking van persoonsgegevens voor uitsluitend persoonlijke doeleinden en voor de interne bedrijfsvoering. Daarvoor geldt de AVG.

§ 1 (art. 1-7a) van de Wpg bevat algemene bepalingen: definities en bepalingen over onder meer reikwijdte, noodzakelijkheid, rechtmatigheid en doelbinding, bijzondere categorieën politiegegevens, autorisaties en toegang tot politiegegevens. § 2 (art. 8-15a) regelt de verwerking van politiegegevens met het oog op de uitvoering van de politietaak. § 3 (art. 16-24) gaat over de doorgifte of verstrekking van politiegegevens aan anderen dan politie en KMar. In § 4 en 4a (art. 24a-31c) zijn de rechten van betrokkenen en rechtsbescherming vastgelegd. § 5 (art. 31d-36) ziet op controle en toezicht. De wet is ook beperkt van toepassing op de BES-eilanden (§ 5a). Voor de verstrekking van politiegegevens gelden de BES-eilanden, Aruba, Curaçao en Sint Maarten op grond van § 3 Wpg als derde land.

§ 2 van de Wpg onderscheidt verschillende grondslagen voor de verwerking van politiegegevens:

- **Art. 8** maakt verwerking mogelijk met het oog op de uitvoering van de dagelijkse politietaak;
- Op grond van **art. 9** kunnen politiegegevens gericht worden verwerkt ten behoeve van een onderzoek met het oog op de handhaving van de rechtsorde in een bepaald geval;
- **Art. 10** biedt de grondslag voor gerichte verwerking voor het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde;
- **Art. 11** bevat het kader voor geautomatiseerd vergelijken en in combinatie zoeken van gegevens die worden verwerkt op grond van art. 8, 9 of 10.
- **Art 12** maakt verwerking mogelijk voor de controle op en het beheer van een informant en de beoordeling en verantwoording van het gebruik van informantgegevens.
- Op grond van **art. 13** kunnen ten behoeve van de ondersteuning van de politietaak, de politiegegevens die worden verwerkt volgens art. 8, 9 en 10, verder worden verwerkt voor zover zij relevant zijn voor in het artikel opgesomde doelen, zoals het ophelderen van strafbare feiten die nog niet herleid konden worden tot een verdachte (onder b).

Onder de Wpg hangen verschillende AMvB's, waaronder:

- Besluit politiegegevens (bevat onder meer nadere regels voor autorisatie)
- Besluit politiegegevens bijzondere opsporingsdiensten
- Besluit politiegegevens buitengewoon opsporingsambtenaren
- Besluit verplichte politiegegevens (bevat regels over 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 en de wijze van verwerking)

Een volledig overzicht van op de Wpg gebaseerde/met de Wpg verband houdende regelgeving is opgenomen in bijlage 2.

3.3 Evaluatie van de Wpg

3.3.1 Knelpunten 2013

In 2012/2013 is de Wpg geëvalueerd.[18] Uit de evaluatie kwam op basis van interviews met onder meer politie (regionale en landelijke eenheden), het toenmalige ministerie van Veiligheid en Justitie, het OM, het toenmalige College bescherming persoonsgegevens (CBP), de KMar en bijzondere opsporingsdiensten een groot aantal ervaren knelpunten naar voren. Ook leverde het evaluatieonderzoek verklaringen voor de knelpunten op, die terug te voeren waren op de politieorganisatie, de Wpg zelf, de implementatiestrategie van de politie en omgevingsfactoren. Daarnaast hebben de onderzoekers op basis van in 2011 uitgevoerde externe audits de naleving van de Wpg onderzocht. Het evaluatierapport omschreef de implementatie en naleving van de Wpg als een 'worstelende praktijk'. De knelpunten die uit de evaluatie naar voren kwamen, worden in deze paragraaf uiteengezet.

Knelpunten bij verwerken

Het grootste knelpunt bij verwerken was het wettelijke onderscheid tussen art. 8 Wpg (dagelijkse politietaken) en art. 9 Wpg (onderzoek). Gegevens zijn niet makkelijk in te delen in een van de categorieën met bijbehorende verwerkingsregimes. Daarnaast sloten de politieregistratiesystemen niet goed op elkaar aan, wat onder andere leidde tot problemen bij de bewaartermijnen. Ook moesten art. 9-gegevens handmatig uit de systemen verwijderd worden wat zorgde voor hoge administratieve lasten. Verder kwam uit de evaluatie naar voren dat de bewaartermijnen te kort werden bevonden. Vernietiging van gegevens vijf jaar na verwerking was volgens betrokkenen te kort en zou ten koste gaan van de informatiepositie van de politie.

Knelpunten bij verstrekken

Uit de evaluatie kwam naar voren dat het voor politiemedewerkers nog vaak onduidelijk was of en zo ja, wat ze mochten verstrekken. Dit zag vooral op het verstrekken van gegevens in de fase voorafgaand aan een art. 9-onderzoek. Dit leidde in de praktijk, zeker in deze fase, tot terughoudendheid bij het delen van informatie. Daarnaast was er in de praktijk sprake van een stapeling van convenanten tussen de politie en andere actoren en konden er verschillende wettelijke regimes van toepassing zijn op gezamenlijke databestanden.[19]

Knelpunten rond rechten van betrokkenen

Bij het gebruik maken van het recht op kennisneming werden vooral knelpunten ervaren in de administratieve last rond kennisgevingsverzoeken inzake CIE-gegevens[20] en de toename in verzoeken om kennisneming om andere reden dan de wetgever had beoogd. Daarnaast gaf de politie aan de samenloop met de Wet openbaarheid van bestuur (Wob) als knelpunt te ervaren. Ook hier werden de administratieve lasten als te veel ervaren.

Knelpunten bij toezicht

Bij het toezicht ervoeren betrokkenen vooral de administratieve lasten van de protocollering als knelpunt, in het bijzonder bij verstrekking van politiegegevens met betrekking tot de uitvoering van dagelijkse politietaken (art. 8 Wpg). Hierbij speelde de gebrekkige ondersteuning

[18] Smits e.a. 2013.

[19] 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 het Wetboek van Strafvordering (WvSv) en de Wjsg van toepassing.

[20] CIE: criminele inlichtingen-eenheid. CIE's heten nu Teams Criminele Inlichtingen (TCI's).

van de ICT, maar ook de grote hoeveelheid verstrekkingen een rol. Daarnaast leidde de stapeling van toezichtfiguren soms tot bureaucratisering van het toezicht en lag de nadruk vooral op de organisatie-eisen.

Knelpunt samenloop met andere wetten

Dit knelpunt is ook al deels omschreven bij de knelpunten verstrekken en verwerken, maar werd in de evaluatie genoemd als apart knelpunt. Wanneer de politie samenwerkte met andere partners, golden verschillende bijzondere wetten waarin specifieke regels waren opgenomen over gegevensuitwisseling en geheimhouding. Het interpreteren van de verschillende regelingen bleek lastig en het was niet altijd duidelijk welke regelgeving op welke gegevens van toepassing was. Het was niet duidelijk welke bewaartermijnen golden, doordat meerdere wettelijke regelingen van toepassing konden zijn.

Uit bovenstaande knelpunten zijn grofweg twee overkoepelende knelpunten te destilleren:

Algemeen: naleving en 'naleefbaarheid'[21] van de Wpg

In de evaluatie wordt de implementatie en naleving van de Wpg, zoals hierboven al bleek, een 'worstelende praktijk' genoemd. De geïnterviewde ketenpartners vonden de wet moeilijk te lezen en te interpreteren en daardoor moeilijk na te leven. '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.'[22]

Onvoldoende organisatorische voorbereiding van de politie (zowel werkprocessen als ICT) en abstracte normen in de wet zoals noodzaak, geheimhouding en doelbinding zorgden ervoor dat de implementatie van de Wpg moeilijk verliep. In de evaluatie constateren de onderzoekers dat de Wpg nauwelijks prioriteit had bij de politie(leiding), en dat de wijze waarop aan de implementatie vorm is gegeven (focus op administratief beheer) ertoe heeft bijgedragen dat de Wpg (lange tijd) vooral werd gezien als 'moetje'.

Algemeen: categorisering van gegevens en samenloop met andere wetgeving

Twee punten kwamen bij allerlei vormen van verwerken van politiegegevens (verkrijgen, bewerken, bewaren, verstrekken) als knelpunt terug: de indeling in categorieën politiegegevens en de samenloop met andere wet- en regelgeving.

Zoals eerder al aan de orde kwam, worden politiegegevens op grond van de Wpg gecategoriseerd naar het doel waarvoor de gegevens worden verwerkt binnen de politietaak (art. 8-13). Bij elke categorie hoort een verwerkingsregime met bewaartermijn. Uit de evaluatie kwam naar voren dat gegevens in de praktijk niet statisch in te delen waren in een van de verwerkingsregimes. Vooral het onderscheid tussen art. 8 en art. 9 werd als niet praktisch en kunstmatig ervaren. Gegevens kunnen voor meerdere doelen relevant zijn en gegevens veranderen in de praktijk vaak van status.

Daarnaast werd in de evaluatie vastgesteld dat andere wetten waarin de verwerking van persoonsgegevens en de bescherming van de privacy worden geregeld tot onduidelijkheid leid-

[21] Met 'naleefbaarheid' bedoelen we de mate waarin de praktijk in staat is de wet na te leven. Zoals onder dit kopje uiteengezet hangt de naleefbaarheid af van factoren in de wet zelf (zoals de leesbaarheid van de wet), factoren in de uitvoeringspraktijk (zoals de politieorganisatie) en organisatorische randvoorwaarden/ICT.

[22] Smits e.a. 2013, p. 5 en 8.

den. In de praktijk werden knelpunten ervaren bij het bepalen welk wettelijk regime en bijbehorende bewaartermijn van toepassing was. Dit knelpunt deed zich vooral voor met de Wet justitiële en strafvorderlijke gegevens (Wjsg), het Wetboek van Strafvordering (Sv) en de toenmalige Wet bescherming persoonsgegevens (Wbp) (de implementatie van de Europese Privacyrichtlijn, de voorloper van de AVG). Daarnaast was het in de gevallen van gezamenlijk aangelegde bestanden waarop verschillende regimes van toepassing waren, niet duidelijk welk regime moest worden gevolgd. Dit probleem speelde ook bij het verstrekken van sommige gegevens.

3.3.2 Verklaringen 2013

Uit de evaluatie komt naar voren dat de bovenstaande knelpunten konden worden verklaard door vier hoofdfactoren.

Kenmerken van de politieorganisatie

Bij de gehele politieorganisatie, in het bijzonder de leiding van de organisatie, ontbrak het aan het gevoel van noodzaak, nodig voor de implementatie van de Wpg. Er was tot 2011 geen centrale sturing om de politiekorpsen 'te dwingen' tot implementatie. Ook liep de overgang naar één politieorganisatie dwars door de implementatieperiode heen, wat het proces bemoeilijkte. Die overgang vroeg veel tijd en aandacht, wat voor minder focus op de implementatie van de Wpg zorgde. Daarnaast speelde de ICT een rol. De verouderde en gefragmenteerde ICT heeft de invoering van de Wpg bemoeilijkt. Er was wel een technische invoeringsstrategie, maar geen duidelijke veranderstrategie die kon meebewegen met de veranderingen.

De implementatiestrategie van de politie

Bij de implementatie van de Wpg is er gekozen voor een bedrijfstechnische benadering. Er is weinig tot geen aandacht besteed aan kennisopbouw en bewustwording rond de essentie van de wet. Hierdoor is de Wpg lang als 'moetje' ervaren en had de wet een bureaucratisch imago.

De opzet en inhoud van de Wpg

De Wpg zelf sloot op een aantal punten niet goed aan bij dynamische praktijk. Dit geldt met name voor de (aansluiting tussen) verschillende verwerkingsregimes en de overlap van de Wpg met andere wetten. Daarnaast legde de Wpg een relatief zwaar accent op organisatie-eisen en toezicht, wat niet goed aansloot op de bedrijfsprocessen van de politie.

Omgevingsfactoren

De context waarbinnen politietaken werden uitgevoerd veranderde. Dit geldt voor de opgaven en taakstelling van de politie, de organisatiestructuur, onderzoeksmethoden, het informatieaanbod, de informatiepositie van de politie en de opvattingen over privacy. Er was een spanningsveld tussen het statische inrichtingskaraker van de Wpg en de dynamiek van de praktijk.

3.4 Herzieningstrajecten en tussenperiode

3.4.1 Reactie minister op de evaluatie

Minister Opstelten van Veiligheid en Justitie kondigde in zijn reactie op de evaluatie (en die van de Wjsg) een aantal maatregelen aan.[23] Op hoofdlijnen:

[23] *Kamerstukken II* 2013/14, 33842, 2.

- harmonisatie van de verschillende wettelijke regimes voor politiële, justitiële en strafvorderlijke gegevens (met name de Wpg en Wjsg, de minister neemt in overweging deze tot één wet samen te voegen als dat dienstig is voor de samenhang, maar ook andere regimes die van invloed zijn zoals het WvSv en de Wob, en – van groot belang – het Europeesrechtelijke kader worden meegenomen);
- uitgangspunt van de regelgeving moet zijn het gebruik van gegevens. Nu staan de bewaartermijnen te veel centraal. De bewaartermijn moet echter een afgeleide zijn van de noodzaak tot gebruik van de gegevens, niet andersom;
- het toezicht op het gebruik en de verstrekking van gegevens moet worden versterkt. Moderne ICT kan en moet hierbij behulpzaam zijn. Ook moet het toezicht op de werkvloer, zowel preventief als repressief, worden versterkt en moet er via opleidingen worden gewerkt aan meer bewustwording van het belang van nauwgezette regelnaleving.[24]

Hiermee onderschrijft hij de in de evaluatie gevonden knelpunten en erkent hij dat voor de aanpak hiervan een veranderopgave nodig is in zowel wetgeving als praktijk (organisatie; kennis, houding en gedrag; en ICT). Digitalisering is volgens de minister in deze Kamerbrief een belangrijke ontwikkeling die een grondige heroverweging van de Wpg en Wjsg noodzakelijk maakt. De samenleving stelt hogere eisen aan zowel de sociale veiligheid en het gebruik van ICT als aan de bescherming van de persoonlijke levenssfeer. Wetgeving beoogt deze belangen te verzoenen.[25] De minister geeft aan dat bovenstaande maatregelen deel uitmaken van een ambitieuze langetermijnagenda. ‘Vergaande digitalisering van de strafrechtketen is een zaak van lange adem’. De herziening van het Wetboek van Strafvordering en het introduceren van het digitaal strafdossier hadden daarbij eerst prioriteit. Daarna zou volgens de minister de herziening van het wettelijk kader voor politiële, justitiële en strafvorderlijke gegevens in kleine stapjes moeten worden gerealiseerd, met daarbij in het bijzonder aandacht voor de ontwikkelingen op EU-niveau op het gebied van gegevensbescherming.[26]

3.4.2 De implementatie van Richtlijn 2016/680

De Europese Richtlijn gegevensbescherming opsporing en vervolging is in Nederland geïmplementeerd door wijziging van de Wpg en de Wjsg.[27] De implementatiewet is – met uitzondering van enkele artikelen – in werking getreden op 1 januari 2019.[28] Bij besluit van 6 februari 2019 (Besluit politiegegevens buitengewone opsporingsambtenaren) is deze wet ten dele ook van toepassing verklaard op gegevensverwerking door personen die als buitengewoon opsporingsambtenaar belast zijn met de opsporing van strafbare feiten.[29]

In de MvT gaf de minister voor Rechtsbescherming aan dat het uitgangspunt minimumimplementatie is, met dien verstande dat voor enkele specifieke kwesties de implementatie doorwerking heeft voor de BES-eilanden en er met het wetsvoorstel wordt voldaan aan een eerdere toezegging van het kabinet aan de Tweede Kamer in reactie op het rapport *Big Data in*

[24] Overigens wordt in de evaluatie niet zozeer de conclusie getrokken dat het toezicht tekort schiet, maar dat het ‘privacybewustzijn’ onvoldoende in de ‘mores’ van de politieorganisatie zit. In het rapport wordt juist gepleit voor professionele en bedrijfsmatige borging en wordt gewezen op te veel een ‘moetje’ zijn van de Wpg door administratief beheer, controle en afrekening.
[25] *Kamerstukken II* 2013/14, 33842, 2, p. 2.
[26] *Kamerstukken II* 2013/14, 33842, 2, p. 3 en 5.
[27] *Stb.* 2018, 401.
[28] *Stb.* 2018, 495.
[29] *Stb.* 2019, 85.

een vrije en veilige samenleving van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR).[30] Het kabinet had toegezegd te bezien of enkele verplichtingen in de AVG ook in de implementatie van de Richtlijn zouden moeten worden opgenomen.[31] Het wetsvoorstel was onderdeel van een breder pakket van implementatiemaatregelen voor het Europese kader voor gegevensbescherming (de AVG en de Richtlijn gegevensbescherming opsporing en vervolging). De implementatie moest leiden tot een beter beschermingsniveau voor betrokkenen van wie persoonsgegevens worden verwerkt, bijvoorbeeld op het gebied van rechtsbescherming.

Omdat Nederland bij de implementatie van het Kaderbesluit dataprotectie politiële en justitiële samenwerking in strafzaken in 2011[32] al had besloten de regels uit het Kaderbesluit ook te laten gelden voor gegevensverwerking op nationaal niveau, hoefde de wetgever bij de implementatie van de Richtlijn niet bij nul te beginnen.[33] Wel had de Richtlijn de volgende consequenties (we zoomen hier vooral in op de gevolgen voor de Wpg):

- Zoals in hoofdstuk 2 besproken ziet de Richtlijn op de *opsporing* en *vervolging* van *strafbare feiten (inclusief de bescherming tegen/voorkoming van gevaren voor de openbare veiligheid)* door *bevoegde autoriteiten*. Dit zorgde voor zowel een verruiming als een versmalling van de reikwijdte van de Wpg op bepaalde punten.
    - De belangrijkste verruiming die dit met zich meebracht is dat de verwerking van persoonsgegevens met het oog op de opsporing door de buitengewone opsporingsambtenaren (boa's), die zijn belast met de opsporing van bepaalde categorieën strafbare feiten, voortaan onder de reikwijdte van de Wpg valt.[34]
    - Een versmalling heeft plaatsgevonden op het gebied van de verwerking van gegevens door de politie ten behoeve van de uitvoering van wettelijke voorschriften waarmee de minister van Justitie en Veiligheid is belast, te weten: de Wet Wapens en munitie, de Wet natuurbescherming, de Wet particuliere beveiligings- en recherchebureaus en de Wet explosieven voor civiel gebruik. Deze taken hebben geen betrekking op de opsporing of vervolging van strafbare feiten en vallen dus niet onder de doeleinden van de Richtlijn. Dit betekent dat de verwerking van persoonsgegevens onder deze wetten door de politie voortaan niet onder de reikwijdte van de Wpg vallen, maar onder de reikwijdte van de AVG.[35] Ook voorschriften gesteld bij of krachtens de Vreemdelingenwet 2000 hebben geen betrekking op de uitvoering van de taken van de Richtlijn en vallen sinds de implementatie van de Richtlijn onder de AVG. Een andere versmalling ziet op de gelding van de Wpg op de BES-eilanden op grond van art. 36a Wpg. In § 5a van de Wpg zijn een aantal uitvoeringsbepalingen in de gewijzigde Wpg waarin verplichtingen uit de Richtlijn zijn opgenomen, uitgezonderd van toepassing op de BES-eilanden.[36]

[30] *Kamerstukken II* 2017/18, 34889, 3 (MvT implementatie Richtlijn 2016/680), p. 1 en 14; WRR 2016.
[31] *Kamerstukken II* 2016/17, 26643, 426, bijlage par. 6. Het gaat om verplichtingen van de verwerkingsverantwoordelijke om te toetsen of de verwerking overeenkomstig de gegevensbeschermingseffectbeoordeling wordt uitgevoerd (art. 35 lid 11 AVG) en om bij big data-analyses en de daarop gebaseerde beslissing aan te kunnen tonen waarop deze beslissing is gebaseerd en welke factoren en wegingen daarin zijn meegenomen (art. 14 lid 2 sub g AVG).
[32] *Stb.* 2011, 490.
[33] *Kamerstukken II* 2017/18, 34889, 3 (MvT implementatie Richtlijn 2016/680), p. 2-3.
[34] *Kamerstukken II* 2017/18, 34889, 3 (MvT implementatie Richtlijn 2016/680), p. 11.
[35] *Kamerstukken II* 2017/18, 34889, 3 (MvT implementatie Richtlijn 2016/680), p. 12.
[36] *Kamerstukken II* 2017/18, 34889, 3 (MvT implementatie Richtlijn 2016/680), p. 12-13.

- De Richtlijn maakt onderscheid tussen de verwerking van persoonsgegevens in EU-lidstaten enerzijds en de doorgifte van persoonsgegevens aan derde landen en internationale organisaties anderzijds. Vanwege de Richtlijn is het onderscheid tussen verwerking op nationaal niveau, de verstrekking aan andere landen waarbij een nader onderscheid werd gemaakt tussen verstrekking aan derde landen en EU-lidstaten, losgelaten.[37] De Richtlijn maakt namelijk het onderscheid tussen terbeschikkingstelling binnen de EU en terbeschikkingstelling aan derde landen. De terbeschikkingstelling van politiegegevens tussen politiediensten (*free flow of information*) binnen de EU is nu geregeld in art. 15a Wpg, de doorgifte aan derde landen en internationale organisaties in art. 17a Wpg (zie uitgebreider over het systeem van verstrekking van politiegegevens en de knelpunten hierbij paragraaf 3.5.2, onder *Verstrekken*). Opgemerkt wordt dat de BES-eilanden en de andere landen van ons koninkrijk in de gewijzigde Wpg als 'derde land' worden aangemerkt. De doorgifte van politiegegevens aan deze (ei)landen kan sinds de wijzigingen enkel plaatsvinden binnen de kaders die gelden voor de doorgifte van politiegegevens aan derde landen.
- Verder zijn nieuwe verplichtingen voor de verwerkingsverantwoordelijke uit de Richtlijn overgenomen in de Wpg, bijvoorbeeld de (actieve) beschikbaarstelling van informatie over de gegevensverwerking aan de betrokkene, het bijhouden van logbestanden, de registratie van gegevens over de gegevensverwerkingen, het verrichten van gegevensbeschermingseffectbeoordelingen en het melden van datalekken aan de betrokkene en aan de toezichthoudende autoriteit.[38]
- De Richtlijn bevat uitgebreide regels over de toezichthoudende autoriteit (in Nederland: de Autoriteit Persoonsgegevens, AP); waar nodig is de Wpg hierop aangepast.[39] Zo zijn bijvoorbeeld in artikel 35b Wpg (taken Autoriteit Persoonsgegevens) en artikel 35c Wpg (bevoegdheden Autoriteit Persoonsgegevens) de taken en bevoegdheden van de AP binnen het Wpg-domein expliciet opgenomen. Hiermee zijn de eisen vanuit de Richtlijn geïmplementeerd. De belangrijkste taken van de AP zijn toezicht te houden op de verwerking van persoonsgegevens op grond van de Wpg en het geven van advies over voorstellen van wet en ontwerpen van algemene maatregelen van bestuur. De belangrijkste bevoegdheden zijn het waarschuwen van verwerkingsverantwoordelijken, het opleggen van een bestuurlijke boete en het toepassen van bestuursdwang ter handhaving van de normen die volgen uit de Wpg.

3.4.3 Veranderende context

Afgezien van de implementatie van de Richtlijn gegevensbescherming opsporing en vervolging is de Wpg sinds de evaluatie nauwelijks gewijzigd. Met de in de beleidsreactie op de evaluatie van de Wpg en Wjsg aangekondigde herziening van het wettelijk kader voor de verwerking van politie-, justitie- en strafvorderlijke gegevens, waarvoor onder andere dit onderzoek input moet leveren, is, zoals in die reactie ook al uiteengezet, om verschillende redenen pas vanaf 2018/2019 een start gemaakt. De modernisering van het Wetboek van Strafvordering en het invoeren van het digitaal strafdossier hadden de hoogste prioriteit. Ook had de herziening van het politiebestel – de overgang van een stelsel van regionale korpsen naar één nationale politie met de Politiewet 2012 – voorrang. Hoewel de nieuwe politiewet al van kracht was voor de evaluatie van 2013, zat men nog midden in de transitieperiode en de taakuitvoering van de politie moest blijven functioneren. Vervolgens is ervoor gekozen om eerst

[37] *Kamerstukken II* 2017/18, 34889, 3 (MvT implementatie Richtlijn 2016/680), p. 6.
[38] *Kamerstukken II* 2017/18, 34889, 3 (MvT implementatie Richtlijn 2016/680), p. 7.
[39] *Kamerstukken II* 2017/18, 34889, 3 (MvT implementatie Richtlijn 2016/680), p. 7.

de Richtlijn te implementeren in de bestaande Wpg en Wjsg, omdat hiermee het Europeesrechtelijke kader voor het nieuw te ontwikkelen beleid vast kwam te staan. Inmiddels is de vorming van de nationale politie afgerond en is de Richtlijn geïmplementeerd. Verder hebben zich geen grote veranderingen voorgedaan op het gebied van organisatiestructuur en wetgeving.

De context waarbinnen de politie haar werk doet is de laatste jaren daarentegen wel sterk veranderd. De ontwikkelingen waartoe de politie zich te verhouden heeft, worden benoemd in het rapport *Visie op de politiële taakuitvoering: de invloed van globalisering, netwerksamenleving, digitalisering, technologisering en het gebruik van intelligence in het veiligheidsdomein* van het ministerie van Veiligheid en Justitie uit 2016.[40] Het rapport gaat in op de veranderende samenleving, globalisering, digitalisering en technologisering. Hierbij wordt het belang van technologisering, digitalisering van de politie en het inzetten van *intelligence* door de politie benadrukt. Op het gebied van toezicht en handhaving is door technologisering veel meer informatie beschikbaar. Dit kan bijvoorbeeld worden gebruikt voor risicoprofielen en voorspellen, met gerichte inzet van mensen en middelen tot gevolg.[41]

Tegelijkertijd zorgen digitalisering en technologisering ook voor nieuwe dreigingen en problemen. Door digitalisering ontstaan nieuwe vormen van criminaliteit, zoals hacken en *phishing*. Daarnaast zorgt technologisering ervoor dat klassieke vormen van criminaliteit met behulp van nieuwe technologieën kunnen worden gepleegd. Hierbij kan bijvoorbeeld gedacht worden aan digitaal bedreigen. Door digitalisering van de samenleving verschuiven de grenzen van de criminaliteit voortdurend.[42]

Digitalisering en technologisering zijn nog steeds complexe vraagstukken voor de politie. Technologisering maakt dat zich zowel voor de politie als voor criminelen nieuwe mogelijkheden voordoen. De politie zal ervoor moeten waken dat de crimineel niet te ver voorloopt op het gebied van techniek.[43]

3.5 Huidige knelpunten en uitdagingen

3.5.1 Inleiding

Zoals omschreven is er sinds de evaluatie van de Wpg veel veranderd. Niet alleen de Wpg is met de implementatie van de Richtlijn aangepast, maar ook de context waarbinnen de politie zijn werk doet is sterk veranderd. Daarom is het van belang om te kijken welke knelpunten nu nog worden ervaren. Om dit te achterhalen zijn we begonnen met de knelpunten inventariseren die in de evaluatie zijn geconstateerd (zie paragraaf 3.3). In de onderzoeksuitvraag van het WODC voor dit onderzoek (eind 2019), waarvoor het ministerie van Justitie en Veiligheid (dat met de herziening van de Wpg is belast) input heeft geleverd, is ook een aantal knelpunten genoemd. Deze hebben we naast de knelpunten uit de evaluatie gelegd om te zien waar overlap bestaat. Ook hebben we een beperkte documentenstudie uitgevoerd om te zien welke knelpunten nog bestaan en welke eventuele nieuwe knelpunten erbij zijn gekomen; zie bijlage 1 voor de geraadpleegde bronnen. Dit vormde de basis voor een interviewleidraad voor vier oriënterende interviews met Nederlandse experts:

[40] Ministerie van Veiligheid en Justitie 2016.
[41] Ministerie van Veiligheid en Justitie 2016, p.15.
[42] Ministerie van Veiligheid en Justitie 2016, p.14.
[43] Ministerie van Veiligheid en Justitie 2016, p.15.

- Ministerie van JenV: een coördinerend beleidsmedewerker van het Directoraat-Generaal Politie en Veiligheidsregio's (Programma Politiebestel, Bevoegdheden en Informatiefunctie) en een strategisch raadadviseur van de Directie Wetgeving en Juridische Zaken, Sector straf- en sanctierecht, die zich bezighoudt met de herziening;
- Politie: strategisch adviseur wet- en regelgeving bij de Gegevensautoriteit;
- Kmar: functionaris gegevensbescherming Wpg;
- Universitair hoofddocent bij eLaw, de afdeling Internetrecht en IT-recht bij de Universiteit Leiden en oprichter Considerati (adviesbureau op het gebied van privacy, gegevensbescherming, data en digitale technologie)

In deze gesprekken zijn we nagegaan in hoeverre de in paragraaf 3.3 beschreven knelpunten uit de evaluatie van de Wpg nog steeds bestaan en welke eventuele nieuwe knelpunten zich voordoen. Hierbij plaatsen we de kanttekening dat het onmogelijk is om in vier gesprekken van een uur à anderhalf uur alle knelpunten langs te lopen. Dit was ook niet de ambitie; dit onderzoek is niet een volledige tweede evaluatie van de Wpg, maar een inventarisatie van de manieren waarop in vijf andere landen met de verwerking van politiegegevens wordt omgegaan (in wet en – beperkt – uitvoeringspraktijk). In paragraaf 3.5.2 en 3.5.3 beschrijven we het resultaat van onze beperkte 'nulmeting' van de Nederlandse situatie (uit documentenstudie en interviews).

3.5.2 Oude, nog steeds bestaande knelpunten

Bewaren van gegevens

De Wpg bepaalt nu per verwerkingsdoel hoe lang de politie de gegevens mag gebruiken. Na afloop van die gebruikstermijn moeten gegevens worden verwijderd. Dat betekent dat gegevens gedurende een bepaalde termijn achter een 'schot' moeten worden geplaatst en alleen nog maar mogen worden gebruikt voor een aantal specifieke doelen. Na afloop van die termijn moeten de gegevens worden vernietigd. Dit systeem leidt in de praktijk tot een aantal grijze gebieden. De verwijderingstermijnen zijn niet eenduidig geformuleerd, waardoor onduidelijkheid bestaat over de toepassing ervan. Geïnterviewden geven ook aan dat binnen de nationale wetgeving in verschillende wetten bewaartermijnen zijn opgenomen, waardoor het niet altijd duidelijk is hoe lang gegevens mogen worden bewaard.

Daarnaast komt het voor dat dezelfde gegevens voor meerdere doelen worden gebruikt, waardoor voor die gegevens verschillende bewaartermijnen gelden. Vervolgens is onduidelijk welke bewaartermijn van toepassing is. Zo kan bijvoorbeeld een aangifte in eerste instantie worden geregistreerd als een art. 8 Wpg-gegeven, maar in een later onderzoek worden gebruikt als art. 9 Wpg-gegeven.

Ook ervaart de politie een spanningsveld tussen de geldende bewaartermijnen en de wens om een langere periode toegang te hebben tot persoonsgegevens. Op het oog betekenisloze data kunnen cruciaal blijken te zijn voor het oplossen van een misdrijf, bijvoorbeeld bij *cold case*-zaken.[44] Voor bepaalde big data-analyses is het ook wenselijk om verder terug kunnen kijken om goed inzicht te kunnen krijgen. Daarvoor moet je nog wel kunnen beschikken over die data. Dat gaat bijvoorbeeld over het in kaart brengen van langdurige criminele verbanden (zoals maffiastructuren). Het vernietigen van informatie ligt dan ook gevoelig.

[44] Zie bijvoorbeeld de brief van de minister van JenV van 4 februari 2019, 2487378.

Algemeen: naleving en 'naleefbaarheid' van de Wpg

Een gesprekspartner noemt 2012/2013 niet het ideale evaluatiemoment voor de Wpg; de omvorming van 25 regionale korpsen naar één nationale politie liep namelijk door alles heen. De Wpg was oorspronkelijk geschreven voor de verwerking van gegevens door en uitwisseling tussen regionale korpsen binnen Nederland, waardoor de wet nu 'aan alle kanten knelt' en 'enkele artikelen inmiddels zinledig zijn geworden'. Ook heeft de implementatie van de Richtlijn de naleefbaarheid van de Wpg niet verbeterd. Een gesprekspartner geeft aan dat enkele bestaande artikelen (zoals art. 25 over het recht op inzage (voorheen: kennisneming)) niet zijn aangepast bij de implementatie, maar dat deze artikelen nu gelezen/geïnterpreteerd worden in het licht van de Richtlijn. Dat betekent dat de memorie van toelichting uit 2007 niet meer bruikbaar is voor de uitleg van deze artikelen, terwijl de wettekst niet is veranderd. In de praktijk levert dit onduidelijkheid op.

Art. 33 Wpg bepaalt dat de korpschef ten minste elke vier jaar een externe privacy audit moet laten verrichten. Op 21 april 2020 heeft de minister van JenV de auditresultaten over 2015-2019 naar de Tweede Kamer gestuurd.[45] Uit de audit blijkt een stijgende lijn ten opzichte van de audits in 2011 en 2015; zo scoort de politie nu groen op de onderdelen 'autorisatie' en 'rechten van betrokkene'. Wel is er nog verbetering nodig op punten als het intrekken van oude autorisaties.

Uit de interviews blijkt dat de wet nog steeds veel open en/of vaag geformuleerde normen bevat die voor onduidelijkheid en verschillen in toepassing/interpretatie zorgen; dat de wet op andere punten juist misschien te gedetailleerd is en daardoor moeilijk naleefbaar; en dat de driehoek wet- en regelgeving/uitvoeringspraktijk/ICT en organisatorische maatregelen nog altijd niet goed op elkaar aansluit.

Voorbeelden van zulke open normen/vage formuleringen zijn 'gecombineerd verwerken' en 'geautomatiseerd vergelijken' (in onder meer art. 11 Wpg) en 'geautomatiseerde besluitvorming'. Het is voor verwerkingsverantwoordelijken en verwerkers in de praktijk niet altijd duidelijk wat hiermee bedoeld wordt, waardoor interpretatieverschillen ontstaan.

Algemeen: categorisering van gegevens en samenloop met andere wetgeving

Zoals eerder al aan de orde kwam, worden politiegegevens op grond van de Wpg gecategoriseerd naar het doel waarvoor de gegevens worden verwerkt binnen de politietaak (art. 8-13). Bij de verschillende categorieën horen verschillende verwerkingsregimes (inclusief bewaartermijnen). Volgens meerdere gesprekspartners is deze indeling niet (meer) relevant en in de praktijk lastig werkbaar. Gegevens kunnen tot meerdere categorieën behoren. Daarnaast zorgt de indeling in categorieën bij het bestuderen van gegevens op het niveau van fenomenen of thema's en de toepassing van *big data*-technieken voor onduidelijkheid over welke vergelijking wel en niet kan worden uitgevoerd, omdat gegevens niet zonder meer vergeleken kunnen en mogen worden omdat zij slechts verwerkt mogen worden voor een bepaald doel. Verder is het lastig om op grote schaal vast te stellen welke gegevens zijn geverifieerd en welke niet; sowieso gaat het bij politiegegevens vaak om informatie waarvan (nog) niet vastgesteld is of deze juist zijn (of zij overeenkomen met de feitelijke gebeurtenis). Denk bijvoorbeeld aan een aangifte of een getuigenverklaring. Met de Richtlijn gegevensbescherming opsporing en vervolging zijn er nog labelings- en categoriseringsverplich-tingen bij gekomen: zo moet onderscheid zoveel mogelijk worden gemaakt tussen feiten en meningen en tussen categorieën betrokkenen (op basis van hun rol in het strafrechtelijk onderzoek; bijvoorbeeld verdachte, slachtoffer of getuige).

[45] Brief van de minister van JenV van 21 april 2020, 2868162.

De knelpunten als gevolg van samenloop van de Wpg met andere wetgeving (met name het Wetboek van Strafvordering, de Wjsg, de AVG, de Politiewet 2012, de Archiefwet en de Wob) bestaan ook nog steeds of zijn door de inwerkingtreding van het nieuwe Europese gegevensbeschermingskader zelfs groter geworden. Een gesprekspartner noemt het volgende voorbeeld: het Nederlands Forensisch Instituut (NFI) verwerkt gegevens ten behoeve van de opsporing. Is het NFI dan zelfstandig verwerkingsverantwoordelijke (AVG), verwerker voor de politie (Wpg) of valt de verwerking onder de Wjsg omdat de gegevens deel gaan uitmaken van een strafdossier? Het onderscheid tussen Wpg en Wsjg noemt deze gesprekspartner begrijpelijk, maar tot op zekere hoogte kunstmatig. De verhouding tussen Wpg, Wjsg en WvSv is niet altijd even duidelijk. De officier van justitie heeft in de aansturing van de politie bijvoorbeeld ook toegang tot allerlei politiegegevens, maar de gegevens vallen dan onder een ander juridisch kader.

3.5.3 Nieuwe knelpunten

Verkrijgen van gegevens

Door digitalisering kan de politie bij haar werk gebruik maken van nieuwe hulpmiddelen zoals drones, bodycams en andere camera's, en kunnen er daardoor steeds meer (persoonsgerelateerde) data verkregen worden uit nieuwe en steeds uiteenlopender bronnen. Zo is op het internet een steeds groter wordende hoeveelheid data beschikbaar. Daarnaast werkt de politie met grote datasets die het niveau van individuele zaken/onderzoeken ver overstijgen. Het verzamelen van gegevens wordt vooral gereguleerd in andere wetten: het WvSv en de Politiewet 2012. Vooral die laatste wet schiet naar verwachting tekort in het licht van (toekomstige) technologische mogelijkheden voor het verzamelen en bewerken van data.

Verder mist de politie een verkrijgingsgrond voor andere taken dan strafvordering. Art. 3 Politiewet 2012, op grond waarvan politiemensen een beperkte inbreuk mogen maken op iemands persoonlijke levenssfeer, is een belangrijke grondslag voor het verkrijgen van gegevens voor bijvoorbeeld de handhaving van openbare orde. Deze grondslag wordt momenteel ook vaak gebruikt voor het verkrijgen van gegevens met nieuwe technieken. Denk hierbij bijvoorbeeld aan het verkrijgen van informatie met bodycams. Gesprekspartners geven aan dat het vaak de vraag is of bij het inzetten van nieuwe technieken sprake is van een geringe inbreuk en de verkrijging valt onder art. 3 Politiewet 2012, of dat het gaat om een grotere inbreuk op de persoonlijke levenssfeer. Dit zou beteken dat er een andere, specifiekere wettelijke grondslag nodig is.

Bewerken van gegevens

In de Wpg wordt het bewerken van politiegegevens op een aantal plekken gereguleerd, maar dit sluit niet altijd goed aan bij de praktijk. Zo biedt de Wpg onvoldoende handvatten voor het gebruik van gegevens in big data- en AI-toepassingen. Gesprekspartners geven aan dat de Wpg niet is toegerust op toepassing van deze nieuwe technologieën en stellen dat het onduidelijk is wanneer en hoe welke gegevens mogen worden bewerkt. Een gesprekspartner kaart aan dat wanneer gegevens eenmaal rechtmatig zijn verkregen de Wpg relatief weinig heeft geregeld met betrekking tot het verdere gebruik; de reikwijdte van het gebruik en de controle op het gebruik. Het huidige wettelijk systeem is daarnaast volgens deze geïnterviewde (te veel) ingericht op individuele zaken en niet op data(sets). Op het moment dat binnen een strafrechtelijk onderzoek onrechtmatig gegevens zijn verzameld, heeft dit effect op de desbetreffende strafzaak. Het kan leiden tot strafvermindering of zelfs tot bewijsuitsluiting. De

onrechtmatig verkregen data kunnen echter worden bewaard en mogen worden gebruikt voor een ander onderzoek.

Andere knelpunten zijn, onder meer, het gebruik van politiegegevens voor trainingsdoeleinden en het gebruik van politiegegevens voor (wetenschappelijk) onderzoek; in hoeverre en onder welke voorwaarden is dit mogelijk?

Verstrekken van gegevens

Voor het verstrekken van gegevens onderscheidt de Wpg verschillende 'niveaus'/vormen. De eerste vorm is het verstrekken van gegevens tussen de partijen die gegevens verwerken onder de Wpg. Dit valt binnen de reikwijdte van Richtlijn 2016/680. Verstrekking tussen Wpg-partners heet in Wpg-termen 'ter beschikking stellen'. Hiervoor geldt dat gegevens worden verstrekt als dat noodzakelijk en proportioneel is voor het doel, tenzij er een wettelijke beperking is ('ja, tenzij'). Wpg-partners kunnen elkaar ook autoriseren om gegevens te raadplegen.

De tweede vorm van verstrekking is de verstrekking aan derden. Voor de verstrekking aan partijen die gegevens verwerken onder een ander regime dan de Wpg (derde partijen) geldt het uitgangspunt 'nee, tenzij' (§ 3 Wpg). Dat betekent dat gegevens alleen kunnen worden verstrekt als er een wettelijke grondslag is in of op grond van de Wpg, en de verstrekking noodzakelijk en proportioneel is.

De verstrekking aan derden is mogelijk op basis van een bepaling in de Wpg zelf, het Besluit politiegegevens, een machtiging, een incidentele verstrekking of een verstrekking aan een partner in een samenwerkingsverband. Alleen de verstrekking aan het gezag (officier van justitie en burgemeester) is een verplichte verstrekking (art. 16 Wpg). De Wjsg-organisaties vallen ook onder verstrekking aan derden. Dit vormt een obstakel in de praktijk: de Wpg is oorspronkelijk een semi-gesloten regime, waarbij het delen van politiegegevens buiten het Wpg-domein slechts bij uitzondering mogelijk is. Dit past niet bij de huidige schaal van samenwerking met andere partijen binnen Nederland, bijvoorbeeld op het gebied van het tegengaan van ondermijning. Tegelijkertijd geven gesprekspartners aan dat politiegegevens veelal bestaan uit gevoelige en soms zachte informatie. Er moet dus goed worden nagedacht wat met wie en op welke gronden wordt gedeeld.

De derde vorm van gegevensverstrekking is neergelegd in artikel 15a Wpg. Dit artikel stimuleert dat politiediensten binnen de EU goed samenwerken. Bij deze verstrekking doen zich op dit moment – voor zover bekend – geen bijzondere problemen voor.

De vierde vorm van gegevensverstrekking is de verstrekking aan derde landen en internationale organisaties. Hier vallen de BES-eilanden, Aruba, Curaçao en Sint Maarten ook onder. De verstrekking aan derde landen is neergelegd in de 'drietrapsraket' van art. 17a Wpg. Lid 1 maakt structurele verstrekking van gegevens mogelijk wanneer de Europese Commissie ten aanzien van het desbetreffende land een adequaatheidsbesluit heeft genomen. Dit is nog niet gebeurd en wordt ook niet op korte termijn verwacht. Lid 2 stelt dat gegevens kunnen worden verstrekt als er sprake is van een juridisch bindend instrument zoals een verdrag of wetgeving, óf wanneer de verwerkingsverantwoordelijke heeft beoordeeld dat het derde land of de organisatie anderszins voldoende waarborgen biedt. Tot slot zijn in lid 3 de uitzonderingen neergelegd. Dit moet de verwerkingsverantwoordelijke zelf per casus beoordelen.

In de praktijk komt het erop neer dat geen enkel derde land en geen enkele internationale organisatie onder lid 1 valt. Wanneer niet eerder is vastgesteld dat het land/de organisatie

onder lid 2 valt, moet de verwerkingsverantwoordelijke elke keer zelf kijken of in de praktijk passende waarborgen zijn geregeld. Verwerkingsverantwoordelijken in Nederland werken hierbij samen. Dit systeem kan in de praktijk problemen opleveren, vooral wanneer vanuit een bepaald veiligheidsprobleem met een land moet worden samenwerkt, maar het desbetreffende land niet de passende privacywaarborgen biedt. Dit roept vragen op over de mogelijke gegevensuitwisseling. Wat kan wel en wat kan niet worden gedeeld?

Toezicht

Een gesprekspartner noemt als knelpunt dat de AP, vanwege het grote takenpakket, onvoldoende menskracht en middelen heeft voor toereikend toezicht op zowel de naleving van de AVG als de Wpg. Het toezicht door de AP bestaat op dit moment vooral uit toezicht achteraf. Er zou volgens deze gesprekspartner vooraf een onafhankelijke toets moeten komen door bijvoorbeeld een officier van justitie, een rechter-commissaris of een toetsingscommissie, met name bij grootschalig gebruik van data. Momenteel is de toetsing vooraf beperkt. Als de gegevens eenmaal binnen de politie zijn, is het relatief eenvoudig ze verder te verwerken en te delen. Wel moet een voorgenomen verwerking bij een hoog risico en bij nieuwe technologieën worden voorgelegd aan de AP. De functionaris gegevensbescherming van de politie kan ongeacht wat de AP doet optreden. Daarnaast zijn er interne privacyfunctionarissen bij de politie. Er is in de Richtlijn bewust voor gekozen de externe toezichthouder niet de bevoegdheid te geven om de verwerking stil te leggen. Een gesprekspartner vraagt zich af of de AP in de toekomst ook bevoegd moet worden om gegevens die in strijd met de wet zijn verwerkt te verwijderen. Gesprekspartners zijn benieuwd hoe andere landen dit hebben ingevuld.

3.6 Samenvatting

De Wpg is sinds de inwerkintreding in 2008 niet wezenlijk gewijzigd; de EU-Richtlijn gegevensbescherming opsporing en vervolging is geïmplementeerd in de bestaande Wpg en de systematiek, structuur en opbouw zijn verder nauwelijks veranderd. Veel van de in de evaluatie van 2012/2013 geconstateerde knelpunten zijn nog steeds niet weggenomen. Ook zijn er nieuwe knelpunten en dilemma's bij gekomen, bijvoorbeeld doordat de reikwijdte van de Richtlijn niet één op één op die van de Wpg past en doordat de politieorganisatie, samenleving en opsporingsmiddelen (ICT, drones, bodycams, etc.) zijn veranderd en verregaand zijn gedigitaliseerd.

Op basis van de – vanwege de scope, de internationale focus en het tijdsbestek van het onderzoek beperkte, verkennende – analyse in dit hoofdstuk komen wij tot de volgende nog openstaande knelpunten, dilemma's, vraag- en aandachtspunten voor de casestudy's in de vergelijkingslanden.

Structuur wet past niet meer op structuur politieorganisatie

Uit de evaluatie van de Wpg in 2012/2013 bleek een worstelende nalevingspraktijk. De Wpg bevat nog steeds veel open en/of vaag geformuleerde normen die voor onduidelijkheid en verschillen in toepassing/interpretatie zorgen. Op andere punten is de wet juist misschien te gedetailleerd en daardoor moeilijk naleefbaar. Ook was de Wpg oorspronkelijk geschreven voor de verwerking van gegevens door en uitwisseling tussen regionale korpsen binnen Nederland, waardoor de wet nu 'aan alle kanten knelt' en 'enkele artikelen inmiddels zinledig zijn geworden'. Ook heeft de implementatie van de Richtlijn de naleefbaarheid van de Wpg niet verbeterd. De driehoek wet- en regelgeving/uitvoeringspraktijk/ICT en organisatorische maatregelen sluit nog altijd niet goed op elkaar aan. Wel blijkt uit externe privacy audits dat de naleving een stijgende lijn vertoont.

Categorisering van gegevens sluit niet aan bij politiewerk

Politiegegevens worden op grond van de Wpg gecategoriseerd naar politietaak (art. 8-13). Bij elke categorie hoort een verwerkingsregime met bewaartermijn. Volgens meerdere gesprekspartners in de evaluatie van de Wpg en in de oriënterende interviews voor dit onderzoek is deze indeling echter niet (meer) relevant en in de praktijk niet werkbaar. Gegevens kunnen tot meerdere categorieën behoren, waardoor niet duidelijk is welk regime van toepassing is. Hierdoor kan enerzijds de privacy in het geding komen en kan anderzijds 'verschotting' de effectieve uitoefening van de politietaak in de weg staan.

Overlap met andere regimes voor gegevensverwerking geeft onduidelijkheid

De Wpg overlapt en heeft raakvlakken met diverse andere wetten en regimes voor gegevensverwerking. Voor politie- en justitiële gegevens geldt de Richtlijn gegevensbescherming opsporing en vervolging, maar op alle andere verwerkingen van persoonsgegevens is de AVG van toepassing. Verder is er samenloop met de Wjsg, het WvSv, de Politiewet 2012, de Archiefwet en de Wob. Dit zorgt voor onduidelijkheid, bijvoorbeeld bij het verstrekken van gegevens aan partijen die onder de AVG vallen.

Grondslag voor verkrijgen gegevens te beperkend voor politiewerk

Art. 3 Politiewet 2012 (omschrijving van de politietaak) is vaak de grondslag voor verkrijging van gegevens met nieuwe technieken, zoals bodycams, om de openbare orde te handhaven. 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. Gesprekspartners geven aan dat het maar de vraag is of er daadwerkelijk sprake is van een geringe inbreuk en geven aan dat de 'rek' eruit is; het risico bestaat dat er meer kan en gebeurt dan op grond van art. 3 Politiewet 2012 is toegestaan en dat risico wordt steeds groter naarmate de technologische ontwikkelingen verder gaan.

Meerdere dilemma's met bewaartermijnen

De verwijderingstermijnen zijn niet eenduidig geformuleerd, waardoor onduidelijkheid bestaat over de toepassing ervan. In verschillende wetten zijn bewaartermijnen opgenomen, waardoor het niet altijd duidelijk is hoe lang gegevens mogen worden bewaard. Daarnaast komt het voor dat dezelfde gegevens in meerdere categorieën vallen/voor meerdere doelen worden gebruikt, waardoor voor die gegevens verschillende bewaartermijnen gelden. Tot slot zorgt de cultuur bij de politie ervoor dat gegevens te lang bewaard worden.

Dit leidt (net als/in samenhang met de categorisering van politiegegevens) tot een spanningsveld tussen het belang van privacy en de vrees voor het verlies van voor het politiewerk waardevolle informatie. De verschillende regimes en 'verschotting' zorgen daarnaast voor onnodige administratieve lasten.

Semi-gesloten verstrekkingsregime Wpg wringt met behoefte aan samenwerking

De Wpg is bedoeld als een semi-gesloten regime, waarbij het delen van politiegegevens buiten het Wpg-domein slechts bij uitzondering mogelijk is. Dit past niet bij de huidige schaal van samenwerking met andere partijen binnen Nederland, bijvoorbeeld op het gebied van het tegengaan van ondermijning. Daarbij kunnen politiegegevens ook bestaan uit gevoelige en soms zachte informatie. Er moet dus goed worden nagedacht wat met wie en op welke gronden wordt gedeeld.

Controle op waarborgen bij verstrekking aan derde landen omslachtig

Verder vormt de verstrekking aan derde landen op grond van art. 17a Wpg een potentieel knelpunt. Als er geen adequaatheidsbesluit is (lid 1), geen juridisch bindend instrument (lid 2

onder a) en geen passende waarborgen zijn geconstateerd (lid 2 onder b), dan moet steeds een afweging worden gemaakt tussen noodzaak van verstrekking en inbreuk op rechten van de betrokkene. Dit kan slechts voor aantal specifiek genoemde doelen (lid 3).

Extern toezicht heeft nog open eindjes

Een gesprekspartner noemt als knelpunt dat de AP over de hele linie (dus ook voor de AVG) onvoldoende menskracht en middelen heeft voor het toezicht. Daarnaast speelt de vraag of de toezichthouder meer bevoegdheden zou moeten krijgen, bijvoorbeeld om de verwerking stil te leggen of onrechtmatig verwerkte gegevens zelf te verwijderen.

Discrepantie tussen wet en digitale en technologische werkelijkheid

Het wettelijk stelsel dat het politiewerk en de verwerking van politiegegevens reguleert (met name de Politiewet 2012, het WvSv en de Wpg) is niet berekend op de technologische mogelijkheden en uitdagingen in de huidige tijd. Door het uitdijende internet en social media zijn steeds grotere hoeveelheden data beschikbaar. Ook zijn er nieuwe hulpmiddelen voor de politie, zoals drones en bodycams, en nieuwe analysetechnieken om toe te passen op grote datasets die het niveau van individuele zaken/onderzoeken ver overstijgen. Bij de inwerkingtreding van deze wetgeving kon de wetgever hier onmogelijk op anticiperen en nog steeds gaan de ontwikkelingen zo snel dat het een uitdaging is om een ‘houdbare’ wettelijke kaders te schetsen met voldoende privacywaarborgen én voldoende speelruimte voor het politiewerk.

4

Landenvergelijking

4.1 Inleiding

In dit hoofdstuk vergelijken we aan de hand van de onderzoeksthema's en onderzoeksvragen de vijf onderzochte landen: België, Denemarken, Duitsland (focus Nordrhein-Westfalen in relatie tot Bondsrecht), Finland en Ierland. Een uitgebreidere uitwerking per casestudyland is te vinden in de bijlagen I t/m V.

In de volgende paragrafen houden we grofweg dezelfde structuur aan als in de aparte landenstudies: in paragraaf 4.2 vergelijken we de wettelijke systemen van de vijf landen voor de verwerking van de politiegegevens. Paragraaf 4.3 behandelt de op grond van Richtlijn 2016/680 bevoegde autoriteiten in de onderzochte landen. Vervolgens gaan we in paragraaf 4.4 in op de verschillende aspecten van de verwerking van politiegegevens in wet en (waar relevant en mogelijk) praktijk: verkrijgen, bewerken, categoriseren/labelen, bewaren en verstrekken/delen. In paragraaf 4.5 bespreken we hoe het toezicht in de verschillende landen is vormgegeven.

4.2 Wettelijk kader

4.2.1 Algemeen

Allereerst is het belangrijk om op te merken dat de vergelijkingslanden niet met het begrip 'politiegegevens' werken. Ze gaan in de wetgeving uit van de verwerking en bescherming van persoonsgegevens (door de politie en andere bevoegde autoriteiten). Dit was een uitdaging voor de afbakening van het onderzoek en het selecteren van gespreksonderwerpen en gesprekspartners. We hebben geprobeerd zo goed mogelijk aan te sluiten bij de scope van de Nederlandse Wet politiegegevens (die ook nog eens niet één op één past op de reikwijdte van de Richtlijn gegevensbescherming opsporing en vervolging), maar moesten vanwege het verkennende karakter (en dus de beperkte tijd voor het bestuderen van een groot aantal landen en onderwerpen) ook keuzes maken. Daarom hebben we vooral gefocust op – en gesproken met – de politie en niet op (de buitenlandse tegenhangers van) andere bevoegde autoriteiten. Omdat het toepassingsbereik van de Richtlijn gegevensbescherming opsporing en vervolging (en daarmee van de implementatiewetgeving) wel een belangrijk en interessant (knel)punt is, besteden we in paragraaf 4.3 wel apart aandacht aan de bevoegde autoriteiten.

4.2.2 Wetgeving die ziet op de verwerking van politiegegevens

In België wordt de verwerking van persoonsgegevens door politiediensten vooral gereguleerd in twee wetten: de Wet bescherming persoonsgegevens (Wbp) en de Wpa (Wet op het politieambt). In de Wbp zijn de Richtlijn en de AVG omgezet; titel 2 gaat over de Richtlijn. In de Wpa vermeldt art. 44 lid 1 expliciet dat gegevensverwerking door de politie gebeurt conform (art. 27 van) de Wbp. Verder is de Camerawet van belang voor het inzetten van bewakingscamera's en de omgang met camerabeelden door overheden.

Denemarken is lid van de EU, maar heeft op grond van het Edinburgh-akkoord op enkele punten opt-outs op het Verdrag van Maastricht. Dit betekent dat Denemarken niet hoeft deel te nemen aan Europese wetgeving op bepaalde beleidsterreinen, zoals justitie en binnenlandse zaken. Denemarken was dus niet verplicht om deel te nemen aan de Richtlijn gegevensbescherming opsporing en vervolging. Omdat het niet meedoen als gevolg zou hebben dat Denemarken geen deel meer zou uitmaken van Europol, is besloten de Richtlijn toch om te zetten. Binnen een maand heeft Denemarken vervolgens de Richtlijn geïmplementeerd in de Processing of personal data by law enforcement Act. Mede door de korte implementatieperiode zijn er geen (grote) verschillen tussen de inhoud en tekst van de Act en de Richtlijn.

In Duitsland bestond er al uitgebreide privacywetgeving op Bonds- en Landsniveau. Deze wordt sterk beïnvloed door de jurisprudentie van het grondwettelijk hof, het Bundesverfassungsgericht. Richtlijn 2016/680 en de AVG zijn omgezet in de Bondsgegevensbeschermingswet (Bundesdatenschutzgesetz), die geldt voor overheidsdiensten en private organisaties op Bondsniveau – waaronder drie Bondspolitiediensten[46] – en op Landsniveau voor zover de Landen zelf niets geregeld hebben. Alle Landen hebben ook een eigen Gegevensbeschermingswet; in Nordrhein-Westfalen (NRW) is dat de Gegevensbeschermingswet NRW (Datenschutzgesetz NRW). In de Bondsgegevensbeschermingswet en de Gegevensbeschermingswet NRW, die qua structuur sterk op elkaar lijken, bevat Deel 3 de omzetting van de Richtlijn. Deze algemene privacywetten zijn *lex generalis*; ze gelden alleen als een kwestie niet in specifieke wetgeving geregeld is. Voor verwerking van persoonsgegevens in het kader van politietaken zijn die specifieke wetten met name (geldend voor ons aandachtsgebied Nordrhein-Westfalen in relatie tot de Bond):

- het Wetboek van Strafvordering (*Strafprozessordnung*)
- de *Ordnungswidrigkeitenwet* (*Ordnungswidrigkeiten* zijn administratiefrechtelijke overtredingen die bestraft kunnen worden met een geldboete)
- de politiewetten op Bonds- en Landsniveau, zoals de Wet op het Bundeskriminalamt (BKA, de federale recherche) en de Politiewet Nordrhein-Westfalen (Polizeigesetz NRW)
- de *Ordnungsbehördengesetz NRW* (*Ordnungsbehörden* zijn bestuursrechtelijke, bijvoorbeeld gemeentelijke, autoriteiten belast met de afweer van gevaren voor de openbare orde en veiligheid en soms de opsporing/vervolging van *Ordnungswidrigkeiten*)

Een schematisch overzicht van de relevante wetgeving en de onderlinge verhoudingen staat in de bijlage Casestudy V – Duitsland.

[46] De Bondspolitie, de politie voor het parlement (de Bondsdag) en het Bundeskriminalamt (BKA, de federale recherche). Die laatste heeft een belangrijke rol bij het coördineren van de politionele samenwerking tussen Bond en de zestien Länder en de internationale politionele samenwerking. Daarom hebben we in het onderzoek op Bondsniveau ingezoomd op de Wet op het Bundeskriminalamt (BKA-Gesetz) en gesproken met het BKA.

Belangrijk in het Duitse politierecht is het scherpe onderscheid tussen de preventieve (*Gefahrenabwehr*, gevarenafweer) en de repressieve (*Strafverfolgung*) politietaak. Gevarenafweer is de afweer van gevaren voor de openbare orde en veiligheid, en het in het kader daarvan preventief bestrijden van strafbare feiten. *Strafverfolgung* beslaat de opsporing, het onderzoek en de vervolging *nadat* een strafbaar feit is gepleegd. Deze scheiding bepaalt in welke wet een opsporingsambtenaar moet kijken: bij gevarenafweer geldt de politiewet, bij *Strafverfolgung* het Wetboek van Strafvordering. De politiewetten hebben aparte, uitgebreide hoofdstukken over gegevensverwerking, waarbij de wetgever onderscheid heeft gemaakt tussen gegevensverkrijging/verzameling en verdere verwerking van gegevens. In het Wetboek van Strafvordering staat bij de verschillende opsporingsmaatregelen en -bevoegdheden uitgebreid omschreven onder welke voorwaarden welke gegevens mogen worden verzameld en verwerkt.

In Finland is de Richtlijn omgezet door wijziging van twee bestaande wetten. Ten eerste de algemene wet met betrekking tot de verwerking van persoonsgegevens in strafzaken: de *Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018; Law Enforcement Data Protection Act)*. Deze wet geeft de algemene regels voor het verwerken van persoonsgegevens in het kader van strafzaken. De verwerking van persoonsgegevens specifiek door de politie wordt ook beheerst door de *Act on the Processing of Personal Data by the Police (616/2019)*. Een opvallend punt in de Finse wetgeving is het feit dat er in de inleidende bepalingen expliciet aandacht wordt gegeven aan het respecteren van de fundamentele rechten van de mens en een aantal fundamentele beginselen. Het beginsel van openbaarheid van overheidshandelen is al lang een traditioneel uitgangspunt in Finland. Algemeen is de opvatting dat in beginsel alles wat de overheid doet openbaar moet zijn omdat het daarmee ook controleerbaar is. Burgers moeten toegang hebben tot overheidsinformatie en belangrijke documenten. Dit zorgt soms voor conflicten met de EU-databeschermingsregels. Ook bijvoorbeeld in Duitsland wordt de koppeling gemaakt tussen enerzijds bescherming van persoonsgegevens en anderzijds vrijheid/openbaarheid van overheidsinformatie: de toezichthoudende autoriteiten heten veelal *(Landes/Bundes)beauftragte für Datenschutz und Informationsfreiheit* ((Lands/Bonds)agent voor Gegevensbescherming en Informatievrijheid).

Ierland heeft de AVG en Richtlijn 2016/680 uitgewerkt in de Data Protection Act 2018. Deel 5 gaat over de Richtlijn en is zeer algemeen en open geformuleerd. Zo is niet gespecificeerd wie de bevoegde autoriteiten in de zin van de Richtlijn zijn en wie verwerkingsverantwoordelijken. Dit komt door de korte implementatietermijn en door het grote aantal (potentiële) bevoegde autoriteiten in Ierland. Verder is voor gegevensverwerking in het kader van de politietaak onder meer de Ierse politiewet van belang: de Garda Síochána Act 2005 (An Garda Síochána of de Garda is de Ierse nationale politie en veiligheidsdienst).

4.2.3 Resumé

Samenvattend valt op dat drie van de onderzochte landen (België, Duitsland en Ierland) hebben gekozen voor één wet die het hele (Europese) kader voor gegevensbescherming vastlegt, waarin een hoofdstuk is gereserveerd voor de omzetting van de Richtlijn gegevensbescherming opsporing en vervolging. Denemarken heeft de richtlijn omgezet in een aparte wet. In Finland is ervoor gekozen de Richtlijn om te zetten door twee bestaande wetten te wijzigen. Een van deze wetten ziet specifiek op gegevensverwerking door de politie. In welke mate de onderzochte landen letterlijk de tekst van de Richtlijn volgen – en daarmee nog veel open en algemene normen in de wet hebben staan – verschilt en hangt af van onder meer de mate waarin er al wetgeving op dit gebied bestond. Duitsland heeft bijvoorbeeld een lange geschie-

denis met privacywetgeving; de eerste Bondsgegevensbeschermingswet stamt uit 1977. Gesprekspartners geven aan dat er daarom met de komst van de Richtlijn niet bijster veel hoefde te worden veranderd aan de bestaande wetgeving.

4.3 De bevoegde autoriteiten

Zoals in de vorige hoofdstukken al aan de orde kwam, is EU-Richtlijn 2016/680 van toepassing op de verwerking van persoonsgegevens door bevoegde autoriteiten[47] met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid. Het toepassingsbereik van de Richtlijn bestaat dus uit twee elementen: *bevoegde autoriteit* (actor) en *voorkoming, onderzoek, opsporing van strafbare feiten etc.* (doel/taak).

De Nederlandse Wet politiegegevens is van toepassing op de verwerking van politiegegevens door bevoegde autoriteiten, waarbij politiegegevens slaan op – kort gezegd – alle persoonsgegevens die worden verwerkt in het kader van de uitvoering van de politietaak zoals omschreven in de Politiewet.[48] Nederland koppelt de privacyregels uit de Richtlijn op deze manier dus aan de politietaak zoals Nederland die in de wet heeft geformuleerd, en niet aan bovenstaande verder reikende formulering van de verwerkingsdoelen uit de Richtlijn; hierbij speelt mee dat Nederland ervoor heeft gekozen de tweedeling in Wet politiegegevens en Wet justitiële en strafvorderlijke gegevens intact te laten.

De andere onderzochte landen gaan verschillend om met de reikwijdte van de Richtlijn. België en Denemarken hebben de bevoegde autoriteiten expliciet opgesomd in hun wetgeving,[49]

[47] Art. 3 onder 7 Richtlijn: „bevoegde autoriteit": a) iedere overheidsinstantie die bevoegd is voor de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid; of b) ieder ander orgaan dat of iedere andere entiteit die krachtens het lidstatelijke recht is gemachtigd openbaar gezag en openbare bevoegdheden uit te oefenen met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

[48] Zie voor de uitzonderingen hoofdstuk 3 over de Nederlandse situatie.

[49] België: a) de politiediensten;
b) de gerechtelijke overheden (de gemeenrechtelijke hoven en rechtbanken en het openbaar ministerie);
c) de Dienst Enquêtes van het Vast Comité van Toezicht op de politiediensten in het kader van zijn gerechtelijke opdrachten (…);
d) de Algemene Inspectie van de federale politie en van de lokale politie;
e) de Algemene administratie van de douane en accijnzen, in het kader van haar opdracht inzake opsporing, vaststelling en vervolging van de misdrijven zoals bepaald in de algemene wet inzake douane en accijnzen van 18 juli 1977, en in de wet van 22 april 2003 houdende toekenning van de hoedanigheid van officier van gerechtelijke politie aan bepaalde ambtenaren van de administratie der douane en accijnzen;
f) de Passagiersinformatie-eenheid;
g) de Cel voor financiële informatieverwerking (…);
h) de Dienst Enquêtes van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten in het kader van zijn gerechtelijke opdrachten (…); (art. 26 lid 7 Wet bescherming persoonsgegevens).
Denemarken: de politie, het openbaar ministerie (Prosecution Service), de rechtbanken, de

waar Finland en vooral Ierland ervoor hebben gekozen dit open te laten door min of meer woordelijk de definitie van de Richtlijn aan te houden. In Ierland komt dit doordat er zeer veel organisaties en entiteiten zijn met opsporings- en vervolgingsbevoegdheden in de zin van de Richtlijn. Of het handelen onder de Richtlijn valt moet daarom per geval worden bekeken aan de hand van de twee elementen (a. gaat het om een bevoegde autoriteit en b. gaat het om *law enforcement purposes* in de zin van de Richtlijn?), zoals de Ierse toezichthoudende autoriteit, de Data Protection Commission (DPC) uitlegt op haar website.[50] Finland noemt in de wet nog wel de politie, het leger en de grenswacht bij naam als bevoegde autoriteiten, wanneer zij Richtlijn-taken uitvoeren.[51] Het beeld in Duitsland is diffuser door het federale stelsel; de Bondsgegevensbeschermingswet volgt haast letterlijk de Richtlijn en wijst geen specifieke bevoegde autoriteiten aan, terwijl de Gegevensbeschermingswet Nordrhein-Westfalen wel een lijstje kent met bevoegde autoriteiten.[52] Het scala aan bevoegde autoriteiten loopt dus uiteen; zo kan in Ierland Dublin Bus onder de Richtlijn vallen bij het sanctioneren van zwartrijders, en heeft Finland de inlichtingendienst onder de Law Enforcement Data Protection Act gebracht, terwijl de nationale veiligheid buiten de scope van het EU-recht valt.[53]

De politietaak speelt in de privacywetgeving van de bestudeerde landen vooral een rol bij (het beoordelen van) de doelbinding, noodzakelijkheid en proportionaliteit van de verwerking van persoonsgegevens; het verzamelen, gebruiken of delen van gegevens is op grond van de Europese en nationale regelgeving alleen rechtmatig als daarvoor een wettelijke grondslag is en voor zover noodzakelijk met het oog op het doel. Zo'n doel kan zijn het uitvoeren van een politietaak zoals omschreven in de politiewet of andere specifieke wetten (die dan tegelijk de wettelijke grondslag bieden). Het detailniveau waarop de politietaak in de wet is omschreven en de reikwijdte van de politietaak verschilt per land, net als de organisatie van de politie (nationale politie of meerdere niveaus of verschillende 'themapolitiediensten' (zoals een grens-, spoorbaan- en/of luchthavenpolitie); politie- en veiligheidsdienst ineen of juist niet; bestuurlijke politie of niet); zie voor een uitgebreide beschrijving van de politiestructuur de afzonderlijke casestudy's.

gevangenissen (reclassering), de klachtencommissie politietoezicht (strafrechtelijk onderzoek tegen wetshandhavers) en de rechter-advocaat-generaal (militaire vervolging) (paragraaf 3 Processing of personal data by law enforcement Act).

[50] Data Protection Commission, *Law Enforcement Directive - Guidance on Competent Authorities and Scope*, www.dataprotection.ie/en/organisations/law-enforcement-directive (laatst geraadpleegd op 26 september 2020).

[51] Art. 3 sub 5 Law Enforcement Data Protection Act. De Finse politie noemt nog op haar website de politie, algemene rechtbanken, de Criminal Sanctions Agency, de douane en de grenspolitie;

https://www.poliisi.fi/about_the_police/data_protection_and_the_rights_of_data_subjects/data_protection_legislation.

[52] Art. 35 Gegevensbeschermingswet NRW benoemt als bevoegde autoriteiten, in het kader van hun taken als bedoeld in art. 1 Richtlijn:
1. De politie
2. De gerechten in strafzaken en het OM
3. De strafvoltrekkingsautoriteiten
4. De autoriteiten belast met de voltrekking van maatregelen
5. De financiële opsporingsdiensten (*Finanzverwaltung*)
Voor *Ordnungsbehörden* geldt deel 3 (Richtlijn 2016/680) van de Gegevensbeschermingswet NRW voor zover zij *Ordnungswidrigkeiten* vervolgen en afdoen en/of sancties voltrekken.

[53] In Ierland is de Garda zowel nationale politie als inlichtingen- en veiligheidsdienst, maar voor wat betreft de nationale veiligheid geldt nog de Data Protection Act 1988.

4.4 Verwerken van politiegegevens

4.4.1 Verkrijgen van politiegegevens

Alle bestudeerde landen hebben in hun wetgeving die ziet op de verwerking van persoonsgegevens (in het kader van de politietaak) aandacht besteed aan de Europese privacybasisprincipes, en dan met name zoals die verwoord zijn in de Richtlijn gegevensbescherming opsporing en vervolging. Het gaat dan om algemene uitgangspunten zoals dat persoonsgegevens voor welbepaalde, uitdrukkelijk omschreven en legitieme doeleinden moeten worden verzameld en niet op een met die doeleinden onverenigbare wijze mogen worden verwerkt (art. 4 lid 1 sub b Richtlijn), en dat de gegevens toereikend, ter zake dienend en niet bovenmatig in verhouding tot die doeleinden zijn (art. 4 lid 1 sub c Richtlijn); de beginselen van noodzakelijkheid, proportionaliteit en doelbinding en het legaliteitsbeginsel. Gesprekspartners in de interviews in alle landen benadrukken dat er altijd een voldoende specifieke wettelijke grondslag moet zijn voor het verwerken – waaronder dus ook het verzamelen – van persoonsgegevens moet zijn. Dat betekent dat er in de casestudylanden, net als in Nederland, naast de algemene grondslag van de politietaak in de politiewet veel verschillende, gedetailleerdere wettelijke grondslagen zijn voor bevoegde autoriteiten om zelf gegevens te verzamelen of gegevens te verkrijgen van andere organisaties (zie ook paragraaf 4.4.5 over het delen van politiegegevens). Zo bestaan er in Ierland vele kinderbeschermingswetten op grond waarvan het mogelijk is informatie te delen om de veiligheid van kinderen te garanderen. Ook de Wetboeken van Strafvordering spelen net als in Nederland een belangrijke rol bij het reguleren van de opsporingsbevoegdheden (en dus het verzamelen van data voor de opsporing). Wat opvalt is dat in België en Denemarken de nadruk meer lijkt te liggen op de informatiepositie van de politie; in België is bijvoorbeeld expliciet opgenomen dat het vrije verkeer van persoonsgegevens[54] zo min mogelijk mag worden beperkt of verboden om privacyredenen. In Denemarken blijkt uit de (let wel: beperkte) gesprekken dat er groot vertrouwen is in de politie en dat de basishouding is dat de uitvoering van de politietaken niet onnodig belemmerd mag worden door regelgeving. In andere landen ligt het zwaartepunt juist veel meer op de bescherming van betrokkenen en is in de wet daarom uitgebreid dichtgetimmerd wat de politie mag doen, met welk opsporingsmiddel, met welke doelen en onder welke voorwaarden. Zo bevat de Duitse politiewetgeving in de afdelingen over gegevensverzameling (*Datenerhebung*) veelal per soort opsporingsbevoegdheid (zoals identiteitsvaststelling (al dan niet door middel van DNA-onderzoek), observatie, infiltratie, gebruik van bodycams) regels, grenzen en waarborgen. Hoe zwaarder de inbreuk op de persoonlijke levenssfeer, hoe strenger de beperkingen en waarborgen.

De meeste vergelijkingslanden hebben specifieke regelgeving over cameratoezicht en bodycams, maar andere nieuwe technologieën voor dataverzameling, zoals het binnenhalen van grote datasets met *open source intelligence* en andere *big data*-technieken, blijven onderbelicht. De wetgeving is nog op individuele zaken/onderzoeken/personen ingericht, en niet op grote hoeveelheden data. Zo zorgt het ontbreken van een algemene wettelijke grondslag voor het gebruik van Artificial Intelligence bij de analyse van big-data sets in Finland ervoor dat daar in de praktijk amper gebruik kan worden gemaakt van dergelijke sets, omdat dit grotendeels handmatig zou moeten gebeuren. Ook op het gebied van gezichtsherkenning hebben we geconstateerd dat deze nog niet kan worden ingezet (of dat er op zijn minst discussie over de inzet is) omdat een wettelijke grondslag ontbreekt of hier onduidelijkheid over bestaat. In de andere landen zien we eveneens dat dergelijke technologieën op zijn minst discussie oproepen.

[54] En met name de uitwisseling van persoonsgegevens door instanties handelend met het oog op doelen uit art. 23 lid 1 sub a t/m h AVG (o.a. nationale veiligheid en de opsporings- en vervolgingsdoelen uit de Richtlijn).

Over het algemeen zien we dat de wetgever in de verschillende landen de regels technologieneutraal heeft willen formuleren, maar dat dit net als in Nederland de vraag oproept naar de verhouding met het vereiste van een specifieke grondslag, en (dus) naar de toekomstbestendigheid.

4.4.2 Bewerken van politiegegevens

De term 'bewerken' van politiegegevens is erg breed; art. 1 sub c Wet politiegegevens definieert *verwerken van politiegegevens*, in navolging van de Richtlijn en de AVG, zelfs als:

> *'elke bewerking of elk geheel van bewerkingen met betrekking tot politiegegevens of een geheel van politiegegevens, al dan niet uitgevoerd op geautomatiseerde wijze, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, afschermen of vernietigen van politiegegevens.'*

In het licht van onderzoeksvraag 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*?') hebben we 'bewerken' bij het bestuderen van de vijf landen vooral opgevat als: wat voor mogelijkheden voor gebruik van gegevens hebben de bevoegde autoriteiten als ze de gegevens eenmaal in hun bezit hebben, niet zijnde labelen/categoriseren, bewaren/vernietigen en verstrekken/delen, want daar zien andere onderzoeksvragen op. Het gaat in deze paragraaf dus vooral om de kaders voor verdere (technische) gebruiks- en analysemogelijkheden, waaronder gebruik voor andere doelen dan waarvoor de data zijn verkregen (zoals wetenschappelijke of opleidingsdoelen).

De meeste onderzochte landen hebben het *bewerken* van politiegegevens zoals hierboven afgebakend niet specifiek geregeld, maar gaan uit van de Europeesrechtelijke term *verwerken* (*processing*), waar dus elke handeling met persoonsgegevens onder valt. De regels, kaders en basisbeginselen gelden voor alle verwerkingen. In Ierland, Finland, Denemarken en België zijn de regels – met kleine tekstuele en volgordeverschillen – één op één overgenomen uit de Richtlijn en dus weinig specifiek.[55] Ze zijn technologieneutraal opgesteld en gaan niet expliciet in op het inzetten van *big data* en *artificial intelligence (AI)* of het koppelen van databestanden, maar geven algemene richtsnoeren gebaseerd op noodzakelijkheid, proportionaliteit en doelbinding en passende technische en organisatorische maatregelen om de gegevens te beveiligen. Wel zijn de bepalingen uit de Richtlijn overgenomen over het uitvoeren van een Data Protection Impact Assessment (DPIA) en het eventueel raadplegen van de FG en/of de toezichthoudende autoriteit vóór het inzetten van een mogelijk risicovolle nieuwe techniek. Er worden geen nadere voorwaarden gesteld ten opzichte van de Richtlijn voor bijvoorbeeld het gebruik van gegevens voor wetenschappelijk onderzoek of trainingsdoeleinden.

In Duitsland wordt zoals gezegd onderscheid gemaakt tussen verzameling en verdere verwerking van gegevens. De hoofdstukken 'Verdere verwerking van gegevens' van de politiewetten (zoals de Wet op het Bundeskriminalamt en de Politiewet Nordrhein-Westfalen) bevatten eerst een algemeen artikel met principiële uitgangspunten, zoals doelbinding en het in de

[55] Een aantal bepalingen in de Finse wetgeving vormen hierop een uitzondering, bijvoorbeeld de bepalingen over de speciale categorieën persoonsgegevens.

jurisprudentie van het Bundesverfassungsgericht ontwikkelde 'beginsel van hypothetische nieuwe verzameling van gegevens'. Dit beginsel geldt als men gegevens wil gebruiken voor een ander doel dan waarvoor ze zijn verkregen en houdt in dat dan een minstens zo ernstig strafbaar feit of een minstens zo zwaarwegend belang of rechtsgoed aan de orde moet zijn als bij de verkrijging. Met andere woorden, dezelfde (wettelijke) voorwaarden en waarborgen gelden die golden voor de verkrijging. Zo wordt te lichtvaardig gebruik van gevoelige of met ingrijpende opsporingsbevoegdheden verkregen gegevens voorkomen. Verder kent de Politiewet NRW bijvoorbeeld een bepaling over vergelijking van gegevens en regelt de Wet op het Bundeskriminalamt het politionele informatieverbond tussen Bond en Landen, met (privacy)regels over het bijbehorende informatiesysteem. Ook in het Duitse Wetboek van Strafvordering zijn enkele bepalingen te vinden over bijvoorbeeld geautomatiseerd vergelijken van persoonsgegevens die al voorhanden zijn. De wetgever definieert 'geautomatiseerd vergelijken' net als in Nederland verder niet. Wel zijn het uitgebreide artikelen met veel aandacht voor het voorkomen van de verwerking van onnodige gegevens en gegevens die het 'kernbereik van de persoonlijke levenssfeer' betreffen.

Uit de interviews blijkt dat in elk geval in Duitsland, Ierland en Finland in de politiepraktijk erg voorzichtig met persoonsgegevens en de technologische mogelijkheden daarmee wordt omgesprongen. De Ierse politie verzamelt en verwerkt bijvoorbeeld (nog) geen grote datasets met *big data*-technieken als *data mining*, om ethische en praktische redenen (het systeem is er nog niet op ingericht en het heeft nog niet de prioriteit). In Duitsland is de ervaring van gesprekspartners dat de politie zeer zorgvuldig bij elke voorgenomen maatregel nagaat of deze past binnen de strenge privacykaders, en zo nodig de FG of andere experts om hulp vraagt bij de afweging. De Finse politie heeft behoefte aan een specifieke wettelijke grondslag voor nieuwe technieken zoals gezichtsherkenning en zet deze niet of zeer terughoudend in tot die basis er is. Daarnaast heeft de Finse politie behoefte aan mogelijkheden om Artificial Intelligence in te zetten bij de analyse van big-data.

Een opvallend verschil tussen België en andere EU-landen ziet op de rechten van betrokkenen. In België is voor een betrokkene alleen 'onrechtstreekse toegang' mogelijk tot hem/haar betreffende persoonsgegevens die in het bezit zijn van een bevoegde autoriteit, via een verzoek aan de toezichthoudende autoriteit, het Controleorgaan op de politionele informatie (COC). De vraag speelt, bijvoorbeeld bij academici in België, of dit een te beperkte opvatting is van art. 15 Richtlijn. Ierland heeft overigens ook een voorbehoud opgenomen bij de omzetting van dit artikel: '*Nothing in this section shall require the Commission to disclose to a data subject whether or not a controller has processed, or is processing, personal data relating to him or her.*'[56] Het gaat om een spanningsveld tussen de rechten van betrokkenen en het belang om als overheid openheid van zaken te geven enerzijds en het belang van de uitvoering van de politietaak anderzijds, waar meer lidstaten mee worstelen en dat ook is erkend door de mogelijkheid van indirecte toegang in de Richtlijn op te nemen.

4.4.3 Categoriseren/labelen van politiegegevens

De onderzochte lidstaten hebben de verplichte categorisering van persoonsgegevens die volgt uit de Richtlijn overgenomen in hun wetgeving. Het gaat dan om de indeling in rol van de betrokkene ((potentiële) verdachte, slachtoffer, getuige etc.); categorieën bijzondere persoonsgegevens (zoals gezondheidsgegevens en gegevens over seksuele geaardheid); en gegevens gebaseerd op feiten en meningen. Dit kan in de praktijk voor dezelfde problemen zorgen als in Nederland, blijkt uit de gesprekken, zoals dat het vaak lastig te bepalen is wat feit

[56] Art. 95 lid 4 Data Protection Act 2018.

en wat mening is, en dat rollen van betrokkenen kunnen verschillen per zaak, of kunnen veranderen binnen een zaak. Ook had Ierland bijvoorbeeld grote bezwaren tegen de categorie potentiële verdachte: die druist rechtstreeks in tegen de onschuldpresumptie. Ierland heeft dit opgelost door op te nemen dat het onderscheid '*where relevant and in so far as possible'* moet worden gemaakt (een subtiel verschil met de formulering '*where applicable and as far as possible*' uit de Richtlijn).

Verder houden enkele onderzochte landen er in wet en/of praktijk nog eigen categoriseringen op na. Wijdverbreid is de verplichting om het doel en de rechtsgrondslag van de verwerking vast te leggen. In Duitsland en Finland moet onder meer het middel (opsporingsmethode) waarmee de gegevens zijn verzameld worden vastgelegd en Ierland maakt onderscheid naar regime (AVG of Richtlijn). Ierland kent daarnaast een zeer gedetailleerd politieprotocol met vele categorieën en bijbehorende bewaartermijnen. In Finland speelt het onderscheid tussen openbare, niet-openbare en geheime informatie ook een rol. Andere criteria die in meerdere landen worden gebruikt zijn (de ernst van) het strafbare feit waar het om gaat en wie de gegevens heeft verzameld. Een preciezere beschrijving is te vinden in de vijf landenstudies in de bijlage. Net als in Nederland speelt in de andere landen de vraag hoe deze categoriseringseisen, die geschreven lijken te zijn voor individuele gevallen, zich verhouden tot grote datasets. In Duitsland heeft de politie hiervoor een 'stoplichtsysteem' in het leven geroepen, al naar gelang de ingrijpendheid van de inbreuk op de persoonlijke levenssfeer. De kleuren rood, geel en groen geven aan hoe zwaar de gebruikte maatregel/opsporingsmethode inbreuk maakt op de privacy. Ook wordt bij grote datasets soms gecommuniceerd naar de betrokkene(n) (bijvoorbeeld de verdachte in een grote misbruikzaak waarbij 500 terabyte aan data onderzocht moest worden) dat de politie tijd nodig heeft om de gegevens te beoordelen (onder meer de noodzakelijkheid en daarmee samenhangend een prognose hoe lang ze bewaard moeten/kunnen worden). Verder kunnen in alle landen gegevens in meerdere categorieën vallen, wat knelpunten kan opleveren als de categorieën samenhangen met voorwaarden voor verder gebruik (in de zin van een stapeling van voorwaarden en restricties).

4.4.4 Bewaartermijnen en vernietigingsvoorwaarden

De mate waarin de bestudeerde landen bewaartermijnen in de wet hebben opgenomen verschilt. Belangrijk is hierbij het onderscheid tussen bewaartermijnen en 'controletermijnen', dat ook de Richtlijn maakt. Een bewaartermijn is een vaste termijn waarna de gegevens verwijderd, vernietigd of gearchiveerd moeten worden; bij controletermijnen gaat het om vaste momenten waarop gekeken moet worden – meestal door de verwerkingsverantwoordelijke – of het nog noodzakelijk is om de gegevens langer te bewaren, voor het doel waarvoor ze zijn verzameld of voor een ander legitiem doel/de uitvoering van een andere (politie)taak. Finland heeft in hoofdstuk 5 van de *Act on the Processing of Personal Data by the Police* heel precies per categorie persoonsgegevens – dat ziet met name de vraag voor welk doel de data zijn verzameld - bewaar- en controletermijnen gegeven. In Finland geldt daarnaast de strenge eis dat verzamelde data die niet noodzakelijk blijken te zijn zonder 'onnodige vertraging' moeten worden verwijderd. In Denemarken en Ierland is meer geregeld in protocollen van de bevoegde autoriteiten zelf, waarbij Denemarken veel overlaat aan de beoordeling van de betrokken functionarissen. Denemarken kent wel bijzondere wetten en ministeriële regelingen met bewaartermijnen voor eenvoudiger zaken, zoals over verkeersboetes. Ook is de Deense verantwoordelijke minister een *executive order* aan het ontwikkelen voor controletermijnen op *big data*. Duitsland werkt met door de bevoegde autoriteit vast te leggen controletermijnen, waarvan de maximumduur op sommige plekken in de politiewetten of het Wetboek van Strafvordering is vastgelegd (bijvoorbeeld in de Politiewet NRW, op grond waarvan de termijn bij volwassenen maximaal tien jaar mag zijn, bij jongeren maximaal vijf en bij kinderen maximaal twee). Ook staan bij bepaalde zeer ingrijpende inbreuken op de persoonlijke levenssfeer

korte verwijderingstermijnen in de wet (zoals twee weken voor beelden van bodycams); deze laten echter altijd een mogelijkheid om de gegevens onder bepaalde (in de wet omschreven) voorwaarden langer te bewaren, als dat noodzakelijk is. België kent vaste wettelijke archiveringstermijnen, waarbij onderscheid wordt gemaakt tussen de bestuurlijke en gerechtelijke politie.

4.4.5 Verstrekken/delen van politiegegevens

Bij het verstrekken en delen van politiegegevens maken we onderscheid tussen binnenlandse en buitenlandse instanties.

Verstrekking aan binnenlandse instanties

Bij verstrekking van gegevens aan binnenlandse instanties zien we dat dit vooral binnen het domein van de bevoegde autoriteiten die onder de Richtlijn vallen in alle landen laagdrempelig is. In alle landen zijn artikelen in de wetgeving opgenomen die deze gegevensverstrekking regelen, volledig in lijn met de Richtlijn. België is momenteel een project gestart (genaamd I-police) wat als doel heeft verschillende gegevensbanken op elkaar aan te sluiten en er zo voor te zorgen dat binnen de geïntegreerde politie eenvoudig toegang tot gegevens verkregen wordt. Ook Duitsland heeft een politioneel informatieverbond met bijbehorend informatiesysteem.

Voor het delen van gegevens buiten de politie bestaan in de meeste landen twee niveaus met verschillende regimes. Zo is in België voor een beperkt aantal openbare overheden, publieke organen of instellingen of instellingen van openbaar belang vastgesteld dat gegevens gedeeld mogen worden conform door de minister vastgestelde Richtlijnen. Voor instanties buiten die selectie geldt dat bij 'herhaalde of volumineuze mededeling van persoonsgegevens' protocolakkoorden moeten worden opgesteld (met voorschriften over onder meer beveiliging en bewaring van gegevens). In Ierland wordt ook veelvuldig gebruik gemaakt van wettelijke mogelijkheden om gegevens met organisaties buiten het domein van politie en justitie te delen, onder voorwaarde dat dit in het algemeen belang is (ter beoordeling van de verstrekkende partij) en nodig voor de taakuitvoering van de ontvanger. In die gevallen wordt gewerkt met *data sharing agreements* of *joint control agreements.* Kanttekening hierbij is dat er soms nog wel onduidelijkheid is over wie het oordeel kan vellen over de noodzaak en proportionaliteit van het delen van de gegevens. In Duitsland wordt er naast politiediensten onderscheid gemaakt in andere entiteiten met een publieke taak (*offentliche Stellen*) en private organisaties of personen (*nicht-offentliche Stellen*). Uitwisselen van gegevens mag voor zover dat voor het uitvoeren van de eigen taak of voor gevarenafweer door de ontvangende partij noodzakelijk is. Voor uitwisseling met AVG-organisaties gelden strengere waarborgen. Ook in Denemarken worden gegevens uitgewisseld zolang dit noodzakelijk is voor de uitvoering van wettelijke taken van ontvangende organisaties. In Finland spelen praktische problemen bij de gegevensuitwisseling met plaatselijke gemeenschappen en autoriteiten. Voor het delen van gegevens met lokale autoriteiten is er op dit moment namelijk geen formele wettelijke grondslag, terwijl de politie het wel van belang acht gegevens te kunnen uitwisselen.

Verstrekking aan buitenlandse instanties

Voor verstrekking aan buitenlandse instanties geldt dat in alle landen de bepalingen die hierover in de Richtlijn zijn opgenomen volledig zijn vertaald in nationale wetgeving. Dit mag gezien het feit dat verbeterde gegevensdeling door bevoegde autoriteiten binnen de EU een van de hoofddoelen van de Richtlijn was geen verrassing heten. In de praktijk zijn hier ook geen problemen geconstateerd. In Ierland is men momenteel wel druk doende de gevolgen van de Brexit in kaart te brengen, specifiek omdat er relatief veel gegevens worden uitgewisseld met Britse autoriteiten en met name die in/van Noord-Ierland. In Finland valt op dat in

de wet aparte artikelen zijn opgenomen over het delen van gegevens met Europol en het delen van gegevens binnen het Schengen-informatiesysteem. Dergelijke bepalingen zijn niet terug te vinden in de Richtlijn.

De uitwisseling van gegevens met (organisaties in) derde landen is ook in alle landen conform de Richtlijn geregeld. Hier blijken in de praktijk wel vragen te leven over de werking. Zo zijn in Duitsland vragen gesteld over het beschermingsniveau van internationale organisaties als Interpol. Ook Ierland volgt deze kwestie met belangstelling. Bij de uitwisseling met derde landen is in Duitsland naar aanleiding van jurisprudentie van het grondwettelijk hof een toets aan rechtsstatelijkheid en mensenrechten in de wet opgenomen. Duitsland heeft behoefte aan een uniforme Europese invulling van het Unierechtelijke begrip 'passende waarborgen', en ondersteuning/onderlinge informatieuitwisseling bij de beoordeling hiervan. In Denemarken is gegevensuitwisseling met derde landen in het bijzonder van belang omdat Groenland en de Faeröer hieronder vallen en er daarom niet zonder meer kan worden samengewerkt. Denemarken werkt daarom aan de implementatie van voldoende gegevensbeschermingsregels die gelden in de overzeese gebieden om een adequaatheidsbesluit van de Europese Commissie te krijgen.

4.5 Toezicht

In alle casestudy-landen is het intern toezicht op naleving van de Richtlijn belegd bij minimaal een functionaris voor gegevensbescherming, conform de Richtlijn. Deze interne toezichthouders hebben geen dwingende instrumenten om naleving van de regelgeving te handhaven. In België zijn verschillende interne toezichthouders die op verschillende onderdelen van de politie en niveaus (van procedureel tot individuele gevallen) toezicht moeten houden. In Duitsland is zowel op landelijk niveau als op Landesniveau een interne toezichthouder aangesteld.

Het externe toezicht is in de meeste landen belegd bij de instantie die ook toezicht houdt op de naleving van de AVG. Alleen in België is er een andere toezichthouder op aangewezen voor toezicht op de naleving van de Richtlijn. Dit controleorgaan bestond al voor implementatie van de Richtlijn en is in licht aangepaste vorm nu ingesteld specifiek voor het toezicht op de geïntegreerde politie. De gedachte hierachter is dat er meer specifieke expertise op het werkterrein van politie en justitie kan worden ingezet bij het toezicht, al wordt als keerzijde genoemd dat deze expertise veelal binnen de onder toezicht staande organisaties is opgedaan, wat nadelig kan zijn voor de neutraliteit van de toezichthouder. In Nordrhein-Westfalen is de mogelijkheid van een dergelijke gespecialiseerde toezichthouder (gestationeerd bij het parlement voor extra onafhankelijkheid) ook overwogen, maar dit werd uiteindelijk niet wenselijk gevonden.

In de meeste onderzochte landen gebruiken de externe toezichthouders overwegend 'zachte' instrumenten voor de handhaving van regelgeving. Hierbij zien we in Duitsland een opvallend verschil tussen de toezichthoudende autoriteit op Bondsniveau en die in Nordrhein-Westfalen; die eerste kan vooral waarschuwen en aanwijzingen geven, terwijl die laatste bijvoorbeeld ook verwerkingsbeperkingen kan opleggen. Een belangrijke functie is de afhandeling van klachten en ondersteuning bij de uitoefening van rechten van betrokkenen. De toezichthouders geven doorgaans gevraagd en ongevraagd advies over onder meer de uitvoering van werkzaamheden, bewaartermijnen, rechtmatig gebruik van technologie. Ze kunnen ook richtlijnen schrijven die door de onder toezicht staande organisaties gebruikt kunnen worden. België en Finland hebben aangegeven dat de toezichthouder in de praktijk zeer zelden de verwerking stopzet, hoewel dit wel wettelijk mogelijk is, vanwege de ingrijpende gevolgen voor

de uitvoering van wettelijke taken. In Nordrhein-Westfalen bestaat ook de mogelijkheid tot het opleggen van boetes, maar we hebben geen gegevens over de inzet in de praktijk van dit instrument. In Ierland doet de toezichthoudende autoriteit ook regelmatig proactief onderzoek.

4.6 Afsluitend

Dit hoofdstuk geeft een uitvoerig overzicht van de bevindingen In het volgende hoofdstuk, de slotbeschouwing, proberen we de balans op te maken van de knelpunten in Nederland en de bevindingen ten aanzien van die punten in de casestudylanden; wat kan Nederland daadwerkelijk meenemen uit deze landen, welke problemen zijn ook in deze landen nog niet opgelost en wat is te 'landspecifiek' om over te nemen?

5

Slotbeschouwing

5.1 Inleiding

Doel van dit verkennende onderzoek was inspiratie opdoen uit vijf andere EU-lidstaten voor de herziening van het Nederlandse wettelijke kader voor de verwerking van politiegegevens. Daarvoor hebben we in België, Denemarken, Duitsland, Finland en Ierland gekeken naar de wet- en regelgeving over politiegegevens (en – beperkt – de visie van en uitvoering in de praktijk), en hun invulling van het Europese kader voor de verwerking van politiegegevens (EU-Richtlijn 2016/680, de Richtlijn gegevensbescherming opsporing en vervolging). Zwaartepunt bij de interviews en documentenstudie in de andere landen waren de manieren waarop zij met in Nederland bestaande en eventuele andere knelpunten omgaan. Daarom hebben we eerst een – beperkte – inventarisatie gemaakt van de stand van zaken in Nederland wat betreft de wet- en regelgeving voor het verwerken van politiegegevens sinds de evaluatie van de Wet politiegegevens in 2012/2013; van de nog openstaande en nieuwe knelpunten.

In deze slotbeschouwing grijpen we eerst kort terug op het in hoofdstuk 3 geschetste beeld van de Nederlandse situatie (paragraaf 5.2). Vervolgens beschrijven we themagewijs de belangrijkste bevindingen uit de landenvergelijking, en dan vooral wat Nederland daaruit mee zou kunnen nemen: met betrekking tot de wetssystematiek, de invulling van het Europese kader en het toepassingsbereik van de wetgeving (paragraaf 5.3), de verschillende aspecten van verwerking van politiegegevens (paragraaf 5.4) en toezicht (paragraaf 5.5). In paragraaf 5.6 proberen we expliciet de verbinding te leggen tussen de in hoofdstuk 3 geformuleerde Nederlandse knelpunten en de opgehaalde informatie uit de casestudylanden; paragraaf 5.7 bevat een bondige conclusie.

5.2 Nederland: nog openstaande knelpunten en uitdagingen

Uit het deelonderzoek in Nederland komt het beeld naar voren van een sinds de inwerkintreding in 2008 nauwelijks veranderde Wet politiegegevens in een sterk veranderde, gedigitaliseerde wereld. Ook een ontwikkeling als de overgang van 25 regionale politiekorpsen naar één Nationale Politie heeft niet tot een herziening van de Wpg geleid. De wetgever heeft geprobeerd het nieuwe Europese kader voor gegevensbescherming (de Richtlijn gegevensbescherming opsporing en vervolging) te integreren in de bestaande systematiek van de Wet

politiegegevens, de Wet justitiële en strafvorderlijke gegevens en de daarmee samenhangende wetgeving, zonder de tekst en structuur van de Wpg wezenlijk te herzien. Hierdoor is het begrip 'politiegegeven' uitgangspunt van de wet gebleven, maar met een Richtlijn 2016/680-inkleuring.

De Richtlijn is van toepassing op, kortweg, *opsporing en vervolging van strafbare feiten (inclusief afweer van gevaren voor de openbare orde en veiligheid)* (doel/taak, element 1) door (daartoe) *bevoegde autoriteiten* (actor, element 2). De Wpg definieert *politiegegeven* net als vóór de Richtlijn als elk persoonsgegeven dat wordt verwerkt in het kader van de uitvoering van de politietaak[57]; wel is met de inwerkingtreding van het Europese kader een aantal taken onder de AVG komen te vallen,[58] wat voor veel verwarring en afbakeningsproblematiek zorgt. 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. Sinds de inwerkingtreding van de Richtlijn is de Wpg ook van toepassing op buitengewoon opsporingsambtenaren (boa's), voor zover zij politietaken uitvoeren. Bovendien was de Wpg al langer van toepassing op de vier buitengewone opsporingsdiensten. Dit wordt echter niet direct duidelijk bij het lezen van de Wpg; de naam *Wet politiegegevens* is in die zin misleidend en het achterliggende systeem wordt door geen enkel ander land gedeeld (zie ook hierna).

De herziening van de Wpg en de Wjsg is overigens bewust op de langetermijnagenda van het ministerie van JenV gezet, als onderdeel van een breder programma van modernisering en digitalisering van de strafrechtketen. Dit omdat de samenleving steeds hogere eisen stelt aan zowel sociale veiligheid als bescherming van de privacy. De modernisering van het Wetboek van Strafvordering en de ontwikkeling van digitaal procederen hadden eerst prioriteit. Dit betekent dat veel van de in de evaluatie van 2012/2013 geconstateerde knelpunten nog openstaan. Er zijn twee belangrijkste/overkoepelende knelpunten te onderscheiden:

- Ten aanzien van naleving en 'naleefbaarheid' van de Wpg is vastgesteld dat de Wpg moeilijk na te leven is omdat deze veel open normen bevat, op andere punten wellicht juist te gedetailleerd is en niet goed aansluit op de uitvoeringspraktijk, de organisatie en de ICT-voorzieningen;
- Met betrekking tot categorisering van gegevens en samenloop met andere wetgeving is vast komen te staan dat de categorisering naar politietaak/doeleinde van art. 8-13 Wpg, met bijbehorende verschillende verwerkingsregimes (waaronder bewaartermijnen), zorgt voor 'verschotting' en dat dit in de praktijk niet werkbaar is omdat gegevens in meerdere categorieën kunnen vallen. Bovendien is er nog samenloop met andere wettelijke regimes voor gegevensverwerking.

Digitalisering en technologisering zorgen voor nieuwe, grote uitdagingen voor de uitvoering van de politietaken en het beschermen van persoonsgegevens daarbij. Er zijn steeds meer gegevens beschikbaar uit steeds meer verschillende bronnen, zoals drones, bodycams en het internet. Bovendien bestaan er steeds meer technieken om die gegevens te analyseren. De (Europese) privacywetgeving eist een specifieke wettelijke basis voor elke inbreuk op de persoonlijke levenssfeer; 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.

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

5.3 Wettelijk systeem

Zoals gezegd lijkt het begrip 'politiegegevens' en de bijbehorende wetssystematiek, met de koppeling met de in de Nederlandse wet omschreven politietaken en een knip tussen Wet politiegegevens en Wet justitiële en strafvorderlijke gegevens, iets typisch Nederlands te zijn. De vijf onderzochte landen en ook de andere EU-lidstaten die we vluchtig hebben bekeken in het kader van de quickscan voor de landenselectie gaan uit van de bescherming van persoonsgegevens (in Europeesrechtelijke zin) door de politie en andere bevoegde autoriteiten. Dit is ook wel het geval bij de Wpg en Wjsg, maar de ongelijksoortige terminologie maakt het lastig om het toepassingsbereik te vergelijken en het heeft naar het lijkt ook de implementatie en het werken volgens de Richtlijn bemoeilijkt (wat betreft de positie van de boa's etc.); er zijn meerdere kaders die niet precies op elkaar passen.

Enkele landen hebben de AVG en de Richtlijn omgezet/uitgewerkt in één privacywet, met een apart hoofdstuk voor de implementatie van de Richtlijn; andere landen hebben een aparte omzettingswet voor de Richtlijn en soms daarnaast nog specifieke wetgeving over de verwerking van persoonsgegevens door de verschillende bevoegde autoriteiten. Duitsland heeft in elke politiewet (in elk geval op Bondsniveau en in Nordrhein-Westfalen) een hoofdstuk over gegevensverwerking opgenomen.

Ook gaan de onderzochte landen verschillend met het begrip 'bevoegde autoriteiten' om: België, Denemarken en Nordrhein-Westfalen hebben de bevoegde autoriteiten bijvoorbeeld expliciet opgesomd in de Gegevensbeschermingswet, terwijl andere landen letterlijk de definitie van de Richtlijn volgen en deze niet nader specificeren. In Ierland moet per geval worden bepaald of het handelen onder de Richtlijn valt. De politietaak komt in de (privacy-)wetgeving van de bestudeerde landen vooral in beeld bij (het beoordelen van) de doelbinding, noodzakelijkheid en proportionaliteit van de verwerking van persoonsgegevens. Het verzamelen, gebruiken of delen van gegevens is op grond van de Europese en nationale regelgeving alleen rechtmatig als daarvoor een wettelijke grondslag is en voor zover noodzakelijk met het oog op het doel. Zo'n doel en wettelijke grondslag kan zijn het uitvoeren van een in de wet omschreven politietaak.

5.4 Verwerken van politiegegevens

5.4.1 Verkrijgen van politiegegevens

Samenvattend kunnen we zeggen dat de grondslagen waarop in de vergelijkingslanden politiegegevens kunnen worden verkregen min of meer overeenkomen met het Nederlandse systeem. De algemene voorwaarden en waarborgen komen voort uit de Europese beginselen van gegevensbescherming uit de AVG en – meer specifiek voor dit terrein – de Richtlijn gegevensbescherming opsporing en vervolging. Een van die waarborgen is dat er voor een inbreuk op de persoonlijke levenssfeer een wettelijke basis moet zijn – hoe ingrijpender de inbreuk, hoe specifieker de vereiste rechtsgrondslag. Net als Nederland kennen de andere landen daarom veel verschillende wettelijke grondslagen voor politiehandelen in bijzondere wetten, naast de algemene basis in de privacywetgeving, politiewetgeving en het wetboek van strafvordering. In het ene land ligt de nadruk daarbij meer op de informatiepositie van de politie, in het andere land meer op de bescherming van persoonsgegevens. Alle bestudeerde landen staan wat betreft digitalisering en technologisering voor dezelfde uitdaging als Nederland: aan de ene kant is er de wens de wetgeving zo 'technologieneutraal' mogelijk te formuleren om ruimte open te houden voor de snelle ontwikkelingen, aan de andere kant is er vanuit

grondrechtenoogpunt de eis om zo specifiek mogelijk te zijn. Geen enkel bestudeerd land lijkt nog een pasklare oplossing te hebben gevonden voor dit dilemma.

5.4.2 Bewerken van gegevens

In de vijf vergelijkingslanden hebben we vervolgens bekeken welke mogelijkheden voor gebruik van gegevens de bevoegde autoriteiten hebben wanneer de gegevens eenmaal in hun bezit zijn. Daarbij lag de focus op de kaders voor verdere (technische) gebruiks- en analysemogelijkheden, waaronder gebruik voor andere doelen dan waarvoor de data zijn verkregen. Hierbij valt ten eerste op dat in de meeste landen de Richtlijn vrijwel één op één is overgenomen. Ook voor verwerking is daarmee sprake van technologieneutrale formuleringen; er is geen specifieke regelgeving voor bijvoorbeeld de inzet van *big data*, maar er zijn algemene richtsnoeren gebaseerd op noodzakelijkheid, proportionaliteit en doelbinding en passende technische en organisatorische beveiligingsmaatregelen.

In de praktijk zien we dat dit tot gevolg heeft dat er erg voorzichtig wordt omgegaan met de inzet van nieuwe technologische mogelijkheden bij de verwerking van persoonsgegevens. In Finland is zelfs expliciet door de politie uitgesproken dat die de mogelijkheden te beperkt vindt en graag een specifieke uitbreiding van wettelijke mogelijkheden zouden zien.

In Duitsland is de verwerking voor een ander doel dan waarvoor ze zijn verkregen aan scherpe voorwaarden gebonden wat inhoudt dat dan een minstens zo ernstig strafbaar feit of een minstens zo zwaarwegend belang of rechtsgoed aan de orde moet zijn als bij de verkrijging. Andere landen stellen daarin minder hoge eisen, bijvoorbeeld alleen dat het nieuwe doeleinde moet passen binnen het takenveld van politie en justitie.

Wanneer we de toegang van betrokkenen tot de over hen verzamelde en verwerkte gegevens beschouwen, zien we dat alle landen behalve België hierin de Richtlijn volledig volgen en directe toegang tot gegevens (na een verzoek) hebben geregeld. België interpreteert de Richtlijn zodanig dat het al langer gebruikte systeem van ‘onrechtstreekse toegang’ in stand is gehouden. 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. Dit systeem zou de bevoegde autoriteiten administratief ontlasten, maar heeft tot de nodige maatschappelijke kritiek geleid en het is bovendien zeer de vraag of deze interpretatie van de Richtlijn binnen de EU houdbaar is.

5.4.3 Categoriseren en labelen

Alle landen hebben de in de Richtlijn verplichte categorisering van persoonsgegevens overgenomen in hun wetgeving. In veel gevallen zijn daar nog aanvullende categorieën aan toegevoegd, zoals rechtsgrondslag van de verzameling, opsporingsmethode, openbaarheid en ernst van het strafbare feit. In de praktijk zien we dat in de vergelijkingslanden dezelfde problemen als in Nederland leven: het onderscheid tussen feit en mening is soms lastig te maken, en de rol van de betrokkene kan per dossier verschillen. Daarnaast kan de categorisering van grote datasets problematisch zijn omdat de eisen aan categorisering meer op individuele gevallen toegesneden zijn.

5.4.4 Bewaren en vernietigen

De bestudeerde landen verschillen in de manieren waarop de bewaring en vernietiging van gegevens en termijnen daarvoor zijn vastgelegd in wet- en regelgeving. In Finland is bijvoorbeeld bij wet vastgelegd wanneer gegevens vernietigd moeten worden en hoe vaak gecontroleerd moet worden of vernietiging nodig is. In België is ook in wetgeving vastgelegd wat

bewaartermijnen zijn, waarbij ook onderscheid wordt gemaakt voor gegevens die door gerechtelijke politie gebruikt worden. In Duitsland, Denemarken en Ierland is dit voornamelijk vastgelegd in protocollen van bevoegde autoriteiten, waarbij Duitsland bepaalde maximumtermijnen (voor controle of gegevens langer moeten/mogen worden bewaard) vervolgens wel weer opneemt in wetgeving.

5.4.5 Verstrekken en delen van politiegegevens

Bij het verstrekken en delen van politiegegevens aan/met binnenlandse autoriteiten wordt in alle landen onderscheid gemaakt tussen drie groepen: andere autoriteiten binnen het regime van de Richtlijn, instanties met een publieke en wettelijke taak waarvoor gegevensdeling passend is, en instanties die daarbuiten vallen. Bij de eerste groep is gegevensdeling laagdrempelig, zoals bedoeld in de Richtlijn, bij de tweede en derde groep verschillen uitgangspunten en eisen. Wel zien we dat er altijd een bepaalde vorm van regulering wordt opgezet op basis van overeenkomsten waarin afspraken worden gemaakt over bijvoorbeeld verwerking, beveiliging en verwijdering.

Bij verstrekking aan buitenlandse instanties wordt de Richtlijn bij verstrekking binnen de EU overal nauw gevolgd. Bij (organisaties in) derde landen is dit ook geval, maar zijn in de praktijk wel discussies op gang gekomen over het beschermingsniveau van internationale organisaties als Interpol. Duitsland heeft ook een extra toets aan rechtsstatelijkheid en mensenrechten in de wet opgenomen voordat tot delen van gegevens wordt overgegaan. Denemarken kent met de Faeroër en Groenland twee gebieden die binnen het koninkrijk vallen maar wel als derde land gelden. Het land werkt daarom aan de implementatie van voldoende gegevensbeschermingsregels in die gebieden om een adequaatheidsbesluit van de Europese Commissie te krijgen.

5.5 Toezicht

In de meeste casestudy-landen is het externe toezicht belegd bij een algemene autoriteit die toeziet op zowel de AVG als op de Richtlijn. Alleen België heeft hier een afwijkend regime: er is een externe toezichthouder specifiek voor de uitvoering van de Richtlijn aangewezen. Deze toezichthouder bestond voor de implementatie van de Richtlijn al in iets andere vorm en is opgericht met overweging dat deze meer expertise zou kunnen inzetten ten aanzien van het werk van bevoegde autoriteiten. Als nadeel wordt erkend dat de expertise vaak in het veld zelf wordt opgedaan, en dat daardoor de neutraliteit van functionarissen onder druk kan staan.

In alle landen geldt dat externe toezichthouders in de praktijk veelal zachte instrumenten inzetten om naleving van de regels te handhaven. In de meeste landen zijn er wel wettelijke mogelijkheden om bijvoorbeeld verwerkingsprocessen te laten stopzetten, maar dit middel blijkt in de praktijk vaak onwenselijk ingrijpend.

In Duitsland en Ierland is in enkele interviews aangegeven dat er behoefte is aan meer overleg en kennisdeling in Europees verband over de uitleg van Europeesrechtelijke begrippen (zoals ‘passende waarborgen’) en de omgang door verschillende lidstaten daarmee in concrete toezichtcasussen.

5.6 Buitenlandse lessen bij Nederlandse knelpunten

In paragraaf 3.6 zijn de belangrijkste openstaande knelpunten bij de Wpg op een rij gezet. Een van de doelen van dit onderzoek is om te kijken in hoeverre de situatie in de casestudy-landen lessen op kan leveren die van pas kunnen komen bij de oplossen van de Nederlandse knelpunten. In deze paragraaf gaan we na in hoeverre deze aansluiting is te vinden.

Structuur wet past niet meer op structuur politieorganisatie

Uit de evaluatie van de Wpg in 2012/2013 bleek een worstelende nalevingspraktijk, omdat de Wpg op sommige punten open en/of vaag geformuleerde normen bevatte en op andere punten juist te gedetailleerd en moeilijk naleefbaar was. Ook sloot de Wpg niet meer goed aan op de huidige organisatie(structuur) van de politie. In enkele vergelijkingslanden zagen we dat de vormgeving van de wetten mogelijk inspiratie kan opleveren bij het herzien van de Wpg. Zo is men in Denemarken zeer tevreden over de manier waarop de Richtlijn met open normen is vertaald en amper is aangevuld in nationale wetgeving. In Duitsland zijn de ervaringen positief met een aparte sectie voor gegevensbescherming bij elke wet die over een politietaak of bevoegde autoriteit gaat. In Finland is men zeer tevreden over de heldere hoofdstukindeling en –benaming in de wetgeving. Hoewel deze voorbeelden dus deels elkaar tegen lijken te spreken, lijkt er dus wel sprake van mogelijkheden om ideeën op te doen en verder onderzoek te doen naar ervaringen met de structuur en vorm van wetgeving in deze landen.

Categorisering en bewaartermijnen

De categorisering van politiegegevens sluit niet meer aan bij de werkelijkheid, wat onder meer tot onduidelijkheid over de van toepassing zijnde bewaartermijnen heeft geleid. De vergelijkingslanden bieden hiervoor verschillende aanknopingspunten. In Duitsland gaat de wet uit van het beoordelingsvermogen van de professional en zet men meer in op vaste evaluatiemomenten waarop beslist wordt of bewaring van gegevens nog passend is. In Finland is juist heel duidelijk voor elke categorie gegevens vastgelegd wat de wettelijke bewaartermijn is. Ook hier zien we dus geen eenduidig beeld maar wel genoeg punten van mogelijke inspiratie.

Overlap met andere regimes voor gegevensverwerking geeft onduidelijkheid

Het probleem met overlap tussen regimes waar gegevens voor gebruikt worden kan mogelijk worden opgelost met de Duitse aanpak, waarbij op veel plekken in de wetgeving steeds weer apart ingegaan wordt op aspecten van gegevensbescherming die relevant zijn. Ook in Ierland heeft men de nationale wet eenduidig en eenvoudig ingericht en zegt men weinig onduidelijkheid te ervaren over het van toepassing zijnde nationale regime. Wel is er ook daar vaak twijfel over de afbakening tussen Richtlijn en AVG.

Grondslag voor verkrijgen gegevens te beperkend voor politiewerk

Het ontbreekt in de Nederlandse wetgeving soms aan een grondslag in de wet voor het verkrijgen van gegevens, met name met nieuwe technologie. Dit probleem wordt bijvoorbeeld in Finland ook herkend. Er is daar nog geen oplossing gevonden, maar het kan aanbevelenswaardig zijn om de ontwikkelingen daar in het oog te houden om daar ook inspiratie op te doen.

Semi-gesloten verstrekkingsregime Wpg wringt met behoefte aan samenwerking

De Wpg is bedoeld als een semi-gesloten regime, waarbij het delen van politiegegevens buiten het Wpg-domein slechts bij uitzondering mogelijk is. Dit past niet bij de huidige schaal van samenwerking met andere partijen binnen Nederland, bijvoorbeeld op het gebied van

het tegengaan van ondermijning. Daarbij kunnen politiegegevens ook bestaan uit gevoelige en soms zachte informatie. Er moet dus goed worden nagedacht wat met wie en op welke gronden wordt gedeeld. In bijvoorbeeld Duitsland wordt hier in de verschillende politiewetten uitgebreider en systematischer aandacht aan besteed, bijvoorbeeld in de bepalingen over het politionele informatieverbond en het bijbehorende informatiesysteem.

Controle op waarborgen bij verstrekking aan derde landen omslachtig

Geconstateerd is dat verstrekking aan derde landen buiten het Europese grondgebied problematisch is. In Denemarken is voor de overzeese gebieden besloten in te zetten op een adequaatheidsbesluit door de Europese Commissie, waardoor de barrières voor het delen van gegevens verminderd of weggehaald kunnen worden. Het strekt tot aanbeveling dit proces te volgen omdat dit mogelijk aanknopingspunten biedt voor de Nederlandse situatie.

Extern toezicht heeft nog open eindjes

Een gesprekspartner noemt als knelpunt dat de AP onvoldoende menskracht en middelen heeft voor het toezicht en er mogelijk bevoegdheden bij zou moeten krijgen om effectief toezicht te kunnen houden. In België en in Finland is op dat laatste punt ervaring opgedaan met de bevoegdheid door de toezichthouder om gegevensverwerking stop te zetten als ultiem instrument. Ten aanzien van de capaciteit kan ook worden gekeken naar België, waar een aparte toezichthouder voor gegevensverwerking onder de Richtlijn bestaat.

Discrepantie tussen wet en digitale en technologische werkelijkheid

Het wettelijk stelsel dat het politiewerk en de verwerking van politiegegevens reguleert is niet berekend op de technologische mogelijkheden en uitdagingen van de huidige tijd. Dit is een feit waar meer landen mee te kampen hebben. Zowel in Finland als in Denemarken heeft men momenteel aandacht (gevraagd) voor deze problematiek, in Denemarken is een wetgevingsproces gestart dat zich specifiek richt op open source intelligence. Mogelijk kan verdere en meer diepgaande kennis worden opgedaan in deze landen.

5.7 Tot slot

Dit onderzoek heeft, ondanks de interviews die in veel landen met personen binnen de politie hebben plaatsgevonden, toch vooral een verkennend en uitwendig karakter gehouden. Daarmee is niet gezegd dat er geen lessen uit te trekken zijn. Integendeel, zeker voor de wetgever hebben we aanknopingspunten gevonden om ontwikkelingen en insteken uit andere landen nader te onderzoeken. Deze aanknopingspunten kunnen aanleiding vormen voor verder verdiepend onderzoek, waarbij wij aan zouden raden om meer partijen te spreken, meer de diepte te zoeken over de praktische uitwerking van de gemaakte keuzes in wet- en regelgeving en vanuit verschillende perspectieven deze praktijk te beschouwen.

Een belangrijke kanttekening hierbij is dat we in dit onderzoek vooral in zijn gegaan op het wetgevingsaspect, terwijl de knelpunten in Nederland worden veroorzaakt door zowel de wet zelf als de uitvoeringspraktijk als ICT en organisatorische maatregelen. Bij eventueel verder onderzoek in de casestudylanden zou dus ook goed moeten worden meegenomen hoe de wet ‘op de werkvloer’ uitpakt.

Bijlage 1: geraadpleegde bronnen

Literatuur

Custers & Vergouw 2019
B. Custers & B. Vergouw, 'Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies', Computer Law & Security Review 31 (2015), p. 518-526.

Controleorgaan op de politionele informatie 2020
Controleorgaan op de politionele informatie, *Activiteiten Verslag 2016-2019*, 2020.

Federale Politie 2018
Federale Politie, *Informatiebeheer, de kern van onze zaak. Jaarverslag Federale Politie 2017*, 2018.

Gritter 2018
E. Gritter, 'De rechtmatigheid van datamining door de politie', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2018, 2, p. 113-115.

Data Protection Commission
Data Protection Commission, *Law Enforcement Directive - Guidance on Competent Authorities and Scope*, www.dataprotection.ie/en/organisations/law-enforcement-directive (laatst geraadpleegd op 7 augustus 2020).

Reinsel e.a. 2018
D. Reinsel, J. Gantz & J. Rydning, *The Digitization of the World – From Edge to Core. An IDC White Paper,* Framingham: IDC 2018.

Leiser & Custers 2019
M. Leiser & B. Custers, 'The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680', *European Data Protection Law Review* 2019, 3, p. 367-378.

Ministerie van Veiligheid en Justitie 2016
Ministerie van Veiligheid en Justitie, *Visie op de politiële taakuitvoering: de invloed van globalisering, netwerksamenleving, digitalisering, technologisering en het gebruik van intelligence in het veiligheidsdomein*, Den Haag: Ministerie van Veiligheid en Justitie 2016.

Schermer 2017
B.W. Schermer, 'Het gebruik van Big Data voor opsporingsdoeleinden: tussen Strafvordering en Wet politiegegevens', *Tijdschrift voor Bijzonder Strafrecht & Handhaving* 2017, 4, p. 207-216.

Schermer & Oerlemans 2020
B.W. Schermer & J.J. Oerlemans, 'AI, strafrecht en het recht op een eerlijk proces', *Computerrecht* 2020, 1, p. 14-21.

Smits e.a. 2013
J. Smits e.a., *Glazen privacy. Knelpuntenonderzoek uitvoering Wet politiegegevens (Wpg)*, Den Haag: WODC 2013.

De Schutter & De Hert 1995
B. De Schutter & P. De Hert, 'Is België klaar met zijn politie-privacywetgeving' *Vigiles, Tijdschrift voor Politierecht*, Jaargang 1, nr. 3, september 1995.

Van Brakel 2020
R. Van Brakel, 'Een reflectie over het huidig toezicht van het gebruik van surveilancetechnologie door de lokale politie in België', *Cahiers Politiestudies*, 55: 139-160.

WRR 2016
Wetenschappelijke Raad voor het Regeringsbeleid, *Big Data in een vrije en veilige samenleving,* Amsterdam: Amsterdam University Press 2016.

Jurisprudentie

Duitsland
BVerfG 15 december 1983, ECLI:DE:BVerfG:1983:rs19831215.1bvr020983 (*Volkszählungsurteil*).
BVerfG 2 maart 2010, ECLI:DE:BVerfG:2010:rs20100302.1bvr025608.

Wetten, besluiten en beleidskaders

Agreement on operational and strategic cooperation between the Kingdom of Denmark and the European Police Office.

Lov om forbud mod tv-overvågning mv., jf. lov nr. 278 af 9. juni 1982 med de ændringer http://www.retsinfo.dk/_GETDOC_/ACCN/A20000007629-REGL.

***Stb.* 2007, 300**
Wet van 21 juli 2007, houdende regels inzake de verwerking van politiegegevens (Wet politiegegevens), *Stb.* 2007, 300.

***Stb.* 2007, 549**
Besluit van 14 december 2007 tot vaststelling van het tijdstip van inwerkingtreding van de Wet politiegegevens, *Stb.* 2007, 549.

***Stb.* 2011, 490**
Wet van 6 oktober 2011 tot wijziging van de Wet politiegegevens en van de Wet justitiële en strafvorderlijke gegevens in verband met de implementatie van het kaderbesluit van de Raad van de Europese Unie 2008/977/JBZ over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken en de implementatie van het Besluit van de Raad 2009/371/JBZ van 6 april 2009 tot oprichting van de Europese politiedienst (Europol), *Stb*. 2011, 490.

***Stb.* 2018, 401**
Wet van 17 oktober 2018 tot wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking

van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen, *Stb.* 2018/401.

***Stb.* 2018, 495**
Besluit van 6 december 2018 tot vaststelling van het tijdstip van inwerkingtreding van de Wet tot wijziging van de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen van 17 oktober 2018, *Stb.* 2018, 401.

***Stb.* 2019, 85**
Besluit van 6 februari 2019, houdende bepalingen inzake de overeenkomstige toepassing van de Wet politiegegevens op de verwerking van persoonsgegevens door personen die als buitengewoon opsporingsambtenaar zijn belast met de opsporing van strafbare feiten (Besluit politiegegevens buitengewoon opsporingsambtenaren), *Stb.* 2019, 85.

Kamerstukken

Kamerstukken II 2005/06, 30327, 3 (MvT).
Kamerstukken II 2013/14, 33842, 2.
Kamerstukken II 2016/17, 26643, 426.
Kamerstukken II 2017/18, 34889, 3 (MvT implementatie Richtlijn 2016/680).
Kamerstukken II 2016/17, 26643, 426.
Kamerstukken II 2018/19, 29682, 859 (Brief van de minister van Justitie en Veiligheid van 4 februari 2019).
Kamerstukken II 2019/20, 33842, 5 (Brief van de minister van Justitie en Veiligheid van 21 april 2020).

Bijlage 2: lijst van de op de Wpg gebaseerde/betrekking hebbende regelgeving[59]

1. Aanpassingsbesluit openbare lichamen Bonaire, Sint Eustatius en Saba;
2. Aanpassingsbesluit Politiewet 2012;
3. Aanpassingsbesluit Wnra;
4. Beleidsregels prioritering klachtenonderzoek AP;
5. Besluit beheer politie;
6. Besluit ex artikel 24 Wet politiegegevens;
7. Besluit gegevensverstrekking ongebruikelijke transacties BES;
8. Besluit implementatie richtlijn gegevensbescherming opsporing en vervolging;
9. Besluit Jeugdwet;
10. Besluit modern migratiebeleid;
11. Besluit natuurbescherming;
12. Besluit onderzoek in een geautomatiseerd werk;
13. Besluit politiegegevens;
14. Besluit politiegegevens bijzondere opsporingsdiensten;
15. Besluit politiegegevens buitengewoon opsporingsambtenaren;
16. Besluit ter voorkoming van witwassen en financieren van terrorisme BES;
17. Besluit toezicht trustkantoren 2018;
18. Besluit vaststelling nadere regels vastleggen en bewaren kentekengegevens ex artikel 126jj Wetboek van Strafvordering door politie;
19. Besluit verplichte politiegegevens;
20. Besluit verwerking persoonsgegevens bij selectieve woningtoewijzing ter beperking van overlastgevend en crimineel gedrag;
21. Boetebeleidsregels Autoriteit Persoonsgegevens 2019;
22. Herstelbesluit financiële markten 2018;
23. Invoeringsbesluit herziening tenuitvoerlegging strafrechtelijke beslissingen;
24. Mandaatbesluit Wet Politiegegevens FIOD-ECD;
25. Regeling team criminele inlichtingen FIOD;
26. Regeling team criminele inlichtingen Inspectie SZW-DO;
27. Verlenging Wpg-machtigingsbesluit RIEC's/werkproces integrale casusanalyse;
28. Verzamelbesluit evaluatie en uitbreiding Wet Bibob;
29. Wpg-machtigingsbesluit ACM;
30. Wpg-machtigingsbesluit persoonsgerichte aanpak voorkoming radicalisering en extremisme;
31. Wpg-machtigingsbesluit schadebeperkende maatregelen zorgfraude;
32. Wpg-machtigingsbesluit Wet aanpak woonoverlast.

Aanwijzingen van het OM

1. Aanwijzing Wet politiegegevens en de rol van de officier van justitie;

[59] Laatst bijgewerkt op 25 mei 2020.

2. Aanwijzing afstemmingsprotocol onderzoeksraad voor de veiligheid - openbaar ministerie.

Bijlage 3: wetsartikelen Duitsland en Finland

Duitsland

Overzicht relevante bepalingen Wet op het Bundeskriminalamt (BKA-Gesetz)

Voor de leesbaarheid maken we hier gebruik van een niet-officiële Engelse vertaling van het Bundeskriminalamt zelf.

CHAPTER 1 Central facilities for cooperation in criminal police matters, tasks of the Bundeskriminalamt
Section 1 Central facilities for cooperation in criminal police matters
Section 2 Central agency
Section 3 International cooperation
Section 4 Criminal prosecution
Section 5 Countering risks from international terrorism
Section 6 Protection of members of the constitutional bodies and of the management of the Bundeskriminalamt
Section 7 Witness protection
Section 8 Protection of the Bundeskriminalamt, self-protection of the agency
CHAPTER 2 General powers to process data
SUBCHAPTER 1 Data collection
Section 9 General data collection by and data transmission to the Bundeskriminalamt
Section 10 Provision of subscriber information
Section 11 Recording of incoming phone calls
SUBCHAPTER 2 Further processing of data
Section 12 Purpose limitation, principle of hypothetical new collection of data
Section 13 Information system of the Bundeskriminalamt
Section 14 Marking
Section 15 Access authorisation
Section 16 Further processing of data in the information system
Section 17 Project-related joint data files
Section 18 Data on convicted persons, persons charged, suspects and potential offenders
Section 19 Data on other persons
Section 20 Power to issue statutory instruments
Section 21 Further processing for scientific research purposes
Section 22 Further processing of data for basic and advanced training, for statistical and case management purposes
Section 23 Electronic file keeping
Section 24 Storing DNA profiles to identify misleading DNA traces
SUBCHAPTER 3 Data transmission
Section 25 Data transmission at national level
Section 26 Data transmission to member states of the European Union
Section 27 Data transmission at international level
Section 28 Transmission bans and grounds for refusal
CHAPTER 3 Central agency
Section 29 Police information network, power to issue statutory instruments

Section 30 Relevance to the network
Section 31 Responsibility for compliance with data protection legislation in the police information network
Section 32 Provision of information to the central agency
Section 33 Wanted notices within the scope of international cooperation
CHAPTER 4 Powers in criminal prosecution
Section 34 Use of technical means for self-protection
Section 35 Support to the Länder police authorities in criminal prosecution
Section 36 Coordination of criminal prosecution
Section 37 Official acts, support obligations of the Länder
CHAPTER 5 Powers to counter risks from international terrorism
Section 38 General powers
Section 39 Collection of personal data
Section 40 Provision of subscriber information
Section 41 Interview and obligation to provide information
Section 42 Establishing identity and inspecting permits
Section 43 Forensic identification measures
Section 44 Summons
Section 45 Special means of data collection
Section 46 Special provisions on the use of technical means in or from homes
Section 47 Alert for the purpose of discreet or specific checks
Section 48 Computerised profile-based searches
Section 49 Covert intrusion into information technology systems
Section 50 Confiscation of postal items
Section 51 Monitoring of telecommunications
Section 52 Collection of telecommunications traffic data and usage data
Section 53 Identifying and locating mobile telecommunications cards and terminal devices
Section 54 Direction to leave
Section 55 Direction to stay and contact ban
Section 56 Electronic monitoring of whereabouts
Section 57 Custody
Section 58 Search of persons
Section 59 Search of property items
Section 60 Seizure
Section 61 Entering and searching homes
Section 62 Protection of persons having the right to refuse to give evidence
(…)
CHAPTER 9 Data protection and data security, rights of the data subject
SUBCHAPTER 1 Data protection supervision
Section 69 Tasks and powers of the Federal Commissioner for Data Protection and Freedom of Information
SUBCHAPTER 2 Data protection officer
Section 70 Designation of the Data Protection Officer of the Bundeskriminalamt
Section 71 Tasks of the Data Protection Officer of the Bundeskriminalamt
Section 72 Status of the Data Protection Officer of the Bundeskriminalamt and cooperation with the Federal Commissioner for Data Protection and Freedom of
SUBCHAPTER 3 Responsibility under data protection legislation for the activity of the liaison officers of the Bundeskriminalamt seconded to German missions abroad
Section 73 Responsibility of the liaison officers of the Bundeskriminalamt under data protection legislation
SUBCHAPTER 4 Duties of the Bundeskriminalamt

Section 74 Notification in the case of covert and intensively intrusive measures
Section 75 Notification of the storage of personal data of children
Section 76 Subsequent notification of discreet checks alerts in the Schengen Information System
Section 77 Time limit for reviewing whether the data have to be deleted; information about deletion obligations
Section 78 Rectification of personal data, restriction of their processing in files, destruction of files
Section 79 Deletion of personal data obtained by measures to counter risks from international terrorism or by similar measures
Section 80 Records of processing activities
Section 81 Logging
Section 82 Logging in the case of covert and intensively intrusive measures
Section 83 Notification of personal data breaches to the Federal Commissioner for Data Protection and Freedom of Information
SUBCHAPTER 5 Rights of the data subject
Section 84 Rights of the data subject
Section 85 Exercise of the rights of the data subjects in the police information network and in the case of project-related joint data files
SUBCHAPTER 6 Compensation
Section 86 Compensation within the police information network
CHAPTER 10 Final provisions
Section 87 Penal provisions
Section 88 Reporting obligation to the German Bundestag
Section 89 Restrictions of basic rights
Section 90 Jurisdiction, procedure
Section 91 Transitional provision

Overzicht relevante bepalingen Politiewet Nordrhein-Westfalen (Polizeigesetz NRW)[60]

Hoofdstuk 1 – Taken en algemene voorschriften
§ 1 Politietaken
(…)
Hoofdstuk 2 - Politiebevoegdheden
(…)
Afdeling 2 – Gegevensverwerking
Titel 1 - Gegevensverkrijging

I. Ondervraging, Inlichtingenplicht, Algemene regels voor gegevensverzameling, Vorladung[61]

- § 9 Algemene regels, Ondervraging, Inlichtingenplicht
- § 10 *Vorladung*

II. Gegevensverzameling in bepaalde gevallen

- § 11 Verzameling van personalia ter voorbereiding voor hulpverlening en het handelen in geval van gevaar
- § 12 Identiteitsvaststelling
- § 12a Politionele staandehoudings- en 'zichtcontrole' (strategische zoekactie)
- § 13 Controle van papieren

[60] Vertaling Pro Facto.
[61] *Vorladung* betekent iets als 'voorgeleiding' of 'ophouden voor onderzoek'.

- § 14 Identificatiemaatregelen
- § 14a Moleculairgenetische onderzoeken ter vaststelling van de identiteit
- § 15 Gegevensverzameling bij openbare evenementen en bijeenkomsten/samenscholingen
- § 15a Gegevensverzameling door de openlijke inzet van optisch-technische middelen
- § 15b Gegevensverzameling ter zelfbescherming

III. Bijzondere middelen voor gegevensverzameling

- § 15c Gegevensverzameling door de inzet van op het lichaam gedragen opnameapparatuur
- § 16 Bescherming van het kernbereik van de persoonlijke levenssfeer bij gegevensverzameling met bijzondere middelen
- § 16a Gegevensverzameling door observatie
- § 17 Gegevensverzameling door de verdekte inzet van technische middelen
- § 18 Gegevensverzameling door de verdekte inzet van technische middelen in of buiten woningen
- § 19 Gegevensverzameling door de inzet van personen, van wie de samenwerking met de politie aan derden niet bekend is
- § 20 Gegevensverzameling door de inzet van undercoveragenten
- § 20a Opvragen van telecommunicatie- en telemediadata
- § 20b Inzet van technische middelen bij mobiele *devices*[62]
- § 20c Gegevensverzameling door monitoring van lopende telecommunicatie
- § 21 Politionele *Beobachtung*

Titel 2 – Verder verwerken van gegevens

- § 22 Opslag van gegevens, *Prüfungstermine*[63]
- § 22a Verwerking van bijzondere categorieën persoonsgegevens
- § 22b Labeling/categorisering (*Kennzeichnung*) in politionele bestandensystemen[64]
- § 23 Verdere verwerking van persoonsgegevens, Doelbinding, Wijziging van het doel[65]
- § 24 Verdere verwerking voor bijzondere doelen
- § 24a Verdere verwerking voor wetenschappelijke doelen
- § 25 Vergelijking van gegevens

Titel 3 – Verstrekken/delen van gegevens

I. Algemene regels voor gegevensverstrekking

- § 26 Algemene regels voor gegevensverstrekking, verstrekkingsverboden en weigeringsgronden

II. Gegevensverstrekking door de politie

- § 27 Gegevensverstrekking binnen Duitsland
- § 28 Gegevensverstrekking in de Europese Unie en haar lidstaten
- § 29 Internationale gegevensverstrekking[66]

III. Gegevensverstrekking aan de politie

- § 30 Gegevensverstrekking aan de politie

IV. Sleepnet-zoekactie

- § 31 Sleepnet-zoekactie

Titel 4 – Rectificatie, verwijdering en beperking van de verdere verwerking van gegevens

[62] *Mobilfunkendgeräte*; het gaat om smartphones, routers, tablets etc. (apparaten met mobiele verbinding, een IP-adres e.d.).

[63] *Prüfungstermine* zijn controlemomenten waarop moet worden gekeken of de gegevens nog noodzakelijk zijn; hierover meer in par. III.4.5 over bewaartermijnen.

[64] Hierover meer in par. III.4.4 over categorisering.

[65] Bedoeld wordt het gebruik van gegevens voor een ander doel dan waarvoor ze zijn verkregen.

[6666] Bedoeld worden hier derde landen en internationale organisaties.

- § 32 Rectificatie, verwijdering en beperking van de verdere verwerking van gegevens

Titel 5 – *Sicherung des Datenschutzes*

- § 33 Kennisgeving bij verdekte en intensief ingrijpende maatregelen
- § 33a Kennisgeving in gevallen van een inbreuk in verband met persoonsgegevens
- § 33b Procollering bij verdekte en intensief ingrijpende maatregelen
- § 33c Controle op gegevensbescherming

Finland

Act on the Processing of Personal Data by the Police

Section 4 Processing of basic personal data

The police may process the following basic personal data for the purposes laid down in sections 5, 7, 9 and 11:

1) names;
2) date and place of birth;
3) personal identity code;
4) gender;
5) native language;
6) communication language;
7) civil status;
8) citizenship or lack of citizenship and nationality;
9) domicile and place of residence;
10) occupation and education;
11) contact details;
12) information in the documentation necessary to establish identity;
13) in the case of foreign nationals, the names, citizenship and nationality of the parents;
14) travel document information and other information concerning entry into the country and border-crossing;
15) customer number issued by the authorities;
16) information on the person's death or declaration of death;
17) information on guardianship, declaration of bankruptcy or imposition of a business prohibition;
18) information on completing military service.

Section 15 Processing of data belonging to special categories of personal data

The police may process data belonging to special categories of personal data only if the processing is strictly necessary for the purpose of the processing.

Biometric data processed for the performance of the duties laid down in the Identity Card Act and the Passport Act may be used only for purposes other than the initial purpose if this is strictly necessary for identifying victims of a natural disaster, major accident or other disaster or an offence, or victims remaining unidentified for some other reason. The right of access only pertains to persons who absolutely need this data for the performance of their duties. Data taken for comparison purposes may only be used for the duration of the comparison and shall be destroyed immediately thereafter.

With the consent of the person in question, the fingerprints of a passport applicant may also be used for the preparation of identification documents later applied for by the person concerned.

Biometric data processed for the performance of the duties laid down in section 131 of the Aliens Act (301/2004) may be used only for purposes other than the initial purpose in the circumstances referred to in subsection 2 and whenever the use of such data is strictly necessary for the purposes of prevention, detection or investigation of an offence referred to in chapter 11–14; chapter 17, sections 2–4, 7, 7c or 8a; chapter 34, section 3 or 5; chapter 34a; or chapter 46, section 1 or 2 of the Criminal Code. The right of access only pertains to persons who absolutely need this data for the performance of their duties. Data taken for comparison purposes may only be used for the duration of the comparison and shall be destroyed immediately thereafter.

Data processed for the purpose of quality assurance of DNA samples may only be used for the initial purpose. Such data may also be used for oversight of legality, analysis, planning and development activities and in training activities if the data are essential for carrying out the training.

Information contained in a firearms notice referred to in section 114 of the Firearms Act (1/1998) may only be used for the purpose of processing data concerning firearm licences.

Bijlage 4: samenstelling begeleidingscommissie

Voorzitter

De heer prof. dr. mr. G.K. Sluiter	Universiteit van Amsterdam

Leden

Mevrouw dr. C.H.M. Geuijen	Universiteit Utrecht
De heer dr. B. Van der Sloot	Universiteit van Tilburg
Mevrouw mr. C.A.N. Huisman	Ministerie van Justitie en Veiligheid - DG Politie en Veiligheidsregio's
Mevrouw dr. L.M. Van der Knaap	WODC

Bijlage 5: deelnemerslijst expertmeeting 2 september 2020

- Marjolein Viersma – Juridisch Beleidsmedewerker bij het Ministerie van Justitie en Veiligheid;
- Vincent Cozijn - Strategisch adviseur wet- en regelgeving bij de Gegevensautoriteit van de Nationale Politie;
- Kees Weijers - Functionaris Gegevensbescherming Wet Politiegegevens bij de Koninklijke Marechaussee;
- Saskia Laaper - Coördinerend Beleidsadviseur gegevensuitwisseling & privacyvraagstukken bij het Parket-Generaal van het Openbaar Ministerie;
- Erwin van Vuuren - Functionaris Gegevensbescherming Wpg bij de Inspectie SZW;
- Vertegenwoordiger van de Autoriteit Persoonsgegevens
- Vincent Böhre – Directeur en jurist bij Privacy First.

Bijlage 6: lijst met gesprekspartners oriënterende interviews

- Vincent Cozijn - Strategisch adviseur wet- en regelgeving bij de Gegevensautoriteit van de Nationale Politie;
- Cécile Huisman – Coördinerend beleidsmedewerker bij het Directoraat-Generaal Politie en Veiligheidsregio's van het ministerie van Justitie en Veiligheid (Programma Politiebestel, Bevoegdheden en Informatiefunctie);
- Jacob Struyker Boudier – Strategisch raadadviseur bij de Directie Wetgeving en Juridische Zaken, Sector straf- en sanctierecht van het ministerie van Justitie en Veiligheid;
- Bart Schermer – Partner en hoofd juridische projecten bij Considerati, tevens universitair hoofddocent bij eLaw (de afdeling Internetrecht en IT-recht bij de universiteit Leiden);
- Kees Weijers - Functionaris Gegevensbescherming Wet Politiegegevens bij de Koninklijke Marechaussee.

Bijlage 7: lijst met gesprekspartners casestudylanden

België

- Alexander Hoefmans – Diensthoofd Privacy & Gelijke kansen bij het Directoraat Generaal Wetgeving, Fundamentele Rechten & Vrijheden van het Ministerie van Justitie (betrokken bij het ontwerp van de WVP);
- Christophe Bierlaire – Eerste Hoofdcommissaris van de Federale Politie (binnen die politiedienst verantwoordelijk voor de implementatie van de wetgeving);
- Frank Schuermans – Lid-raadsheer van het Controleorgaan op de politionele informatie (COC);
- Paul de Hert – Hoogleraar aan de Vrije Universiteit Brussel, gespecialiseerd in privacy en Europees strafrecht.

Denemarken

- Tanja Kammersgaard Christensen – Voormalig advocaat en post-doc aan de universiteit van Aalborg;
- Christian Wiese Svanberg – Hoofd van het centrum voor gegevensbescherming bij Deense nationale politie, tevens Functionaris Gegevensbescherming.

Duitsland

Bondsniveau

- Hagen Nollau – Medewerker Referat ÖS I 3 (Polizeiliches Informationswesen; Datenschutz im Sicherheitsbereich; BKA-Gesetz) van het Bondsministerie van Binnenlandse Zaken;
- Frank Thiede – Afdelingsleider adviesafdeling voor politiepraktische rechtsvragen en rechtspolitiek van het Bundeskriminalamt;
- Andrea Koch – Medewerker adviesafdeling voor politiepraktische rechtsvragen en rechtspolitiek van het Bundeskriminalamt;
- Dr. iur. Dr. rer. publ. Markus Thiel – Afdelingshoofd afdeling III.4 (Publiekrecht met focus op politierecht, onderdeel van Afdeling III Strafwetenschappen en juridische wetenschappen) en voorzitter van de ethische commissie van de Deutsche Hochschule der Polizei.

Nordrhein-Westfalen

- Prof. Dr. Klaus Schönenbroicher – Wetgevingsspecialist bij het verantwoordelijke ministerie van Binnenlandse Zaken;
- Frank Bettendorf – Functionaris gegevensbescherming en eerste hoofdcommissaris bij het Landeskriminalamt Nordrhein-Westfalen;
- Norbert Spinrath – Medewerker van de afdeling Internationale politionele samenwerking bij het ministerie van Binnenlandse Zaken, tevens eerste hoofdcommissaris bij de politie;

- Jörg-Konrad Unkrig – Hoofd van de afdelingen Criminaliteitspreventie en Internationale politionele samenwerking bij het ministerie van Binnenlandse Zaken.

Finland

- Suvi Pato-Oja – Senior adviseur ministerie van Binnenlandse Zaken;
- Jari Råman – Deputy Data Protection Ombudsman;
- Susanna Lindroos-Hovinheimo – Hoogleraar publiekrecht aan de universiteit van Helsinki;
- Annina Hautala – Chief of Information Management van de Finse politie, tevens lid van het Finse National Police Board.

Ierland

- Seamus Carroll – Principal Officer Civil Justice and Equality (Legislation) bij het Department of Justice and Equality (Ministerie van Justitie en Gelijkheid);
- Barry Lavin – Data Protection Officer van An Garda Síochána (de Ierse nationale politie en veiligheidsdienst);
- Eunice Delaney – Hoofd van de Complaints and Inquiries Unit bij de Data Protection Commission (DPC, de toezichthoudende autoriteit);
- David Fennelly - Advocaat en assistant professor of law aan het Trinity College Dublin (gespecialiseerd in Europees en internationaal recht, met een focus op gegevensbescherming).

Casestudy I - België

I.1 Inleiding

België is geselecteerd voor een casestudy omdat het een buurland van Nederland is waarmee relatief veel samengewerkt wordt. Daarnaast is het qua omvang vergelijkbaar met Nederland. Ten derde is het vanuit cultuurhistorisch oogpunt interessant om te kijken hoe de ervaringen in de zaak Dutroux en de daarop volgende herstructurering van de politie effect heeft gehad op de omgang met verwerking van persoonsgegevens.

Voor deze casestudy hebben we gesprekken gevoerd met een ambtenaar van het Ministerie van Justitie die betrokken was bij het ontwerp van de Wbp, een Eerste Hoofdcommissaris van de Federale Politie die binnen die politiedienst verantwoordelijk was voor de implementatie van de wetgeving, een lid-raadsheer van het Controleorgaan op de politionele informatie (COC) en een hoogleraar gespecialiseerd in privacy en Europees strafrecht. Daarnaast zijn de wetteksten bestudeerd, als ook enkele aanbevolen publicaties uit vakliteratuur en documenten van het COC.

I.2 Wettelijk kader

In deze paragraaf wordt het wettelijk systeem van België geschetst, wordt een overzicht gegeven van de wet- en regelgeving waarin de richtlijn is omgezet, wordt de systematiek van deze wetten toegelicht en komt een aantal punten aan de orde die in het algemeen opvallen.

I.2.1 Wet- en regelgeving waarin de richtlijn is geïmplementeerd

De richtlijn 2016/680 is in België vastgelegd in de zogeheten Wet Verwerking Persoonsgegevens (hierna: Wbp) van 30 juli 2018. In deze wet zijn zowel de richtlijn als de tenuitvoerlegging van de AVG-verordening opgenomen en specifieke wetgeving voor inlichtingendiensten.

De structuur van de wet kent drie titels die zien op de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door overheden. De eerste betreft de tenuitvoerlegging van de AVG-verordening en regelt de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens. In Titel 2 is de richtlijn 2016/680 vertaald en vastgelegd. Deze titel regelt volgens de wettekst “de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens door de bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid”. In de derde titel is een kader beschreven voor overheden en verwerkingen die buiten het toepassingsgebied van de EU (en dus buiten titels 1 en 2) vallen (met name inlichtingen- en veiligheidsdiensten).

De tweede titel is dus met name van belang voor de verwerking van politiegegevens. Deze titel is opgedeeld in een zestal hoofdstukken.

- In Hoofdstuk I zijn algemene bepalingen vastgelegd. Hieronder vallen de gehanteerde definities, zoals ook die van de 'bevoegde overheden' (zie paragraaf I.2)
- Hoofdstuk II beschrijft de beginselen op basis waarvan verwerking mag geschieden. Hier gaan we dieper op in paragraaf I.3.
- In Hoofdstuk III zijn de rechten van de betrokkene (verdachte, dader, of anderszins (bijvoorbeeld getuige)) vastgelegd.
- Hoofdstuk IV gaat in op de verdeling en invulling van bevoegdheden en plichten wanneer de verwerkingsverantwoordelijke besluit om gegevens door een andere partij te laten verwerken (die partij wordt als Verwerker aangemerkt). In vijf afdelingen wordt ingegaan op te nemen organisatorische en technische maatregelen, de situatie bij gezamenlijke verwerkingsverantwoordelijkheid, eisen aan (de overeenkomst met) de verwerker, verplichtingen die bestaan bij verwerking door een Verwerker, en regelingen met betrekking tot een functionaris voor gegevensbescherming.
- Hoofdstuk V behandelt de doorgiften van persoonsgegevens aan derde landen of internationale organisaties.
- Hoofdstuk VI beschrijft de instelling van een nieuw[67] Controleorgaan op de politionele informatie die optreedt als onafhankelijke toezichthoudende autoriteit. Deze beschrijven we in paragraaf I.4.

In de Wet op het Politieambt (Wpa) staat vermeld onder Art. 44/1 dat politiediensten informatie en persoonsgegevens kunnen verwerken overeenkomstig artikel 27 van de Wbp. Er wordt dus expliciet in de Wpa geborgd dat verwerking van persoonsgegevens door de politie gebeurt conform de Wbp. Verder geldt dat:

- In de rest van artikel 44/1 Wpa is vastgelegd onder welke voorwaarden bepaalde persoonsgegevens (biometrisch, gezondheidsgerelateerd, genetisch) verwerkt mogen worden en welke waarborgen daarbij van toepassing zijn.
- Artikel 44/2 de oprichting van de Algemene Nationale Gegevensbank (hierna: ANG), de basisgegevensbank en bijzondere gegevensbanken, technische (en gemeenschappelijke) gegevensbanken regelt.

De Algemene Nationale Gegevensbank (ANG) wordt in publieke informatie omschreven als het geheel van informatiesystemen van de geïntegreerde politie dat bestemd is om de opdrachten van gerechtelijke of bestuurlijke politie te ondersteunen zodat er een maximaal gestructureerd en beveiligd informatiebeheer wordt gewaarborgd.

- Artikel 44/3 lid stelt dat verwerking van persoonsgegevens niet alleen conform de Wbp maar ook conform de Archiefwet geschiedt.
- In artikel 44/4 is vastgelegd wie de verwerkingsverantwoordelijke partijen zijn voor verschillende gegevensverwerkingen. Dit betreft het Ministerie van Binnenlandse Zaken voor de gegevens in de ANG en basisgegevensbanken ten behoeve van bestuurlijke politie, het Ministerie van Justitie voor wat betreft dezelfde databanken voor de gerechtelijke politie, en bij bijzondere gegevensbanken gaat het om de korpschefs, de commissaris-generaal, de directeurs-generaal of de directeurs die de doeleinden van en de middelen voor deze gegevensbanken hebben bepaald. Ook hoe de verwerkingsverantwoordelijke partijen deze rol invullen is in dit artikel vastgelegd.
- Artikel 44/5 de categorieën van in de ANG en in de basisgegevensbanken geregistreerde persoonsgegevens beschrijft.

[67] Een dergelijk controleorgaan met dezelfde naam bestond ook al voor inwerkingtreding van de Wbp. Zie paragraaf I.4 voor verdere toelichting.

- Artikelen 44/7 tot en met 44/11 de inrichting en omgang met en toegang tot de ANG en andere gegevensbanken beschrijven.
- in 44/9 de bewaartermijnen worden beschreven.
- Verdere artikelen regelen de communicatie van persoonsgegevens.

Tot slot is noemenswaardig dat het inzetten van bewakingscamera's is geregeld in de Wet tot regeling van de plaatsing en het gebruik van bewakingscamera's (Camerawet). Hierin is onder meer de toegang tot de beelden door de politie en door gefilmde personen zelf geregeld. Belangrijke opmerking hierbij is dat voor wat betreft het gebruik van politiecamera's niet de camerawet geldt, maar nog steeds de Wpa.

I.2.3 Opvallende punten in de wet- en regelgeving

Een opvallend punt is dat de wet- en regelgeving voor verwerking van persoonsgegevens door politiediensten voor het overgrote deel in twee wetten (de Wbp en de Wpa) is vastgelegd. De Camerawet vormt nog een noemenswaardige aanvulling voor de inzet van een specifieke informatiebron bij gegevensverzameling.

Daarnaast valt het op dat de wetgeving vooral op punten een tweedeling in gerechtelijke of bestuurlijke politie bevat, maar dat de structuur van de politie zelf (met een federale politie en lokale politiediensten) in de wetgeving aangaande verwerking van persoonsgegevens amper een rol speelt.

I.3 De bevoegde autoriteiten

I.3.1 Algemeen

Zoals eerder beschreven is in Titel 2 van de Wbp beschreven hoe met de bescherming van persoonsgegevens zoals bedoeld in de richtlijn omgegaan dient te worden. In hoofdstuk 1, artikel 26, zevende lid staat een limitatieve opsomming en beschrijving van de bevoegde autoriteiten die onder de wetgeving in deze Titel 2 vallen:

a) *de politiediensten in de zin van artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie gestructureerd op twee niveaus;*
b) *de gerechtelijke overheden, te verstaan als de gemeenrechtelijke hoven en rechtbanken en het openbaar ministerie;*
c) *de Dienst Enquêtes van het Vast Comité van Toezicht op de politiediensten in het kader van zijn gerechtelijke opdrachten zoals bedoeld in artikel 16, 3e lid van de organieke wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse;*
d) *de Algemene Inspectie van de federale politie en van de lokale politie bedoeld in artikel 2 van de wet van 15 mei 2007 op de Algemene Inspectie en houdende diverse bepalingen betreffende de rechtspositie van sommige leden van de politiediensten;*
e) *de Algemene administratie van de douane en accijnzen, in het kader van haar opdracht inzake opsporing, vaststelling en vervolging van de misdrijven zoals bepaald in de algemene wet inzake douane en accijnzen van 18 juli 1977, en in de wet van 22 april 2003 houdende toekenning van de hoedanigheid van officier van gerechtelijke politie aan bepaalde ambtenaren van de administratie der douane en accijnzen;*
f) *de Passagiersinformatie-eenheid bedoeld in hoofdstuk 7 van de wet van 25 december 2016 betreffende de verwerking van passagiersgegevens;*
g) *de Cel voor financiële informatieverwerking bedoeld in artikel 76 van de wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten;*
h) *de Dienst Enquêtes van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten in het kader van zijn gerechtelijke opdrachten zoals bedoeld in artikel 40, derde lid, van de wet*

> *van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coordinatieorgaan voor de dreigingsanalyse;*

Bij sub a) wordt verwezen naar andere wetgeving, waarin de politiediensten zijn gespecificeerd. Deze onderverdeling wordt verder beschreven in paragraaf I.2.2. De onder sub c) en sub d) beschreven instanties komen aan bod in paragraaf I.4.

I.3.2 Structuur van de politie

De in artikel 2, 2°, van de wet van 7 december 1998 tot organisatie van een geïntegreerde politie gestructureerd op twee niveaus (hierna: Wet geïntegreerde politiedienst) worden de politiediensten gedefinieerd als de federale politie en de korpsen van de lokale politie. Deze twee typen instanties vormen samen de geïntegreerde politie.
Artikel 3 van de wet definieert hoe de politieniveaus zich tot elkaar verhouden en wat hun taakgebieden zijn:

> *Art. 3. De politiediensten worden georganiseerd en gestructureerd op twee niveaus : het federale niveau en het lokale niveau, die samen de geïntegreerde politiezorg verzekeren. Deze niveaus zijn autonoom en hangen van verschillende overheden af. Deze wet regelt de functionele banden tussen deze twee niveaus.*
>
> *Overeenkomstig Titel II van de huidige wet, verzekert de lokale politie op het lokale niveau de basispolitiezorg, meer bepaald alle opdrachten van bestuurlijke en gerechtelijke politie die nodig zijn voor het beheren van lokale gebeurtenissen en fenomenen die zich voordoen op het grondgebied van de politiezone, evenals het vervullen van sommige politieopdrachten van federale aard.*
>
> *Overeenkomstig Titel III van de huidige wet, verzekert de federale politie over het gehele grondgebied, met inachtneming van de principes van specialiteit en subsidiariteit, de gespecialiseerde en de supralokale opdrachten van bestuurlijke en gerechtelijke politie, evenals ondersteunende opdrachten voor de lokale politiediensten en voor de politieoverheden.*
>
> *De geïntegreerde politiedienst waarborgt de overheden en de burgers een minimale gelijkwaardige dienstverlening over het gehele grondgebied van het Rijk.*

De door de lokale politie verschafte basispolitiezorg is niet als zodanig in de wet gedefinieerd. In een ministeriële omzendbrief zijn de zeven onderdelen beschreven: werk in de wijk, onthaal (loketfunctie voor aangiftes, meldingen, informatie etc.), interventie (ingrijpen bij dreiging of crimineel gedrag), slachtofferbejegening, (lokale) recherche, openbare orde en verkeer.[68] Er zijn 185 lokale politiezones in België, die één of meer gemeenten omvatten.

De federale politie heeft een gecentraliseerde structuur, onder leiding van het Commissariaat-generaal (CG). Dit CG stuurt direct een aantal diensten aan op het gebied van onder meer communicatie en internationale samenwerking, en daarbij ook de dienst Information Security and Privacy Office (ISPO) die onder meer verantwoordelijk is voor de coördinatie van de uitvoering van die nieuwe Europese wettelijke verplichtingen in het kader van de Richtlijn 2016/680 en de AVG en de integratie met de informatieveiligheid.[69]

[68] Ministeriële Omzendbrief PLP 10 inzake de organisatie- en werkingsnormen van de lokale politie met het oog op het waarborgen van een minimale gelijkwaardige dienstverlening aan de bevolking, 9 oktober 2001.
[69] Federale Politie, Informatiebeheer, de kern van onze zaak, Jaarverslag Federale Politie 2017, 2018.

De federale politie bestaat verder nog uit drie algemene directies:

- Middelenbeheer en informatie (met daaronder onder meer de Directie van politionele informatie en de ICT-middelen)
- Bestuurlijke politie
- Gerechtelijke politie

Daarnaast is er nog een aantal gedeconcentreerde diensten.

De geïntegreerde politie valt onder verantwoordelijkheid van zowel de Minister van Binnenlandse Zaken als de Minister van Justitie. De Minister van Binnenlandse Zaken is bevoegd voor de bestuurlijke politie, de Minister van Justitie voor de gerechtelijke politie. Deze bevoegdheid doorkruist dus de twee niveaus van de geïntegreerde politie; ook bij de uitvoering van taken door lokale politieafdelingen zijn er dus twee verantwoordelijke ministers.

I.4 Verwerken van politiegegevens

I.4.1 Verkrijgen van politiegegevens

De wettelijke basis voor het verzamelen van gegevens door politiediensten ligt in de Wet op het Politieambt (Wpa). Hierin staat onder meer vermeld onder Art. 44/1. § 1:

> *In het kader van de uitoefening van hun opdrachten, bedoeld in hoofdstuk III, afdeling 1 [van de Wpa] en overeenkomstig de doeleinden omschreven in artikel 27 van de [Wbp] kunnen de politiediensten informatie en persoonsgegevens verwerken voor zover deze laatste toereikend, terzake dienend en niet overmatig van aard zijn in het licht van de doeleinden van bestuurlijke en van gerechtelijke politie waarvoor ze verkregen worden en waarvoor ze later verwerkt worden.*

In het aangehaalde artikel 27 van de Wbp staat vervolgens:

> *Deze titel [Titel 2] is van toepassing op de verwerkingen van persoonsgegevens door de bevoegde overheden met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.*

Zoals gezegd is Titel 2 het deel van de Wbp waarin de verwerking van persoonsgegevens door politie- en justitiediensten geregeld is. De gesprekspartner van de federale politie geeft aan dat hiermee expliciet ervoor is gekozen om gegevensverwerking voor de bestuurlijke en gerechtelijke politietaken met dezelfde artikelen te regelen.

De gesprekspartner bij het ministerie van Justitie stelt dat nog is overwogen om ook het Wetboek van Strafvordering en het Gerechtelijk Wetboek te herzien, maar na een analyse van de huidige wetgeving is besloten dat daar geen noodzaak toe was. Alleen de Wpa is zoals gezegd voor het politiewerk aangepast aan de invoering van de Wbp.

Om de verschillende voorschriften van zowel de AVG als de Richtlijn in een coherent systeem te vatten en ervoor te zorgen dat verschillende datastromen gestroomlijnd zijn ondanks de verschillende regimes, is in het eerste hoofdstuk de Wbp een aantal artikelen opgesteld over omgang met het verkrijgen en delen van informatie, ook in het geval dat er uitwisseling plaatsvindt tussen de verschillende regimes. Met name art. 3 van de Wbp gaat hierop in:

> *Het vrije verkeer van persoonsgegevens wordt noch beperkt noch verboden om redenen die verband houden met de bescherming van natuurlijke personen ten aanzien van de verwerking van persoonsgegevens. In het bijzonder kan de uitwisseling van persoonsgegevens tussen de verwerkingsverantwoordelijken, de bevoegde overheden, de diensten, organen en de ontvangers bedoeld in de titels 1 tot 3 van deze wet en die binnen het kader van de doelstellingen bedoeld in artikel 23.1.a) tot h), van de Verordening handelen, niet worden beperkt noch verboden omwille van dergelijke redenen. Een beperking of verbod kan evenwel plaatsvinden indien er een hoog risico bestaat dat de uitwisseling van gegevens zou leiden tot het omzeilen van deze wet.*

In de MvT bij de wet is wordt over dit artikel geschreven dat dit betekent dat "een verwerkingsverantwoordelijke een gegevensstroom niet kan blokkeren onder het voorwendsel van het garanderen van de bescherming van persoonsgegevens. Hij zal alleen dezelfde gegevensbeschermingsregels kunnen toepassen die het toepast voor zijn eigen gegevensverwerking. Een overheidsdienst mag vooral dus nooit tekort komen aan het volbrengen van zijn opdrachten om een reden gelinkt aan de gegevensbescherming." Dit artikel is dus een uitwerking van artikel 1, derde punt van de AVG met specifieke aandacht voor de driedeling van instanties die in de Wbp is aangebracht.

Het gebruikmaken van gegevens uit beveiligingscamera's van derden is geregeld in de Camerawet. Hierin staat onder meer beschreven onder welke voorwaarden camera's geplaatst mogen worden in de openbare ruimte, hoe de politie betrokken is hierbij en dat de beelden overgedragen moeten worden indien dit behulpzaam kan zijn bij het onderzoek naar een misdrijf in een publiekelijk toegankelijke ruimte. Bij inbeslagname van beelden van niet publiekelijk toegankelijke ruimtes is een gerechtelijk mandaat nodig alvorens tot overdracht van beelden overgegaan moet worden. Een gesprekspartner vanuit het academische veld heeft aangegeven dat de mogelijkheden die deze wetgeving biedt aan politiediensten als zeer ruim wordt gezien.

Het gebruik van mobiele camera's (waaronder *bodycams*) is geregeld in Art. 25/3 van de Wpa, de inzet van vaste camera's in Art. 25/4.

De opkomst van het werken met nieuwe technieken op het gebied van surveillance, *big data* en kunstmatige intelligentie is mogelijk nog niet goed geregeld in de huidige wetgeving. Daarin wordt nog gesproken over databanken. De gesprekspartner bij de politie heeft aangegeven dat er momenteel een IT project in (genaamd I-police, of *information police*). is gestart om alle IT systemen te vervangen door nieuwe technologieën op het gebied van gegevensverwerking. Daarmee zal veel worden ingezet op het samenbrengen van systemen, waarbij door middel van het toekennen van systeemrechten waarborgen ten aanzien van bescherming van persoonsgegevens ingebouwd moeten worden. Afhankelijk van onder meer de ernst van de zaak moeten de mogelijkheden tot een volledige zoeking worden toegekend.

In een recente wetenschappelijke publicatie is uitgebreid ingegaan op de opkomst van deze technologische ontwikkelingen bij de lokale politie en het mogelijke toezicht hierop. De voornaamste conclusie van de auteur is "dat de focus op de risico's voor individuele rechten en meer specifiek privacy en databescherming tekortschiet om een antwoord te bieden aan de risico's van nieuwe technologische ontwikkelingen".[70] Daarmee lijkt het erop dat de wetgeving nog niet volledig toekomstbestendig wordt beschouwd door wetenschappelijke veld.

[70] R. Van Brakel (2020) Een reflectie over het huidig toezicht van het gebruik van surveilancetechnologie door de lokale politie in België, Cahiers Politiestudies, 55: 139-160.

I.4.2 Bewerken van politiegegevens door de bevoegde autoriteiten

De bewerking van politiegegevens is geregeld in Hoofdstuk 2 Wbp. We bespreken kort de artikelen in dit hoofdstuk:

- In artikel 28 is vastgelegd dat persoonsgegevens correct, met een bepaald doeleinde en rechtmatig worden verwerkt. Daarnaast wordt in dit artikel gewaarborgd dat de gegevens geactualiseerd en goed beveiligd worden, en dat deze bewaard worden in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt.
- In artikel 29 wordt de verdere verwerking door een andere verwerkingsverantwoordelijke geregeld. Hierin is onder meer vastgelegd dat de verder verwerkende partij conform wet- en regelgeving gemachtigd dient te zijn de gegevens te verwerken. Daarnaast geldt dat de verwerking met een ander doeleinde dan het oorspronkelijke doeleinde van verzameling van de gegevens is toegestaan mits dit nieuwe doeleinde past binnen het bredere artikel 27 (zie I.4.1).
- Artikel 30 beschrijft de bewaartermijnen (zie paragraaf I.4.3).
- In artikel 31 is de categorisering van de personen waarover gegevens zijn verzameld beschreven; verdachten, veroordeelden, slachtoffers of overige personen.
- Artikel 32 regelt de scheiding van feitelijke informatie van subjectieve informatie.
- Artikel 33 beschrijft voorwaarden voor rechtmatigheid van verwerking. Dit houdt in dat de verwerking noodzakelijk moet zijn voor de uitvoering van politionele taken en dat deze is gebaseerd op een wettelijke of reglementaire verplichting, waarbij is vastgelegd welke categorieën gegevens verwerkt kunnen worden en met welk doeleinde.
- Artikel 34 stelt extra strenge eisen aan verwerking van bijzondere persoonsgegevens, zoals gegevens over afkomst, politieke voorkeur, geaardheid, alsmede biometrische en genetische gegevens. Dit kan alleen wanneer de verwerking strikt noodzakelijk is en in een limitatief aantal gevallen.[71]
- Artikel 35 bepaalt dat geautomatiseerde verwerking aan aanvullende voorwaarden voldoet en dat het verboden is dat dit leidt tot discriminatie van natuurlijke personen.

Afgezien van een herschikking en enkele herformuleringen van de artikelen volgt de wetgeving integraal de tekst in hoofdstuk 2 van de richtlijn.

In artikel 44/5 van de Wpa wordt onder meer ingegaan op categorisering van persoonsgegevens die in de ANG en in de basisgegevensbanken kunnen worden opgeslagen. Hierbij wordt een onderscheid gemaakt tussen gegevens opgeslagen ten behoeve van de bestuurlijke politie en van de gerechtelijke politie. In artikel 44/1 is daarnaast nog beschreven welke speciale categorieën persoonsgegevens opgeslagen kunnen worden met welk doeleinde. Hierbij gaat het om biometrische gegevens (voor identificatie van personen), gezondheidsgegevens (voor het begrijpen van persoonlijke omstandigheden en/of ten behoeve van te nemen veiligheidsmaatregelen) en genetische gegevens.

België wijkt op één punt sterk af van de Nederlandse praktijk bij de verwerking van persoonsgegevens en dan met name het recht op inzage van de betrokkene. Volgens artikel 14 van de richtlijn dient een betrokkene inzage te krijgen om de verzamelde persoonsgegevens in te zien en informatie op te vragen over onder meer het doeleinde van de gegevensverwerking, de categorieën van opgeslagen gegevens, de partijen die de gegevens krijgen en hoe lang de

[71] Deze gevallen zijn als volgt gespecificeerd: 1° wanneer de verwerking door de wet, het decreet, de ordonnantie, de Europese regelgeving of de internationale overeenkomst is toegestaan; 2° wanneer de verwerking noodzakelijk is ter verdediging van de vitale belangen van de betrokkene of van een andere natuurlijke persoon; 3° wanneer de verwerking betrekking heeft op gegevens die kennelijk openbaar zijn gemaakt door de betrokkene.

gegevens naar verwachting opgeslagen blijven. In artikel 15 is vervolgens geregeld dat deze rechten beperkt kunnen worden wanneer dit noodzakelijk en evenredig is om – kort gezegd – ervoor te zorgen dat het werk van politie en/of justitie niet wordt belemmerd, de nationale veiligheid en de rechten en vrijheden van anderen beschermd worden.

België kiest voor wat betreft de interpretatie van deze twee artikelen een andere interpretatie dan gebruikelijk is in Europese landen. In België is al sinds de invoering van de voorloper van de Wbp, de Privacywet uit 1992, een systeem van niet rechtstreekse toegang tot gegevens opgezet. Dit houdt in dat de betrokkene niet direct bij de politiediensten een verzoek tot inzage van gegevens zoals bedoeld in artikel 14 van de richtlijn kan indienen, maar dat dit via het controleorgaan[72] dient te geschieden. In artikel 42 van de Wbp is dit wederom vastgelegd:

> *Het verzoek tot uitoefening van de rechten […] wordt aan de toezichthoudende autoriteit […] gericht.*
> *In de in de artikelen 37, § 2, 38, § 2, 39, § 4, en 62, § 1, bedoelde gevallen deelt de toezichthoudende autoriteit bedoeld in artikel 71 uitsluitend mee aan de betrokkene dat de nodige verificaties werden verricht.*

De vier aangehaalde artikelen in de tweede alinea hierboven beschrijven verschillende redenen zoals opgenomen in artikel 15 van de richtlijn voor beperking van de rechten tot inzage van de betrokkene. De laatste zin van dit artikel behelst een ernstige inperking van de rechten van de betrokkene: het is het controleorgaan is immers alleen toegestaan om te verifiëren dat de gegevens conform wet- en regelgeving is verwerkt en hierover terugkoppeling te geven, maar niet om inhoudelijk ook informatie te geven over de precieze aard en inhoud van de gegevensverwerking (welke gegevens, welk doeleinde, etc.). Het controleorgaan heeft overigens zelf toegang tot de ANG en een beperkt aantal andere gegevensbanken. Het verzoekt namens de betrokkene aan de bevoegde autoriteiten in kwestie om informatie over de gegevensverzameling in andere gegevensbanken.

Tijdens een interview met een vertegenwoordiger van de toezichthoudende autoriteit is uitgelegd dat deze constructie ook een voordeel voor de betrokkene oplevert. Deze staat immers als individu mogelijk zwakker tegen de politiediensten dan een overheidsinstantie met expertise op het gebied van de verwerking van politiegegevens. De academische expert die wij spraken is echter zeer kritisch op het gekozen systeem. In een artikel over de Privacywet (waarin het systeem van niet rechtstreekse toegang voorheen was geregeld) schrijft hij daarover dat deze regeling “strijdt met de Europese politieaanbeveling die vertrekt van een toegangsrecht voor de geregistreerde, dat door de politie in een aantal gevallen evenwel ontzegd kan worden”. De auteurs verwijzen naar het model van de Franse privacycommissie, die per geval nagaat of rechtstreekse mededeling verzoenbaar is met het politiewerk.[73]

De gesprekspartner van het ministerie van Justitie zegt hierover dat België een compromis had bereikt met de Europese Commissie rondom de toegang tot data. De flexibiliteit in de wetgeving die men veronderstelde blijkt nu waarschijnlijk niet zo groot te zijn als gedacht. Een systeem van rechtstreekse toegang blijkt verplicht, met daarnaast de mogelijkheid tot een systeem van niet rechtstreekse toegang, maar dan slechts een in uitzondering op het systeem van rechtstreekse toegang. De vrees bestaat dat de verandering naar een systeem

[72] Het controleorgaan wordt in paragraaf I.4 uitgebreid beschreven.
[73] De Schutter, B., De Hert, P. (1995) *Is België klaar met zijn politie-privacywetgeving*, Vigiles, Tijdschrift voor Politierecht, Jaargang 1, nummer 3, september 1995.

met rechtstreekse toegang een aanzienlijke administratieve last met zich mee zal brengen voor de politiediensten.

I.4.3 Bewaartermijnen en vernietigingsgronden

De bewaartermijnen van politiegegevens zijn geregeld in artikel 30 van de Wbp:

> *Behoudens de gevallen waarin de maximale bewaartermijn van de gegevens wordt bepaald in de Europese regelgeving of de internationale overeenkomst die de basis vormt voor de betrokken bewaring, bepaalt de wet, het decreet of de ordonnantie de maximale bewaartermijn. Na afloop van die termijn worden de gegevens gewist.*
> *In afwijking van het eerste lid kan de wet, het decreet of de ordonnantie voorzien dat na afloop van een eerste bewaartermijn een analyse moet worden uitgevoerd op basis van verschillende noodzakelijkheids- en proportionaliteitscriteria om te bepalen of het nodig is dat de gegevens bewaard blijven, en in voorkomend geval, de nieuwe bewaartermijn.*
> *In dat geval voorziet de wet, het decreet of de ordonnantie in een maximale bewaartermijn.*

Hierin wordt dus voornamelijk verwezen naar landelijke wetgeving, in dit geval de Wpa en specifiek artikel 44/9. Dit artikel stelt ten eerste de kwalitatieve eis dat de gegevens “worden gearchiveerd wanneer zij ontoereikend, niet ter zake dienend of overmatig van aard zijn”. Daarbij worden aanvullende termijnen gesteld. Paragraaf 1 stelt een aantal termijnen vast voor gegevens gebruikt door de bestuurlijke politie. Afhankelijk van de categorie waaronder de persoon valt is dit drie of vijf jaar na de laatste registratie. Uitzonderingen zijn mogelijk wanneer persoonsgegevens ook zijn opgeslagen ten behoeve van de gerechtelijke politie. Paragraaf 2 stelt bewaartermijnen vast voor de gerechtelijke politie. Afhankelijk van de categorie waartoe de persoon behoort waarvan gegevens zijn opgeslagen variëren de termijnen van een tot tien jaar.

Overigens worden de gegevens niet volledig verwijderd na het verlopen van de bewaartermijn, maar worden ze gearchiveerd, volgens artikel 44/10 voor maximaal 30 jaar.

In de praktijk verloopt de archivering van gegevens volgens de gesprekspartner van het controleorgaan op de politionele informatie nog niet conform de wetgeving. Hoewel de verplichting tot archivering bestaat sinds 2017 wordt deze tot op heden niet (goed) toegepast. Het controleorgaan is in gesprek met de federale politie die beheerder is van de ANG en heeft hen – naar eigen zeggen - weten te overtuigen snel maatregelen te treffen. Vooralsnog is dit echter nog niet opgelost.

I.4.4 Delen van politiegegevens

Deze subparagraaf gaat over het delen van politiegegevens. Daarbij wordt stilgestaan bij de vraag aan welke partijen politiegegevens mogen worden verstrekt en het afwegingskader dat hier eventueel voor geldt.

In artikel 44/11/9 van de Wpa is vastgelegd met welke partijen politiegegevens gedeeld mogen worden. Dit is in elk geval mogelijk voor de Cel van financiële informatieverwerking, de Dienst Vreemdelingenzaken en enkele onderdelen van de Algemene Administratie der douane en accijnzen, ten behoeve van de uitvoering van hun wettelijke taken. Hiervoor moeten de ministeries nog richtlijnen vaststellen en publiceren. Dat geldt ook voor het delen van persoonsgegevens en informatie met de Belgische openbare overheden, publieke organen of instellingen of instellingen van openbaar nut die door de wet belast zijn met de toepassing van de strafwet of die wettelijke verplichtingen inzake de openbare veiligheid hebben, wanneer ze deze nodig hebben voor de uitoefening van hun wettelijke opdrachten.

Bij 'herhaalde of volumineuze mededeling van persoonsgegevens' dienen protocolakkoorden te worden opgesteld, waarin tenminste de te nemen veiligheidsmaatregelen en de duur van bewaring van de gegevens is opgenomen.

I.5 Toezicht

In deze paragraaf staat het toezicht op de verwerking en verkrijging van politiegegevens centraal. Eerst zal worden stilgestaan bij de vraag wie de externe en interne toezichthouders zijn, daarna zal worden ingegaan op de bevoegdheden van deze toezichthouders en ten slotte zal worden stilgestaan bij het proces van toezichthouden.

De politiediensten kennen een aantal toezichthouders. Ten eerste heeft elke lokale politiedienst en de federale politie een Dienst Intern Toezicht, die klachten of meldingen over het optreden van de korpsleden onderzoekt. Ook is er in elke politiedienst een functionaris gegevensbescherming aangesteld. Dit zijn beide interne toezichthouders. Ten derde is er het Comité P, die als opdracht heeft "om te onderzoeken hoe politiediensten de beslissingen van de gerechtelijke overheid, het openbaar ministerie en de bestuurlijke overheid (met name de ministers van Binnenlandse Zaken of van Justitie, de provinciegouverneurs, de arrondissementscommissarissen en de burgemeesters) uitvoeren"[74]. Deze toezichthouder heeft ook een brede focus op het geheel aan taakuitvoering door de politie en legt zich toe op beleid, regels en processen en niet op individuele gevallen. Hetzelfde geldt voor de algemene inspectie van de federale en lokale politie (AIG), die meer individuele (waaronder tucht-)zaken behandelt.

Met de inwerkingtreding van de Wbp controleorgaan op de politionele informatie (afgekort COC) richt zich specifiek op het toezicht op de verwerking van politiegegevens. Het vindt dan ook zijn wettelijke basis in de Wbp, artikel 71:

> *Bij de Kamer van volksvertegenwoordigers wordt een onafhankelijke toezichthoudende autoriteit op de politionele informatie opgericht, Controleorgaan op de politionele informatie genoemd.*
> *Zij is de rechtsopvolger van het Controleorgaan op de politionele informatie opgericht bij artikel 36ter, § 1, eerste lid, van de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.*
> *Zij is ten aanzien van de bevoegde overheden bedoeld in artikel 26, § 1, 7°, a), d) en f), belast, met :*
> *1° het toezicht op de toepassing van deze titel, zoals voorzien door artikel 26, 15° ;*
> *2° de controle van de verwerking van de informatie en de persoonsgegevens bedoeld in de artikelen 44/1 tot 44/11/13 van de wet van 5 augustus 1992 op het politieambt, met inbegrip van deze ingevoegd in de gegevensbanken bedoeld in artikel 44/2 van dezelfde wet;*
> *3° elke andere opdracht haar door of krachtens andere wetten verleend.*

Dit is de 'toezichthoudende autoriteit' zoals deze is gedefinieerd in artikel 26 van de Wbp, die toeziet op de verwerking van persoonsgegevens zoals vastgelegd in het eerder uitvoerig besproken artikel 44 Wpa. In haar eigen jaarverslag[75] presenteert de COC haar vier autoriteiten:

[74] Website Comité P, https://comitep.be/, geraadpleegd 20 augustus 2020.
[75] Controleorgaan op de politionele informatie (2020), *Activiteiten Verslag 2016-2019*.

- Toezicht op toepassing van titel II van de Wbp door de geïntegreerde politie (en ook door de AIG en de Belgische Passagiersinformatie eenheid);
- toezicht op toepassing van de AVG door de politie (bijvoorbeeld bij rekrutering en selectie);
- controle van verwerking van politieinformatie inzake terrorismebestrijding;
- overige wettelijke toezichtstaken, waaronder op gebruik van camerabeelden door de geïntegreerde politie.

In Titel 7 van de Wbp is de wettelijke basis voor het COC vastgelegd. In het jaarverslag van het COC worden de bevoegdheden samengevat als "klassieke inspectieopdrachten die gaan van een onbeperkt recht op toegang tot alle informatie en gegevens, onderzoeken ter plaatste met een onbeperkt recht tot toegang, voorwerpen/documenten/gegevens in beslag nemen, alle nuttige vaststellingen doen, dwingende antwoordtermijnen opleggen, toegang tot het rijksregister en gebruik van het nummer, verhoren afnemen, deskundigen en tolken vorderen, enz."

Onze gesprekspartner bij het COC heeft aangegeven dat 90% van het werk uit toezicht op de GPI bestaat. Ten aanzien van de algemene inspectie zijn eigenlijk nog nooit toezichtactiviteiten uitgevoerd. Bij de passagiersinformatie eenheid (BELPIU) wordt jaarlijks een onderzoek uitgevoerd, maar dat doet het COC samen met de DPA voor de inlichtingendiensten: het Vast Comité I. Het COC bestaat in totaal uit 10 mensen. In de situatie van vóór 2018 was er maar één jurist van de Belgische privacycommissie betrokken bij het controleren van de politie.

De huidige prioriteiten van het COC zijn gericht op de volledige informatiehuishouding van de GPI. Dit ziet ook op (kosten)efficiëntie en effectiviteit naast dataprotectie. Sinds 2018 gaat evenwel 75% van de capaciteit naar toezicht op privacy en dataprotectie, omdat zich hier de meeste problemen voordoen en de grootste vooruitgang is te boeken.

Per jaar worden een aantal politiezones en een aantal entiteiten van de federale politie gecontroleerd. Dit zijn algemene toezichtonderzoeken met al dan niet uitgebreide visitaties over bijvoorbeeld informatieveiligheid, privacy en gegevensbescherming, de activiteiten van de Data Protectie Officier, enz. De ervaring leert dat de resultaten van onderzoeken die worden uitgevoerd in specifieke zones, zich doorgaans snel verspreiden naar andere zones. De rapporten zijn in een publieke versie raadpleegbaar op de website en men ziet dat de vaststellingen, tekortkomingen, aanbevelingen en sancties opgepikt worden door de andere politie-entiteiten van de GPI.

Het controleorgaan heeft een aantal corrigerende bevoegdheden, vastgelegd in de Wbp, die overgenomen zijn van regelgeving uit de AVG. Het COC kan verwerkingen en operationele gegevensstromen stilleggen of waarschuwingen afgeven. De gesprekspartner heeft aangegeven dat bij vrijwel elk onderzoek bij een lokale politiezone een waarschuwing afgegeven wordt of een verbetertraject wordt gestart. Slechts in hoogst uitzonderlijke gevallen wordt besloten gegevensstromen stil te leggen. Gebruikelijker is het om een (tijdelijk) gedoogbeleid te voeren om het politiewerk door te kunnen laten gaan terwijl de processen worden verbeterd.

Wanneer het COC bij de politiezones of federale politie-eenheden patronen herkent kan dat uitmonden in een globaal advies dat door de gehele organisatie van het GPI wordt gecommuniceerd.

Vanuit het academische veld heeft een gesprekspartner kanttekeningen geplaatst ten aanzien van de schijn van afhankelijkheid bij de toezichthoudende autoriteit. Zo is bekend dat het lidraadsheer van het COC ook een functie heeft als advocaat-generaal bij het Openbaar Ministerie. De ratio hierachter is dat op die manier veel expertise van het werkveld is binnengehaald bij de toezichthouder, maar onze gesprekspartner wijst op het risico dat hierdoor de afstand tussen toezichthouder en onder toezicht staande instanties te klein is.

I.6 Opvallende punten en eventuele leerpunten voor Nederland

Er zijn twee belangrijke punten waarop België sterk afwijkt van Nederland en die daarmee mogelijk leerpunten opleveren.

Ten eerste is de inrichting van de toegang tot persoonsgegevens door de betrokkene in België geregeld via zogeheten niet rechtstreekse toegang, wat wil zeggen dat een verzoek om inzage in de persoonsgegevens die door politiediensten zijn opgeslagen moet worden gericht aan de toezichthoudende autoriteit. We hebben vanuit onze interviews hiervoor twee voordelen horen noemen. Een direct voordeel is dat een burger een overheidsinstantie kan inschakelen om de politiediensten te benaderen, en daarmee een geïnformeerde instantie met autoriteit aan zijn kant heeft om de afhandeling van het verzoek in de gaten te houden. Ten tweede is aangegeven dat wanneer de Belgische politie toch gedwongen wordt om rechtstreekse toegang te faciliteren, die naar de verwachting van de autoriteiten zelf waarschijnlijk extra administratieve kosten gaat opleveren. Oftewel, het huidige systeem levert een kostenbesparing op ten opzichte van de situatie in Nederland. Als groot nadeel is door een andere gesprekspartner genoemd dat de betrokken personen nu amper inzicht krijgen in wat er daadwerkelijk over hun geregistreerd staat, met welk doeleinde, voor hoe lang (naar verwachting) enzovoorts. De terugkoppeling op een verzoek is zeer summier te noemen en dit is dan ook in veel gevallen een ernstige inperking van de rechten zoals die bedoeld zijn vast te leggen in artikel 14 van de richtlijn. De zorgen van de Belgische wetgever over een mogelijk op handen zijnde opdracht om alsnog rechtstreekse toegang mogelijk te maken spreekt wat dat betreft boekdelen over de wenselijkheid van een dergelijk systeem voor Nederland.

Een tweede belangrijk mogelijk leerpunt betreft de inrichting van het toezicht. In België is een apart orgaan opgezet voor het toezicht op de verwerking van informatie door politiediensten. De ratio hierachter is dat de juridische context van dergelijke gegevensverwerking op veel punten afwijkt, evenals de praktische situatie omtrent de verzameling en verwerking van deze gegevens. Door een gespecialiseerde toezichthouder op te zetten kan het toezicht effectiever worden ingericht. Als kanttekening hebben we wel kritische noten gehoord als het gaat om de afstand tot het werkveld wanneer de aangewezen toezichthouders hun expertise vooral hebben opgedaan tijdens een carrière in datzelfde werkveld. Op zijn minst zou dat een punt van aandacht moeten zijn bij het aanwijzen van mensen op sleutelposities, om de schijn van partijdigheid te voorkomen.

Ook de verdergaande bevoegdheden van de toezichthouder ten aanzien van het stilleggen van gegevensverwerking is een interessant punt. Hoewel hier zeer terughoudend mee om moet worden gegaan kan het een overweging waard zijn om dergelijke bevoegdheden ook in Nederland in te richten, ook als stok achter de deur bij de inzet van het minder vergaande instrumentarium.

Casestudy II: Denemarken

Denemarken is geselecteerd voor een casestudy omdat Denemarken overeenkomsten vertoont met Nederland. Zo komt de organisatie van de politie in Denemarken overeen met het Nederlandse politiebestel. Daarnaast is Denemarken net als Nederland een koninkrijk met overzeese gebieden die niet behoren tot de Europese Unie. Denemarken heeft twee overzeese gebieden, namelijk de Faeröer in de noordelijke Atlantische Oceaan en Groenland in Noord-Amerika. Verder lijkt het Deense staatsbestel op het Nederlandse. Al met al is Denemarken een interessante casestudy.

Voor de Deense casestudy hebben we gesprekken gevoerd met een postdoc van de universiteit van Aalborg. Haar promotieonderzoek richtte zich op de samenhang tussen de wettelijke regeling van politietoezicht in Denemarken en de grondrechten in het EU-handvest en het mensenrechtenverdragen. Daarnaast is gesproken met het hoofd van het centrum voor gegevensbescherming bij de Deense nationale politie. Deze persoon is tevens de functionaris gegevensbescherming van de Deense politie. Er is geprobeerd om in contact te komen met de toezichthoudende autoriteiten en ambtenaren van het Ministerie van Justitie die betrokken waren bij de implementatie van de richtlijn. Ondanks herhaaldelijke pogingen is het niet gelukt om deze partijen te spreken. Naast de gevoerde gesprekken zijn voor zover mogelijk de wetteksten bestudeerd. Van de relevante Deense wetgevingen zijn geen Engelse vertalingen beschikbaar. Dit is deels opgevangen door bronnen te raadplegen die wel in het Engels beschikbaar zijn, zoals de website van de Deense nationale Politie en de website van de Danish Data Protection Agency. Deze sites omschrijven voor een deel de relevante wet- en regelgeving. Gezien het bovenstaande moet de informatie uit deze casestudy met enig voorbehoud bekeken worden.

II.1 Wettelijk kader

II.1.1 Wettelijk systeem

De taken van de politie zijn vastgelegd in de wet *Lov om politiets virksomhed.* De eerste sectie van de wet noemt de volgende taken als politietaak:

"De politie moet zich inzetten voor veiligheid, vrede en orde in de samenleving. De politie moet dit doel bevorderen door middel van preventie, het verlenen van bijstand en handhaving."

De verwerking van persoonsgegevens door de politie is in Denemarken geregeld in de *Processing of personal data by law enforcement Act (Act).*[76] De politie mag in overeenstemming

[76] LOV nr 410 af 27/04/2017 (Act)

met deze Act persoonsgegevens verwerken. Paragraaf 9 van de Act geeft aan voor welke doeleinden de politie tijdens haar taakuitvoering gegevens mag verzamelen. De doelen zijn breed geformuleerd en komen er op neer dat de politie gegevens verwerkt met als doel strafbare feiten te voorkomen, onderzoeken uit te voeren, personen op te sporen of te vervolgen. Ook kan de politie gegevens verwerken wanneer dit nodig is om strafrechtelijke sancties uit te voeren of wanneer er sprake is van een bedreiging voor de openbare veiligheid.[77]

Anders dan in Nederland wordt in de Deense wet niet gesproken over politiegegevens, maar over persoonsgegevens die worden verwerkt door de politie.[78]

Omzetting van de Richtlijn

Denemarken is lid van de Europese Unie, maar heeft op grond van *The Edinburgh Agreement* op enkele punten opt-outs op het Verdrag van Maastricht. Dit betekent dat Denemarken niet hoeft deel te nemen aan Europese wetgeving op bepaalde beleidsterreinen. Een van de opt-outs ziet op de beleidsterreinen van binnenlandse zaken en justitie. Denemarken was dus niet verplicht om deel te nemen aan de Law Enforcement Directive (LED). Het niet deelnemen aan de LED zou echter als gevolg hebben dat Denemarken geen deel meer zou uitmaken van Europol. Hierom is besloten toch deel te nemen aan de LED.[79] Omdat dit pas laat duidelijk werd, moest de richtlijn in een zeer korte tijd worden omgezet in nationale wetgeving. Binnen een maand was de LED geïmplementeerd.

Mede door de korte implementatieperiode zijn er geen (grote) verschillen tussen de inhoud en tekst van de Act en de LED. Een punt waarop de Act wel afwijkt van de LED is het inzagerecht. Deense autoriteiten die onder de werking van de Act vallen kunnen inzage verzoeken van burgers weigeren en zij hoeven hierbij geen motivering te geven waarom een persoon geen toegang krijgt tot zijn of haar persoonsgegevens. [80]

II.2 De bevoegde autoriteiten

II.2.1 Algemeen

In Denemarken zijn maar een beperkt aantal bevoegde autoriteiten die vallen onder de werking van de LED. Dit zijn de politie, het openbaar ministerie (Prosecution Service), de rechtbanken, de gevangenissen (reclassering), de klachtencommissie politietoezicht (strafrechtelijk onderzoek tegen wetshandhavers) en de rechter-advocaat-generaal (militaire vervolging).[81] Dit zijn de enige zes autoriteiten die als bevoegde autoriteiten worden beschouwd. Alle andere (bestuurs)organen vallen niet onder de werking van de LED maar onder de AVG.

II.2.2 Structuur van de politie

Denemarken was tot 1 januari 2007 opgedeeld in 54 politiezones. In 2006 is een grote politiehervorming doorgevoerd die gevolgen had voor de organisatiestructuur van de politie. De 54 politiezones werden samengevoegd in 12 nieuwe politiedistricten in Denemarken, die elk worden geleid door een commissaris. De commissaris is het hoofd van de politiedienst van het district en is verantwoordelijk voor de uitvoering van politietaken en de gevolgen daarvan.

[77] The police's use of personal data, https://politi.dk/
[78] § 1 Act
[79] Agreement on operational and strategic cooperation between the Kingdom of Denmark and the European Police Office
[80] § 13 jo. §16 Act
[81] § 3 Act.

Alle regionale politiecommissarissen maken deel uit van een gezamenlijk managementteam met aan het hoofd de Landelijk Commissaris van politie. De landelijk commissaris draagt de algemene, professionele, financiële en administratieve verantwoordelijkheid voor de gehele Deense politie en is verantwoording verschuldigd aan de minister van Justitie.

De politie in Denemarken, de Faeröer en Groenland vormt één nationale macht. Groenland en de Faeröer zijn ook onafhankelijke politiedistricten gelegen buiten het land Denemarken, maar binnen het Deense Koninkrijk. In het totaal bestaat de Deense politie dus uit 14 districten, waarvan twee gelegen buiten het Europese grondgebied. Hierom zijn Groenland en de Faeröer derde landen in de zin van de LED.

II.3 Verwerken van politiegegevens

II.3.1 Verkrijgen van politiegegevens

Zoals al eerder benoemd verkrijgt de politie het recht om persoonsgegevens te verwerken en dus ook te verkrijgen in de Act. De politie mag in overeenstemming met deze Act persoonsgegevens verkrijgen wanneer dat nodig is om haar taak uit te voeren. In de praktijk komt dit er op neer dat de politie gegevens mag verkrijgen om strafbare feiten te voorkomen, onderzoeken uit te voeren, personen op te sporen, personen te vervolgen of wanneer er sprake is van een bedreiging voor de openbare veiligheid. Tot slot kan de politie gegevens verkrijgen wanneer dwangmaatregelen worden genomen zoals een arrestatie of het optreden bij ongeregeldheden. Of het nodig is om politiegegevens te verzamelen, wordt bepaald door de individuele politieagent, zaakbehandelaar of officier van justitie. Gesprekspartners geven aan hier veel vrijheid te genieten omdat het vertrouwen in de politie groot is en men begrijpt dat er altijd overbodige data worden verzameld in een onderzoek. Regels hierover zouden de politie niet onnodig moeten hinderen bij het uitvoeren van haar werk. Of dit werkelijk de achterliggende gedachte is, kan in dit onderzoek niet worden onderzocht. Wel laat onderzoek zien dat de Denen een groot vertrouwen hebben in de politie.[82]

Desalniettemin bestaan specifieke wetten die het verkrijgen van speciale soorten data reguleren. Zo worden in de administration of Justice Act aanvullende regels gegeven over het verkrijgen van foto's, bloedmonsters of vingerafdrukken. Gesprekspartners geven aan dat er ongeveer dertig tot veertig van dit soort specifieke wetten en regelingen bestaan. Het kan hier gaan om Europese wetgeving maar ook om nationale wet- en regelgeving. Vaak zien deze wetten niet specifiek op gegevensbescherming of de verwerking door de politie, maar reguleren zij het verzamelen, verkrijgen en/of gebruik van data in het algemeen en daarmee het gebruik van data als bewijsmateriaal door de politie. Zo zijn bijvoorbeeld cctv-camerabewakingssystemen voor privaat gebruik bij wet verboden in Denemarken.[83]

II.3.2 Bewerken van politiegegevens door de bevoegde autoriteiten

Wettelijke regelingen die zien op het verwerken van politiegegevens

De politie mag in overeenstemming met de Act persoonsgegevens verwerken wanneer dat nodig is om haar taak uit te voeren. De inhoud van de Act lijkt sterk op de richtlijn en is op veel punten dus vrij vaag en breed. De politie geniet veel vrijheid bij de invulling van deze

[82] Eurostat, https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=ilc_pw03&lang=en

[83] Lov om forbud mod tv-overvågning mv., jf. lov nr. 278 af 9. juni 1982 med de ændringer, http://www.retsinfo.dk/_GETDOC_/ACCN/A20000007629-REGL

open normen. Doordat de politie hierbij veel vrijheid geniet is er niet snel sprake van bewerken van gegevens, maar spreekt met veelal van verwerken. In de praktijk levert dit weinig tot geen klachten op, volgens gesprekspartners mede doordat de Deense bevolking een groot vertrouwen heeft in de politie. Data lijkt dit te onderbouwen. [84]

De verhouding tussen de verschillende regelingen

Wanneer de politie zich bij de uitvoering van haar taken in een grijs gebied begeeft, worden er ministeriele regelingen vastgesteld om helderheid te geven.[85] Voorbeelden hiervan zijn de executive Order No. 1078 on Police Data Processing in connection with Cross-system Information Analyses en de executive Order No. 1079 of September 20, 2017, on Processing of Personal Data in the Police's Investigation Support Database (PED). Daarnaast bestaan er interne regelingen om verdere invulling te geven aan de regels.

Verwerking in de praktijk

Gesprekspartners geven aan dat de politie een breed mandaat geniet: ''wij leggen de wet niet zo strikt uit dat wij voor ieder soort data een specifieke wettelijke bevoegdheid nodig hebben, wij hanteren een breed noodzakelijkheidsbeginsel.'' Of data verwerkt mogen worden is in Denemarken dus niet afhankelijk van een specifiek doeleinde. De doeleinden in de wet zijn breed en vaag geformuleerd. Wanneer onduidelijkheid bestaat over de noodzakelijkheid van een verwerking/bewerking omdat die niet direct te linken is aan de politietaak (zoals het uitvoeren van informatieanalyses op verschillende systemen), kan dit worden verholpen aan de hand van een ministeriele regeling. Hier wordt de koppeling gemaakt tussen bepaalde, nog steeds ruim geformuleerde, verwerkingsdoelen en de noodzakelijkheid. [86]

II.3.3 Categoriseren en labelen van gegevens

Politiegegevens worden niet of nauwelijks gelabeld en worden ook niet gecategoriseerd. De algemene verplichting uit de Act om over gegevens te beschikken die de data duiden, wordt niet gezien als een verplichting om een gedetailleerde beschrijvingen van data(sets) te hebben. De labeling die plaatsvindt beperkt zich tussen het aanmerken of de data gaan over een slachtoffer, verdachte, dader of andere partij (bijv. getuigen). Gesprekspartners geven aan dat het gedetailleerd labelen van gegevens in de praktijk zo goed als onmogelijk zou zijn omdat dit afhangt van de feiten van de zaak die vaak (nog) niet bekend zijn. Gesprekspartners omschrijven de politiesystemen als gevoelig en geven aan dat zij tekort schieten voor gedetailleerde labeling. Wanneer in een bepaalde case meer gedetailleerde labeling mogelijk zou zijn, zouden de systemen dit niet zonder meer kunnen: ''de casehandelingsystemen zijn gevoelig en daardoor soms inefficiënt.''

De gegevens die door de politie worden verwerkt, dienen te worden gelogd. Hier zijn de systemen van de politie nog niet op toegerust. Om die reden is besloten hier pas in 2023 mee te beginnen. Gesprekpartners geven aan dat dit een risico vormt omdat politiegegevens vaak gevoelige informatie bevatten en nu relatief gemakkelijk misbruikt kunnen worden.

II.3.4 Bewaartermijnen en vernietigingsgronden

Bewaartermijnen

[84] Eurostat, https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=ilc_pw03&lang=en
[85] EDRI 2017 https://edri.org/new-legal-framework-for-predictive-policing-in-denmark/
[86] Zie bijv. art.6 en 7 Executive Order on Police Data Processing in connection with Cross-system Information Analyses

§6 van de Act spreekt over “passende bewaartermijnen”. Deze termijnen worden niet geconcretiseerd. Het is volgens gesprekspartners niet toegestaan om tijdens een lopend strafrechtelijk onderzoek data te verwijderen, omdat dit nog bewijsmateriaal is. Dit heeft als gevolg dat hetzelfde soort data in de ene zaak veel langer kan worden bewaard dan in andere zaken. Gesprekspartners geven aan dat het niet mogelijk is om algemene bewaartermijnen op te stellen doordat zaken teveel van elkaar verschillen. Momenteel beslist de officier van justitie of de commissaris van het district of data al dan niet relevant zijn en bewaard blijven.

Bovenstaande heeft als gevolg dat data afkomstig uit big data sets en open-source intelligence systemen lang bewaard kunnen worden. De data worden momenteel in hun geheel bewaard indien het onderzoek nog loopt. Op dit moment wordt er gewerkt aan een executive order met daarin tijdslimieten wanneer opnieuw moet worden beoordeeld of het nog steeds relevant is om (een deel van) deze gegevens te bewaren.

Er zijn bepaalde categorieën zaken, zoals verkeersboetes, die eenvoudiger te duiden zijn. Met betrekking tot deze gegevens gelden wettelijke beperkingen voor de bewaartermijn van gegevens, ook als de zaak op dat moment niet is afgesloten. Deze beperkingen zijn veelal opgenomen in bijzondere wetten of in ministeriele regelingen. Gesprekspartners geven aan dat er veel van dit soort wetten bestaan.

Vernietigingsgronden

Wanneer over iemand data wordt verwerkt door de politie heeft diegene het recht om bezwaar te maken tegen de verwerking van gegevens door de politie. De wet biedt ook de mogelijkheid om te eisen dat de gegevens worden verwijderd. Dergelijke verzoeken moeten worden gericht aan de Deense nationale politie of de politie in het relevante politiedistrict.

Als er over de aanvrager gegevens worden verwerkt, moet de politie in principe inzage geven in de gegevens en het volgende inzichtelijk maken:

- Het doel van en de wettelijke basis voor de verwerking;
- Op welke wijze de data zijn verzameld;
- Welke partijen toegang hebben tot de data;
- Hoe lang de gegevens worden bewaard of de criteria die bepalen hoe lang de gegevens worden bewaard.

De politie kan een verzoek om inzage weigeren, opschorten of beperken wanneer dit particuliere of openbare belangen zou schaden. In principe moet de politie een reden geven voor de weigering van inzagen en/of vernietiging. De wet biedt echter de mogelijkheid om te volstaan met slechts een weigering. Gesprekspartners geven aan dat er niet veel jurisprudentie bestaat over klachten over de politie en dat dit kan komen door het grote vertrouwen dat de Denen in de politiebestel hebben.

II.3.5 Delen van politiegegevens

Partijen waarmee politiegegevens mogen worden gedeeld

Gesprekspartners geven aan dat er geen strikte regels zijn over het delen van data tussen de politie en andere partijen. Tussen de bevoegde autoriteiten bestaan geen restricties voor het delen van data. De politie mag gegevens delen met andere autoriteiten wanneer dit nodig is voor de succesvolle uitvoering van de taken. Gesprekspartners geven aan dat zich hier eigenlijk geen problemen voordoen. Wel doen zich problemen voor bij het verkrijgen van gegevens van andere autoriteiten dan de bevoegde autoriteiten. Zij verwerken data onder het AVG-regime en zijn vaak terughoudend in het delen van informatie

Afwegingskader

Wanneer de politie gegevens met andere partijen dan de bevoegde autoriteiten wil delen moet de politie altijd een individuele beoordeling maken omdat gegevens worden verzameld met een specifieke rechtsgrond (bijvoorbeeld een gerechtelijk bevel) of voor een specifiek doel (opsporing van misdaad). Er moet dus altijd een individuele beoordeling plaatsvinden of het delen van gegevens noodzakelijk en proportioneel is.

Groenland en Faeröer

Groenland en de Faeröer zijn derde landen in het licht van de EU-wetgeving en daarom kan niet zonder meer worden samengewerkt en informatie worden gedeeld met die gebieden. Denemarken werkt aan de implementatie van voldoende gegevensbeschermingsregels in de overzeese gebieden om een adequaatheidsbesluit van de Europese Commissie te krijgen. Met een adequaatheidsbesluit geeft de Commissie aan dat een derde land een passend beschermingsniveau van de verwerking van persoonsgegevens waarborgt en dat met het land structureel persoonsgegevens kunnen worden uitgewisseld. Op dit moment is dit niet het geval bij Faeröer en Groenland, wat de samenwerking lastig maakt. Of het delen van gegevens met Faeröer en Groenland mag, moet momenteel steeds per individueel geval worden beoordeeld. Gesprekspartners geven aan het frustrerend te vinden niet goed te kunnen samenwerken met de eigen politiemacht omdat die officieel werkzaam is in een derde land.

II.3.6 Technologische aspecten

Omgang met nieuwe technologieën bij het verkrijgen van politiegegevens

De Act zelf gaat niet in op de toepassing van nieuwe technologieën. De wet laat dus ruimte voor de toepassing van nieuwe technologieën. Gesprekspartners geven aan in de praktijk gegevensbeschermingsbeoordelingen uit te voeren als onderdeel van nieuwe aanbestedingsprocessen. Op dit moment wordt bijvoorbeeld een systeem voor gezichtsherkenning getest.

Op het gebied van open-source intelligence wordt op dit moment wetgeving ontwikkeld. Er is een wettelijke grondslag nodig om open-source intelligence grootschalig toe te passen en er bestaat onduidelijkheid over de bewaartermijnen, omdat de informatie niet altijd direct gerelateerd kan worden aan strafrechtelijke onderzoeken. De wetgeving zal een grondslag creëren om open-source intelligence toe te passen als dit de taakuitvoering van de politie bevordert. Ook zal de wetgeving zien op de bewaartermijnen: wanneer moet opnieuw worden beoordeeld of open-source intelligence data nog steeds relevant is.

II.4 Toezicht

II.4.1 De interne en externe toezichthouders

Het interne toezicht Deense nationale politie is belegd bij het centrum voor gegevensbescherming. Het team bestaat uit ongeveer 15-20 medewerkers waarvan het merendeel jurist is. Het centrum denkt actief na bij wetsvoorstellen en adviseert in zaken als het introduceren van nieuwe technologieën, bijvoorbeeld gezichtsherkenning, vingerafdrukken en andere zaken die betrekking hebben op het verwerken van persoonsgegevens door de politie. Daarnaast houdt het centrum zich bezig met het geven van trainingen aan politieagenten, voert het inspecties uit naar gegevensverwerking in de districten en wordt het betrokken bij het in gebruik nemen van nieuwe IT-programma's

De Deense autoriteit voor gegevensbescherming is de onafhankelijke en externe autoriteit die toezicht houdt op de naleving van de regels voor de bescherming van persoonsgegevens in Denemarken. In de LED is geregeld dat de toezichthoudende autoriteiten in alle lidstaten dezelfde taken en feitelijke bevoegdheden te hebben.

Bevoegdheden van de toezichthouders

De bevoegdheden en taken zijn neergelegd in § 40, 41, 42 en 43 van de Act. Wanneer de Deense gegevensbeschermingsautoriteit van mening is dat de politie de gegevens niet correct behandelt, kan zij een onderzoek instellen, corrigerende maatregelen treffen en gevraagd en ongevraagd advies geven. Ook heeft de Deense gegevensbeschermingsautoriteit de taak om het parlement te adviseren, de kennis van bewerkers te bevorderen en ziet zij toe de klachtenafhandeling.

II.4.2 Proces van toezichthouden

Over het proces van toezichthouden valt helaas weinig te zeggen. Er is meerdere malen contact gezocht met de Data Protection Agency, de Deense autoriteit voor gegevensbescherming, maar alle keren werd ons medegedeeld dat het niet mogelijk was om met ons in gesprek te gaan vanwege de drukte, mede gecreëerd door corona. Als alternatief is contact gezocht met het Klachtenbureau Politie, zij hebben een algemenere toezichtstaak bij de politie. Ook hier gaf men aan dat een gesprek niet mogelijk was. Wel is gesproken met het hoofd van het centrum voor gegevensbescherming. Echter, dat centrum houdt zich nauwelijks bezig met toezicht maar richten zij zich voornamelijk op trainingen en het ondersteunen bij het ontwikkelen van wet- en regelgeving.

Een van de gesprekspartners geef aan dat de Data Protection Agency zich in de praktijk vooral richt op de AVG. Omdat de Data Protection Agency niet openstond voor een gesprek hebben wij dit niet kunnen controleren. Echter wekt de website wel deze suggestie. Wanneer men bijvoorbeeld kijkt naar de webpagina van de gegevensbeschermingsautoriteit wordt enkele gerefereerd naar de GDPR en de implementatie wetgeving.

II.5 Lessen voor Nederland

II.5.1 Wettelijk kader

Evenmin als de andere onderzochte landen werkt Denemarken niet met de term ‘politiegegevens’. De Deense wet is bijna letterlijk een vertaling van de richtlijn en ziet dus op de verwerking van persoonsgegevens door bevoegde autoriteiten. Geen van de gesprekspartners gaf aan dat het delen van data met bevoegde autoriteiten problemen oplevert. Het hanteren van de term persoonsgegevens in plaats van politiegegevens lijkt het delen van data gemakkelijker te maken.

Denemarken heeft de Richtlijn geïmplementeerd in de Act. De bewoordingen van de Act zijn bijna gelijk aan die van de richtlijn en nadere invulling is achterwege gelaten. Het gevolg hiervan is dat politie veel vrijheid geniet bij de invulling van deze open normen. Ook lijkt er geen strenge controle (nodig) te zijn. Om te controleren of dit daadwerkelijk zo is, is verder onderzoek is nodig. Indien het vervolg onderzoek het beeld bevestigd en kan verklaren, is dit een interessante les voor Nederland

II.5.2 Overzeese gebieden

Het koninkrijk der Nederlanden heeft net als het koninkrijk Denemarken overzeese gebieden. Denemarken probeert te bewerkstelligen dat er voor de Faeröer eilanden en Groenland een

adequaatheidsbesluit wordt genomen door de Europese Commissie. Op dit moment is dit niet het geval, wat samenwerken lastig maakt. Of het adequaatheidsbesluit er komt en hoe het proces verloopt is interessant voor Nederland, gezien het feit dat zij ook overzeese gebieden heeft waar op dit moment moeilijk mee kan worden samengewerkt.

II.5.3 Gebruik van nieuwe technologieën

Denemarken is op dit moment bezig met de ontwikkeling van een open source intelligence verkrijgingswet. Op dit moment is er nog weinig bekend over de inhoud van deze wet, maar de wet zou mogelijk als inspiratie kunnen dienen voor een soortgelijke wet in Nederland.

Casestudy III: Duitsland/Nordrhein-Westfalen

III.1 Inleiding

Duitsland is geselecteerd omdat het een buurland is van Nederland, waardoor er veel (politionele) samenwerking is. Dan helpt het als de wetgeving (en de uitvoeringspraktijk) op elkaar afgestemd is. Daarnaast heeft Duitsland vanwege het nazi- en Stasiverleden een heel bewuste omgang met privacy. Verder is het interessant om de verhouding tussen Bonds- en Landsrecht te onderzoeken. Daarnaast voldoet Duitsland aan de randvoorwaarde taal/toegankelijkheid. Om het onderzoek behapbaar te houden hebben we ervoor gekozen één Bundesland gedetailleerder te bestuderen. Dit is Nordrhein-Westfalen geworden, omdat het grenst aan Nederland en net zoveel inwoners heeft.

Voor een blik op het relevante Bondsrecht in het 'Wet politiegegevens-domein'[87] hebben we contact gezocht met een wetgevingsambtenaar van het verantwoordelijke Bondsministerie van Binnenlandse Zaken (*Bundesministerium des Innern, für Bau und Heimat*).[88] Deze raadde ons aan ook het *Bundeskriminalamt (BKA)* te betrekken: de federale recherche die verantwoordelijk is voor de politionele samenwerking (en informatiedeling) tussen de deelstaten en internationaal. Daarom hebben we een groepsgesprek gehouden met deze wetgevingsambtenaar en twee medewerkers van het BKA.[89]

In Nordrhein-Westfalen hebben we een groepsgesprek gehouden met:

- Een wetgevingsspecialist bij het verantwoordelijke ministerie van Binnenlandse Zaken[90]

[87] Lastig voor de afbakening van het onderzoek is het feit dat de onderzochte landen het begrip 'politiegegevens' niet kennen. Zij gaan uit van de bescherming en verwerking van *persoonsgegevens*. In Duitsland bestond er, zoals we in deze casestudy uiteenzetten, al wel veel wet- en regelgeving over de verwerking van persoonsgegevens door de politie en andere bevoegde autoriteiten in het kader van de politietaken. Met de omzetting van de Europese Richtlijn gegevensbescherming opsporing en vervolging is de scope/terminologie daaraan aangepast, maar dit past niet één op één op het toepassingsbereik van de Nederlandse Wpg.

[88] Afdeling ÖS I 3, Polizeiliches Informationswesen; Datenschutz im Sicherheitsbereich; Bundeskriminalamt-Gesetz.

[89] De afdelingsleider en een senior medewerker van de adviesafdeling voor politiepraktische rechtsvragen en rechtspolitiek.

[90] Ministerium des Innern des Landes Nordrhein-Westfalen – Leitender Ministerialrat, stellv. Gruppenleiter Gruppen 43 - o.a. Recht der Polizei.

- De functionaris gegevensbescherming en eerste hoofdcommissaris bij het Landeskriminalamt Nordrhein-Westfalen (elke deelstaat heeft een Landeskriminalamt, dat de schakel is tussen de deelstaatpolitie en het BKA)[91]
- Een medewerker van de afdeling Internationale politionele samenwerking bij het ministerie van Binnenlandse Zaken, ook eerste hoofdcommissaris bij de politie[92]
- Het hoofd van de afdelingen Criminaliteitspreventie en Internationale politionele samenwerking bij het ministerie van Binnenlandse Zaken[93] (vooral toehoorder)

Daarnaast was als toehoorder de Nederlandse 'contactambtenaar' aanwezig tussen de Nederlandse politie en het Landeskriminalamt Nordrhein-Westfalen (deze is werkzaam bij de Nederlandse Nationale Politie).

Tot slot hebben we gesproken met een hoogleraar aan de Deutsche Hochschule der Polizei.[94]

Het aantal gesprekspartners is dus, net als in alle casestudy's, beperkt; een belangrijke kanttekening bij de bevindingen uit de interviews. Deze geven mogelijk geen volledig beeld van de (visie op de) praktijk.

Hieronder gaan we eerst in op het wettelijk kader (paragraaf III.2) en vervolgens op de bevoegde autoriteiten en in het bijzonder op de politie (paragraaf III.3). In paragraaf III.4 komen de verschillende aspecten van verwerking van politiegegevens aan bod: na een algemene opmerking (paragraaf III.4.1) bespreken we verkrijgen (paragraaf III.4.2), bewerken (paragraaf III.4.3), categoriseren en labelen (paragraaf III.4.4), bewaartermijnen en vernietigingsvoorwaarden (paragraaf III.4.5) en verstrekken/delen (paragraaf III.4.6). Paragraaf III.5 gaat over het toezicht en in paragraaf III.6 doen we een voorzet voor wat Nederland van Duitsland/Nordrhein-Westfalen zou kunnen leren. Hierbij houden we zoveel mogelijk dezelfde volgorde aan: eerst Bondsniveau, vervolgens wetgeving die voor zowel Bond als Länder geldt en dan Landsniveau (Nordrhein-Westfalen). Net zoals bij de andere landenstudies hebben we ons, in ieder geval wat de interviews betreft, grotendeels beperkt tot de politie en gaan we dus niet uitgebreid in op de andere bevoegde autoriteiten onder de Richtlijn gegevensbescherming opsporing en vervolging.

III.2 Wettelijk kader

III.2.1 Wettelijk systeem

Wetgevingssystematiek

Duitsland heeft als federatie (bondsstaat) zowel wetgeving op Bondsniveau als op het niveau van de zestien Länder, waaronder Nordrhein-Westfalen (NRW). Dit geldt ook voor de wetgeving over bescherming van persoonsgegevens (*Datenschutz*) en de verwerking daarvan door

[91] Landeskriminalamt NRW – Erster Kriminalhauptkommissar, Datenschutzbeauftragter.
[92] Ministerium des Innern des Landes Nordrhein-Westfalen – Erster Polizeihauptkommissar, Referat 425 (Internationale Polizeiliche Zusammenarbeit).
[93] Ministerium des Innern des Landes Nordrhein-Westfalen – Leitender Kriminaldirektor; Leiter Referat 424 (Kriminalprävention) und Referat 425 (Internationale Polizeiliche Zusammenarbeit).
[94] Sprecher der Lehrenden, Fachgebietsleiter Fachgebiet III.4 – Öffentliches Recht mit Schwerpunkt Polizeirecht; Department III – Kriminal- und Rechtswissenschaften, Vorsitzender der Ethik-Kommission; Deutsche Hochschule der Polizei.

de politie. Op grond van de artikelen 30[95] en 70-74 van de Grondwet (Grundgesetz, GG), die de verdeling van de wetgevende bevoegdheid regelt, zijn de Länder bevoegd voor zover de Grondwet niet anders regelt. Daarom hebben de Länder wetgevingsbevoegdheid voor de politie (hierna te bespreken uitzonderingen daargelaten). Er is 'concurrerende wetgevingsbevoegdheid' over onder meer het strafrecht. Dat betekent dat de Länder bevoegd zijn, zolang de Bond niet van zijn bevoegdheid gebruik gemaakt heeft. De Bond heeft volgens art. 73 GG 'uitsluitende wetgevingsbevoegdheid' over onder meer:

- Douane en grensbewaking
- Het luchtverkeer
- Het spoorbaanverkeer over Bondsspoorbanen
- Afweer van gevaren van internationaal terrorisme door het Bundeskriminalamt in geval van Länderoverstijgend gevaar, als geen Landspolitie-eenheid duidelijk bevoegd is of het hoogste gezag in een Land om overname verzoekt
- Samenwerking van Bond en Länder
  - in de recherche (*Kriminalpolizei*)
  - bij bescherming tegen activiteiten op het grondgebied van de Bond die de externe belangen van Duitsland in gevaar brengen
  - bij het instellen van een Bundeskriminalamt en internationale criminaliteitsbestrijding

De Länder mogen over deze onderwerpen alleen wetgeving maken als een Bondswet ze daartoe uitdrukkelijk machtigt. Deze en enkele andere bepalingen in de Grondwet vormen de basis voor het Bundeskriminalamt (BKA, de federale recherche) en de Bundespolizei (voornamelijk grens- en spoorbaanpolitie). Daarnaast is er nog een *Polizei beim Deutschen Bundestag*, die het parlement beschermt. Daarmee zijn er drie politiediensten op Bondsniveau (zie verder paragraaf III.3). Omdat deze casestudy focust op NRW in relatie tot Bondsrecht, hebben we op Bondsniveau behalve met het verantwoordelijke ministerie (het Bundesministerium des Innern, Bondsministerie van Binnenlandse Zaken) alleen met het BKA gesproken. Het BKA is namelijk verantwoordelijk voor de politionele samenwerking tussen Länder (met elk een Landeskriminalamt, LKA), Bond en buitenland op het gebied van Länderoverstijgende en internationale criminaliteit. Hierna gaan we daarom vooral in op het BKA en de politie in NRW.

Achtergrond privacybescherming

Duitsland hecht vanwege de twintigste-eeuwse geschiedenis veel waarde aan de (wettelijke) bescherming van de privacy. Dit komt tot uiting in de zeer gedetailleerde wetgeving en strenge controle door het grondwettelijk hof, het Bundesverfassungsgericht (BVerfG). In 1983 heeft het BVerfG in het Volkstellingsarrest een grondrecht in het leven geroepen dat niet in de grondwet staat:[96] het *Grundrecht auf Informationelle Selbstbestimmung* (grondrecht op informationele zelfbeschikking).[97] Het betekent dat een ieder het recht heeft zelf te beslissen wat er met zijn persoonsgegevens gebeurt. Sindsdien staat wat privacy betreft het handelen van de overheid, waaronder de politie, maar ook van private partijen onder streng toezicht van het BVerfG en is de politie zo mogelijk nog meer *privacy-minded* geworden, blijkt uit de interviews. De Duitse privacywetgeving is volgens een van de gesprekspartners vanwege het hoge beschermingsniveau zelfs als voorbeeld genomen voor het Europeesrechtelijke kader.

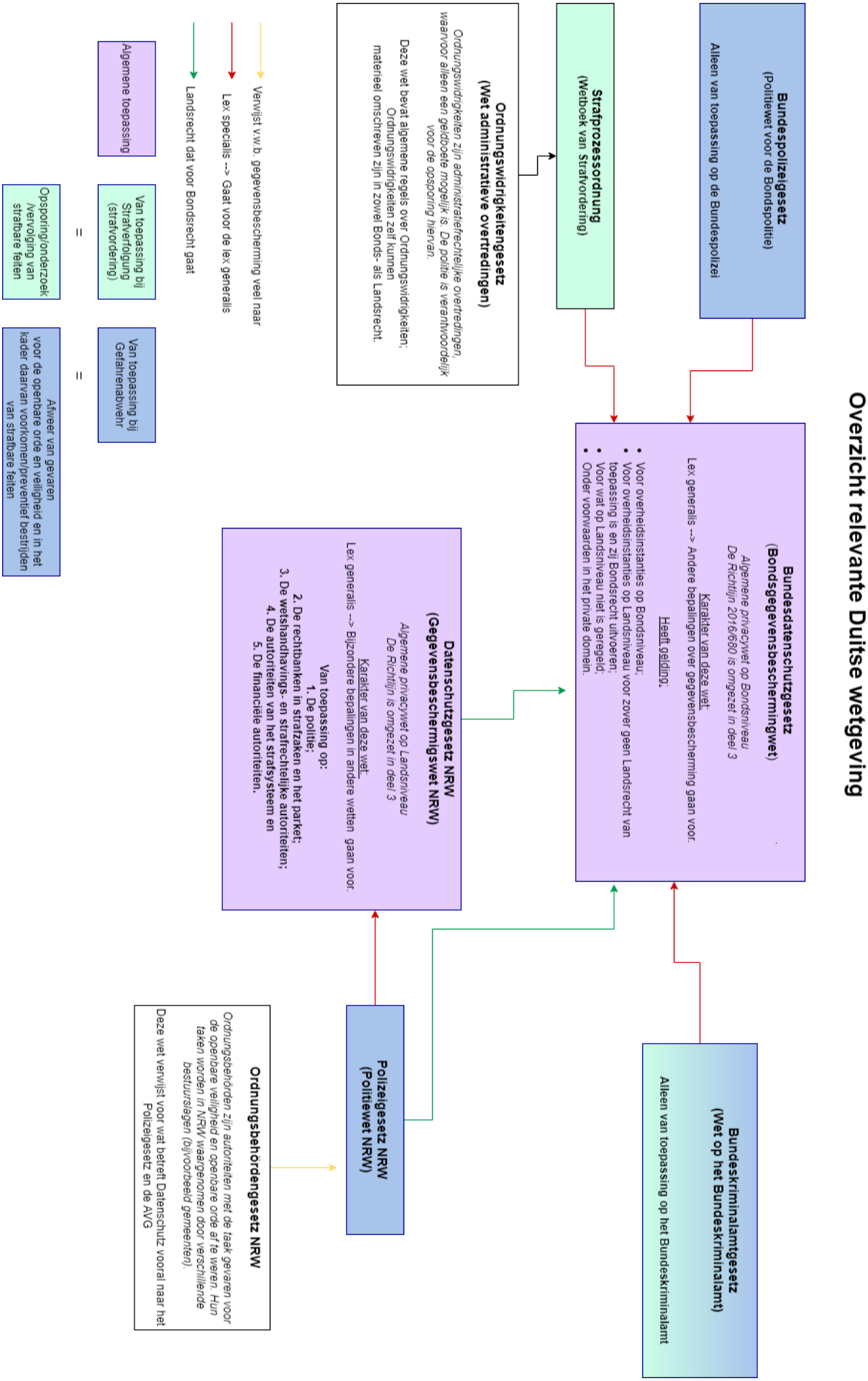
[95] De uitoefening van staatsbevoegdheden en de uitvoering van overheidstaken is zaak van de Länder, voor zover deze Grondwet geen andere regeling treft of toelaat.

[96] BVerfG 15 december 1983, ECLI:DE:BVerfG:1983:rs19831215.1bvr020983 (*Volkszählungsurteil*).

[97] Overigens staat een grondrecht op bescherming van persoonsgegevens (*Grundrecht auf Datenschutz*) wel in de grondwetten van veel Länder, waaronder NRW (art. 4 lid 2 Verfassung für das Land Nordrhein-Westfalen).

Omdat *Datenschutz* (gegevensbescherming) een complex en veelomvattend begrip is, is de wetgevingsbevoegdheid hierover niet eenduidig aan Bund of Länder toebedeeld[98] en zijn op beide niveaus verschillende wetten en bepalingen in bijzondere wetten over gegevensbescherming te vinden. Waar nodig zijn of worden de AVG en de Richtlijn in al deze wetten geïmplementeerd.

[98] Zie bijvoorbeeld BVerfG 2 maart 2010, ECLI:DE:BVerfG:2010:rs20100302.1bvr025608.


Overzicht relevante Duitse wetgeving
Bundespolizeigesetz
(Politiewet voor de Bondspolitie)
Alleen van toepassing op de Bundespolizei
Strafprozessordnung
(Wetboek van Strafvordering)
Ordnungswidrigkeitengesetz
(Wet administratieve overtredingen)
Ordnungswidrigkeiten zijn administratiefrechtelijke overtredingen, waarvoor alleen een geldboete mogelijk is. De politie is verantwoordelijk voor de opsporing hiervan.
Deze wet bevat algemene regels over Ordnungswidrigkeiten; Ordnungswidrigkeiten zelf kunnen materieel omschreven zijn in zowel Bonds- als Landsrecht.
Bundesdatenschutzgesetz
(Bondsgegevensbeschermingwet)
Algemene privacywet op Bondsniveau
De Richtlijn 2016/680 is omgezet in deel 3
Karakter van deze wet:
Lex generalis --> Andere bepalingen over gegevensbescherming gaan voor.
Heeft gelding:
Voor overheidsinstanties op Bondsniveau;
Voor overheidsinstanties op Landsniveau voor zover geen Landsrecht van toepassing is en zij Bondsrecht uitvoeren;
Voor wat op Landsniveau niet is geregeld;
Onder voorwaarden in het private domein.
Datenschutzgesetz NRW
(Gegevensbeschermigswet NRW)
Algemene privacywet op Landsniveau
De Richtlijn is omgezet in deel 3
Karakter van deze wet:
Lex generalis --> Bijzondere bepalingen in andere wetten gaan voor.
Van toepassing op:
1. De politie;
2. De rechtbanken in strafzaken en het parket;
3. De wetshandhavings- en strafrechtelijke autoriteiten;
4. De autoriteiten van het strafsysteem en
5. De financiële autoriteiten.
Bundeskriminalamtgesetz
(Wet op het Bundeskriminalamt)
Alleen van toepassing op het Bundeskriminalamt
Polizeigesetz NRW
(Politiewet NRW)
Ordnungsbehördengesetz NRW
Ordnungsbehörden zijn autoriteiten met de taak gevaren voor de openbare veiligheid en openbare orde af te weren. Hun taken worden in NRW waargenomen door verschillende bestuurslagen (bijvoorbeeld gemeenten).
Deze wet vervijst voor wat betreft Datenschutz vooral naar het Polizeigesetz en de AVG
Vervijst v.w.b. gegevensbescherming veel naar
Lex specialis --> Gaat voor de lex generalis
Landsrecht dat voor Bondsrecht gaat
Algemene toepassing
Van toepassing bij Strafverfolgung (strafvordering)
Van toepassing bij Gefahrenabwehr
=
=
Opsporing/onderzoek /vervolging van strafbare feiten
Afweer van gevaren voor de openbare orde en veiligheid en in het kader daarvan voorkomen/preventief bestrijden van strafbare feiten

Gegevensbescherming en politierecht

In Duitsland is de politietaak heel duidelijk gesplitst in twee onderdelen: een repressieve (*Strafverfolgung*; opsporing/onderzoek/vervolging van strafbare feiten) en een preventieve (*Gefahrenabwehr*, de afweer van gevaren voor de openbare veiligheid of orde en het voorkomen/preventief bestrijden van strafbare feiten in het kader daarvan). Met *Gefahrenabwehr* zijn de politie en de Ordnungsbehörden belast. *Ordnungsbehörden* zijn autoriteiten met de taak gevaren voor de openbare veiligheid en openbare orde af te weren, ook wel aangeduid als *Verwaltungspolizei* (bestuur(srechte)lijke politie).[99] Regels over de Ordnungsbehörden staan in wetten op Landsniveau, zoals in Nordrhein-Westfalen de Ordnungsbehördengesetz NRW. Deze verwijst voor wat betreft gegevensbescherming vooral naar de Politiewet NRW en de AVG.

Dit onderscheid tussen preventief en repressief politiehandelen is van belang voor de maatregelen die de politie mag nemen en in welke wet zij daarvoor moet kijken, en dus voor de doelbinding en daarmee de rechtmatigheid van gegevensverwerking door de politie. *Strafverfolgung* is hoofdzakelijk geregeld in de Strafprozessordnung (StPO, Wetboek van Strafvordering), een wet op Bondsniveau.[100] *Gefahrenabwehr* is geregeld in de politiewetten van de Länder en de afzonderlijke wetten over de Bondspolitiediensten. Zie bijvoorbeeld art. 1 lid 1 Polizeigesetz (Politiewet) NRW, waarin de *Gefahrenabwehr*-taak uitvoerig is omschreven. Deze omvat de afweer van gevaren voor de openbare orde en veiligheid, het in het kader van deze taak voorkomen en preventief bestrijden van strafbare feiten, en het treffen van voorbereidingen voor hulpverlening en het handelen in geval van gevaar voor de openbare orde en veiligheid.

Het scherpe onderscheid tussen deze twee politietaken was zeer problematisch bij het omzetten van de Richtlijn gegevensbescherming opsporing en vervolging, omdat de Richtlijn (in de Duitse vertaling) zowel *Gefahrenabwehr* als *Strafverfolgung* in één adem noemt (art. 1 lid 1): '*durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.*' De Richtlijn lijkt dus *Gefahrenabwehr* als een onderdeel van *Strafverfolgung* te zien, terwijl dit in Duitsland twee verschillende, in de tijd opvolgende zaken zijn.

In de wet op het Bundeskriminalamt (BKA-Gesetz) en in de Politiewet NRW zijn de politietaken gedetailleerder omschreven dan in art. 3 van de Nederlandse Politiewet 2012 (art. 4 over de taken van de Kmar is dan weer wel specifieker). Het bereik van de Nederlandse Wet politiegegevens (Wpg) hangt samen met de politietaak en is niet gelijk aan dat van de Europese Richtlijn gegevensbescherming opsporing en vervolging; Nederland heeft immers ook een Wet justitiële en strafvorderlijke gegevens, waarin de Richtlijn is omgezet. Ook dit was een uitdaging bij het bepalen van de scope van het onderzoek in de andere landen. De politie van Nordrhein-Westfalen heeft bijvoorbeeld ook expliciet hulpverlening bij de tenuitvoerlegging van sancties als taak (art. 1 lid 3 Politiewet NRW). In deze casestudy zullen we vooral ingaan

[99] Zie bijvoorbeeld art. 3 Ordnungsbehördengesetz NRW, dat bepaalt dat de taken van de Ordnungsbehörden worden waargenomen door verschillende bestuurslagen: gemeenten, *Kreise* en 'kreisvrije' steden, en *Bezirksregierungen* (districts-/provincieregeringen).

[100] En in de Gesetz über Ordnungswidrigkeiten (Ordnungswidrigkeitengesetz), eveneens een Bondswet. *Ordnungswidrigkeiten* zijn bestuursrechtelijke overtredingen die alleen met een geldboete bestraft kunnen worden. Zie verder paragraaf III.3 over de bevoegde autoriteiten. De Ordnungswidrigkeitengesetz verwijst voor wat betreft gegevensbescherming overigens hoofdzakelijk naar het Wetboek van Strafvordering.

op *Gefahrenabwehr* en *Strafverfolgung* en zoveel mogelijk aansluiten bij het Nederlandse Wpg-domein.

III.2.2 Overzicht wetgeving

Hierna bespreken we kort de belangrijkste relevante wetten op Bondsniveau en in Nordrhein-Westfalen; zie ook het schema in paragraaf III.2.1. Ter illustratie en verduidelijking hebben we in bijlage 3 inhoudsopgaven opgenomen van relevante delen van de Politiewet NRW en de Wet op het Bundeskriminalamt.

Bond

De volgende Bondswetten zijn van grote invloed op het verwerken van politiegegevens:

- Wetboek van Strafvordering (Strafprozessordnung (StPO))
- Bundesdatenschutzgesetz (BDSG, Bondsgegevensbeschermingswet)
- Bundespolizeigesetz (politiewet voor de Bondspolitie)
- Bundeskriminalamtgesetz (BKA-Gesetz, Wet op het Bundeskriminalamt)

De Bundesdatenschutzgesetz is de algemene privacywet op Bondsniveau. Deze bestaat al sinds 1978 en is in 2018 aangepast aan het Europeesrechtelijke privacykader. In Deel 3 is de Richtlijn gegevensbescherming opsporing en vervolging omgezet. Van belang is dat de BDSG een *lex generalis* is; andere bepalingen over gegevensbescherming van de Bond (zoals die in het BKA-gesetz) gaan voor (art. 1 lid 2 BDSG). De wet geldt voor overheidsinstanties op Bondsniveau (zoals de Bondspolitiediensten) en op Landsniveau voor zover geen Landsrecht van toepassing is en zij Bondsrecht uitvoeren (art. 1 lid 1 BDSG).[101] Ook voor wat op Landsniveau niet geregeld is, geldt de BDSG. Daarnaast geldt de BDSG – onder een aantal voorwaarden – ook in het private domein (art. 1 lid 1, tweede zin e.v.).

Van het BKA-gesetz zijn vooral de volgende hoofdstukken relevant: hoofdstuk 1 (Centrale voorzieningen voor samenwerking in rechercheaangelegenheden; Taken van het Bundeskriminalamt), 2 (Algemene bevoegdheden voor gegevensverwerking), 3 (Centrale dienst), 4 (Bevoegdheden in het kader van *Strafverfolgung*), 5 (Bevoegdheden voor afweer van gevaren van internationaal terrorisme), 9 (Gegevensbescherming en veiligheid van gegevens; Rechten van betrokkenen) en 10 (Slotbepalingen, met art. 89 (inperking van grondrechten)).

In de Bundespolizeigesetz is gegevensbescherming (vooral) geregeld in art. 21-28a (verzameling van gegevens) en 29-37 (verwerking en gebruik van gegevens). De Richtlijn gegevensbescherming opsporing en vervolging is nog niet omgezet in de Bundespolizeigesetz.[102] Wel geldt de algemene omzettingsregeling uit (deel 1 en 3 van) de Bundesdatenschutzgesetz. Om deze reden, maar vooral omwille van afbakening van het onderzoek en onze focus op Nordrhein-Westfalen in relatie tot Bondsrecht, gaan we in deze casestudy niet gedetailleerd in op de Bundespolizei en de Bundespolizeigesetz.

Nordrhein-Westfalen

In NRW wordt de verwerking van politiegegevens vooral gereguleerd door:

- Datenschutzgesetz NRW (Gegevensbeschermingswet, DSG NRW)

[101] 'oder b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.'

[102] Zie bijvoorbeeld de website van de Duitse toezichthoudende autoriteit op Bondsniveau, de Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI): BfDI, *Umsetzung der JI-Richtlinie in Deutschland*, www.bfdi.bund.de (laatst geraadpleegd op 2 oktober 2020).

- Polizeigesetz (Politiewet) NRW[103]

Volgens de geïnterviewden bij het Ministerium des Innern (Binnenlandse Zaken) NRW, waaronder het Landeskriminalamt en de politie van NRW vallen, zijn de gegevensbeschermingswetten en politiewetten van de zestien Länder redelijk vergelijkbaar met elkaar en met de wetgeving op Bondsniveau. Er heeft ook onderlinge afstemming plaatsgevonden, bijvoorbeeld over het omzetten van de Richtlijn. Sommige Länder hebben de Richtlijn echter nog niet (helemaal) omgezet. NRW heeft dit wel gedaan; in december 2018 zijn de Datenschutzgesetz en het Polizeigesetz beide aangepast. Men is ook bezig met het ontwikkelen van een 'Musterpolizeigesetz' voor Duitsland: een blauwdruk om de politiewetten van de Länder verder te harmoniseren. Hierop is kritiek van belangenbehartigers op het gebied van privacy. Zij zijn van mening dat de politiewetten door de jaren heen te veel worden aangescherpt. In het ene Land heeft de politie meer bevoegdheden dan in het andere en zij vrezen voor (verdere) inbreuk op/inperking van grondrechten als een van de politiewetten met ruime politiebevoegdheden als blauwdruk voor alle Länder wordt genomen; politierecht is volgens het federale systeem georganiseerd (dat wil zeggen, met veel autonomie en discretionaire ruimte voor de Länder) en dat moet zo blijven.[104]

Net als in de Bundesdatenschutzgesetz bevat de Datenschutzgesetz van NRW een Deel 3 met de implementatie van Richtlijn 2016/680. Ook hier hebben bijzondere bepalingen in andere wetten voorrang (art. 35 lid 3 DSG NRW).

De Politiewet NRW kent in hoofdstuk 2 (Politiebevoegdheden) een uitgebreide afdeling (onderafdeling 2) over gegevensverwerking. Belangrijk is dat deze alleen van toepassing is op preventief politiehandelen dat als *Gefahrenabwehr* kan worden gekwalificeerd; voor repressieve *Strafverfolgung* geldt het Wetboek van Strafvordering. Er is dus geen aparte wet over politiegegevens; men heeft geprobeerd alles wat de politie betreft zoveel mogelijk in de politiewet te regelen.

Slotsom

Vanwege de federale structuur en een aantal historisch gegroeide verschijnselen (zoals de strikte scheiding tussen preventief en repressief politiehandelen en de intensieve controle door het Bundesverfassungsgericht op het waarborgen van grondrechten) hebben de bevoegde autoriteiten in Duitsland te maken met een groot aantal regelingen en jurisprudentie waarmee ze rekening moeten houden. Naast de hierboven genoemde wetten zijn er ook wetten op specifieke terreinen die het politiehandelen (waaronder het verzamelen en verwerken van persoonsgegevens) inperken, zoals de *Versammlungsgesetz*, die het recht van vergadering en betoging garandeert en in dat kader de politiebevoegdheden vergaand begrenst.[105]

[103] Er zijn ook Verwaltungsvorschriften zum Polizeigesetz (vergelijkbaar met AMvB's), alleen die zijn nog niet aangepast aan het Europese kader voor gegevensbescherming en konden dus volgens een van de gesprekspartners beter niet worden meegenomen in dit onderzoek.

[104] Zie bijvoorbeeld Digitalcourage, *Musterpolizeigesetz,* www.digitalcourage.de/musterpolizeigesetz (laatst geraadpleegd op 20 augustus 2020).

[105] Er is nu alleen nog een *Versammlungsgesetz* op Bondsniveau; Nordrhein-Westfalen werkt aan een op Landsniveau.

III.3 De bevoegde autoriteiten

III.3.1 Algemeen

Omdat in Duitsland de politietaak hoofdzakelijk is toebedeeld aan de politiediensten en de *Ordnungsbehörden*, heeft Duitsland minder dan andere landen het probleem van een veelheid aan (mogelijke) bevoegde autoriteiten, in elk geval binnen het bereik van verwerking van politiegegevens.

Bundesdatenschutzgesetz

Art. 45 BDSG bepaalt het toepassingsbereik van Deel 3 van de Bundesdatenschutzgesetz (het deel waarin de Richtlijn is omgezet). Hierin zijn de bevoegde autoriteiten niet opgesomd; het artikel volgt min of meer de bewoordingen van art. 1 Richtlijn en de definitie van art. 3 sub 7 Richtlijn.

Gezien het toepassingsbereik van de BDSG (overheden op Bondsniveau) zijn de belangrijkste bevoegde autoriteiten op Bondsniveau voor wat betreft de voorkoming (*Verhütung*), het onderzoek (*Ermittlung*) en de opsporing (*Aufdeckung*) van strafbare feiten (dus op het gebied van politiegegevens/de scope van dit onderzoek) de Bundespolizei, het BKA en de politie voor de Bondsdag.

In Duitsland zijn ook *Ordnungswidrigkeiten* onder het bereik van dit deel van de BDSG (en dus de Richtlijn) gebracht. Dit is een begrip dat de meeste andere lidstaten niet op die manier kennen. De Richtlijn spreekt alleen van strafbare feiten, 'met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid' – een zinsdeel dat in Duitsland ondanks de bezwaren vanwege de tweeledige politietaak (*Gefahrenabwehr* en *Strafverfolgung*) min of meer letterlijk is overgenomen. Ordnungswidrigkeiten zijn administratiefrechtelijke overtredingen, waarvoor alleen een geldboete mogelijk is. Het Ordnungswidrigkeitenrecht wordt wel het 'kleine broertje' van het Duitse strafrecht genoemd. Volgens de artikelsgewijze toelichting ondersteunt overweging 13 bij de Richtlijn[106] de toepassing van de Richtlijn op Ordnungswidrigkeiten en wordt hiermee eenheid in de regelgeving over politionele gegevensverwerking bereikt.[107] Algemene regels over Ordnungswidrigkeiten staan in de Ordnungswidrigkeitenwet (op Bondsniveau); Ordnungswidrigkeiten zelf kunnen materieel omschreven zijn in zowel Bonds- als Landsrecht. De bevoegde autoriteiten voor de vervolging en afdoening van Ordnungswidrigkeiten zijn de *Verwaltungsbehörden*[108] (bestuursorganen op verschillende niveaus en beleidsterreinen, van Landsregeringen tot gemeentelijke bestuursorganen en *Gesundheidsämter*, *Finanzämter* etc.). De politie is belast met de opsporing van Ordnungswidrigkeiten (art. 53 Ordnungswidrigkeitengesetz). Het Wetboek van Strafvordering is, met een aantal uitzonderingen, van toepassing op Ordnungswidrigkeiten (art. 46 Ordnungswidrigkeitengesetz).

[106] Een strafbaar feit in de zin van deze richtlijn moet een autonoom Unierechtelijk begrip zijn zoals uitgelegd door het Hof van Justitie van de Europese Unie.

[107] Wetsontwerp aanpassing BDSG (Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)), p. 110 (artikelsgewijze toelichting, toelichting bij art. 45).

[108] Art. 35 Ordnungswidrigkeitengesetz; voor zover op grond van die wet niet het OM (Staatsanwaltschaft) of in zijn plaats de rechter bevoegd is.

Datenschutzgesetz NRW

Zuständige Behörde (bevoegde autoriteit) wordt in art. 36 sub 8 DSG NRW gedefinieerd in algemene bewoordingen die overeenkomen met die van de Richtlijn; ook hier betreft het de opsporing, vervolging etc. van zowel *Straftaten* als *Ordnungswidrigkeiten*.

Art. 35 DSG NRW wijst als bevoegde autoriteiten aan, in het kader van hun taken uit art. 1 lid 1 Richtlijn[109]:

1. De politie
2. De gerechten in strafzaken en het OM
3. De tenuitvoerleggingsautoriteiten
4. De autoriteiten belast met de voltrekking van maatregelen
5. De financiële autoriteiten (*Finanzverwaltung*)

Voor *Ordnungsbehörden* geldt dit deel van de Gegevensbeschermingswet NRW voor zover zij *Ordnungswidrigkeiten* vervolgen en afdoen en/of sancties voltrekken.

III.3.2 Structuur van de politiediensten

Bondsniveau

Bundespolizei en politie voor de Bondsdag

De taken van de Bundespolizei staan in art. 1-13 Bundespolizeigesetz (Wet op de Bondspolitie). Ze is van oorsprong vooral grens-, spoorbaan- en luchthavenpolitie, maar heeft er door de jaren heen meer taken en personeel bij gekregen. Zoals gezegd is Richtlijn 2016/680 nog niet geïmplementeerd in de politiewet voor de Bundespolizei. De Bondsdagpolitie beschermt de Bondsdag, het parlement op Bondsniveau. We laten de Bundespolizei en de politie voor de Bondsdag verder buiten beschouwing.

Bundeskriminalamt (BKA)

Art. 1 BKA-Gesetz (Wet op het Bundeskriminalamt) roept een systeem van Bundeskriminalamt en Landeskriminalämter in het leven, om samenwerking tussen Bond en Länder op recherchegebied te bewerkstelligen. Elk Land heeft in principe een Landeskriminalamt, maar het is ook mogelijk om met meerdere Länder samen een Landeskriminalamt te onderhouden. Belangrijk is dat *Strafverfolgung* en *Gefahrenabwehr* – de politietaken – Landsaangelegenheid blijven, tenzij wettelijk anders bepaald is.

[109] Eventuele andere taken van deze autoriteiten vallen dus niet onder de Richtlijn en onder dit deel van de DSG NRW.

In de artikelen 2-8 zijn de taken van de BKA uitgewerkt: functie van *Zentralstelle* (centrale dienst) voor politionele samenwerking bij Länderoverstijgende, internationale of grootschalige criminaliteit (art. 2), internationale samenwerking (art. 3), *Strafverfolgung* (art. 4),[110] *Gefahrenabwehr* van internationaal terrorisme (art. 5),[111] beveiliging van leden van *Verfassungsorgane* en de BKA-leiding (art. 6), getuigenbescherming (art. 7), bescherming/beveiliging eigen eigendommen etc. (art. 8).

Nordrhein-Westfalen

De politieorganisatie in NRW is geregeld in de Polizeiorganisationsgesetz NRW (Politieorganisatiewet NRW) en ziet er als volgt uit.

[110] '(1) Das Bundeskriminalamt nimmt die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung wahr
1. in Fällen des international organisierten ungesetzlichen Handels mit Waffen, Munition, Sprengstoffen, Betäubungsmitteln, neuen psychoaktiven Stoffen oder Arzneimitteln und der international organisierten Herstellung oder Verbreitung von Falschgeld, die eine Sachaufklärung im Ausland erfordern, sowie damit im Zusammenhang begangener Straftaten einschließlich der international organisierten Geldwäsche,
2. in Fällen von Straftaten, die sich gegen das Leben (…) oder die Freiheit (…) des Bundespräsidenten, von Mitgliedern der Bundesregierung, des Deutschen Bundestages und des Bundesverfassungsgerichts oder der Gäste der Verfassungsorgane des Bundes aus anderen Staaten oder der Leitungen und Mitglieder der bei der Bundesrepublik Deutschland beglaubigten diplomatischen Vertretungen richten, wenn anzunehmen ist, dass der Täter aus politischen Motiven gehandelt hat und die Tat bundes- oder außenpolitische Belange berührt, (…)' Sub 3-6 sommen nog een aantal gevallen op, zoals bij internationaal georganiseerde misdaden. Op grond van lid 2 neemt het BKA daarnaast politietaken op het gebied van Strafverfolgung waar als Landsautoriteiten, het Bondsministerie van Binnenlandse Zaken of de Generalbundesanwalt (federale aanklager) daarom verzoeken/daartoe opdracht geven.

[111] Opnieuw alleen in gevallen met een Länderoverstijgende component of als een Land daarom verzoekt.

Ministerium des Innern NRW

Kreispolizeibehörden

§ 4 KHSt-VO	§ 2 KHSt-VO		
PP Bielefeld[1]	PP Bielefeld	LR Gütersloh LR Herford LR Höxter	LR Lippe LR Minden-Lübbecke LR Paderborn
PP Dortmund[1]	PP Dortmund	PP Hamm LR Hochsauerlandkreis	LR Soest LR Unna
	PP Bochum		
	PP Hagen	LR Ennepe-Ruhr-Kreis LR Märkischer Kreis	LR Olpe LR Siegen-Wittgenstein
PP Düsseldorf[1]	PP Düsseldorf	LR Mettmann	LR Rhein-Kreis Neuss
	PP Mönchengladbach	LR Viersen	
	PP Wuppertal		
PP Essen	PP Essen	PP Oberhausen	
	PP Duisburg[2]	LR Wesel	
	PP Krefeld	LR Kleve	
PP Köln[1]	PP Köln	LR Rhein-Erft-Kreis LR Rheinisch-Bergischer-Kreis	LR Oberbergischer Kreis
	PP Aachen	LR Düren	LR Heinsberg
	PP Bonn	LR Euskirchen	LR Rhein-Sieg-Kreis
PP Münster[1]	PP Münster	LR Borken LR Coesfeld	LR Steinfurt LR Warendorf
	PP Gelsenkirchen		
	PP Recklinghausen		

Landesoberbehörden

LAFP NRW
Landesamt für Ausbildung, Fortbildung und Personalangelegenheiten der Polizei NRW

LKA NRW
Landeskriminalamt NRW

LZPD NRW
Landesamt für Zentrale Polizeiliche Dienste NRW

Legende:

[1] PP mit Autobahnpolizei

[2] PP met Wasserschutzpolizei

PP betekent Polizeipräsidium; LR betekent Landesrat.

Bron: www.polizei.nrw.

III.4 Verwerken van politiegegevens

III.4.1 Algemeen

In algemene zin merkt de geïnterviewde hoogleraar aan de Deutsche Hochschule der Polizei op dat de Duitse wetgever de wetgeving 'technologieneutraal' heeft willen formuleren om ruimte te laten voor nieuwe ontwikkelingen, maar dat de wetgeving (net als in Nederland op dit moment) nog erg gericht is op het verwerken van kleine hoeveelheden gegevens in enkelvoudige gevallen/zaken. Met grote hoeveelheden data is te weinig rekening gehouden, waardoor de vraag is of de bestaande regels voor het verzamelen en verder verwerken hiervan voldoende specifiek zijn om de toets van het Bundesverfassungsgericht te kunnen doorstaan.

III.4.2 Verkrijgen van politiegegevens

BKA-Gesetz

Voor het verkrijgen van gegevens in het kader van Strafverfolgung/strafrechtelijk onderzoek[112] moet het BKA het Wetboek van Strafvordering (Strafprozessordnung/StPO) in acht nemen, voor bijvoorbeeld de Centrale Dienst-functie en Gefahrenabwehr het BKA-Gesetz.

Het Bundesverfassungsgericht heeft op 20 april 2016 geoordeeld dat bepaalde regelingen uit het BKA-Gesetz niet in overeenstemming waren met de Grondwet. Het ging om verdekte maatregelen met het oog op afweer van gevaren van internationaal terrorisme. Over gegevensverzameling (*Datenerhebung*) oordeelde het BVerfG (samengevat en in de Engelse vertaling):

> *'1. a) The authorisation of the Federal Criminal Police Office [BKA] to carry out covert surveillance measures (surveillance of private homes, remote searches of information technology systems, telecommunications surveillance, collection of telecommunications traffic data and surveillance outside of private homes using special means of data collection) is, for the purpose of protecting against threats from international terrorism, in principle compatible with the fundamental rights enshrined in the Basic Law.*
>
> *b) The design of these powers must satisfy the principle of proportionality. Powers that constitute a serious interference with privacy must be limited to the protection or legal reinforcement of sufficiently weighty legal interests; require that a threat to these interests is sufficiently specifically foreseeable; may, only under limited conditions, also extend to third parties from whom the threat does not emanate and who belong to the target person's sphere; require, for the most part, particular rules for the protection of the core area of private life as well as the protection of persons subject to professional confidentiality; are subject to requirements of transparency, individual legal protection, and supervisory control; and must be supplemented by deletion requirements with regard to the recorded data.'*[113]

Deze en andere eisen die het BVerfG aan de wetgeving stelt, zijn bij de wijziging van het BKA-Gesetz in 2018 samen met de AVG en de Richtlijn in deze wet verwerkt.

Art. 9-11 BKA-Gesetz geven algemene regels voor gegevensverzameling: art. 9 is het algemene artikel over verzameling door en verstrekking aan het BKA, art. 10 gaat over informatie

[112] Het BKA omschrijft het zelf in het interview als *im Ermittlungsverfahren*.
[113] BVerfG 20 april 2016, ECLI:DE:BVerfG:2016:rs20160420.1bvr096609.

van providers[114] en art. 11 over het opnemen van inkomende telefoontjes naar openbaar bekende nummers.

In de hoofdstukken daarna (bijvoorbeeld hoofdstuk 5 over afweer van gevaren van internationaal terrorisme) zijn naast deze algemene bepalingen ook bijzondere bepalingen over gegevensverkrijging te vinden, met voorwaarden per specifieke opsporingsmethode.

Het belangrijkst zijn de begrippen *Erforderlichkeit* (noodzakelijkheid (met het oog op de taakuitvoering/het doel)) en *Verhältnismäßigkeit* (proportionaliteit). Zie bijvoorbeeld art. 9 lid 1 BKA-Gesetz: 'Het Bundeskriminalamt kan, voor zover dit voor de uitvoering van zijn taak als centrale dienst op grond van art. 2 lid 2 sub 1 en lid 6 noodzakelijk is, persoonsgegevens verzamelen om bestaande informatie aan te vullen of voor analyse door middel van verzoeken om inlichtingen of informatieuitvraag bij publieke en niet-publieke entiteiten.'

Bij het bestuderen van de wetgeving valt op, en dit blijkt ook uit de interviews, dat de wetgeving moeilijk te lezen is vanwege de verschillende niveaus en vele verwijzingen naar andere artikelen in dezelfde wet en andere wetten. Daarbij komt nog jurisprudentie waar de politie op moet letten. Dit maakt het voor de politie in de dagelijkse praktijk lastig te bepalen wat in het concrete geval toelaatbaar is, bijvoorbeeld bij het verzamelen van grote hoeveelheden data uit openbare online bronnen.

Wetboek van Strafvordering (Strafprozessordnung, StPO)

Het achtste hoofdstuk van het Duitse Wetboek van Strafvordering (art. 94-111q) bevat *Ermittlungsmaßnahmen* (onderzoeks-/opsporingsmethoden/maatregelen) en de eisen daaraan. Zie bijvoorbeeld art. 100a-100j over onder andere *Telekommunikationsüberwachung* (art. 100a), online-doorzoeking (art. 100b), het afluisteren in woningen (art. 100c) en het opvragen van data van providers (art. 100j).

Hierbij proberen bepalingen als art. 100d StPO te voorkomen dat te veel data worden verzameld, en zo de noodzakelijkheid en proportionaliteit te verzekeren. Een belangrijk begrip in het Duitse privacyrecht is het *Kernbereich privater Lebensgestaltung* (kernbereik van de persoonlijke levenssfeer/*core area of private life*), dat zo min mogelijk mag worden aangetast. Het gaat om de meest intieme, hoogstpersoonlijke informatie/details over iemands privéleven. Op grond van art. 100d StPO mogen de opsporingsbevoegdheden uit art. 100a-100c bijvoorbeeld niet worden ingezet als aannemelijk is dat daaruit alleen gegevens uit dit kernbereik worden verkregen. Verder moet zoveel mogelijk (technisch) worden bewerkstelligd dat deze persoonsgegevens niet worden verzameld, en als ze toch worden verzameld, mogen ze niet worden gebruikt en moeten ze meteen worden verwijderd.

Maar ook elders, verspreid over het hele Wetboek van Strafvordering zijn bepalingen te vinden over de omgang met persoonsgegevens. Opsporing en vervolging van strafbare feiten maken immers vaak een diepe inbreuk op de persoonlijke levenssfeer van alle betrokkenen, waarvoor een specifieke wettelijke grondslag nodig is.

[114] Bij dit soort maatregelen is ook de Telekommunikationsgesetz (een Bondswet) van belang.

Wetgeving Nordrhein-Westfalen

In de Politiewet NRW is in art. 2 het proportionaliteitsbeginsel vastgelegd.[115] Titel 1 (Gegevensverkrijging) van Onderafdeling 2 (Gegevensverwerking) van hoofdstuk 2 (Politiebevoegdheden) – art. 9-21 – bevat de bevoegdheden met betrekking tot gegevensverzameling, gesorteerd per opsporingsbevoegdheid/maatregel. In bijlage 3 is de inhoudsopgave weergegeven.

Het Ordnungsbehördengesetz NRW verwijst voor wat betreft gegevensbescherming vooral naar de Politiewet NRW en voor het overige naar de AVG (art. 24 Ordnungsbehördengesetz NRW).

De bepalingen zijn zeer uitgebreid geformuleerd. Uitgangspunt is ook hier steeds dat de maatregel die inbreuk maakt op de persoonlijke levenssfeer *erforderlich* moet zijn met het oog op een politietaak (= noodzakelijkheid, proportionaliteit en doelbinding). Volgens de geïnterviewden gaat de politie zeer voorzichtig te werk, zijn ze van de basisprincipes doordrongen en vragen ze zich voortdurend per geval af (en vragen ze vaak ook aan experts (zoals van de politieacademie), de functionaris gegevensbescherming of de toezichthoudende autoriteit) of voorgenomen handelingen binnen de privacykaders passen.

Een tekortkoming in de wetgeving is, zoals hierboven ook genoemd, volgens de geïnterviewde hoogleraar politierecht dat deze op het gebied van nieuwe technologieën niet toereikend is voor de hoge eisen die het Bundesverfassungsgericht aan zulke inbreuken op grondrechten stelt. Middelen zoals bodycams en camera's zijn wel geregeld (zie bijvoorbeeld art. 15b en 15c Polizeigesetz NRW) en er zijn uitgebreide waarborgen opgenomen gericht op bescherming van het kernbereik van de persoonlijke levenssfeer en het tegengaan van het verzamelen van onnodige data van bijvoorbeeld niet betrokken derden; maar volgens deze gesprekspartner (en volgens hem ook andere experts) is de wetgeving achterhaald, want gericht op enkelvoudige gevallen in plaats van op de enorme datasets die nu gegenereerd worden. Het concept van *big data* is niet verdisconteerd in de wetgeving. *Data mining, web scraping, open source intelligence, Recherchen in sozialen Netzwerken* (sociale media) en überhaupt bredere *Internetrecherchen*, etc. zijn niet specifiek geregeld. Dat betekent niet dat deze mogelijkheden niet verkend/gebruikt worden, maar dit wordt nu gestoeld op de algemene grondslagen, waarbij dus veel aan het oordeel van de opsporingsambtenaar (en het toezicht) wordt overgelaten. Wel hebben alle geïnterviewden de indruk dat de politie zich bewust is van dit spanningsveld en niet zomaar maatregelen inzet.

III.4.3 Bewerken van politiegegevens

BKA-Gesetz

In het BKA-Gesetz gaat onderafdeling 2 (Verdere verwerking van gegevens; art. 12-24) van hoofdstuk 2 (Algemene bevoegdheden voor gegevensverwerking) over het verdere verwerken en dus ook het bewerken van persoonsgegevens door het Bundeskriminalamt; zie bijlage 3 voor de volledige indeling.

[115] (1) Von mehreren möglichen und geeigneten Maßnahmen hat die Polizei diejenige zu treffen, die den Einzelnen und die Allgemeinheit voraussichtlich am wenigsten beeinträchtigt.
(2) Eine Maßnahme darf nicht zu einem Nachteil führen, der zu dem erstrebten Erfolg erkennbar außer Verhältnis steht.
(3) Eine Maßnahme ist nur solange zulässig, bis ihr Zweck erreicht ist oder sich zeigt, dass er nicht erreicht werden kann.

In andere hoofdstukken staan nog bijzondere bepalingen. Zo wordt in hoofdstuk 3 over de centrale dienst-functie van het BKA art. 13 over het informatiesysteem verder uitgewerkt; in het kader van het politionele informatieverbond tussen Bund en Länder is er ook een geharmoniseerd verbondssysteem (art. 29).[116] Art. 30 begrenst welke gegevens hierin mogen worden verwerkt (samenhangend met de doelen van het informatieverbond, dus bestrijding van zware en/of Länderoverstijgende en/of internationale criminaliteit) en art. 31 regelt de privacyrechtelijke verantwoording hiervoor (de verantwoordelijkheid voor rechtmatige gegevensverwerking ligt bij degene die de gegevens heeft aangeleverd; controle door de toezichthoudende autoriteit, de Bundesbeauftragte für den Datenschutz und die Informationsfreiheit).

Kernbepaling is art. 12 BKA-Gesetz, dat in uitgebreide bewoordingen de doelen, doelbinding en voorwaarden voor het verder verwerken van persoonsgegevens door het BKA uiteenzet. Hierbij geldt het door het Bundesverfassungsgericht ontwikkelde 'beginsel van hypothetische nieuwe verzameling van gegevens': verder gebruik van gegevens voor een ander doel is alleen toelaatbaar voor de opsporing en vervolging van vergelijkbaar ernstige strafbare feiten of ter bescherming van vergelijkbaar belangrijke rechtsgoederen. Voor het verder verwerken van gegevens die zijn verkregen met ingrijpender maatregelen, zoals de verdekte inzet van technische middelen in/buiten woningen, gelden extra voorwaarden: er moet dan (kort door de bocht) sprake zijn van ernstig gevaar voor lijf, leven of de veiligheid van de Bond of een land, en de verwerkingsdoelen zijn extra begrensd.

Het informatiesysteem van het BKA heeft op grond van art. 13 de volgende functies:

1. ondersteuning bij politieonderzoeken
2. ondersteuning bij zoekacties naar personen en zaken
3. ondersteuning bij de consolidatie[117] van politie-informatie door de opheldering van aanwijzingen en sporen
4. het vergelijken/matchen[118] van persoonsgegevens
5. ondersteuning bij strategische analyses en statistieken

Het vergelijken en analyseren van persoonsgegevens is op grond van dit artikel dus mogelijk, maar opengelaten wordt op welke manieren en met welke technieken dit kan. Ook andere artikelen besteden niet specifiek aandacht aan bijvoorbeeld het koppelen van bestanden of *big data*-analyse. Een uitzondering hierop is misschien art. 17 BKA-Gesetz (projectgerelateerde gezamenlijke databestanden); dit artikel geeft het BKA de mogelijkheid om op projectbasis tijdelijk gezamenlijke databestanden aan te leggen met de inlichtingendiensten en politiediensten op bonds- en landsniveau en de recherche van de douane (*Zollkriminalamt*). Maar dit gaat meer over de voorwaarden voor het delen van gegevens (zie verder par. III.4.6 over verstrekken/delen) en niet over de technische aspecten.

Wetboek van Strafvordering (Strafprozessordnung, StPO)

De StPO bevat verscheidene bepalingen over het bewerken/verdere gebruik van gegevens. Technologische mogelijkheden zijn hierin meegenomen, maar wel 'met de kennis van toen'; zie bijvoorbeeld art. 98a (*Rasterfahndung* oftewel sleepnetonderzoek/-zoekactie) en art. 98c (geautomatiseerde vergelijking/matching[119] met gegevens die al voorhanden zijn). Dat eerste artikel is specifieker dan het tweede, dat erg ruim geformuleerd is. Art. 98b bevat nog aanvullende procedurele voorwaarden voor sleepnet-zoekacties. In alle drie de artikelen wordt

[116] Zie verder paragraaf III.4.6 over het delen van politiegegevens.
[117] Het Duitse woord is *Informationsverdichtung*, informatieverdichting.
[118] *Abgleich*, vertaalt het beste met 'matching'.
[119] Duits: maschineller Abgleich.

maschinell abgleichen (geautomatiseerd vergelijken/matchen) niet verder gedefinieerd. Volgens een van de geïnterviewden dateren dit soort artikelen uit het Wetboek van Strafvordering alweer van een aantal jaar geleden, waardoor de nieuwste ontwikkelingen niet zijn meegenomen.

Wetgeving Nordrhein-Westfalen

Het Polizeigesetz NRW regelt het verder verwerken/gebruik van gegevens in Titel 3 (Verdere verwerking van gegevens) van onderafdeling 2 (Gegevensverwerking) van hoofdstuk 2 (Politiebevoegdheden) – art. 22-25 (zie verder bijlage 3):

'Verwerking voor bijzondere doelen' in de zin van art. 24 is ten eerste het opnemen van noodtelefoontjes, ten tweede het gebruik van gegevens voor politionele statistische doeleinden en ten derde voor opleidingsdoeleinden.

Art. 23 Politiewet NRW is een soortgelijke algemene bepaling met de kaders voor het verder verwerken van gegevens als art. 12 BKA-Gesetz. De opbouw en inhoud is bijna hetzelfde, onder invloed van de rechtspraak van het Bundesverfassungsgericht: lid 1 bepaalt dat de politie persoonsgegevens die ze zelf heeft verzameld, mag verwerken voor de vervulling van dezelfde taak, ter bescherming van dezelfde rechtsgoederen/rechten, of ter voorkoming of preventieve bestrijding van dezelfde strafbare feiten. Lid 2 bevat de voorwaarden voor verwerking voor andere doelen dan waarvoor de data verkregen zijn, ook hier volgens het principe van hypothetische nieuwe gegevensverzameling. Lid 3-5 bevatten een aantal uitzonderingen en bijzondere bepalingen. Opnieuw valt op dat de wettekst zeer lang en gedetailleerd is en vol verwijzingen staat naar andere artikelen.

Deze artikelen gaan niet specifiek in op het gebruik van nieuwe technologische middelen of (analyse)methoden. Ook in de Gegevensbeschermingswet (Datenschutzgesetz) NRW is dit niet verder uitgewerkt. Volgens de gesprekspartners bij de politie NRW golden in ieder geval in Duitsland altijd al strenge eisen voor inbreuken op de persoonlijke levenssfeer in het kader van de politietaak; de Richtlijn heeft hier niet wezenlijk verandering in gebracht. Bij elke maatregel geldt het grondrecht op informationele zelfbeschikking en moet de rechts-/machtigingsgrondslag (*Ermächtigungsgrundlage*), passendheid, noodzakelijkheid en proportionaliteit getoetst worden. De technologieën die de politie voorheen gebruikte, kan ze nog steeds gebruiken, met inachtneming van die voorwaarden. Het gaat dan bijvoorbeeld om methoden voor criminaliteitsprognose/*predictive policing* en zoekacties op internet. Volgens deze gesprekspartner laten de regels hiervoor tamelijk veel speelruimte.

III.4.4 Categoriseren en labelen van gegevens

BKA

Art. 14 BKA-Gesetz bevat conform de Richtlijn gegevensbescherming opsporing en vervolging een *Kennzeichnungspflicht* oftewel categoriserings-/labelingsplicht.
Bij de opslag van persoonsgegevens in het informatiesysteem moet het volgende worden ingevoerd:

1. Middel van verkrijging, inclusief of de gegevens open of verdekt zijn verkregen; eventueel ook de rechtsgrondslag
2. Categorie van personen (veroordeelden, verdachten en andere potentiële daders/verdachten (art. 18 BKA-Gesetz) en andere personen (art. 19 BKA-Gesetz)) bij personen van wie basisgegevens zijn geregistreerd
3. Rechtsgoederen ter bescherming waarvan de gegevens zijn verzameld of strafbare feiten ter vervolging of voorkoming waarvan de gegevens zijn verzameld

4. Degene die de gegevens verzameld heeft voor zover dat niet het BKA zelf is

Bij de herziening van het BKA-Gesetz is/wordt hiervoor ook een nieuw politioneel IT-systeem geschapen voor Bund en Länder, waarin voor elke verwerkingsverantwoordelijke de voorwaarden duidelijk zijn onderscheiden. Dit is een complexe operatie, die nog steeds tot uitdagingen leidt, bijvoorbeeld bij grote hoeveelheden data.

Belangrijk is dus het aangeven van het doel waarvoor de gegevens verzameld zijn, met welke maatregel/welk middel dit is gebeurd, in welke mate deze maatregel ingrijpt in de persoonlijke levenssfeer en de rol van de betrokkene(n). Om grote datasets goed te kunnen indelen wordt door de Duitse politie gewerkt met een 'stoplichtsysteem', waarbij rood, geel en groen de ingrijpendheid van de inbreuk laten zien. Dat leidt echter in de praktijk nog steeds tot vragen; in hoeverre en op wat voor manier mogen geel en rood gemarkeerde gegevens verder worden verwerkt?

Daarnaast worden op grond van de Richtlijn categorieën bijzondere persoonsgegevens onderscheiden, waarvoor strengere voorwaarden gelden (art. 48 Bundesdatenschutzgesetz).

Nordrhein-Westfalen

Art. 22b Polizeigesetz NRW (labeling/categorisering in politionele bestandensystemen) is min of meer woordelijk gelijk aan art. 14 BKA-Gesetz. Art. 22a regelt daarnaast de omgang met categorieën bijzondere persoonsgegevens. Verder wordt onderscheiden of het om adresgegevens gaat, telecommunicatiegegevens etc. Ook bij de categorisering is volgens de hoogleraar aan de Deutsche Hochschule der Polizei het probleem dat de wetgever niet aan massadataverzameling heeft gedacht.

III.4.5 Bewaartermijnen en vernietigingsvoorwaarden

In het Duitse systeem wordt – in navolging van de Richtlijn – gewerkt met *Aufbewahrungsfristen* (bewaartermijnen) en *Prüfungstermine*, vertellen de geïnterviewden. Op veel plekken in de politiewetgeving staan vaste termijnen waarna bepaalde persoonsgegevens verwijderd moeten worden. Deze zijn echter meestal zo geformuleerd dat ze ruimte laten om gegevens langer te bewaren, als dat voor de uitvoering van een taak in het bereik van de Richtlijn – zoals het afronden van het strafrechtelijk onderzoek – noodzakelijk is. Vaak worden de termijnen ook aan de verwerkingsverantwoordelijke overgelaten om vast te leggen. Op vaste momenten – de Prüfungstermine, die zijn ingebouwd in het politiesysteem – moeten de betrokken politiemensen de *Erforderlichkeit* beoordelen, dus of de gegevens nog noodzakelijk zijn voor het doel waarvoor ze verzameld zijn of een ander doel; anders moeten ze worden verwijderd. De ingrijpendheid van de manier waarop de gegevens zijn verkregen (verdekt of open; inbreuk op het kernbereik van de persoonlijke levenssfeer) en de gevoeligheid van de gegevens (bijvoorbeeld of het gaat om bijzondere categorieën persoonsgegevens, en of het verdachten/veroordeelden betreft of slechts contactpersonen of helemaal niet betrokken derden) wegen hierbij mee. In het systeem moet uitdrukkelijk en gemotiveerd worden vastgelegd waarvoor de gegevens nog noodzakelijk zijn en hoe lang (prognose). Gegevens worden niet automatisch na een bepaalde termijn verwijderd; er is altijd een menselijke check nodig. Enkele geïnterviewden geven aan dat het in de praktijk best een lastige opgave is om te beoordelen of gegevens in de toekomst misschien nog nodig zijn, en dat de termijnen daarvoor soms te kort zijn. Tot slot gelden de verjaringstermijnen voor verschillende soorten strafbare feiten.

Hieronder gaan we verder in op hoe een en ander wettelijk is geregeld en in de praktijk werkt.

BKA-Gesetz

Art. 18 en 19 BKA-Gesetz geven voor verschillende groepen personen de voorwaarden voor het verder verwerken en (langer) bewaren van persoonsgegevens weer. Art. 18 gaat over veroordeelden en (potentiële) verdachten. Art. 19 gaat over andere personen, zoals (mogelijke) getuigen, slachtoffers, bekenden van verdachten/daders, gevers van aanwijzingen en inlichtingen, vermisten, onbekende personen en onbekende doden. Per categorie personen staan precies de soorten persoonsgegevens omschreven die mogen worden verwerkt en voor welke doelen. Het valt op dat, hoewel de wettekst lang en gedetailleerd is, aan de opsporingsambtenaren toch – binnen de hierboven geschetste algemene kaders – veel professionele ruimte toekomt, ook op het gebied van bewaartermijnen. In art. 18 en 19 BKA-Gesetz staan wel enkele termijnen genoemd, maar deze gelden alleen in specifieke gevallen. Zo bepaalt art. 18 lid 3 dat het Bundeskriminalamt persoonsgegevens kan verwerken om vast te stellen of personen tot de in dit artikel bedoelde categorieën (veroordeelde, verdachte etc.) kunnen worden gerekend. De gegevens mogen uitsluitend voor dat doel worden verwerkt, moeten in het informatiesysteem apart worden opgeslagen. De gegevens moeten na afloop van deze check en uiterlijk na twaalf maanden worden verwijderd, voor zover niet wordt vastgesteld dat iemand in de in dit artikel beschreven categorieën personen valt.

Een voorbeeld van een specifieke termijn die verband houdt met een bepaalde maatregel is te vinden in art. 11 BKA-Gesetz over het opnemen van inkomende telefoontjes: de opnames moeten meteen en zonder achterlating van sporen worden verwijderd, zodra ze niet meer noodzakelijk zijn voor de taakuitvoering; op zijn laatst na dertig dagen, tenzij ze in een individueel geval nodig zijn voor *Strafverfolgung,* afweer van gevaren voor internationaal terrorisme of bescherming van de leden van de constitutionele organen of de BKA-leiding.

Nordrhein-Westfalen

Art. 22 Politiewet NRW regelt de opslag van persoonsgegevens (*Datenspeicherung*) en de *Prüfungstermine* ('controlemomenten' of de gegevensverwerking nog noodzakelijk is). De verwerkingsverantwoordelijke moet de Prüfungstermine en bewaartermijnen vastleggen (de wet zegt slechts '*sind festzulegen*', dus niet door wie). Deze mogen bij volwassenen niet langer zijn dan tien jaar, bij jongeren vijf, bij kinderen twee en bij *Kontakt- und Begleitpersonen* één. Hier doet zich het probleem voor van de *Mitziehklausel* ('meetrekclausule') (bijvoorbeeld in art. 22 lid 2 éénnalaatste zin Polizeigesetz NRW): als de politie over dezelfde persoon nieuwe informatie verzamelt, gaat voor alle gegevens over die persoon weer een nieuwe termijn in. Dit kan er in theorie toe leiden dat gegevens eindeloos bewaard worden.

Ook het Polizeigesetz NRW kent specifieke, kortere *Löschfristen* (verwijderingstermijnen) voor maatregelen die een diepe inbreuk maken op de persoonlijke levenssfeer, zoals in art. 15a over 'op het lichaam gedragen opnameapparatuur'. De opnamen moeten na twee weken worden verwijderd, tenzij ze nog nodig (in het wetsartikel staat het woord *benötigt*, niet *erforderlich* (noodzakelijk)) zijn voor *Gefahrenabwehr*, vervolging van strafbare feiten of *Ordnungswidrigkeiten* of op verzoek van de betrokkene voor controle op de rechtmatigheid van opgenomen politiemaatregelen. De politiebeambte beslist over de verwijdering, met toestemming van een leidinggevende. Ook hier wordt dus weer een uitzondering gemaakt voor als de gegevens in de toekomst nog nodig zijn.

Als de politie grote datasets verzamelt, is het lastig snel te bepalen wat ze daarvan nodig heeft. De geïnterviewden in NRW geven het voorbeeld van een grote misbruikzaak met 500 terabyte aan data. In zo'n geval worden de gegevens bewaard tot de politie de *Erforderlichkeit* (noodzakelijkheid) heeft kunnen beoordelen; de betrokkene krijgt daarvan bericht.

III.4.6 Verstrekken/delen van politiegegevens

Bundeskriminalamt

De art. 25-28 BKA-Gesetz regelen het verstrekken van gegevens (*Datenübermittlung*). Art. 25 gaat over verstrekking binnen Duitsland, art. 26 over de EU en art. 27 over internationale gegevensuitwisseling (derde landen en internationale organisaties). Art. 28 bevat verstrekkingsverboden en weigeringsgronden; gegevensuitwisseling moet bijvoorbeeld achterwege blijven als de belangen van de betrokkene zwaarder wegen. Hiermee is eenzelfde systeem als in de Richtlijn (en dus als in Nederland) in het leven geroepen. Het BKA heeft als centrale dienst een coördinerende rol bij de politionele samenwerking tussen Bond en Länder en Länder onderling, en een ondersteunende rol bij de internationale uitwisseling van politiegegevens door andere autoriteiten van Länder en Bond. Art. 29-33 over de centrale dienst-functie van het BKA en de samenwerking en gegevensdeling in het Duitse politionele informatieverbond zijn daarbij ook van belang. Het begrip 'verbondrelevantie' is belangrijk voor de beoordeling of persoonsgegevens gedeeld/verwerkt mogen worden door de deelnemende diensten.[120]

Op grond van art. 25 lid 1 BKA-Gesetz mag het BKA persoongegevens verstrekken aan andere politiediensten van Bond en Länder, als dat voor de taakuitvoering van BKA of ontvanger noodzakelijk is. Verstrekking aan andere autoriteiten en aan andere *öffentliche Stellen* (openbare lichamen/entiteiten) is ook toegestaan (lid 2), net als aan niet-*öffentliche Stellen* (lid 3),

- als dit in andere rechtsvoorschriften voorzien is óf
- met inachtneming van art. 12 lid 2-4 over gegevensverwerking voor een ander dan het oorspronkelijke doel, en voor de volgende doelen:
  a) voor de uitvoering van zijn taak op grond van het BKA-gesetz,
  b) voor *Strafverfolgungs*-, strafvoltrekkings- of tenuitvoerleggingsmaatregelen en gratieprocedures,
  c) voor *Gefahrenabwehr*-doeleinden of
  d) om een ernstige inbreuk op de rechten van individuele personen af te wenden,

[120] Art. 30 BKA-Gesetz (Verbondrelevantie) (vertaling Pro Facto): '(1) De aan het politionele informatieverbond deelnemende entiteiten verwerken in het politionele informatieverbond uitsluitend
1. persoonsgegevens, waarvan de verwerking voor de voorkoming en vervolging van strafbare feiten van Länderoverstijgende, internationale of aanzienlijke aard noodzakelijk is;
2. persoonsgegevens, waarvan de verwerking in het informatieverbond noodzakelijk is
a) voor identificatiedoeleinden, voor zover het Bundeskriminalamt deze gegevens op grond van art. 16 lid 5 [voorwaarden voor het verder verwerken van gegevens in het informatiesysteem die zijn verzameld in de context van forensische identificatie] ook verder mocht verwerken in het Informatieverbond of
b) voor zoekacties naar personen en zaken, voor zover het Bundeskriminalamt deze gegevens op grond van art. 16 lid 2 [voorwaarden voor het verder verwerken van gegevens in het informatiesysteem met het oog op zoekacties] ook verder mocht verwerken in het Informatieverbond (Verbondrelevantie).
(2) De aan het politionele informatieverbond deelnemende entiteiten leggen, met raadpleging van de daartoe bevoegde hoogste Bonds- of Landsautoriteiten criteria vast, die bepalen, welke strafbare feiten naar algemene recherche- [*kriminalistische*] ervaring aan de vereisten van lid 1 onder 1 voldoen. De criteria kunnen zijn ingegeven door de verschillende *kriminalistische* fenomenen. De criteria moeten met passende tussenpozen en voor zover noodzakelijk worden geactualiseerd. Deze criteria worden vastgelegd en geactualiseerd met raadpleging van de toezichthoudende autoriteit op Bondsniveau.

en voor zover de verstrekking het strafproces niet hindert.
Voor verstrekking aan niet-*öffentliche Stellen* geldt ook nog de verplichting van elke verstrekking een bewijs op te stellen met daarop onder meer aanleiding, inhoud en datum.

Volgens het BKA loopt de informatiedeling binnen de EU goed; de nieuwe (van Europa uitgaande) regels zijn nog beter uitgewerkt dan de oude. De meeste problemen doen zich voor bij de uitwisseling met derde landen, bijvoorbeeld bij het opvragen van informatie aan Facebook (een private partij in een derde land). De Duitse wetgever op Bondsniveau heeft het Europeesrechtelijke begrip 'passende waarborgen' niet verder ingevuld; dit is aan de praktijk overgelaten. Gesprekspartners geven aan dat er in Duitsland behoefte bestaat aan een eenduidige Europese uitleg en een informatiebron voor de beoordeling hiervan per derde land. De meeste onzekerheden treden volgens de geïnterviewden op bij de samenloop met de Internationale Rechtshulpwet.

De betrokken ambtenaar moet bij de verstrekking aan derde landen niet alleen de omgezette voorschriften uit de Richtlijn gegevensbescherming opsporing en vervolging in acht nemen, maar ook de eisen van het Bundesverfassungsgericht. Het gaat dan om het principe van hypothetische nieuwe dataverzameling, en er mag geen verstrekkingsverbod zijn vanwege een gebrekkige rechtsstaat of mensenrechtenschendingen in het betreffende land. Dit laatste is bijvoorbeeld vastgelegd in art. 28 lid 3 BKA-Gesetz. Het BKA moet een register bijhouden van het rechtsstatelijke, mensenrechten- en gegevensbeschermingsniveau in relevante derde landen.

Nordrhein-Westfalen

In art. 26 Politiewet NRW staan algemene regels voor gegevensverstrekking en weigeringsgronden. Art. 27 bevat het kader voor gegevensverstrekking in Duitsland, art. 28 voor de EU en art. 29 voor derde landen en internationale organisaties. Dit lijkt sterk op de drietrapsraket op Bondsniveau en is ook in de politiewetten van andere Länder min of meer gelijk geregeld. Art. 30 gaat over verstrekking van gegevens aan de politie.

Art. 27 Politiewet NRW over uitwisseling binnen Duitsland maakt net als zijn tegenhanger in de BKA-wet onderscheid tussen politiediensten, andere autoriteiten en andere publieke organen en andere, niet-publieke personen of organen. De politie moet precies bijhouden met wie welke informatie wordt gedeeld, met welk doel en wanneer. Uitwisselen mag voor zover dat voor het uitvoeren van de eigen taak of voor gevarenafweer door de ontvangende partij (onder de in dit artikel uitgeschreven voorwaarden) noodzakelijk is. Voor uitwisseling met AVG-organisaties (en dan vooral voor *nicht-offentliche Stellen*) gelden strengere waarborgen.

De geïnterviewden vertellen dat zich bij het delen van informatie met andere organisaties dan de politie vele vraagstukken voordoen. Zo heeft de minister van Binnenlandse Zaken in NRW 'clancriminaliteit' – door grote familienetwerken – in het Ruhrgebied als aandachtspunt aangewezen. Hierbij moet de politie met veel verschillende organisaties samenwerken, zoals financiële autoriteiten (die ook onder de Richtlijn vallen) en gemeenten. Daarbij is steeds de discussie welke informatie met de politie gedeeld mag worden en andersom. Daarvoor zijn wettelijke grondslagen, maar het blijven afwegingen per individueel geval. Voor het verstrekken van informatie aan de politie zijn er naast de Richtlijn en de AVG ook veel rechtsgrondslagen in bijzondere wetten, zoals boek 10 van het Sozialgesetzbuch voor onder andere de

Jugendämte (Bureaus Jeugdzorg). De politie moet van haar kant bijvoorbeeld informatie verstrekken aan een Jugendamt op grond van art. 27 lid 2 (2)(b)[121] Politiewet NRW als een kind in gevaar is. Aan beide kanten gelden echter privacyrestricties en elke organisatie handelt binnen zijn eigen taken, bevoegdheden en verantwoordelijkheden. De preventieve mogelijkheden van de politie worden hierdoor begrensd, wat een politiek spanningsveld oplevert; de gesprekspartners noemen een grote kindermisbruikzaak, waar de Landtag zich afvroeg waarom de politie niet eerder had ingegrepen. Het is echter niet wenselijk als de politie zomaar alle gegevens van de Jugendämter zou krijgen/kunnen inzien. Er is daarom bijvoorbeeld ook niet een gemeenschappelijk informatiesysteem van politie en gemeenten.

Een ander punt is het delen van informatie met de veiligheids-/inlichtingendiensten. In Duitsland zijn politie en veiligheidsdiensten vanuit historisch oogpunt streng gescheiden; er geldt een 'scheidingsgebod' van het Bundesverfassungsgericht. Gegevensdeling is daarom maar zeer beperkt mogelijk en hierover is weinig wettelijk geregeld.

Bij het verstrekken van gegevens binnen de EU is in een van de interviews het punt genoemd dat nog niet alle lidstaten het Europese privacykader geïmplementeerd hebben. Volgens deze gesprekspartner zal dit op enig moment stuiten op bezwaren van het Bundesverfassungsgericht.

Wat betreft de uitwisseling met derde landen is als voorbeeld genoemd dat er in coronatijd een verzoek kwam van een derde land om de persoonsgegevens (namen, contactgegevens) van onderdanen van dat land die in Duitsland (hadden) verbleven; dat heeft de politie geweigerd. Ook wordt opgemerkt dat de doorlooptijd van internationale rechtshulpverzoeken erg lang is.

III.5 Toezicht

III.5.1 Bondsniveau

Extern toezicht (toegespitst op het BKA/de samenwerking tussen Bond en Länder)

Het toezicht op Bondsniveau ligt zoals eerder genoemd bij de Bundesbeauftragte für den Datenschutz und die Informationsfreiheit[122] (BfDI) (Bondsagent voor Gegevensbescherming en Informatievrijheid). Daarnaast zijn er zestien Landesbeauftragten. Al deze onafhankelijke toezichthouders werken samen in de Gegevensbeschermingsconferentie (art. 18 Bundesdatenschutzgesetz). Deze heeft ook een controletaak.

Deel 1, hoofdstuk 4 van de BDSG (art. 8-16) gaat over de BDI. Op grond van art. 14 is het onder andere de taak van de BDI om:

- toezicht te houden op de naleving van Richtlijn 2016/680;
- hierover bewustwording te genereren;
- betrokkenen informatie te geven over de uitoefening van hun rechten op grond van de Richtlijn;

[121] Art. 27 lid 2 Politiewet NRW: 'Die Polizei kann an andere als die in Absatz 1 genannten Behörden und sonstige öffentliche Stellen personenbezogene Daten übermitteln, soweit dies (…)
2. b) zur Abwehr einer Gefahr durch die empfangende Stelle (…) erforderlich ist.'

[122] *Informationsfreiheit* ziet op de vrije toegang tot (overheids)informatie. Het is interessant dat privacy en openbaarheid van bestuur hier in één adem worden genoemd.

- samen te werken met andere toezichthoudende autoriteiten om eenheid te verzekeren;
- onderzoeken te doen naar de toepassing van de Richtlijn;
- klachten af te handelen op grond van de Richtlijn.

Art. 60 BDSG is de specifieke klachtbepaling voor het bereik van de Richtlijn.

De algemene bevoegdheden van de BfDI staan in art. 16.

De BfDI schrijft op zijn website dat zijn bevoegdheden voor wat betreft het toezicht op de Richtlijn op grond van de Duitse omzettingswetgeving beperkt blijven tot waarschuwingen en klachten/kritiek/het innemen van standpunten, terwijl het Europese recht voorschrijft dat de lidstaten voor de toezichthoudende autoriteit de mogelijkheid moeten scheppen om effectief op te treden bij inbreuken, bijvoorbeeld door bevelen en verboden. Ook moet de toezichthouder de mogelijkheid hebben een gerechtelijke controle op te starten.[123]

De BfDI kan wel geconstateerde onrechtmatigheden openbaar maken. Volgens de geïnterviewden op Bondsniveau gaat hier ook al een afschrikwekkende werking van uit. Hun indruk is dat de BDI met 300 à 400 medewerkers voldoende mankracht heeft voor zijn veelomvattende taak, en dat het toezicht adequaat is.

Op verschillende plekken in de BDSG en in bijzondere wetten, zoals het BKA-gesetz, zijn bijzondere bepalingen over consultatie van en controle door de BfDI opgenomen. Hoofdstuk 9 van het BKA-gesetz (art. 69-86) heet *Gegevensbescherming en dataveiligheid, Rechten van de betrokkene.* Art. 69 bepaalt dat de BfDI in ieder geval elke twee jaar controles uitvoert op verwerking van gegevens verkregen naar onder andere hoofdstuk 5 (Bevoegdheden voor de afweer van gevaren van internationaal terrorisme) en verstrekkingen aan derde landen en internationale organisaties. Ook controleert de BfDI binnen zijn bevoegdheden[124] elke twee jaar of de gegevensverwerking in het politionele informatiesysteem en informatieverbond van Bond en Länder in overeenstemming is met de autorisaties.

Intern toezicht – Bundeskriminalamt

Art. 70-72 BKA-Gesetz gaan over de Datenschutzbeauftragte (functionaris gegevensbescherming) bij het BKA (in overeenstemming met de algemene bepalingen van art. 5-7 Bondsgegevensbeschermingswet over de Datenschutzbeauftragte). Deze heeft regelmatig overleg met de BfDI. Ook werkt hij samen met de FG's van de Bundespolizei, de Landeskriminalämter en het Zollkriminalamt (art. 71 BKA-Gesetz). Op verschillende plekken in het BKA-gesetz is raadpleging van de Datenschutzbeauftragte gewaarborgd, bijvoorbeeld bij de inzet van ingrijpende opsporingsmethoden.

III.5.2 Nordrhein-Westfalen

Extern toezicht

De toezichthoudende autoriteit voor NRW is de Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI) (Landsagent voor Gegevensbescherming en informatievrijheid); zie Deel 2,[125] hoofdstuk 5 (art. 25-30) Gegevensbeschermingswet NRW voor zijn algemene taken

[123] BfDI, *Umsetzung der JI-Richtlinie in Deutschland*, www.bfdi.bund.de (laatst geraadpleegd op 2 oktober 2020).
[124] Die strekken zich niet uit tot zuivere Landsaangelegenheden.
[125] Deel 2 is de uitwerking van de AVG.

en bevoegdheden onder de AVG. Voor het bereik van de Richtlijn zijn vooral art. 60 (algemeen) en 61 (klachtrecht) van belang. Daarnaast gelden ook in NRW veel specifieke raadplegingsbepalingen in de Gegevensbeschermingswet NRW en bijzondere wetten, zoals de Politiewet NRW.

Art. 60 verklaart een aantal taken en bevoegdheden uit art. 57 en 58 AVG van overeenkomstige toepassing, maar lang niet allemaal. Sommige van die bevoegdheden zijn ook niet relevant, zoals die met betrekking tot gedragscodes en certificering, maar andere, zoals de bevoegdheid tot berispingen en gelasten gehoor te geven aan verzoeken van de betrokkene tot uitoefening van zijn rechten (art. 58 lid 2 sub b en c AVG) zouden de LDI een sterkere positie geven. De straf- en boetebepalingen van art. 33 en 34 DSG NRW gelden wel (schakelbepaling art. 69). Ook hebben betrokkenen bij een schending recht op schadevergoeding (art. 68).

De LDI heeft acht afdelingen, waarvan afdeling 2 zich onder meer bezighoudt met politie en justitie. Hij verricht regelmatig controles (*Überprüfungen*) bij de verschillende autoriteiten. Ook heeft de LDI altijd recht op inlichtingen van de bevoegde autoriteiten en kan hij naar aanleiding daarvan, naar aanleiding van nieuwe wetgeving of uit zichzelf *Stellungnahmen* (standpunten) innemen en publiceren. Dit is bijvoorbeeld gebeurd over bodycams.[126] De politie kan de LDI ook proactief vragen stellen. De Datenschutzbeauftragten (FG's) onderling en de FG's met de LDI werken intensief samen. Soms zijn er volgens enkele geïnterviewden meningsverschillen, bijvoorbeeld over de vraag in hoeverre de LDI zich met het materiële politierecht kan bezighouden (bijvoorbeeld in het wetgevingsproces; in hoeverre heeft de LDI zicht op welke voorschriften/maatregelen noodzakelijk zijn voor de uitvoering van de politietaak?).

Ook de geïnterviewden op NRW-niveau hebben de indruk dat het toezicht, alles bij elkaar, intern door FG's en onafhankelijk, in combinatie met de maatregelen die de politieorganisatie zelf treft, voldoende is. Interessant is nog dat in Nordrhein-Westfalen een discussie is gevoerd in de Landtag (het parlement) of er niet een onafhankelijke politietoezichthouder bij de Landtag zou moeten komen; dit wetsvoorstel is uiteindelijk niet aangenomen.[127]

Intern toezicht

Elke bevoegde autoriteit/dienst, zoals het Landeskriminalamt, de verschillende andere *Polizeibehörden* en *Ordnungsbehörden*, heeft conform het Europese recht een eigen Datenschutzbeauftragte (FG). Art. 67 onder 6 Gegevensbeschermingswet NRW verklaart art. 37-39 AVG over de functionaris gegevensbescherming van overeenkomstige toepassing. Ook hier gelden vele bijzondere bepalingen over raadpleging van de Datenschutzbeauftragte in bijvoorbeeld het Polizeigesetz, zoals in art. 16 lid 3 Polizeigesetz (voorleggen gegevens aan FG bij twijfel of iets in het 'kernbereik van de persoonlijke levenssfeer' valt).

[126] Landesbeauftragte für Datenschutz und Informationsfreiheit, *Stellungnahme Videobeobachtung/Kennzeichnung/Bodycam - A09 - 27.09.2016*, te vinden op www.ldi.nrw.de (laatst geraadpleegd op 17 augustus 2019).

[127] Gesetz über die unabhängige Beauftragte oder den unabhängigen Beauftragten für die Polizei des Landes Nordrhein-Westfalen (Polizeibeauftragtengesetz Nordrhein-Westfalen – PolBeaufG NRW), www.landtag.nrw.de (zoek op Polizeibeauftragte) (laatst geraadpleegd op 8 oktober 2020).

III.6 Lessen voor Nederland

III.6.1 Algemeen

Allereerst plaatsen we de volgende kanttekening: ondanks dat we bij de beantwoording van de onderzoeksvragen voor Duitsland vele interessante punten zijn tegengekomen – zie de omvang van dit hoofdstuk –, is de vraag in hoeverre deze bevindingen (direct) bruikbaar zijn voor toepassing in het Nederlandse wettelijk systeem en de Nederlandse praktijk. Het Duitse stelsel verschilt namelijk op een aantal punten erg van het Nederlandse. Het gaat dan om zaken als:

- de federale staatsvorm met bijbehorende gelaagde wets- en bestuursstructuur;
- de beladen twintigste-eeuwse geschiedenis die op vele plekken doorwerkt en heeft geleid tot extra verankering van grondrechten in wetgeving, bestuur en rechtspraak (met een sterke positie voor het grondwettelijk hof);
- de politie, die op verschillende niveaus en op een andere manier is georganiseerd dan in Nederland. (De aan de politie toebedeelde taken zijn relevant voor de beoordeling van de omgang met persoonsgegevens; de verwerking van persoonsgegevens moet onder meer noodzakelijk en proportioneel zijn met het oog op het doel waarvoor ze zijn verkregen. Dat doel is vaak gekoppeld aan taakuitvoering door de politie of een andere bevoegde autoriteit. Ook vormt de in de wet omschreven (politie)taak vaak de wettelijke grondslag die vereist is voor het verwerken van persoonsgegevens. Als de structuur en taakomschrijving van de politie en andere bevoegde autoriteiten dus niet past op die van Nederland, is het moeilijker de buitenlandse regels te vergelijken/één op één over te nemen.);
- het Duitse onderscheid tussen de preventieve (*Gefahrenabwehr*) en repressieve (*Strafverfolgung*) politietaak, dat bepalend is voor de wet waarin de opsporingsambtenaar moet kijken (bij *Strafverfolgung* geldt het Wetboek van Strafvordering, bij *Gefahrenabwehr* de betreffende politiewet).

Toch zullen we in deze paragraaf proberen er een aantal opvallende punten uit te lichten, die misschien inspiratie kunnen geven voor herziening van de Nederlandse wetgeving. Ook benoemen we enkele terreinen waarop Duitsland tegen dezelfde problemen aan loopt als Nederland, en aspecten van de Duitse wetgeving en praktijk die misschien juist een minder goed voorbeeld zijn.

III.6.2 Wetgevingssystematiek en achterliggende gedachtegang

Direct valt op dat Duitsland, net als de andere onderzochte landen, niet denkt vanuit het begrip ‘politiegegevens’, maar de bescherming van *persoonsgegevens* die worden verwerkt met het oog op de politietaken in een breder kader plaatst. Hierdoor kent Duitsland minder de afbakenings-/reikwijdteproblematiek die speelt bij de Nederlandse Wet politiegegevens (en Wet justitiële en strafvorderlijke gegevens). Er zijn algemene privacywetten op Bondsniveau en op Landsniveau (dus ook in Nordrhein-Westfalen) waarin de AVG en de Richtlijn gegevensbescherming opsporing en vervolging zijn uitgewerkt/omgezet, met een apart hoofdstuk over de Richtlijn. Sinds het midden van de vorige eeuw is bescherming van persoonsgegevens zeer sterk verankerd in de Duitse wetgeving en ook in de mentaliteit van de mensen die met (gevoelige) persoonsgegevens moeten werken, ook – juist – bij de politie. Vrijwel elke wet die ziet op de politie(taak)/bevoegde autoriteiten heeft een onderdeel ‘gegevensbescherming’ (‘*Datenschutz*’). Deze wetten gelden als *lex specialis* ten opzichte van de algemene privacywetten. Er is minder onduidelijkheid dan in Nederland op wie welke wetgeving van toepassing is in welke situaties.

In de afdelingen over gegevensbescherming in de politiewetten is verwerkingsvorm en/of opsporingsmiddel zeer gedetailleerd aangegeven wat voor welk doel toegestaan is. Daarbij wordt ook een helder onderscheid gemaakt tussen verkrijging en verdere verwerking van gegevens Dit helpt om te voldoen aan de strenge eisen die Europa en het Bundesverfassungsgericht aan de wettelijke grondslagen voor gegevensverwerking stellen; elke inbreuk op de persoonlijke levenssfeer moet immers een specifieke wettelijke grondslag hebben en noodzakelijk en proportioneel zijn met het oog op het doel. Het Bundesverfassungsgericht heeft begrippen in het leven geroepen als 'kernbereik van de persoonlijke levenssfeer' – dat meest intieme deel van de persoonlijke levenssfeer dat in principe altijd ongemoeid moet blijven – en het 'principe van hypothetische nieuwe gegevensverzameling': bij gebruik van gegevens voor een ander doel dan waarvoor ze zijn verkregen moet een vergelijkbaar groot belang of rechtsgoed aan de orde zijn als bij de verkrijging.

Een les uit Duitsland is dus zeker te vinden in de structuur van de wetgeving, en dan vooral op het niveau van de (hoofdstuk)indeling van de afzonderlijke wetten. Voor de overzichtelijkheid zou het zeker een overweging kunnen zijn om, zoals in Duitsland, alle regels die voor het handelen van de politie (of andere bevoegde autoriteiten) gelden zoveel mogelijk in de politiewet (of de wet over de betreffende autoriteit) zelf op te nemen, en om in een apart hoofdstuk in elke wet aandacht te besteden aan gegevensbescherming, met duidelijke titels voor hoofdstukken, kopjes en wetsartikelen (zie de voorbeelden in bijlage 3). Tegelijkertijd kent ook Duitsland verschillende regelingen op verschillende niveaus, met veel onderlinge verwijzingen naar andere plekken in de wet zelf en naar andere wetten, wat het lastig maakt voor de individuele opsporingsambtenaar om in één oogopslag te weten wat hij in een bepaalde situatie moet doen (nog afgezien van het feit dat hij ook jurisprudentie van het grondwettelijk hof in acht moet nemen). Kijken we op artikelniveau naar de wetteksten, dan valt op dat deze lang en gedetailleerd zijn, wat voordelen en nadelen heeft: aan de ene kant biedt dit veel houvast en is in de uitgebreide aandacht voor specifieke grondrechtelijke waarborgen duidelijk de lijn van het Bundesverfassungsgericht te herkennen, aan de andere kant maakt dit de tekst moeilijk leesbaar en minder flexibel. De tekst laat nog wel ruimte voor het oordeel van de opsporingsambtenaar (en soms ook leidinggevenden en toezichthouders) om open begrippen als 'noodzakelijk', 'geschikt' en 'proportioneel' in te vullen. Daarnaast lijkt ook de Duitse wetgeving nog niet voldoende ingespeeld op de verregaand gedigitaliseerde samenleving en de daarmee gepaard gaande uitdagingen voor privacy en het politiewerk; de wetgever heeft de wetgeving deels bewust 'technologieneutraal' willen formuleren, maar heeft volgens de academische gesprekspartner deels ook simpelweg niet gedacht aan of adequaat ingespeeld op de steeds grotere datasets en geavanceerdere analysemogelijkheden die in deze tijd beschikbaar komen. De wetgeving (bijvoorbeeld de categoriserings- en labelingsverplichtingen) is nog vooral toegesneden op individuele zaken, en gaat niet in op hoe een en ander precies IT-technisch mogelijk is/moet worden georganiseerd.

III.6.3 Verkrijgen van politiegegevens

Zoals hierboven al opgemerkt kennen de Duitse politiewetten een apart hoofdstuk over gegevensverwerking, met daarin een afdeling over gegevensverkrijging/-verzameling. Hierin staan algemene regels en basisbeginselen, maar wordt ook onderscheid gemaakt naar maatregel/bevoegdheid/opsporingsmiddel (waaronder bijvoorbeeld gebruik van bodycams) op basis van ingrijpendheid (waarbij het onder meer uitmaakt of een maatregel verdekt of open wordt ingezet). Ook in het Wetboek van Strafvordering wordt bij de omschrijving van de verschillende opsporingsbevoegdheden aandacht besteed aan bescherming van persoonsgegevens. Zoals gezegd wordt in de Duitse wettekst zeer uitgebreid ingegaan op privacywaarborgen, in het bijzonder het 'kernbereik van de persoonlijke levenssfeer': gegevens die hieronder vallen mogen niet worden verzameld en als dat toch gebeurt mogen ze niet worden gebruikt.

Zo wordt in één oogopslag duidelijk wat voor verschillende opsporings-/politiebevoegdheden de regels zijn (al wordt er zoals opgemerkt in de wettekst ook veel doorverwezen).

III.6.4 Bewerken van politiegegevens

De bestudeerde politiewetten bevatten een onderdeel 'Verdere verwerking van politiegegevens', waaronder ook bewerken valt zoals in dit onderzoek gedefinieerd (namelijk als de verdere gebruiksmogelijkheden als persoonsgegevens eenmaal zijn verkregen, niet zijnde categoriseren/labelen, bewaren en verstrekken (die onderwerpen bespreken we immers apart), met bijzondere aandacht voor technologische aspecten). In deze afdelingen zijn, naast een algemene bepaling over doelbinding en voorwaarden voor gebruik voor een ander doel, zaken geregeld als de opslag van gegevens (zie ook 'Bewaartermijnen'), elektronisch dossierbeheer, het vergelijken van gegevens en het gebruik van gegevens voor wetenschappelijke, statistische, *case management*- en opleidingsdoeleinden. Dit geeft een duidelijke structuur en de tekst van de artikelen zelf geeft ook houvast.

III.6.5 Categoriseren/labelen van politiegegevens

Een indeling in categorieën en labelingsverplichtingen zijn ook opgenomen in de afdelingen 'Verdere verwerking van gegevens' in de politiewetten. Duitsland heeft (vanzelfsprekend) de verplichte categorisering/labeling uit de Richtlijn overgenomen (categorieën bijzondere persoonsgegevens en de verplichting persoonsgegevens in te delen naar feit/mening en voor zover mogelijk categorieën betrokkenen). Duitsland kent een politioneel informatieverbond met het Bundeskriminalamt als spin in het web. Hiervoor is ook een informatiesysteem in het leven geroepen. Verwerking van persoonsgegevens binnen dit informatieverbond en in dit informatiesysteem is wettelijk geregeld. De betreffende opsporingsambtenaar moet (in dit informatiesysteem en/of in de eigen systemen) het doel aangeven waarvoor de gegevens verzameld zijn, met welke maatregel/welk middel dit is gebeurd, in welke mate deze maatregel ingrijpt in de persoonlijke levenssfeer en de rol van de betrokkene(n). Om grote datasets goed te kunnen indelen wordt door de Duitse politie gewerkt met een 'stoplichtsysteem', waarbij rood, geel en groen de ingrijpendheid van de inbreuk laten zien. Dat leidt echter in de praktijk nog steeds tot vragen; in hoeverre en op wat voor manier mogen geel en rood gemarkeerde gegevens verder worden verwerkt?

III.6.6 Bewaartermijnen en vernietigingsvoorwaarden

De Duitse bewaar- en controletermijnen (momenten waarop moet worden beoordeeld of gegevens nog langer moeten/mogen worden bewaard) lijken in Duitsland flexibeler dan in Nederland. De wetgeving lijkt uit te gaan van het beoordelingsvermogen van de professional. Er wordt vooral gewerkt met vaste, door de verwerkingsverantwoordelijke te bepalen controlemomenten waarop de politie(ambtenaar)/andere verwerkingsverantwoordelijke een inschatting moet maken of, waarom (voor welk doel) en hoe lang (prognose) bewaren nog noodzakelijk en proportioneel is. Dit moet worden vastgelegd in het systeem. De stoplichtindeling op basis van de mate van inbreuk op de privacy kan daarbij helpen. Alleen voor zeer gevoelige gegevens verzameld met zeer ingrijpende opsporingsmaatregelen (zoals bodycams) of bijvoorbeeld gegevens verzameld voor de beoordeling op welke manier een persoon betrokken is bij een zaak (categorisering) zijn vaste, korte bewaartermijnen in de wet opgenomen, en ook daarbij is er nog ruimte om de data langer te bewaren als dat noodzakelijk is.

III.6.7 Verstrekken van politiegegevens

Bij gegevensdeling binnen het politiewezen/de strafrechtketen is zoals genoemd het Duitse politionele informatieverbond en het bijbehorende informatiesysteem belangrijk, met het Bundeskriminalamt als centrale coördinerende en ondersteunende dienst; dit is geregeld in

de Wet op het Bundeskriminalamt. Voor gegevensdeling binnen Duitsland met andere partijen maakt de wet onderscheid tussen publieke en niet-publieke organen; de randvoorwaarden zijn gekoppeld aan de politietaak en de taak van de ontvangende partij. Wat betreft gegevensdeling met derde landen en internationale organisaties kent Duitsland als gevolg van rechtspraak van het Bundesverfassungsgericht extra waarborgen bovenop die van de Richtlijn gegevensbescherming opsporing en vervolging: er moet worden getoetst aan rechtsstatelijkheid en mensenrechten; het Bundeskriminalamt houdt hier een overzicht van bij.

Casestudy IV: Finland

IV.1 Inleiding

In deze casestudy staat Finland centraal. Finland is geselecteerd vanwege de grote mate van digitalisering van de Finse overheid en het feit dat Finland een bevolkingsomvang heeft die vergelijkbaar is met Nederland.[128] Tijdens de interviews voor deze casestudy hebben we met een viertal mensen gesproken: een senior adviseur van het Finse ministerie van Binnenlandse Zaken, de deputy Data Protection Ombudsman, een hoogleraar publiekrecht aan de universiteit van Helsinki en de Chief of Information Management van de Finse politie.[129] Voor het deskresearch hebben we gebruik gemaakt van de Engelse vertaling van de twee belangrijkste wetten met betrekking tot de verwerking van politiegegevens. Hoewel deze teksten juridisch niet bindend zijn, nemen we aan dat de vertaling wel up to date is omdat ze ons is verstrekt door de senior adviseur van het Finse ministerie van Binnenlandse Zaken.

Leeswijzer
In de tweede paragraaf van dit hoofdstuk staat het wettelijke kader rondom de Richtlijn centraal. De derde paragraaf staat in het teken van de bevoegde autoriteiten. De verwerking van politiegegevens vormt het onderwerp van de vierde paragraaf. In de vijfde paragraaf wordt vervolgens ingegaan op de vraag hoe het toezicht op deze verwerking van politiegegevens in Finland is geregeld. De laatste paragraaf bevat een aantal lessen die Nederland zou kunnen leren van Finland.

IV.2 Wettelijk kader

IV.2.1 Wettelijk systeem

In Finland is er eigenlijk alleen landelijke regelgeving van toepassing op de politie en het verwerken van persoonsgegevens door de politie. Er is geen significante lokale wet- en regelgeving waar de politie rekening mee moet houden. Op landelijk niveau oefent de regering invloed uit op de politie door middel van regeringsresoluties. Daarnaast zijn er interne politiehandboeken die van toepassing zijn als de politie werkt met persoonsgegevens. Deze handboeken – die niet openbaar zijn – zijn interne richtlijnen over de handelwijze in een bepaalde situatie. Er is daarnaast ook een politiehandboek dat regels geeft ten aanzien van de openbaarheid van het handelen van de politie tijdens strafzaken. Formeel gezien heeft dit handboek niets te maken met gegevensbescherming, de richtlijnen die in dit handboek staan

[128] Ook Estland kent een grote mate van digitalisering van de overheid. Omdat Estland echter een bevolkingsomvang heeft die minder goed vergelijkbaar is met die van Nederland hebben we gekozen voor Finland.
[129] Laatstgenoemde is tevens lid van The National Police Board van de Finse politie.

behoren niet tot het juridische raamwerk van de gegevensbescherming. In een van de interviews kwam ter sprake dat dit handboek in de praktijk wel degelijk ook gaat over databescherming. Zo gaat het bijvoorbeeld over de vraag of je in bepaalde situaties wel of niet iemands naam openbaar mag maken. Daarbij spelen ook vragen rondom databescherming. Hier kunnen conflicten ontstaan tussen het in Finland belangrijke beginsel van openbaarheid van overheidshandelen enerzijds en het belang van databescherming anderzijds. Dit beginsel van openbaarheid is al lang een traditioneel uitgangspunt in Finland. Algemeen is de opvatting dat in beginsel alles wat de overheid doet openbaar moet zijn omdat het daarmee ook controleerbaar is. Burgers moeten toegang hebben tot overheidsinformatie en belangrijke documenten. Dit zorgt soms voor conflicten met de EU-databeschermingsregels.

Omzetting van de Richtlijn gegevensbescherming opsporing en vervolging

De Richtlijn is door Finland omgezet door wijziging van een aantal al bestaande wetten. Er is dus niet één specifieke wet die de Richtlijn omzet. Finland kent één algemene wet met betrekking tot de verwerking van persoonsgegevens in strafzaken. Dat is de *Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (1054/2018; Law Enforcement Data Protection Act)*. Deze wet is gewijzigd onder verantwoordelijkheid van het Finse Ministerie van Justitie en geeft de algemene regels voor het verwerken van persoonsgegevens in het kader van strafzaken. De verwerking van persoonsgegevens specifiek door de politie wordt ook beheerst door de *Act on the Processing of Personal Data by the Police (616/2019)*. Dit is een speciale, aanvullende wet ten opzichte van de algemene wet en geldt alleen voor de politie als bevoegde autoriteit. Deze wet is op grond van de Richtlijn volledig herzien. De herziening heeft plaatsgevonden onder verantwoordelijkheid van het Finse Ministerie van Binnenlandse Zaken, het ministerie dat verantwoordelijk is voor de Finse politie. Ook voor een aantal andere bevoegde autoriteiten is er een speciale wet.[130]

De politie was betrokken tijdens het proces van de omzetting van de Richtlijn. Binnen de politieorganisatie bestaat de indruk dat de betrokken ministeries sowieso goed op de hoogte zijn van de wensen van de politie. Wel is het zo dat er niet altijd goed in beeld is wat de mogelijke knelpunten zijn waar de politie tegenaan zou kunnen lopen. Dat blijkt vaak pas als er in de praktijk met de regelgeving wordt gewerkt. Een van deze knelpunten heeft betrekking op de inzet en het gebruik van nieuwe technologieën. Dit heeft ten dele te maken met een opvallend punt dat uit de interviews naar voren kwam met betrekking tot het omzettingsproces van de Richtlijn. Het Finse parlement heeft namelijk een aantal bepalingen over de inzet van nieuwe technologieën voor het verwerken van data door de politie aangepast. In het oorspronkelijke voorstel van de regering waren enkele bepalingen opgenomen over het bewaren en verwerken van gegevens om zo te kunnen analyseren en beoordelen of deze gegevens nodig zijn voor politietaken. Het idee was dat de politie bijvoorbeeld publiekelijk beschikbare gegevens zes maanden zou kunnen bewaren en de gegevens zou kunnen beoordelen met behulp van 'moderne technologie'. Het deel van deze bepalingen dat sprak over de inzet van 'moderne technologie' is door het parlement uit de wet geamendeerd.[131]

Naast de politie is ook de Data Protection Ombudsman betrokken geweest tijdens het proces van de omzetting van de Richtlijn.[132] Er is in Finland wettelijk vastgelegd dat hij betrokken

[130] Hiervan hebben wij geen Engelse vertaling tot onze beschikking. Daarnaast hebben wij er vanwege de noodzaak tot afbakening van het onderzoek voor gekozen te focussen op de politie.

[131] De definitieve formulering in section 5 en section 7 van de *Act on the Processing of Personal Data by the Police* is geworden: '*The data received in connection with the performance of police duties shall be destroyed immediately after it is established that the information is not needed for the processing purposes referred to in subsection 1 or section 13, subsection 1.*'

[132] De Data Protection Ombudsman is de algemene toezichthouder op het gebied van databescherming in Finland. In paragraaf IV.5 wordt er meer aandacht aan hem en zijn bevoegdheden besteed.

moet worden bij het wetgevingsproces als het gaat om wetgeving die te maken heeft met privacy.

Er zijn ook experts uit de academische wereld betrokken geweest bij de omzetting van Richtlijn 2016/680. Het is in Finland gebruikelijk dat academische experts advies geven tijdens het wetgevingsproces. Een manier waarop dat gebeurt is door middel van een door het betrokken ministerie ingestelde adviesgroep van ambtenaren en academische experts. Ook is het in Finland gebruikelijk dat er alvorens het Finse parlement stemt over een wet een zogenoemde 'constitutionele review' plaats vindt van de wet. Ook bij deze review zijn academische experts betrokken. Het parlement is niet verplicht om de gegeven adviezen over te nemen, maar dat gebeurt vaak wel.

Verhouding tussen de algemene en de speciale wet

Zoals gezegd geeft de *Law Enforcement Data Protection Act* de algemene regels die gelden voor alle bevoegde autoriteiten die zich bezighouden met de verwerking van persoonsgegevens in het kader van strafzaken. De speciale wetten voor deze bevoegde autoriteiten – dus ook de *Act on the Processing of Personal Data by the Police* – zijn bedoeld als aanvullend ten opzichte van de algemene wet. Deze wetten zijn veel gedetailleerder en werken de regels en bevoegdheden die gelden voor de specifieke bevoegde autoriteit nader uit. De *Act on the Processing of Personal Data by the Police* is dus echt bedoeld als een aanvulling op de algemene wet, de politie is ook onderworpen aan de algemene wet en de bevoegdheden die in de beide wetten staan worden geacht niet met elkaar in tegenspraak te zijn. In de interviews werd aangegeven dat dit in de praktijk ook inderdaad het geval is. De beide wetten zijn goed op elkaar afgestemd en er bestaan geen tegenstrijdigheden tussen de beide wetten. De situatie dat er in een specifieke zaak op grond van beide wetten andere regels gelden komt dan ook niet of nauwelijks voor, is de ervaring van de politie.

De wetgeving in de praktijk

De regels die in de *Act on the Processing of Personal Data by the Police* zijn neergelegd, zijn vrij strikt en gedetailleerd geformuleerd. Dit wordt door de politie niet als een heel groot probleem ervaren. Vanwege het belang van databescherming is het voor de politie goed te begrijpen dat de geldende regels strikt en gedetailleerd zijn. In de praktijk blijkt echter wel dat politieagenten die met de verschillende wetten moeten werken soms niet helemaal goed weten welke regels er in hun specifieke zaak van toepassing zijn. Dit komt mede omdat het door de implementatie van de Richtlijn in sommige specifieke cases is veranderd welke wet- en regelgeving er van toepassing is. Ook is het in de praktijk niet altijd duidelijk of in een specifieke casus het wettelijke AVG-regime of het juridische kader van de Richtlijn van toepassing is. De Data Protection Ombudsman vindt het een voordeel dat de wet- en regelgeving vrij gedetailleerd is. Dat geeft namelijk duidelijke handvatten voor het houden van toezicht, het is duidelijk waar precies op moet worden gelet.

Een ander probleem dat speelt is dat de terminologie die er in de wetten wordt gebruikt niet altijd even helder is. Zo geldt de *Act on the Processing of Personal Data by the Police* alleen als er sprake is van een strafzaak, maar de definitie van een strafzaak is erg vaag. In de wet zelf is bijvoorbeeld geen definitie van deze term gegeven. Wat de exacte definitie van deze term en daarmee de reikwijdte van de wet is, is dus niet altijd duidelijk.

IV.2.2 Opvallende punten in de wet- en regelgeving

Expliciete aandacht voor het respecteren van mensenrechten

Een opvallend punt in de Finse wetgeving is de expliciete aandacht die in de inleidende bepalingen wordt gegeven aan het respecteren van de fundamentele rechten van de mens en een aantal fundamentele beginselen. De Finse politie vindt het goed dat er speciale aandacht wordt besteed aan het respecteren van deze fundamentele rechten en beginselen en geeft aan dat dit in de praktijk geen grote problemen voor oplevert. In de tweede section van het eerste hoofdstuk van de *Act on the Processing of Personal Data by the Police* staat bijvoorbeeld de volgende bepaling:

> *'The processing of personal data shall comply with the requirement of respect for fundamental and human rights, the principle of proportionality, the principle of minimum intervention, and the principle of intended purpose laid down in chapter 1 of the Police Act.'*[133]

Een dergelijke expliciete bepaling is niet terug te vinden in de Richtlijn noch in de Nederlandse Wet politiegegevens. Ook in de algemene Finse politiewet[134] die in bovenstaande bepaling wordt genoemd is er expliciet aandacht voor het respecteren van mensenrechten:

> *'The police shall respect fundamental and human rights and, in exercising their powers, choose from all reasonable options the course of action that best asserts these rights.'*[135]

Europol en Interpol

Een tweede opvallend punt is dat er in de Finse wetgeving meer en uitgebreidere bepalingen zijn opgenomen over het delen van gegevens met Europol en Interpol dan dat er in de Richtlijn zijn opgenomen.

IV.3 De bevoegde autoriteiten

IV.3.1 Algemeen

Er is in de Finse wet- en regelgeving nergens een lijstje te vinden wie precies de bevoegde autoriteiten zijn op grond van de Richtlijn. In een van de interviews werd gesteld dat de bevoegde autoriteiten 'die autoriteiten zijn die taken hebben die vallen onder de reikwijdte van de Richtlijn'. Er is in de *Law Enforcement Data Protection Act* wel een algemene definitie opgenomen van het begrip bevoegde autoriteit:

> *'competent authority means any public authority competent for the prevention, detection, investigation, referral for consideration of charges, consideration of charges or other activities relating to the prosecution of criminal offences, conviction and sentencing or the execution of criminal penalties, including safeguarding against and preventing threats to public security, as well as the Defence Forces, the police and the Border Guard when performing duties referred to in section 1, subsection 2;'*[136]

Op de website van de Finse politie is een informatiepagina te vinden over de wetgeving met betrekking tot databescherming. Daar wordt gesteld dat de *Law Enforcement Data Protection*

[133] Section 2.
[134] Van deze wet – in het Engels *Police Act* – is een niet-actuele Engelse vertaling beschikbaar. Deze wet gaat veel meer in op de algemene bevoegdheden, taken en organisatie van de politie.
[135] Section 2.
[136] Section 3 onder 5.

Act van toepassing is op 'de politie, algemene rechtbanken, de Criminal Sanctions Agency, de douane, de grenspolitie en andere bevoegde autoriteiten'.[137] Wij nemen aan dat de in dit citaat genoemde autoriteiten dus in ieder geval bevoegde autoriteiten in de zin van de Richtlijn zijn. Tijdens een van de interviews is ter sprake gekomen dat de *Law Enforcement Data Protection Act* in ieder geval ook van toepassing is op het leger.

In de *Act on the Processing of Personal Data by the Police* is een definitie opgenomen van '*competent Schengen authorities*'.[138] Deze '*competent Schengen authorities*' worden verder alleen genoemd in Section 26 (*Disclosure of personal data in the National Schengen Information System)*; we gaan er dus van uit dat dit niet verwijst naar de term bevoegde autoriteiten zoals die wordt gebruikt in de Richtlijn en de daaruit voortvloeiende wet- en regelgeving. De Finse wetgever heeft ervoor gekozen om in de nationale wetgeving ook de inlichtingen- en veiligheidsdienst (intelligence service) als bevoegde autoriteit te zien, terwijl deze autoriteit formeel gezien niet onder de reikwijdte van de Richtlijn valt.

IV.3.2 Structuur van de politie

De belangrijkste bevoegde autoriteit is de politie. Finland kent één nationale politieorganisatie, die wordt bestuurd door de *National Police Board*. Dit nationale bestuur regisseert en begeleidt politieoperaties en valt onder de verantwoordelijkheid van het Ministerie van Binnenlandse Zaken. Het ministerie oefent invloed uit op de politie door middel van regeringsresoluties. De Finse politie kent elf lokale politieafdelingen, die allemaal vallen onder de verantwoordelijkheid van het nationale bestuur. Op landelijk niveau zijn er twee belangrijke politie units: het nationale onderzoeksbureau (The National Bureau of Investigation; gespecialiseerd in het voorkomen van georganiseerde misdaad) en de politieschool (The Police University College; *'responsible for police training recruitment, for selection of students, for organizing diploma and advanced studies, for further training given in the training institute and for research and development in the police field'*).[139] Ook zij vallen onder verantwoordelijkheid van het *National Police Board.*

Onderstaand organogram geeft een schematische weergave van de structuur van de Finse politie.

[137] ttps://www.poliisi.fi/about_the_police/data_protection_and_the_rights_of_data_subjects/data_protection_legislation.
[138] Section 3 onder 4.
[139] Zie ook: https://www.poliisi.fi/about_the_police/organisation.

THE FINNISH POLICE

SUPREME POLICE COMMAND

Ministry of the Interior, Police Department

NATIONAL POLICE UNITS

National Bureau of Investigation
National Traffic Police
Security Police

POLICE TRAINING INSTITUTES

Police School
The Police College of Finland

OTHER UNITS

Police Technical Centre
Police IT Management Agency

PROVINCIAL POLICE COMMAND

Police Departments of the Provinces

LOCAL POLICE

District Police
Police District of the Åland Islands

Helsinki Police Department

PO/Tiedotus 9/2002

IV.4 Verwerken van politiegegevens

IV.4.1 Algemeen

Eisen voor de verwerking van politiegegevens

Voor het bewerken van politiegegevens geldt ten eerste de algemene eis dat dit alleen mag als dat noodzakelijk is voor de uitoefening van een wettelijke taak van een bevoegde autoriteit en als dat valt binnen de reikwijdte van de eerste section van de *Law Enforcement Data Protection Act*.[140] Op grond van de zesde section van deze wet geldt daarnaast de eis dat de persoonsgegevens die worden verwerkt passend en noodzakelijk moeten zijn in verband met de doeleinden van de verwerking. De gegevens mogen echter niet bovenmatig zijn in verhouding tot de doeleinden waarvoor zij worden verwerkt en moeten juist en up to date zijn.[141]

Ook de *Act on the Processing of Personal Data by the Police* bevat een hoofdstuk waarin regels zijn opgenomen voor de verwerking van persoonsgegevens.[142] Deze regels zijn veel specifieker dan de hierboven genoemde sections en vullen de meer algemene regels waar nodig aan. De *Act on the Processing of Personal Data by the Police* geeft bijvoorbeeld in section 4 en verder aan welke specifieke persoonsgegevens in het kader van welke bevoegdheid/taak mogen worden verwerkt. Het gaat dan bijvoorbeeld om iemands naam, geboortedatum en geboorteplaats, geslacht en woonplaats.[143]

Na deze section volgen er in de sections 5, 7, 9 en 11 vier doelen in het kader waarvan de genoemde gegevens mogen worden verwerkt.

Section 5: Processing of personal data in investigations and surveillance

Section 7: Processing of personal data for the purpose of preventing and detecting offences

Section 9: Processing of data of covert human intelligence sources

Section 11: Processing of personal data in other statutory duties of the police

Daarnaast noemt section 8 nog een extra doel waar bepaalde – aanvullende – persoonsgegevens voor mogen worden verwerkt.

'Section 8 Contents of personal data that are processed for the purposes of prevention and detection of offences

In addition to the basic personal data referred to in section 4, the police may also process the following personal data concerning the persons referred to in section 7:

1) specifications, descriptions and classifications relating to police duties, actions or operations;

[140] Zie de vierde section van deze wet.
[141] Zie voor deze laatste eis section 7 van de *Law Enforcement Data Protection Act*; deze eis volgt rechtstreeks uit de Richtlijn.
[142] Hoofdstuk 2.
[143] Section 4 is integraal opgenomen in Bijlage 3.

2) details concerning the person's connections, lifestyle, financial situation, hobbies, and other interests;

3) personal identifying characteristics to establish identity, including voice samples, facial images and other biometric data;

4) information for the purpose of safeguarding the safety of a person who is the subject of an action or the occupational safety of an official, concerning the person's state of health and its monitoring or the treatment of his or her condition and concerning the danger presented by or unpredictability of the subject or the person; and information that describes or is intended to describe a criminal act, punishment or other consequence of an offence.

Where possible, an assessment of the reliability of the data provider or data source and the accuracy of the data shall be appended to the personal data obtained.'

Verwerken van bijzondere categorieën persoonsgegevens

In art. 10 van Richtlijn 2016/680 is een regeling opgenomen die gaat over de verwerking van bijzondere categorieën persoonsgegevens. Onder bijzondere categorieën van persoonsgegevens wordt verstaan:

'Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijkt, en verwerking van genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een natuurlijke persoon, gegevens over gezondheid of gegevens over seksueel gedrag of seksuele gerichtheid van een natuurlijke persoon.'

Dergelijke persoonsgegevens mogen alleen worden verwerkt als dat strikt noodzakelijk is en *'geschiedt met inachtneming van passende waarborgen voor de rechten en vrijheden van de betrokkene.'* Daarnaast gelden er nog drie criteria waaraan moet zijn voldaan:

a. De verwerking moet bij het Unierecht of het lid statelijke recht zijn toegestaan;
b. De verwerking moet noodzakelijk zijn om vitale belangen van de betrokkene of een andere natuurlijke persoon te beschermen;
c. of die verwerking heeft betrekking op gegevens die kennelijk door de betrokkene zelf openbaar zijn gemaakt.

De Finse wetgever heeft hier nog een vierde criterium aan toegevoegd:

'relates to the consideration of a criminal case in the prosecution service or in court.'[144]

Er mogen onder meer zogenaamde 'gevoelige gegevens' (sensitive data) worden verwerkt als deze verwerking betrekking heeft op de behandeling van een strafzaak door het openbaar ministerie of in de rechtbank, deze verwerking strikt noodzakelijk is en onder voorbehoud van passende waarborgen voor de rechten van de betrokkene.

[144] Zie section 11 van de *Law Enforcement Data Protection Act*.

Het vierde criterium wordt niet genoemd in de Richtlijn. Het opnemen van dit extra criterium werd noodzakelijk geacht door de Finse wetgever omdat de Finse grondwet vereist dat bepalingen inzake de bescherming van persoonsgegevens in de wet worden vastgelegd. De Finse commissie voor constitutioneel recht heeft op grond van de interpretatie van deze bepaling geëist dat met name de verwerking van speciale categorieën persoonsgegevens duidelijk en expliciet in de wet wordt vastgelegd.

De autoriteiten (zoals rechtbanken en aanklagers) hebben altijd een duidelijke rechtsgrond nodig om bijzondere categorieën gegevens te verwerken. Er zijn in Finland specifieke wetten die de verwerking van persoonsgegevens door verschillende bevoegde autoriteiten, zoals de politie, regelen. Normaliter bevatten deze wetten gedetailleerde bepalingen over wanneer, welke speciale categorieën gegevens door die autoriteiten mogen worden verwerkt. Er was echter in Finland geen wet die gegevensbescherming specifiek regelt bij de activiteiten van rechtbanken en openbare aanklagers. De Finse wetgever vond het daarom het beste om deze rechtsgrondslag op te nemen in de *Law Enforcement Data Protection Act*.

In section 11 van de *Law Enforcement Data Protection Act* is daarnaast expliciet benoemd dat het verboden is gebruik te maken van *profiling* als dat resulteert in discriminatie op grond van één van deze bijzondere categorieën van persoonsgegevens. Er is dus geen algeheel verbod voor het inzetten van profiling opgenomen. Ook dit is een uitbreiding die de Finse wetgever heeft gedaan ten opzichte van de Richtlijn. Een dergelijke expliciete verbodsbepaling is in de Richtlijn namelijk niet opgenomen. Het past wel bij de eerdergenoemde speciale aandacht die er in Finland aan wordt gegeven dat de verwerking van data altijd in overeenstemming moet zijn met fundamentele rechten van de mens.

Section 15 van de *Act on the Processing of Personal Data by the Police* geeft nog aanvullende regels voor de verwerking van bijzondere persoonsgegevens. Deze regels zien met name op de verwerking van biometrische data. Zo mogen biometrische data die worden verwerkt voor de uitvoering van de taken die zijn vastgelegd in de Identiteitskaartwet en de Paspoortwet mogen alleen worden gebruikt voor andere doeleinden dan het oorspronkelijke doel als dit strikt noodzakelijk is voor de identificatie van slachtoffers van een natuurramp, een zwaar ongeval of een andere ramp of een misdrijf , of slachtoffers die om een andere reden ongeidentificeerd blijven.[145]

Praktijkervaringen

Zoals al eerder in deze uitwerking aangegeven, is naast de regelgeving die voortvloeit uit de Richtlijn ook de AVG van toepassing in veel individuele strafzaken. Tijdens een van de gesprekken werd de aandacht erop gevestigd dat het niet altijd helder is wanneer welke van de wettelijke regimes van toepassing is. Dat is mede het gevolg van het feit dat dit na de inwerkingtreding en omzetting van de Richtlijn gedeeltelijk is veranderd. In sommige specifieke zaken waar daarvoor de AVG van toepassing is, is dat nu ineens de Richtlijn of omgekeerd. In één van de interviews werd aangegeven dat het voor de politie soms niet duidelijk is wat nu precies de hiërarchie van deze regelingen is. Als op één casus beide regimes van toepassing zijn en beide wat anders vereisen, is veelal niet duidelijk aan welke van de twee systemen voorrang moet worden gegeven. Mede om dit probleem te ondervangen moeten alle politieagenten in Finland tegenwoordig een cursus volgen die specifiek gaat over databescherming en de regels die daarbij komen kijken.

[145] Section 15 is integraal opgenomen in Bijlage 3.

Een ander punt waarop de verkrijging en verwerking van data in de praktijk niet geheel onproblematisch is betreft het verzamelen, analyseren en verwerken van data die onderdeel uitmaken van zogenoemde big-datasets. Op dit moment is er geen wettelijke mogelijkheid voor de politie om bij de verwerking van dergelijke datasets gebruik te maken van Artificial Intelligence. Dat betekent dat de politie deze data veelal handmatig moet verwerken. Dat is in de praktijk niet te doen, met als gevolg dat niet alle data en informatie uit dergelijke grote datasets op de gewenste wijze door de politie kan worden verwerkt. De politie mist daardoor waarschijnlijk relevante informatie die er met behulp van Atificial Intelligence wel uit was gepikt.

De politie heeft niet het idee dat zij *overall* gezien onvoldoende mogelijkheden en grondslagen heeft om de benodigde gegevens te kunnen verwerken. Het enige punt waarbij het daar wel aan schort is, zoals eerder aangestipt, het verzamelen van data met behulp van nieuwe technologie. Hier wordt later nog wat uitgebreider op terug gekomen.

IV.4.2 Verkrijgen van politiegegevens

Algemeen

In de twee eerder genoemde wetten waarmee in Finland de Richtlijn is omgezet, wordt er met betrekking tot de verwerking van politiegegevens één algemene omschrijving gebruikt: verwerken (in het Engels: *processing*). De definitie van deze term is te vinden in Section 3, onder 2 van de *Law Enforcement Data Protection Act*:

> *'processing means collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction and any other operation or set of operations which is performed on personal data or on sets of personal data;'*

Er is slechts één artikel te vinden dat specifiek gaat over het verzamelen van data. Dat betreft de vijfde section van de *Law Enforcement Data Protection Act*, waar met zoveel woorden in staat dat persoonsgegevens alleen mogen worden verzameld in het kader van specifieke, geexpliciteerde en legitieme doeleinden.[146]

> *'The police may process personal data for the purposes of a criminal investigation, police investigation or performing other duties related to investigation of an offence or referral of cases for consideration of charges, and performing duties related to maintaining public order and security or other statutory surveillance duties of the police.'*

Om in het kader van deze doelstellingen gegevens te mogen verzamelen moet het gaan om gegevens die betrekking hebben op een persoon die:

1. Verdacht wordt van een strafbaar feit of medeplichtigheid daaraan;
2. Jonger is dan vijftien jaar en wordt verdacht van een misdrijf;

[146] Law Enforcement Data Protection Act, section 5; data die in het kader van de uitoefening van politietaak worden verkregen moeten worden vernietigd onmiddellijk nadat komt vast te staan dat de gegevens niet nodig zijn voor de verwerkingsdoeleinden, bedoeld in het eerste lid of artikel 13, eerste lid van de *Law Enforcement Data Protection Act.*

3. Het voorwerp is van een strafrechtelijk onderzoek, een politieonderzoek of politieoptreden;
4. Aangifte doet van een misdrijf of de benadeelde partij is;
5. Getuige is;
6. Slachtoffer is;
7. Rechtstreeks verband houdt met een veldoperatie van de politie of een toezichtstaak die afzonderlijk bij wet is bepaald;
8. Een andere informatiebron is met betrekking tot politietaken.

Grondslagen

De redenen en grondslagen voor het verzamelen van gegevens door de politie staan in verschillende wetten. Het is dus niet zo dat er één wet is waar alle redenen en grondslagen voor de politie in staan voor de verzameling en verdere verwerking van persoonsgegevens. In de eerste paragraaf van section 1 van de *Police Act (872/2011)* staat de algemene taak van de Finse politie weergegeven:

> *'The duty of the police is to secure the rule of law; maintain public order and security; prevent, detect and investigate crimes; and submit cases to prosecutors for consideration of charges. The police work in cooperation with other public authorities and with communities and residents in order to maintain security, and they engage in international cooperation pertaining to their duties.'*

De *Act on the Processing of Personal Data by the Police* is van toepassing voor de noodzakelijke verwerking van gegevens ter uitvoering van bovengenoemde taak. Voor de uitoefening van die taken is er daarmee een grondslag voor de verwerking van politiegegevens.

Ook de *Law Enforcement Data Protection Act* – zoals gezegd de algemene wet die geldt voor alle bevoegde autoriteiten in de zin van de Richtlijn – benoemt in welke gevallen de wet van toepassing is:

> *'This Act applies to the processing of personal data by competent authorities in the context of*
>
> *1) preventing, detecting or investigating criminal offences or referring them for consideration of charges;*
>
> *2) consideration of charges and other activities of a prosecutor in relation to a criminal offence;*
>
> *3) hearing a criminal case in court;*
>
> *4) enforcing a criminal sanction;*
>
> *5) safeguarding against, and preventing threats to, public security in connection with activities referred to in paragraphs 1–4.'* [147]

[147] Zie section 1 van de genoemde wet.

Als de politie zich met één van de genoemde taken bezighoudt is er dus een grondslag voor het verkrijgen en verder verwerken van persoonsgegevens. Dat geldt in het bijzonder voor een aantal wettelijke taken anders dan de opsporing en het voorkomen van strafbare feiten.[148]

De vijfde section van de *Law Enforcement Data Protection Act* geeft aan dat naast de andere genoemde grondslagen, data ook mag worden verzameld in het kader van '*scientific, statistical or historical purposes if appropriate safeguards exist for the rights of the data subject*.' Deze bepaling komt voort uit art. 9 lid 2 van de Richtlijn.

IV.4.3 Bewerken van politiegegevens

We hebben zowel in de interviews als in de wet- en regelgeving geen punten kunnen vinden die enkel betrekking hebben op het bewerken van politiegegevens.

IV.4.4 Categoriseren en labelen van politiegegevens

Met betrekking tot het categoriseren van data zijn er geen expliciete regels opgenomen in de twee wetten waarmee de Richtlijn is omgezet. In de interviews is aangegeven dat in de wetgeving wel wordt gesproken over de categorisering van data. Wij vermoeden dat er dan wordt gedoeld op het feit dat er in de *Act on the Processing of Personal Data by the Police* een aantal sections zijn waarin, zoals hierboven al even werd aangestipt, wordt aangeven welke specifieke data de politie in een specifiek soort zaak mag verzamelen. Te denken valt bijvoorbeeld aan de eerder genoemde vier sections over de doelstellingen waarvoor gegevens mogen worden verwerkt.

Section 5: Processing of personal data in investigations and surveillance

Section 7: Processing of personal data for the purpose of preventing and detecting offences

Section 9: Processing of data of covert human intelligence sources

Section 11: Processing of personal data in other statutory duties of the police

Daaruit zou kunnen worden opgemaakt dat dit categorieën zijn waarin de verzamelde gegevens moeten worden ingedeeld. Er zijn in ieder geval geen technische regels opgenomen in de wetgeving. Hoe de categorisering technisch wordt aangepakt in de interne systemen van de politie staat de politie volledig vrij.

Er wordt door de Finse politie in de praktijk wel gedaan aan het categoriseren van de verzamelde politiegegevens. Ten eerste wordt er een onderscheid gemaakt op basis van de doelstelling waarvoor de data worden verzameld en verwerkt en de manier waarop dit gebeurt. De doestellingen van de gegevens verzameling bepalen namelijk welke gegevens door wie mogen worden gebruikt. Op grond daarvan vindt er categorisatie van de gegevens plaats.
Ook wordt er door de politie een onderscheid gemaakt tussen openbare, niet-openbare en geheime data. Met betrekking tot de categorisering van data in strafzaken wordt er volgens een van de geïnterviewden ook een onderscheid gemaakt op grond van de intensiteit van het gepleegde strafbare feit. Deze intensiteit kan worden afgeleid uit de straf die kan worden opgelegd voor het delict.

[148] Zie section 11 van de Act on the Processing of Personal Data by the Police.

Daarnaast wordt er een onderscheid gemaakt tussen feiten en meningen. Dit is expliciet opgenomen in de Finse wetgeving (section 8 van de *Law Enforcement Data Protection Act)* en vloeit rechtstreeks voort uit art. 7 lid 1 van de Richtlijn. De eerder genoemde speciale categorieën van persoonsgegevens worden uiteraard als zodanig gelabeld.

De – op grond van de Richtlijn deels verplichte – categorisering van persoonsgegevens is in de praktijk nog weleens lastig. Dit heeft volgens een van de geïnterviewden te maken met de veelheid aan regels die er bestaan op het gebied van de categorisering van data en het feit dat vele van deze regels vatbaar zijn voor interpretatie.[149] Hierdoor raken politieagenten snel het overzicht kwijt en weten ze soms niet goed in welke categorie bepaalde persoonsgegevens moeten worden ingedeeld.

Categorisering van de verzamelde data is onder andere van belang in het kader van de bescherming van de persoonlijke levenssfeer van personen. Eén van de punten waarop mensen op grond van de Richtlijn inzage kunnen verzoeken, is de categorieën persoonsgegevens die over hen worden verzameld. Daarnaast is de categorisering van data belangrijk omdat de geldende bewaartermijnen voor verzamelde persoonsgegevens gekoppeld zijn aan de categorie waarin de gegevens vallen.

IV.4.5 Bewaartermijnen en vernietigingsgronden

Wettelijk kader

Hoe lang verzamelde persoonsgegevens mogen worden bewaard is afhankelijk van de categorie waarin de data vallen en dan met name de vraag voor welk doel de data zijn verzameld. De bewaartermijnen zijn zeer gedetailleerd neergelegd in het vijfde hoofdstuk van de *Act on the Processing of Personal Data by the Police*.[150] Soms is de bewaartermijn uitgedrukt in een specifiek aantal jaren, soms is er enkel vermeld dat verzamelde persoonsgegevens zo lang mogen worden bewaard als nodig is voor het doen van het strafrechtelijke onderzoek of het uitvoeren van de politietaak waarvoor de gegevens zijn verzameld. De correcte toepassing van deze bewaartermijnen wordt gecontroleerd door de Data Protection Ombudsman.[151] Als algemene regel geldt dat verzamelde data die niet noodzakelijk blijken te zijn zonder 'onnodige vertraging' moeten worden verwijderd.[152]

Praktijkervaringen

Tijdens het proces van de omzetting van de Richtlijn is er met de politie van gedachten gewisseld over de vraag wat een goede bewaartermijn zou zijn voor de verschillende categorieën van data. De politie geeft aan dat de termijnen die er gelden over het algemeen voldoende zijn en dat zij daar goed mee kan werken. Volgens de politie is het voor hen ook duidelijk wanneer data moeten worden gewist. Een van de geïnterviewden wierp de vraag op of burgers van wie de gegevens worden verzameld kunnen weten hoe lang hun gegevens eigenlijk worden bewaard. Omdat de regels die gelden voor categoriseren van data en daarmee het

[149] Er zijn zoals gezegd geen specifieke regels met betrekking tot de categorisering van data opgenomen in de wetgeving. Vermoedelijk zal er hier zoals gezegd dan ook worden gedoeld op de sections van de *Act on the Processing of Personal Data by the Police* waarin wordt aangeven welke specifieke data de politie in een specifiek soort zaak mag verzamelen. Verzamelde persoonsgegevens worden onder andere ingedeeld naar de soort zaak (doelstelling) waarvoor ze worden verzameld.

[150] In hoofdstuk 7 van deze wet zijn nog bepalingen opgenomen die specifiek zien op de veiligheidsdiensten (intelligence services). Omdat deze diensten officieel niet binnen de reikwijdte van de Richtlijn vallen, wordt op deze termijnen in dit onderzoek niet nader ingegaan.

[151] Op het aspect van toezicht wordt uitgebreider ingegaan in paragraaf 5.

[152] Zie Section 6 van de Law Enforcement Data Protection Act.

bewaren van data volgens deze gesprekspartner vrij complex zijn, kan dit lastig zijn. Het is daarmee ook lastiger voor burgers om hun rechten, zoals het krijgen van toegang tot de over hen verzamelde gegevens, uit te oefenen.

IV.4.6 Delen van politiegegevens

Delen van politiegegevens binnen Finland

De Finse politie mag gegevens delen met andere autoriteiten binnen Finland. Hiervoor is een grondslag neergelegd in het vierde hoofdstuk van de *Act on the Processing of Personal Data by the Police*. In section 21 is opgenomen met welke andere bevoegde autoriteiten gegevens mogen worden gedeeld. In de 22e section is een lijst opgenomen van andere – dus niet-bevoegde – autoriteiten waarmee de politie gegevens mag delen. Hierbij geldt wel steeds het expliciete wettelijke voorbehoud dat het niet mag gaan om geheime data, die mogen met geen enkele andere autoriteit worden gedeeld.

Opvallend is dat er een uitgebreid artikel in de bovengenoemde wet is opgenomen over het delen van informatie via publieke informatienetwerken:

> ***'Section 23 Disclosure of personal data via a public information network***
>
> *Notwithstanding secrecy provisions, the police may disclose, via a public information network, information for the purpose of informing the general public and receiving leads from the public, where this is necessary due to crime prevention, returning property to its owner, or investigative reasons. In such cases, personal data may only be retrieved based on individual searches.*
>
> *Notwithstanding secrecy provisions, the police may also disclose, via a public information network, information for the purpose of informing the general public and receiving leads from the public, where this is particularly necessary due to the urgency of the matter, a dangerous situation, crime prevention, and returning property to its owner, or investigative reasons. Personal data may be disclosed in a manner other than that referred to in subsection 1 only if this is materially important for the performance of a duty laid down in chapter 1, section 1, subsection 1 of the Police Act and the disclosure of the data does not conflict with a legitimate interest of the data subject. Data received from another authority may only be disclosed with the consent of the authority that disclosed the data.'*

Volgens één van de geïnterviewden wordt onder publieke informatienetwerken verstaan het internet of andere publiek toegankelijke informatiebronnen. Alle gegevens die publiekelijk toegankelijk zijn via internet of andere publiek toegankelijke informatiebronnen vallen daarmee onder dit artikel. Voor sociale media geldt dat dit artikel alleen van toepassing is zolang de gegevens daarop openbaar zijn en gevonden kunnen worden.

Delen van politiegegevens met andere landen

De Finse politie deelt veel data met andere landen. Er is een uitgebreid juridisch kader hiervoor opgenomen in hoofdstuk 7 van de *Law Enforcement Data Protection Act*. Dit hoofdstuk bevat de volgende artikelen:

- Section 41: General principles for transfers of personal data
- Section 42: Transfer based on appropriate safeguards

- Section 43: Derogations for specific situations
- Section 44: Transfers of personal data to private entities and other recipients established in third countries

In sections 25 en 31 van de *Act on the Processing of Personal Data by the Police* zijn een aantal aanvullende regels neergelegd voor het delen van persoonsgegevens met andere landen. Ook geldt nog de algemene eis dat die is neergelegd in artikel 10 van de *Law Enforcment Data Protection Act*:

> *'When the competent authority transfers personal data to a recipient located within the EU, it shall not impose stricter conditions for the processing of the data than those applied nationally to similar transfers of data.'*

Opvallend is dat in de *Act on the Processing of Personal Data by the Police* aparte artikelen zijn opgenomen over het delen van gegevens met Europol en het delen van gegevens binnen het Schengen-informatiesysteem. Dergelijke bepalingen zijn niet terug te vinden in de Richtlijn.

> ***'Section 26 Disclosure of personal data in the National Schengen Information System***
>
> *Notwithstanding secrecy provisions, the police may disclose data in the National Schengen Information System to competent Schengen authorities in compliance with the legislative basis for the Schengen Information System. Data may also be disclosed with the aid of a technical interface or as a set of data.*
>
> ***Section 27 Disclosure of personal data to states using the Schengen Information System and to the Schengen Information System***
>
> *Notwithstanding secrecy provisions, the police may disclose data referred to in the legislative basis for the Schengen Information System that are necessary for the purposes laid down in the legislative basis to the competent authorities of Schengen States and for recording in the Schengen Information System. The supplementary information referred to in the legislative basis for the Schengen Information System shall be supplied via the Sirene Bureau. The Finnish national Sirene Bureau is the National Bureau of Investigation. Data may also be disclosed with the aid of a technical interface or as a set of data.*
>
> ***Section 28 Disclosure of personal data to Europol***
>
> *Notwithstanding secrecy provisions, the police may disclose personal data to the European Union Agency for Law Enforcement Cooperation in compliance with the Europol Regulation and the Act on the European Union Agency for Law Enforcement Cooperation (214/2017).'*

Praktijkervaringen

De Finse politie ervaart over het algemeen geen moeilijkheden bij het delen van data met andere landen en internationale organisaties. Dat gebeurt dagelijks en verloopt naar tevredenheid. De meeste gegevensuitwisseling verloopt via Europol en Interpol, maar er worden ook gegevens rechtstreeks met andere landen gedeeld. De Data Protection Ombudsman heeft – vanuit zijn betrokkenheid als toezichthouder – de indruk dat er op dit punt nog een

aantal open einden in de wetgeving zitten en dat een dergelijke rechtstreekse gegevens uitwisseling in de praktijk lastig is en moeizaam verloopt. Zo is de manier waarop persoonsgegevens rechtstreeks met andere landen mogen worden uitgewisseld niet wettelijk geregeld en blijven de eisen die daarvoor gelden deels vaag. Een voorbeeld daarvan is de eerste paragraaf van section 42 van de *Act on the Processing of Personal Data by the Police.*

> *'If the Commission has not made a decision referred to in section 41, subsection 1, paragraph 3, personal data may be transferred to a third country or an international organisation if the other conditions laid down in section 41 are met and*
>
> *1) appropriate safeguards with regard to the protection of personal data are provided for in a legally binding instrument; or*
>
> *2) the controller has assessed all the circumstances surrounding the transfer of personal data*
>
> *and concludes that appropriate safeguards exist with regard to the protection of personal data.'*

De termen die heir worden gebruikt scheppen niet op zichzelf helderheid, maar vergen interpretatie.

De politie ervaart in de praktijk problemen in de gegevensuitwisseling met plaatselijke gemeenschappen en autoriteiten. Voor het delen van gegevens met lokale autoriteiten is er op dit moment namelijk geen formele wettelijke grondslag. De politie acht het van belang wel gegevens met hen te kunnen uitwisselen. De politie wijst daarbij expliciet op cases waarin zij gegevens hebben verzameld over jongeren die tussen wal en schip driegen te vallen en extra ondersteuning nodig hebben. Deze gegevens mogen formeel gezien niet met de lokale autoriteiten worden gedeeld, terwijl het volgens de politie in een ieders belang is deze gegevens wel te delen. De politie maakt in dergelijke gevallen zo optimaal mogelijk gebruik van de mogelijkheden die er wel zijn, maar zou hiervoor graag meer formele mogelijkheden willen hebben.[153] De indruk bestaat echter niet dat de politie te voorzichtig handelt en *overall* te weinig gebruik maakt van de mogelijkheden om gegevens uit te wisselen met andere autoriteiten.

IV.4.7 Technologische aspecten

Wettelijke grondslag

In paragraaf IV.2.1. is al kort aangestipt dat de twee wetten waarmee in Finland de Richtlijn is omgezet technologie-neutraal zijn geformuleerd. Er is dus nergens expliciet genoemd dat bepaalde technieken wel of niet mogen worden ingezet voor het verwerken van persoonsgegevens. In een aantal andere wetten wordt wel aandacht besteed aan het gebruik van nieuwe technologieën, bijvoorbeeld in de *Act on the Use of Network Traffic Intelligence in Civilian*

[153] De politie maak dan gebruik van de algemeen geformuleerde grondslag voor het delen van data met autoriteiten aan het eind van section 22 van de *Act on the Processing of Personal Data by the Police*. Er moet in dat geval wel een afweging worden gemaakt of het delen van gegevens noodzakelijk is. Deze afweging is volgens de politie soms lastig te maken. Vandaar dat de politie graag een expliciete grondslag in de wet zou willen zien voor het delen van gegevens met lokale autoriteiten.

Intelligence (582/2019).[154] Onder *network traffic intelligence* wordt verstaan: *'technical information gathering targeted at network traffic in a communications network crossing the Finnish border based on automated screening of the network traffic and the processing of the obtained information'*. Deze wet geldt alleen als daar sprake van is en geeft dus geen algemene bevoegdheid voor het inzetten van modern technologieën. In de *Act on the Use of Network Traffic Intelligence in Civilian Intelligence* heeft de politie enkele mogelijkheden gekregen voor het gebruik van bijvoorbeeld mobiele telefoon data. Voor het krijgen van toegang tot dergelijke data en het verwerken daarvan heeft de politie wel een akkoord (controle) nodig van een algemene rechtbank.
Eén van de gesprekspartners is van mening dat het gebrek aan een algemene wettelijke grondslag geen groot probleem is voor de politiepraktijk. De andere geïnterviewden delen deze opvatting niet.

Praktijkervaringen

De Finse politie is van mening dat zij te weinig wettelijke mogelijkheden heeft om gebruik te kunnen maken van nieuwe technologieën. Dit is met name het geval voor het gebruiken van gezichtsherkenning. Aan de inzet van dat soort technieken heeft de politie echter wel behoefte. De politie zou graag meer gebruik willen kunnen maken van de mogelijkheden die cameratoezicht en gezichtsherkenning bieden. Met name heeft de politie behoefte aan een wettelijke grondslag voor de inzet van dergelijke technieken, omdat dan duidelijk is dat hiervoor een expliciete juridische basis is en daarmee een eventuele inbreuk op de privacy gerechtvaardigd is.

In paragraaf IV.4.1. is al even aangestipt dat met name het gebrek aan een algemene wettelijke grondslag voor het gebruik van Artificial Intelligence bij de analyse van big-data sets een probleem is. De politie geeft aan dat er behoefte is aan de inzet van deze technologie. Zij heeft het idee dat het dan mogelijk is om veel meer en beter van informatie uit deze datasets gebruik te maken. Dat is in het kader van de uitoefening van haar werkzaamheden belangrijk.

In de praktijk maakt de politie wel gebruik van moderne technologieën, dat is bijna niet te voorkomen. Zij heeft echter als wens dat hier een veel duidelijkere wettelijke grondslag voor komt. Juist omdat de politie het belang van een goede gegevensbescherming en het bestaan van strikte regels voor de analyse van data onderschrijft, is deze wettelijke grondslag nodig. Dan weet de politieagent die van de techniek gebruik maakt zeker dat wat hij of zij doet ook juridisch in de haak is.

IV.5 Toezicht

Intern toezicht

Het interne toezicht op de verwerking van politiegegevens wordt uitgeoefend door de Data Protection Officer van de Finse politie.[155] Omdat hij de interne toezichthouder van de politie is, focust hij zich alleen op de verwerking van persoonsgegevens door de politie. Eén van de taken die hij heeft is het gevraagd en ongevraagd geven van adviezen. Politieagenten kunnen zowel meer algemene vragen aan hem stellen als vragen die zien op wat er wel en niet mag

[154] Wij hebben een conceptversie van de Engelse vertaling van deze wet ontvangen van het Finse ministerie van Binnenlandse Zaken. De vertaling staat nog niet vast en kan dus nog worden aangepast. Ook de Engelse titel van deze wet is blijkens opmerkingen in het tekstbestand nog niet definitief.
[155] Elke bevoegde autoriteit/verwerkingsverantwoordelijke heeft een interne toezichthouder op grond van hoofdstuk 6 van de *Law Enforcement Data Protection Act*; de Data Protection Officer is lid van het National Police Board.

in een specifieke casus. Elke lokale politie unit heeft ook een eigen Data Protection Expert, die met name een adviserende rol heeft.
De Data Protection Officer heeft niet de bevoegdheid om sancties zoals boetes op te leggen aan individuele politieagenten als die zich bij het verwerken van politiegegevens niet aan de regels houden. Hij kan wel constateren dat iemand niet volgens de voorschriften heeft gehandeld en aangeven dat het een volgende keer anders moet.

Extern toezicht

Het externe toezicht op de verwerking van politiegegevens wordt uitgeoefend door de Data Protection Ombudsman. Hij is de algemene en onafhankelijke toezichthouder voor de verwerking van persoonsgegevens op grond van de AVG.[156] In section 45 van de *Law Enforcement Data Protection Act* is bepaald dat de Data Protection Ombudsman ook de externe toezichthouder is voor de verwerking van politiegegevens binnen de reikwijdte van de Richtlijn. In de praktijk wordt het toezicht op grond van de Richtlijn uitgeoefend door een deputy Data Protection Ombudsman.[157]

De taken van de Data Protection Ombudsman staan opgesomd in section 46 van de *Law Enforcement Data Protection Act:*

> *'**Section 46 Tasks***
>
> *In addition to the supervision of compliance with this Act, the tasks of the Data Protection Ombudsman include the following:*
>
> *1) to promote public awareness of the risks, legislation, safeguards and rights related to the processing of personal data;*
>
> *2) to promote the awareness of controllers and processors of their obligations under this Act;*
>
> *3) to provide data subjects, on request, with information about the exercise of their rights under this Act;*
>
> *4) to advise on the prior consultation referred to in section 21;*
>
> *5) to examine compliance with this Act;*
>
> *6) to verify the lawfulness of the processing in accordance with section 29;*
>
> *7) to consider requests for measures made by data subjects and organisations referred to in section 56;*
>
> *8) to monitor technological and other developments affecting the protection of personal data.'*

[156] Zie art. 8 van de Data Protection Act (1050/2018).
[157] Binnen het kantoor van de Data Protection Ombudsman is een verdeling van de verschillende toezichthoudende taken gemaakt tussen de Data Protection Ombudsman zelf en zijn twee plaatsvervangers. Omdat in de relevante wet- en regelgeving alleen wordt gesproken over de Data Protection Ombudsman hanteren wij deze term.

Hij heeft dus naast taken die een volledig toezichthoudend karakter hebben ook een meer adviserende rol. Zijn toezichthoudende taak richt zich met name op het toezien op de rechtmatigheid en kwaliteit van de interne controlemechanismen van de politie.

De Data Protection Ombudsman doet zowel proactief als reactief onderzoek. Het reactief onderzoek vindt plaats op grond van klachten die burgers hebben ingediend. Eind 2019 heeft de Data Protection Ombudsman een toezichts- en onderzoeksplan gepresenteerd waarin hij een aantal focusonderwerpen voor het proactieve onderzoek aangeeft. De meeste onderzoeken zijn reactief van aard. Met betrekking tot de bewaartermijnen controleert de Data Protection Ombudsman – op eigen initiatief en op verzoek van de politie – of gegevens die moeten worden verwijderd inderdaad verwijderd zijn en of het inzagerecht correct wordt toegepast.

Ook de Data Protection Ombudsman kan geen sancties zoals boetes opleggen als hij constateert dat de politie of één van de andere bevoegde autoriteiten zich niet aan de regels heeft gehouden. Het is wel mogelijk dat hij de autoriteit dwingt om een onrechtmatige gegevensverwerking te stoppen, maar dat doet hij alleen in uitzonderlijke gevallen. Dat heeft als reden dat dit een nogal ingrijpende maatregel is, de praktische uitoefening van de wettelijke politietaak wordt dan vrijwel onmogelijk maakt. Het komt wel voor dat de Data Protection Ombudsman vordert dat de politie data die niet correct zijn corrigeert.

Er is sprake van een goede samenwerking tussen de Data Protection Ombudsman en de Data Protection Officer. Zij hebben regelmatig contact met elkaar en wisselen ook informatie met elkaar uit. Als de Data Protection Ombudsman bijvoorbeeld constateert dat er in een bepaalde zaak niet volgens de regels is gehandeld, stelt hij de Data Protection Officer daarvan op de hoogte.

IV.6 Lessen voor Nederland

IV.6.1 Wetgevingssystematiek

In Finland zijn de wetten waarmee de Richtlijn is omgezet goed gestructureerd. De artikelen die gaan over hetzelfde onderwerp zijn bij elkaar in een hoofdstuk gegroepeerd. De hoofdstukken en de individuele artikelen hebben duidelijke titels waardoor makkelijk in één oogopslag is te zien waar ze over gaan. Deze overzichtelijke indeling maakt het zoeken van de juiste bepalingen eenvoudiger. Het zou goed zijn als bij de herziening van de WPG aandacht wordt besteed aan de manier waarop de wet is ingedeeld en wordt gekeken hoe overzichtelijk de wet is. De Finse wetten zouden daarbij als een goed voorbeeld kunnen dienen.

IV.6.2 Regeling van de bewaartermijnen

Inhoudelijk gezien zou Nederland iets kunnen hebben aan de manier waarop in Finland de bewaartermijnen in de wet zijn vastgelegd. In art. 14 Wpg – het artikel dat gaat over de bewaartermijnen – wordt verwezen naar art. 8 en 9 Wpg, waarin maar enkele termijnen worden genoemd. In de *Act on the Processing of Personal Data by the Police* is daarentegen op een heel overzichtelijke manier aangegeven welke bewaartermijn van toepassing is voor welke categorie van persoonsgegevens. Dit draagt eraan bij dat het duidelijker is hoe lang bepaalde gegevens precies mogen worden bewaard.

IV.6.3 Toezicht

Op het gebied van toezicht zou Nederland kunnen overwegen om de mogelijkheden die de Autoriteit Persoonsgegevens heeft uit te breiden met de bevoegdheid om in een uiterste ge-

val de stopzetting van een onrechtmatige gegevensverwerking te vorderen. De Data Protection Ombudsman gebruikt deze mogelijkheid zelden, maar het kan een goede stok achter de deur zijn in situaties dat er meerdere keren achter elkaar onregelmatigheden worden geconstateerd.

IV.6.4 Inzet van nieuwe technologieën

Net als in Nederland is er ook in Finland geen algemene wettelijke grondslag opgenomen voor de inzet van nieuwe technologieën voor het verwerken van politiegegevens. Met name de Finse politie geeft aan wel heel erg behoefte te hebben aan meer wettelijke mogelijkheden om moderne technologieën te gebruiken. Dat geeft namelijk een legitieme grondslag voor de inzet van deze technologie, de politie kan er dan later tijdens rechtszaken minder makkelijk op worden aangesproken. Het zou in het licht van het ontbreken van een dergelijke bepaling in de WPG waardevol kunnen zijn te onderzoeken of de Nederlandse politie hier net als haar Finse collega's ook behoefte aan heeft en of er mogelijkheden zijn aan deze wens tegemoet te komen.

Casestudy V: Ierland

V.1 Inleiding

De keuze is oorspronkelijk op Ierland gevallen vanwege: taal/toegankelijkheid; het feit dat de Europese hoofdkantoren van de grote techbedrijven als Google, Facebook en Twitter in Dublin staan, wat interessant kan zijn met het oog op de uitwisseling van persoonsgegevens met/verzameling van persoonsgegevens door de politie (en andere autoriteiten met opsporingsbevoegdheden); en de veronderstelling dat Ierland regelgeving in verschillende opzichten aan lagere overheden heeft overgelaten. Dit laatste blijkt in elk geval voor de verwerking van politiegegevens niet zo te zijn; er is een nationale privacywet en ook de politie- en straf(vorderings)wetgeving is nationaal. Ook heeft Ierland één nationale politie. Wel is het zo dat er in Ierland vele (lagere) autoriteiten en ook private organisaties, zoals vervoersbedrijven, (kunnen) zijn belast met de opsporing en vervolging van strafbare feiten. Ook is in het Ierse systeem de wetgeving over politiegegevens globaal gehouden; er wordt veel ruimte gelaten aan de verwerkingsverantwoordelijken, met controle door de toezichthoudende autoriteit. Wat betreft de aanwezigheid van Google, Facebook en Twitter blijkt uit de interviews niet dat dit speciaal invloed heeft op hoe men omgaat met (de wettelijke regeling van) politiegegevens.

Voor deze casestudy hebben we gesproken met:

- Department of Justice and Equality (Ministerie van Justitie en Gelijkheid), Principal Officer Civil Justice and Equality, Legislation
- De Data Protection Officer van An Garda Síochána (de Ierse nationale politie en veiligheidsdienst)
- Hoofd van de Complaints and Inquiries Unit bij de Data Protection Commission (DPC, de toezichthoudende autoriteit)
- een advocaat en assistant professor of law aan Trinity College Dublin (gespecialiseerd in Europees en internationaal recht, met een focus op gegevensbescherming)

De wetgeving, jurisprudentie en achtergrondinformatie in het Engels was goed toegankelijk. Al met al hebben we ons een goed beeld kunnen vormen van de Ierse situatie.

Hieronder gaan we eerst in op het wettelijk kader (paragraaf V.2) en vervolgens op de bevoegde autoriteiten en in het bijzonder op de politie (paragraaf V.3). In paragraaf V.4 komen de verschillende aspecten van verwerking van politiegegevens aan bod: verkrijgen (paragraaf V.4.1), bewerken (paragraaf V.4.2), categoriseren en labelen (paragraaf V.4.3), bewaartermijnen en vernietigingsvoorwaarden (paragraaf V.4.4) en verstrekken/delen (paragraaf V.4.5). Paragraaf V.5 gaat over het toezicht en in paragraaf V.6 proberen we voor te sorteren op lessen voor Nederland.

V.2 Wettelijk kader

V.2.1 Wettelijk systeem

Op de verwerking van persoonsgegevens, waaronder politiegegevens, in Ierland is in de eerste plaats de Data Protection Act (DPA) 2018 van toepassing. In deze wet is zowel de AVG als de Richtlijn gegevensbescherming opsporing en vervolging omgezet/uitgewerkt. Het parlement en de toenmalige toezichthouder hechtten aan één wet voor beide regimes, geeft de wetgevingsambtenaar in het interview aan. De Ierse nationale politie, An Garda Síochána,[158] is zowel politie als nationale veiligheidsdienst (zie verder paragraaf V.3). Omdat nationale veiligheid geen EU-bevoegdheid is, maar de uitsluitende bevoegdheid van de lidstaten,[159] geldt voor dit deel van het takenpakket van de Garda nog de oude DPA uit 1988. Ierland had dus ook voor de komst van het Europese kader al wetgeving op het gebied van gegevensbescherming, ook voor de politie. Voor de politie golden (net als nu met de Richtlijn) op grond van de oude DPA 1988 meer uitzonderingen vanwege het belang van uitvoering van de politietaak.

De Ierse politiewet is de Garda Síochána Act 2005 (Garda Act). De politietaken staan in artikel 7:

> *'7.—(1) The function of the Garda Síochána is to provide policing and security services for the State with the objective of—*
> *(a) preserving peace and public order,*
> *(b) protecting life and property,*
> *(c) vindicating the human rights of each individual,*
> *(d) protecting the security of the State,*
> *(e) preventing crime,*
> *(f) bringing criminals to justice, including by detecting and investigating crime, and*
> *(g) regulating and controlling road traffic and improving road safety.*
>
> *(2) For the purpose of achieving the objective referred to in subsection (1), the Garda Síochána shall co-operate, as appropriate, with other Departments of State, agencies and bodies having, by law, responsibility for any matter relating to any aspect of that objective.*
>
> *(3) In addition to its function under subsection (1), the Garda Síochána and its members have such functions as are conferred on them by law including those relating to immigration. (…)'*

Dit artikel is onder meer van belang als wettelijke basis voor het uitwisselen van politiegegevens met andere partijen (lid 2 jo. lid 1).

V.2.2 Omzetting van de Richtlijn

Ierland heeft EU-Richtlijn 2016/680 omgezet in Part 5 van de DPA 2018. Part 6 heet Enforcement of Data Protection Regulation and Directive. Hierin staan de instrumenten die de Data Protection Commission (DPC), de op grond van het Europeesrechtelijke kader in het leven geroepen toezichthoudende autoriteit, heeft om toe te zien op de naleving van zowel Richtlijn als AVG.

De formulering van de bepalingen van Part 5 van de DPA is zeer algemeen en open, en sluit grotendeels letterlijk aan bij de bewoordingen van de Richtlijn. Zo wordt het begrip bevoegde

[158] Guardians of the Peace.
[159] Art. 4 lid 2 Verdrag betreffende de Europese Unie (VEU).

autoriteit (*competent authority*) niet nader gespecificeerd voor de situatie in Ierland; art. 69 (begripsbepalingen) noemt geen autoriteiten bij naam, maar volstaat met de definitie uit de Richtlijn. Dit komt doordat Ierland een zeer groot aantal bevoegde autoriteiten heeft (zie verder paragraaf V.3). Vanwege de beperkte tijd die beschikbaar was voor implementatie van de Richtlijn in combinatie met het grote toepassingsbereik heeft Ierland gekozen voor één algemeen geformuleerde wet. De richtlijn is dus ook niet omgezet in de bijzondere wetgeving die geldt voor de verschillende *competent authorities*; zij moeten in de DPA 2018 kijken. Er is ook geen lagere regelgeving over dit onderwerp; meer algemeen is er in het Ierse rechtssysteem[160] weinig lagere/gedecentraliseerde regelgeving. Veel is dus overgelaten aan de verwerkingsverantwoordelijken (*controllers*) en het toezicht door de DPC en de functionarissen gegevensbescherming (*data protection officers,* DPO). Voor de invulling van open normen let Ierland ook op de richtlijnen van de European Data Protection Board (EDPB). Het *accountability principle* ('verantwoordingsprincipe') speelt hierbij een grote rol; dit is het Europeesrechtelijke beginsel (art. 5 lid 2 AVG en art. 4 lid 4 Richtlijn) dat de verwerkingsverantwoordelijke verantwoordelijk is voor de naleving van de andere beginselen van gegevensbescherming en deze kan aantonen.

Wel heeft de Ierse wetgever een aantal bepalingen uit de Richtlijn in de DPA 2018 subtiel anders geformuleerd om ze beter in overeenstemming te brengen met Iers recht. Zo werd art. 6 sub a Richtlijn[161] onverenigbaar geacht met de onschuldpresumptie. In art. 74 DPA 2018 worden daarom de categorieën niet expliciet gespecificeerd; het artikel bepaalt dat het onderscheid 'where relevant and in so far as possible' moet worden gemaakt (tekst van de Richtlijn: 'where applicable and if possible').

Ook zorgden ervaren inconsistenties en ambiguïteiten in de tekst van de Richtlijn in Ierland soms voor vraagstukken bij de implementatie. In artikel 4 lid 1 sub a Richtlijn staat bijvoorbeeld dat gegevens rechtmatig en eerlijk moeten worden verwerkt; in tegenstelling tot in de AVG wordt transparantie hier niet genoemd. Dit komt weer wel terug in overweging 26 van de preambule. Art. 25 Richtlijn beperkt met een limitatieve opsomming de gebruiksdoelen voor persoonsgegevens. In overweging 37 van de preambule worden ook 'discipline procedures' genoemd; deze staan niet in art. 25.

V.3 De bevoegde autoriteiten

V.3.1 Algemeen

Zoals gezegd zijn de *competent authorities* als bedoeld in de Richtlijn in de Ierse wetgeving niet nader uitgewerkt, omdat het er zoveel zijn, meer dan in sommige andere lidstaten. Een geïnterviewde noemt het aantal van 60-65. Vooral de strafvervolgingsbevoegdheid is verdeeld over vele organen/entiteiten. Gemeenten hebben bijvoorbeeld ook enkele beperkte vervolgingsbevoegdheden. De DPC schrijft hierover op haar website:

> *'It will be important to correctly identify cases in which the legal regime of the LED [Law Enforcement Directive] and Part 5 of the Data Protection Act 2018 applies. The LED regime only applies in cases where the data controller is a 'competent authority', and the processing*

[160] Een mix van constitutional, statute en common law.

[161] De lidstaten schrijven voor dat de verwerkingsverantwoordelijke, in voorkomend geval en voor zover mogelijk, een duidelijk onderscheid maakt tussen persoonsgegevens betreffende verschillende categorieën van betrokkenen, zoals: a) personen ten aanzien van wie gegronde vermoedens bestaan dat zij een strafbaar feit hebben gepleegd of zullen plegen;

is done for 'law enforcement purposes'.

However, this is not limited to processing by bodies who might be typically considered as 'law enforcement authorities' (such as An Garda Síochána), but to any processing for law enforcement purposes, carried out by a public or private body who fits the definition of 'competent authority' (such as local authorities when prosecuting litter fines, or Dublin Bus in relation to ticket offences). This means that a potentially very large number and variety of bodies might fall under the scope, and the applicability of this regime will need to be assessed on a case-by-case basis.

It is not as simple as presuming that all processing done by law enforcement authorities will fall under the LED regime, or that a private sector entity will not be subject to the LED – in the former case, the law enforcement authority may conduct data processing which has nothing to do with its law enforcement function (HR matters, procurement, etc.), and in the latter case, private sector entities may have been entrusted with public authority or be performing data processing contracted out to them by a public authority, where their processing is for law enforcement purposes.'[162]

Inmiddels neemt de kennis over de Richtlijn (en de afbakening met de AVG) toe onder potentiële *competent authorities* in Ierland. De DPC en het verantwoordelijke ministerie (Department of Justice and Equality) doen aan voorlichting en de DPC heeft inmiddels ervaring opgedaan met de Richtlijn, onder meer door de afhandeling van 66 klachten.

Vanwege de noodzaak om de casestudy enigszins te beperken en toe te spitsen, en ook omdat de Ierse wetgeving zelf bewust zo breed en flexibel is gehouden op dit gebied, hebben we ervoor gekozen te focussen op de Garda.

V.3.2 Structuur van de politie

An Garda Síochána is dus één nationale politie. Aan het hoofd staat de Garda Commissioner. Ierland is verdeeld in vier politieregio's: de Dublin Metropolitan Region, de North Western Region, de Eastern Region en de Southern Region. De Garda is op dit moment in transitie naar een nieuwe organisatiestructuur (*Operating Model*). De overgang van zes naar vier regio's is daar een onderdeel van en heeft al plaatsgevonden. Daarnaast is het land nu verdeeld in 28 geografische Divisions; dit worden er negentien. Elke Division krijgt vier thematische aandachtsgebieden onder leiding van een Superintendent of Assistant Principal: Community Engagement (hieronder valt een breed scala aan taken, bijvoorbeeld ook Custody en Roads Policing), Crime (hieronder vallen Serious Crime, Specialist Investigation en Security & Intelligence), Governance and Performance Assurance (hieronder valt ook Criminal Justice, dus strafprocesrecht/procedurele waarborgen) en Business Services (de bedrijfsvoeringstak met o.a. HR). Naast de regio's en Divisions is er een behoorlijk aantal operationele en stafafdelingen op nationaal niveau.

Overigens is in september 2018 het rapport *The future of policing in Ireland* verschenen, van een gelijknamige commissie. Het rapport ziet *information-led policing* en *adaptive, innovative and cost effective policing* als twee van tien pijlers onder een nieuw raamwerk voor *policing,*

[162] Data Protection Commission, *Law Enforcement Directive - Guidance on Competent Authorities and Scope*, www.dataprotection.ie/en/organisations/law-enforcement-directive (laatst geraadpleegd op 7 augustus 2020).

security and community safety.[163] Op basis hiervan is een vierjarenplan 2019-2022 ontwikkeld, waar bovenstaande organisatiewijziging onderdeel van is.

V.4 Verwerken van politiegegevens

V.4.1 Verkrijgen van politiegegevens

Ook in Ierland zijn noodzakelijkheid en doelbinding de belangrijkste criteria voor het verzamelen van gegevens door de politie. Er moet altijd een wettelijke grondslag zijn. Dit is, in overeenstemming met de Richtlijn, neergelegd in art. 71 lid 2 DPA 2018:

> *'(2) The processing of personal data shall be lawful where, and to the extent that—*
> *(a) the processing is necessary for the performance of a function of a controller for a purpose specified in section 70(1)(a)[164] and the function has a legal basis in the law of the European Union or the law of the State, or*
> *(b) the data subject has, subject to subsection (3), given his or her consent to the processing.'*

Voor de Garda geldt dus als algemeen kader dat zij alleen gegevens mag verzamelen voor zover dat noodzakelijk is voor de uitvoering van een van haar wettelijke taken uit art. 7 Garda Act[165] én voor een van de opsporings- en vervolgingsdoelen als bedoeld in de Richtlijn.[166]

Art. 41 sub b DPA 2018 (uit het 'AVG-deel' van de wet) vormt voor de Garda de algemene basis om gegevens te verkrijgen van organisaties die onder de AVG vallen:

> *'41. Without prejudice to the processing of personal data for a purpose other than the purpose for which the data has been collected which is lawful under the Data Protection Regulation, the processing of personal data and special categories of personal data for a purpose other than the purpose for which the data has been collected shall be lawful to the extent that such processing is necessary and proportionate for the purposes—*
> *(a) of preventing a threat to national security, defence or public security,*
> *(b) of preventing, detecting, investigating or prosecuting criminal offences, (…)'*

Als de politie gegevens nodig heeft van andere bevoegde autoriteiten op grond van de Richtlijn, dan gebruikt ze art. 71 lid 5 DPA 2018 (*seamless sharing*):

> *'Where a controller collects personal data for a purpose specified in section 70(1)(a), the controller or another controller may process the data for a purpose so specified other than the purpose for which the data were collected, in so far as—*
> *(a) the controller is authorised to process such personal data for such a purpose in accordance with the law of the European Union or the law of the State, and*
> *(b) the processing is necessary and proportionate to the purpose for which the data are being processed.'*

[163] Commission on the Future of Policing in Ireland 2018.
[164] De doelen van de Richtlijn: '(i) the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against, and the prevention of, threats to public security, or (ii) the execution of criminal penalties'.
[165] En op grond van art. 7 lid 3 Garda Act dus ook taken die uit andere wetten voortvloeien.
[166] En op basis van toestemming, maar dit is nog een lastig vraagstuk in de praktijk.

In allerlei andere wetten zijn specifieke bepalingen te vinden die als grondslag voor het verzamelen van persoonsgegevens door de politie kunnen dienen. Voorbeelden zijn de Criminal Justice Act (en zijn vele amendementen, zoals over Forensic Evidence and DNA Database System in 2014 en over Terrorist Offences in 2015) en kinderbeschermingswetten (waarvan Ierland er veel heeft) zoals de Children First Act 2015. Uit een van de interviews blijkt dat de politie *overall* weinig problemen ervaart met de grondslagen voor het verzamelen van gegevens. De Data Protection Unit van de Garda (met aan het hoofd de Data Protection Officer, de functionaris gegevensbescherming) doet veel aan bewustwording. Politiemedewerkers krijgen bij het inloggen in het systeem een reminder over hun *data protection*-verplichtingen. Klachten van burgers gaan niet over de hoeveelheid gegevens die de politie verzamelt of wat ermee gebeurt, maar over het feit dat burgers niet altijd (mogen) weten welke gegevens de politie over hen heeft. Burgers begrijpen volgens de politie dat het lastig kan zijn om van tevoren te bepalen welke gegevens nodig zijn, maar dat de politie probeert om alleen te verzamelen wat strikt noodzakelijk is.

(Part 5 van) de Ierse DPA 2018 is 'technologieneutraal' – oftewel zeer algemeen – geformuleerd; er staan geen specifieke regels in voor het gebruik van bepaalde technologische middelen of technieken. Zie bijvoorbeeld art. 77 (*Security of automated processing*)[167] en art. 84 (*Data protection impact assessment [DPIA] and prior consultation with Commission*). Dat laatste artikel is de omzetting van art. 27 en 28 Richtlijn en spreekt, net als de Richtlijn, alleen van '*a type of processing, and in particular a type of processing using new technology, [that] is likely to result in a high risk to the rights and freedoms of individuals*'. Uit een van de interviews blijkt dat men bij de omzetting van de Richtlijn (en de AVG) moeite had met open begrippen als *risk* en *high risk*.[168] Voor de invulling hiervan wordt onder meer gelet op de EDPB.

De Garda verzamelt in de praktijk (nog) geen grote datasets en doet niet aan *data mining* of profileren gebaseerd op geautomatiseerde verwerking van online bronnen, om ethische en technische redenen. De politiesystemen zijn hier nog niet op ingericht en de politie heeft eerst andere prioriteiten; ze is bezig met een organisatieontwikkeling met het oog op toekomstbestendigheid, en qua techniek ligt de focus nu op bodycams. De wetgeving laat de inzet van nieuwe technologie en (analyse)technieken wel toe, mits op grond van art. 84 DPA 2018 bij *high risk* een DPIA wordt uitgevoerd en op basis daarvan eventueel de DPC wordt geraadpleegd. Dat laatste is bijvoorbeeld gebeurd voor bodycams. Ook Clearview AI/gezichtsherkenning wordt (nog) niet gebruikt.

Een grote uitdaging ligt volgens de geïnterviewde advocaat en expert van Trinity College in de hoge eisen die het Europees Hof van Justitie stelt. Principes als noodzakelijkheid worden door het Hof steeds strikter geïnterpreteerd. Dit legt de lat hoog voor de regelgeving over technologische ontwikkelingen als *big data*-projecten en AI-toepassingen, en de technische en organisatorische maatregelen in de praktijk; zeker voor het opzetten van wat voor grootschalige database dan ook van het soort gevoelige gegevens dat onder de Richtlijn valt. Daarvoor moet er een zeer duidelijke, specifieke wettelijke grondslag zijn. Volgens deze expert zijn deze eisen '*on the ground*' vaak erg lastig in de praktijk te brengen. Daarnaast kunnen vraagtekens worden gezet bij de wenselijkheid vanuit mensenrechtenperspectief van sommige door het Hof gesuggereerde maatregelen, zoals het van tevoren 'targeten'/definiëren van groepen van personen van wie je (telecommunicatie)data wilt verzamelen en bewaren, voor er een strafbaar feit is begaan. Dit brengt het risico mee van profilering en discriminatie.

[167] Waarbij '*automated processing*' niet nader wordt gedefinieerd.
[168] Dit werd genoemd in de context van art. 30 en 31 Richtlijn over datalekken.

In de *Digital Rights Ireland*-zaak heeft het Hof op prejudiciële vragen van de Ierse High Court en het Oostenrijkse Verfassungsgerichtshof geantwoord dat Richtlijn 2006/24/EG betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronischecommunicatiediensten of van openbare communicatienetwerken ongeldig is.[169]

> *'(…) dat richtlijn 2006/24 algemeen van toepassing is op alle personen, alle elektronischecommunicatiemiddelen en alle verkeersgegevens, zonder dat enig onderscheid wordt gemaakt, enige beperking wordt gesteld of enige uitzondering wordt gemaakt op basis van het doel, zware criminaliteit te bestrijden.*
>
> *Richtlijn 2006/24 is om te beginnen algemeen van toepassing op alle personen die gebruikmaken van elektronischecommunicatiediensten, zonder dat de personen van wie de gegevens worden bewaard zich echter, zelfs niet indirect, in een situatie bevinden die aanleiding kan geven tot strafrechtelijke vervolging. (…)*
>
> *Voorts beoogt deze richtlijn weliswaar bij te dragen tot de strijd tegen zware criminaliteit, maar zij vereist geen enkel verband tussen de gegevens die moeten worden bewaard en een bedreiging van de openbare veiligheid. (…)*
>
> *In de tweede plaats bevat richtlijn 2006/24 niet alleen geen beperkingen, maar ook geen objectieve criteria ter begrenzing van de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan met het oog op het voorkomen, opsporen of strafrechtelijk vervolgen van inbreuken die, gelet op de omvang en de ernst van de inmenging in de door de artikelen 7 en 8 van het Handvest erkende fundamentele rechten, voldoende ernstig kunnen worden geacht om een dergelijke inmenging te rechtvaardigen. (…)*
>
> *Bovendien bevat richtlijn 2006/24 geen materiële en procedurele voorwaarden betreffende de toegang van de bevoegde nationale autoriteiten tot de gegevens en het latere gebruik ervan.'*

Digital Rights Ireland heeft nog steeds grote gevolgen voor Ierland; in het arrest heeft het Hof scherpe criteria geformuleerd voor (de wetgeving over) de toegang van de autoriteiten tot telecommunicatiedata. In de *Dwyer*-zaak heeft de Ierse Supreme Court in 2020 voortbouwend hierop ook voorgesteld om prejudiciële vragen te stellen.[170]

> *'I consider that there are three key areas of European Union law where the law is not acte clair but where clarification of that law is necessary to reach a proper decision on this appeal. In simple terms, those areas are:-*
> *(a) Whether a system of universal retention of certain types of metadata for a fixed period of time is never permissible irrespective of how robust any regime for allowing access to such data may be;*
> *(b) The criteria whereby an assessment can be made as to whether any access regime to such data can be found to be sufficiently independent and robust; and*

[169] HvJ EU 8 april 2014, ECLI:EU:C:2014:238 (*Digital Rights Ireland e.a.*).
[170] Supreme Court of Ireland 24 februari 2020, 2019/18 (*Dwyer/The Commissioner of An Garda Síochána e.a.*).

(c) Whether a national court, should it find that national data retention and access legislation is inconsistent with European Union law, can decide that the national law in question should not be regarded as having been invalid at all times but rather can determine invalidity to be prospective only.'

V.4.2 Bewerken van politiegegevens

De DPA 2018 stelt in een aantal bepalingen kaders voor het (verdere) gebruik en bewerken van persoonsgegevens door de bevoegde autoriteiten (en het toezicht daarop, zoals het al genoemde art. 84 met voorwaarden voor het gebruik van nieuwe technologieën). Art. 71 lid 5 en 6 bevat het algemene kader voor gebruik van gegevens voor een ander doel dan waarvoor ze zijn verkregen (lid 5) en voor archivering in het algemeen belang, statistische en onderzoeksdoeleinden (lid 6)[171]; en art. 77 gaat bijvoorbeeld over *Security of automated processing*. Deze voorschriften zijn opnieuw vrij algemeen en direct afgeleid van de Richtlijn. Er wordt niet specifiek ingegaan op nieuwe technologische middelen/methoden. De Garda is hier echter zoals gezegd ook terughoudend mee. Ze gebruikt wel PULSE, de politiedatabase. Met de hierin opgeslagen gegevens wordt onderzoek gedaan en worden analyses uitgevoerd om trends te vinden.

V.4.3 Categoriseren en labelen van politiegegevens

De Ierse politie categoriseert de gegevens die ze verwerkt naar regime: AVG of Richtlijn. Daarnaast maakt ze waar mogelijk onderscheid tussen de rol van de betrokkene in de zaak: verdachte, getuige, slachtoffer etc. – ondanks de bezwaren hiertegen vanwege de onschuldpresumptie, waardoor dit niet in de DPA terecht is gekomen. Iemands rol kan wel verschuiven of verschillen per zaak.

Art. 73 DPA 2018 regelt zeer uitgebreid de voorwaarden voor de verwerking van bijzondere categorieën persoonsgegevens binnen de scope van de Richtlijn gegevensbescherming opsporing en vervolging. Art. 74 lid 1 en 2 bepalen:

'(1) A controller shall, where relevant and in so far as is possible, make a distinction between the personal data of different categories of data subject.
(2) A controller shall, in so far as is possible, ensure that personal data based on facts are distinguished from personal data based on personal assessments.'

Daarnaast heeft de Garda een protocol met als bijlage een lange lijst met categorieën 'records' en bijbehorende bewaartermijnen met het oog op de archiefwetgeving; zie verder hieronder.

V.4.4 Bewaartermijnen en vernietigingsvoorwaarden

Art. 71 lid 7 en 8 DPA 2018, de omzetting van art. 5 Richtlijn, vormen het algemene kader voor de bewaartermijnen:

[171] '(6) A controller may process personal data, whether the data were collected by the controller or another controller, for—
(a) archiving purposes in the public interest,
(b) scientific or historical research purposes, or
(c) statistical purposes,
provided that the said processing—
(i) is for a purpose specified in section 70(1)(a), and
(ii) is subject to appropriate safeguards for the rights and freedoms of data subjects.'

'(7) A controller shall ensure, in relation to personal data for which it is responsible, that an appropriate time limit is established for—
(a) the erasure of the data, or
(b) the carrying out of periodic reviews of the need for the retention of the data.
(8) Where a time limit is established in accordance with subsection (7), the controller shall ensure, by means of procedural measures, that the time limit is observed.'

Dit is dus in de algemene DPA 2018 niet nader uitgewerkt, maar wordt aan de diverse verwerkingsverantwoordelijken overgelaten (*accountability principle*), met controle door de DPC, die de bewaartermijnen meeneemt in haar audits. Het was voor de wetgever onmogelijk om in *primary legislation* per bevoegde autoriteit/verwerkingsverantwoordelijke vaste bewaartermijnen op te nemen. Wel staan er veel bewaartermijnen voor bepaalde typen data in bijzondere wetten, zoals voor telecommunicatiedata. Elke bevoegde autoriteit moet een eigen *retention policy* hebben.

Op grond van de National Archives Act 1986 (en de daaronder hangende Regulations) moeten gegevens na dertig jaar worden gearchiveerd. Dit geldt zowel voor de politie als voor andere overheidsorganen. Deze wet vereist echter ook dat de autoriteiten categorieën data onderscheiden en beslissingen nemen over welke gegevens gearchiveerd moeten worden en welke niet. De Garda heeft daarom een protocol voor de *periodic review* of gegevens nog nodig zijn; anders worden ze verwijderd. *Investigation files* en gegevens in het politiesysteem PULSE worden voor onbepaalde tijd bewaard in overeenstemming met de National Archives Act. De politie heeft een lijst samengesteld met *non-essential records* die kunnen worden verwijderd (*disposed*) na zeven, tien of vijftien jaar als ze niet meer noodzakelijk (*required*) zijn voor de bedrijfsvoering of de wettelijke functies van de Garda. Onder *records* vallen – kort door de bocht – alle soorten gegevens(dragers). *Records* die na zeven jaar kunnen worden verwijderd zijn bijvoorbeeld *accounting files* en *records of unofficial phone calls*; bij de tienjarentermijn gaat het om een fors kleiner aantal categorieën, waaronder veel HR-/bedrijfsvoeringsdocumenten (dus geen politiegegevens); de vijftienjarentermijn geldt alleen voor Fógra Tóra, een '*criminal intelligence bulletin to highlight serious and inter-regional criminality*'.

Ook zijn bewaartermijnen opgenomen in specifieke wetten, zoals de Criminal Justice (Forensic Evidence and DNA Database System) Act 2014; dit is ook meegenomen in het politieprotocol.

Ierland heeft te maken met vele oude misbruikzaken in de katholieke kerk, die nu aan het licht komen, waardoor de noodzaak data lang genoeg te bewaren eens te meer gevoeld wordt.

V.4.5 Verstrekken/delen van politiegegevens

Binnen Ierland

An Garda Síochána gebruikt, zoals eerder genoemd, art. 71 lid 5 van de DPA 2018 voor het delen van gegevens binnen de *'criminal justice family'*. Er is echter nog geen gemeenschappelijk systeem; hier wordt aan gewerkt, maar dit heeft veel voeten in de aarde wat betreft autorisaties voor alle verschillende actoren.

Voor het verstrekken van gegevens door de politie/bevoegde autoriteiten aan derde partijen die onder de AVG vallen is een specifieke wettelijke basis nodig. Art. 41 DPA 2018 geeft AVG-organisaties zoals eerder genoemd een algemene grondslag voor gebruik van gegevens voor een ander doel dan waarvoor ze zijn verkregen, waaronder gegevensverstrekking voor de

Richtlijn-doelen. Ook zijn in de DPA de algemene voorwaarden uit de richtlijn opgenomen waar elke verstrekking aan moet voldoen, bijvoorbeeld artikel 74 lid 3 en 4 over controle op de kwaliteit van data voor verstrekking en maatregelen bij verstrekking van onjuiste/incomplete gegevens.

De Garda deelt in de praktijk veel informatie met organisaties buiten het bereik van de Richtlijn, als hun rol/functie in lijn is met die van de politie. Dit zijn bijvoorbeeld de *road safety authorities*, de *national transport authorities* of de Child Protection Agency. Criteria voor de politie zijn of het delen van informatie in het algemeen belang is en nodig voor de taakuitvoering van de ontvanger. In die gevallen wordt gewerkt met *data sharing agreements* of *joint control agreements.* Volgens de politie functioneert dit goed, en is er nu ook aan beide 'kanten' (Richtlijn- en AVG-organisaties) meer duidelijkheid (dan in 2018) over wat is toegestaan en daardoor minder terughoudendheid. Wel is soms de vraag wie (welke verwerkingsverantwoordelijke) beoordeelt of de verstrekking *necessary* en *proportionate* is. De Garda kan niet altijd beoordelen welke gegevens voor de andere partij noodzakelijk zijn.

Internationale gegevensuitwisseling

Er is in Part 5 van de DPA 2018 geen specifieke regeling voor gegevensverstrekking binnen de EU; de algemene regels op basis van de Richtlijn en ander EU-recht zijn van toepassing. De Garda ervaart geen problemen met het uitwisselen van gegevens met (bevoegde autoriteiten en andere organisaties in) andere EU-lidstaten. De Brexit is wel een punt, omdat er op grote schaal gegevens worden uitgewisseld met Noord-Ierland. De Ierse politie is bezig alles in kaart te brengen om waar nodig verantwoording af te kunnen leggen.

In art. 96-100 DPA 2018 is de verstrekking aan derde landen geregeld:

- 96. Transfer to third country or international organisation
- 97. Adequacy decision
- 98. Transfer subject to appropriate safeguards
- 99. Derogations for specific situations
- 100. Transfer to recipient in third country

Uit de interviews blijkt niet dat Ierland hier knelpunten ervaart. De belangrijkste kanalen voor de informatieuitwisseling met derde landen zijn Europol, Interpol en wederzijdse rechtshulpverdragen. In een van de interviews kwam wel de vraag ter sprake wie toezicht houdt op Interpol. In 2019 heeft het Duitse Verwaltungsgericht Wiesbaden prejudiciële vragen gesteld aan het Europees Hof van Justitie, onder meer de vraag of een internationale organisatie zoals Interpol over een adequaat beschermingsniveau beschikt, als er geen sprake is van een adequaatheidsbesluit zoals bedoeld in art. 36 Richtlijn 2016/680 en/of passende waarborgen zoals bedoeld in art. 37 Richtlijn 2016/680.[172] Dit soort ontwikkelingen wordt met belangstelling gevolgd door de DPC.

V.5 Toezicht

V.5.1 Extern toezicht

Zoals besproken is de Data Protection Commission (DPC) in Ierland de onafhankelijke toezichthoudende autoriteit voor zowel de AVG als de Richtlijn (*Law Enforcement Directive* of LED). Ze is ingesteld bij Part 2 (art. 9-27) van de DPA 2018. Part 6 heet *Enforcement of Data*

[172] Verwaltungsgericht Wiesbaden 3 juli 2019 (*C-509/19*).

Protection Regulation and Directive. Hierin gaat hoofdstuk 3 (art. 118-128) specifiek over de Richtlijn.

Binnen de DPC zijn er verschillende Units die zich met de Richtlijn bezighouden:
- de Law Enforcement Directive Complaints & Inquiries Unit
- de Consultation Unit (deze afdeling houdt zich bezig met raadplegingen door verwerkingsverantwoordelijken, en met DPIA's)
- de Breach Notification Unit
- de Breach Inquiry Unit

Het klachtrecht onder de Richtlijn is neergelegd in art. 119, 121 en 122 DPA 2018. (Art. 120 regelt de vertegenwoordiging van betrokkenen.)

Het toezicht door de DPC is zowel proactief als reactief.
Art. 123 DPA 2018 bepaalt dat de DPC een *Inquiry* kan starten naar aanleiding van een klacht of uit eigen beweging, '*in order to ascertain whether an infringement has occurred or is occurring*'. Hiervoor kan ze in het bijzonder haar bevoegdheden onder hoofdstuk 4 (*Inspection, Audit, and Enforcement*)[173] gebruiken,[174] of een *Investigation* uitvoeren als bedoeld in hoofdstuk 5. Op grond van art. 127 lid 1 heeft de DPC de volgende *corrective powers* onder de Richtlijn:

> *'(a) issue a warning to the controller or processor that intended data processing is likely to infringe a relevant provision;*
> *(b) issue a reprimand to the controller or processor where data processing by the controller or processor has infringed a relevant provision;*
> *(c) order the controller or processor to comply with a data subject's request to exercise his or her rights under a relevant provision;*
> *(d) order the controller or processor to bring processing into compliance with a relevant provision, in a specified manner and within a specified period;*
> *(e) order the controller to communicate a personal data breach to data subjects;*
> *(f) impose a temporary or definitive limitation, including a ban on processing;*
> *(g) impose a restriction on processing by the controller or processor;*
> *(h) order the suspension of data transfers to a recipient in a third country or to an international organisation.'*

Verder staan er verschillende bevoegdheden/taken van de DPC in Part 5 van de DPA 2018, zoals het al eerder genoemde art. 84 over raadpleging van de DPC naar aanleiding van een DPIA.

Sinds de implementatie van de Richtlijn heeft de DPC 66 klachten ontvangen op grond van de Richtlijn.[175] Deze waren niet allemaal gericht tegen de politie, maar ook tegen vervoersbedrijven, lokale autoriteiten, de *prison service* en de *Revenue Commissioners* (Belastingdienst en douane).

[173] Die bevoegdheden bestaan uit allerlei *Powers of authorised officers* (zoals het betreden van elke plaats en het inzien en meenemen van documenten en gegevensdragers; art. 130); *search warrants* (art. 131), *information notice* (art. 131), *enforcement notice* (art. 132); *Data Protection Audit* (art. 136).
[174] Op art. 134 (Application (…) to the High Court for suspension or restriction of processing of data) en 135 (Power to require report) na.
[175] Ten tijde van het interview met de DPC (op 9 juni 2020).

De DPC heeft vijf *reviews* uitgevoerd op grond van art. 95 DPA 2018 (de omzetting van art. 17 Richtlijn) in verband met de beperking van de rechten van betrokkenen door de verwerkingsverantwoordelijke en controle door de toezichthoudende autoriteit. Deze zaken zijn complex. In Ierland is lid 4 opgenomen in dit artikel, om te voorkomen dat het strafrechtelijk onderzoek wordt belemmerd: '*Nothing in this section shall require the Commission to disclose to a data subject whether or not a controller has processed, or is processing, personal data relating to him or her.*' De DPC is dus niet verplicht om de betrokkene te laten weten of deze onderwerp is van strafrechtelijk onderzoek.

Inquiries kunnen worden gedaan naar aanleiding van één klacht, een set klachten over hetzelfde onderwerp of op eigen initiatief van de DPC. De Complaints and Investigations Unit heeft recent een Inquiry gedaan naar hoe organisaties in de private en publieke sector omgaan met verzoeken om data van de politie. Daarbij ging het om vragen als: welke procedures gebruikt de politie om deze verzoeken te doen? Zijn deze verzoeken/verzamelingen van gegevens proportioneel en rechtmatig? De Special Investigations Unit heeft een serie Inquiries uitgevoerd naar het gebruik van CCTV (cameratoezicht), door de Garda, maar ook door andere *community-based organisations* en *local authorities*. Naast de DPA 2018 en de AVG waren hierbij de bepalingen uit de Garda Act over CCTV (art. 38) van belang. Bij een van deze Inquiries bij de politie in een bepaalde regio heeft de DPC schorsing gelast van het gebruik van ANPR-camera's,[176] omdat dit in strijd was met de DPA 2018.

De DPC kan geen boetes opleggen voor inbreuken op de Richtlijn. Dit betekent dat de politie en andere *competent authorities* wel een boete kunnen krijgen voor inbreuken op de AVG, maar niet op grond van de Richtlijn.

V.5.2 Intern toezicht

Elke verwerkingsverantwoordelijke (behalve de rechtspraak) heeft een Data Protection Officer (DPO, functionaris gegevensbescherming). Dit is geregeld in art. 88 van de DPA, en op andere plekken in Part 5 wat betreft raadpleging. De Garda heeft een Data Protection Unit voor de gehele politieorganisatie, die de DPO ondersteunt. De DPO en de DPC hebben dagelijks contact. Daarnaast voert de DPC vier onderzoeken per jaar uit bij de Garda en zijn er twee overleggen per jaar tussen de Data Protection Unit en de DPC op een meer 'macro' niveau. Een uitdaging voor de DPO is welke informatie de politie mag delen met de betrokkene als deze vraagt om inzage in zijn persoonsgegevens en welke niet. Daarnaast is het soms lastig dat de DPO alleen een *advisory and check role* heeft. De DPO zet sterk in op bewustwording van het belang van gegevensbescherming bij politiemensen, bijvoorbeeld bij de opleiding van politieagenten.

V.6 Lessen voor Nederland

Evenmin als de andere onderzochte landen werkt Ierland met het begrip 'politiegegevens'. De wetgeving gaat uit van de bescherming en verwerking van persoonsgegevens in het algemeen, in de betekenis die de Europese regelgeving daaraan geeft. Dit maakt de overgang tussen verschillende fasen van strafrechtelijke opsporing en vervolging en de toepassing van het regime van de Richtlijn op verschillende bevoegde autoriteiten vloeiender.

[176] *Automatic Number Plate Recognition* (automatische nummerbordherkenning).

Ierland heeft ervoor gekozen de regelingen die de Richtlijn omzetten vrij algemeen te houden en daarmee veel over te laten aan de verwerkingsverantwoordelijken. Toezicht is daarbij (extra) belangrijk. De DPC neemt daarom een actieve houding aan.

Daarnaast lijkt Ierland minder last te hebben van samenloop tussen verschillende regelingen. Wel was er zeker in het begin een groot schemergebied tussen Richtlijn en AVG. Net als uit de interviews in andere landen blijkt uit de interviews in Ierland dat de Richtlijn onderbelicht is gebleven, ook in wetenschappelijk onderzoek, in vergelijking met de grote hoeveelheid aandacht voor de AVG.

pro facto