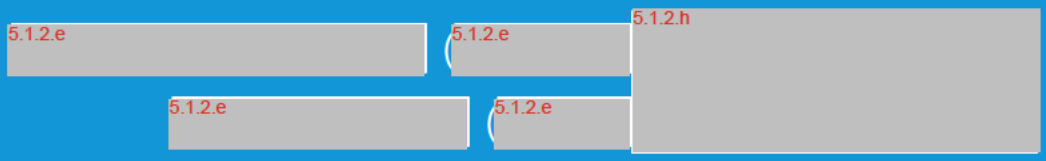
5.1.2.h

Privacy Impact Assessment Raffinaderij 2017

Nationale Politie

30-5-2017



****CONCEPT VERTROUWELIJK****

5.1.2.h

5.1.2.h

Management samenvatting

Dit rapport bevat de bevindingen van de *privacy impact assessment* (PIA) voor de Raffinaderij. Het betreft een herijking van de PIA die 5.1.2.h in 2012-2013 heeft uitgevoerd voor de proeftuinfase van de Raffinaderij. In deze PIA worden de (privacy)risico's van de Raffinaderij geïdentificeerd en geanalyseerd in het licht van de nieuwe methoden, technieken en toepassingen van de Raffinaderij anno 2017. Het doel van de PIA is om tot een systeem of een werkwijze te komen waarbinnen het opsporingsbelang en het beschermen van de rechten van burgers optimaal geregeld zijn. Hiervoor is het noodzakelijk om in beeld te brengen wat de (verwachte) juridische en maatschappelijke grenzen van de toepassing van de Raffinaderij zijn.

Het concept Raffinaderij kan het beste worden omschreven als een werkwijze die rechercheurs en analisten in staat stelt om met behulp van geautomatiseerde gegevensverwerking onderzoek te doen. De Raffinaderij is daarbij geen *tool* maar veeleer een werkwijze die door data-analyse technologie wordt ondersteund. Door de inzet van geavanceerde data-analyse technologieën wordt het mogelijk om op een effectieve en efficiënte wijze grote hoeveelheden (on)gestructureerde politiegegevens in samenhang te ontsluiten, analyseren, verrijken en de resultaten daarvan te visualiseren.

De overkoepelende doelstelling van de Raffinaderij is om de veiligheid te vergroten door betere opsporing en *intelligence*, dat wil zeggen het in stand houden van een zekere informatiepositie die vervolgens aangewend kan worden om concreet te handhaven. Meer specifiek zijn de volgende twee doelstellingen aan te wijzen:

- Het vergroten van de effectiviteit en de efficiëntie van de politie door het leveren van een bijdrage aan de Informatie Gestuurde Opsporing;
- Het proces van waarheidsvinding in de opsporing versnellen en verbeteren door op een meer effectieve manier met grote hoeveelheden ongestructureerde data om te gaan.

Juridische grondslag gebruik Raffinaderij

De juridische basis voor het verzamelen (en verder verwerken) van politiegegevens binnen de Raffinaderij moet gevonden worden in de artikelen 8 tot en met 13 Wpg. Omdat de Raffinaderij primair wordt ingezet voor *intelligence* doeleinden en voor specifieke opsporingsonderzoeken en daarbij gebruik wordt gemaakt van het combineren en

analyseren van verschillende datasets, zijn de belangrijkste grondslagen voor het gebruik van de Raffinaderij artikel 9 en 10 Wpg jo artikel 11 Wpg.

De Raffinaderij wordt momenteel gebruikt voor grote, complexe zaken. Hiertoe worden gegevens uit diverse opsporingsonderzoeken (Titel IVA, Titel V en Titel VB onderzoeken) samengebracht in de Raffinaderij. Een voorwaarde voor het legitieme gebruik van de gegevens uit deze onderzoeken is dat zij op rechtmatige wijze zijn verzameld. Wanneer het verzamelen van deze gegevens een meer dan geringe inbreuk op de persoonlijke levenssfeer van de verdachte of andere betrokkenen vormt, is een specifieke wettelijke basis noodzakelijk. Deze basis moet worden gevonden in het Wetboek van Strafvordering (Sv), bijvoorbeeld in de regelingen omtrent de (bijzondere) opsporingsbevoegdheden. In zoverre de gebruikte gegevens zijn verzameld met behulp van de inzet van bijzondere opsporingsbevoegdheden dient op grond van artikel 126dd Sv toestemming voor het hergebruik van deze gegevens in een ander onderzoek of voor intelligence doeleinden te worden gegeven door de Officier van Justitie.

Voor wat betreft de rechtmatigheid van de verwerking van politiegegevens levert de Raffinaderij ten opzichte van de vorige PIA geen nieuwe vraagstukken op. Raffinaderij put alleen uit politiebronnen en verwerkt deze gegevens ter ondersteuning van het normale recherche- en analyseproces. Wanneer de gegevens die in de politiebronnen zijn opgeslagen legitiem zijn verzameld, geldt dat de verdere verwerking in de Raffinaderij rechtmatig is, zolang wordt voldaan aan de eisen van de Wpg. Indien onrechtmatig verkregen gegevens in deze bronnen aanwezig zijn, werkt dit uiteraard ook door in de Raffinaderij.

Bronnen

Nieuw ten opzichte van de PIA 2013 is dat nu ook open bronnen onderzoek (OSINT) wordt betrokken binnen de Raffinaderij werkwijze. Daar waar er sprake is van een meer dan geringe inbreuk op de persoonlijke levenssfeer wordt het open bronnen onderzoek enkel gedaan op basis van de bevoegdheid tot stelselmatige observatie (artikel 126g Sv). Vanuit het perspectief van dataminimalisatie worden alleen die gegevens binnen de politieorganisatie gehaald die daadwerkelijk relevant zijn voor het onderzoek. In de toekomst wordt binnen het nieuwe boek 2 van het Wetboek van Strafvordering een nieuwe specifieke opsporingsbevoegdheid gecreëerd voor open bronnen onderzoek op internet.

Materiële eisen verwerking

Op grond van de Wpg moeten de verwerkingen binnen de Raffinaderij voldoen aan een aantal eisen. Het gaat daarbij om zaken als dataminimalisatie, datakwaliteit, geheimhouding, beveiliging en het invulling geven aan de rechten van de betrokkenen. Met alle genoemde eisen is voor zover mogelijk rekening gehouden binnen de Raffinaderij. Het betreft technische en organisatorische maatregelen. Deels gaat het om 'standaardprocedures' die bestaan binnen de politie waarbij geen specifieke aanpassingen noodzakelijk zijn voor de Raffinaderij. Op andere punten zijn er binnen de Raffinaderij specifieke (technische) maatregelen genomen. Hierbij kan met name gedacht worden aan zaken als het loggen van het gebruik van de politiegegevens. Op dit specifieke punt is de Raffinaderij zelfs meer 'privacybeschermend' dan de huidige politiepraktijk.

Op basis van het bovenstaande concluderen wij dat er in zijn algemeenheid een juridische grondslag is voor de verzameling en verdere verwerking van de politiegegevens in het kader van de Raffinaderij.

Een punt van aandacht richting de toekomst is wel de verhouding tussen het strafprocesrecht en het gegevensbeschermingsrecht. Zoals de WRR signaleert in haar studie naar Big Data in het veiligheidsdomein[1] liggen de meeste waarborgen in de verzamelfase en niet in de analyse-fase (waar de Wet politiegegevens primair op ziet). Op de langere termijn werpt dit wellicht de vraag op of Wpg een voldoende wettelijke basis vormt ex. artikel 8 EVRM om inbreuken op de persoonlijke levenssfeer van de verdachte en andere betrokkenen te legitimeren. Het betreft hier echter niet zozeer een vraagstuk dat specifiek is voor de Raffinaderij, als wel voor de informatie-huishouding van de politie in zijn algemeenheid. Vanuit het perspectief van de PIA is dit dan ook niet een probleem dat direct geadresseerd kan worden. Met de Raffinaderij wordt binnen de grenzen van de wet geopereerd, maar werkwijzen zoals de Raffinaderij rechtvaardigen misschien een meer fundamentele herijking van het juridisch kader voor de gegevensverwerking door de politie in de toekomst.

[1] Wetenschappelijke Raad voor het Regeringsbeleid (WRR), 'Big Data in een vrije en veilige samenleving', Amsterdam University Press: Amsterdam 2016.

(Privacy)risico's Raffinaderij

Hoewel de Raffinaderij een krachtig middel is voor de opsporing, kan (verkeerd) gebruik van de Raffinaderij ook risico's met zich meebrengen. Deze liggen primair op het gebied van de privacy maar ook andere grondrechten, zoals het recht op een eerlijk proces, kunnen in het geding komen.

Privacyrisico's kunnen onder andere ontstaan door gebrekkige (data)governance (wanneer de Raffinaderij niet goed wordt ingebed binnen de bredere politieorganisatie), gebrekkig beheer van gegevens, schaalvergroting en door beveiligingsincidenten. De impact die deze risico's (indien deze zich manifesteren) kunnen hebben op burgers betreft onder andere onvrijwillige en ongewenste openbaarmaking van gegevens, aantasting van de persoonlijke autonomie en mogelijk een inbreuk op het recht op een eerlijk proces. De mogelijke gevolgen van het manifesteren van deze risico's voor de politie zijn het 'stukgaan' van zaken, reputatieschade, handhaving door de toezichthouder, hogere compliancekosten en een grotere terughoudendheid binnen en buiten de politie om gegevens te delen.

Eén van de belangrijkste privacyrisico's van de Raffinaderij is gelegen in de schaalvergroting die de Raffinaderij mogelijk maakt voor wat betreft de verwerking van gegevens. Schaalvergroting kan leiden tot een 'datahonger' bij de politie. De wens om een gepleegd strafbaar feit op te lossen, kan betekenen dat steeds meer gegevens in een onderzoek ingebracht worden. Het risico op *fishing expeditions* ligt dan op de loer. Een ander risico van schaalvergroting is *mission*- en *function creep*. De kans bestaat dat de Raffinaderij voor steeds meer doelen wordt ingezet en steeds meer functionaliteiten krijgt waarmee vanuit privacy perspectief oorspronkelijk geen rekening is gehouden. Om de negatieve effecten van schaalvergroting te voorkomen en om datahonger en mission- en function creep tegen te gaan, moet altijd rekening worden gehouden met de doelbindingseis uit de Wpg en de beginselen van proportionaliteit en subsidiariteit.

Een specifiek risico, met name voor de politie zelf, betreft de samenwerking met externe leveranciers zoals Palantir. Binnen de Raffinaderij zijn voldoende maatregelen genomen om te voorkomen dat deze leveranciers onrechtmatig kennis kunnen nemen van politiegegevens. In de publieke opinie kan echter het gebruik van met name Palantir geassocieerd worden met de praktijken van de CIA en de NSA, hetgeen mogelijk negatief afstraalt op de politie.

Een ander risico, dat niet zozeer een privacyrisico is als wel een mogelijke aantasting van het recht op een eerlijk proces, betreft de transparantie en controleerbaarheid van analyses gedaan met behulp van de Raffinaderij. Rapportages uit de Raffinaderij kunnen ter terechtzitting moeilijk ter discussie worden gesteld door de verdediging, aangezien de verdediging niet over dezelfde geavanceerde analyse-technieken beschikt. Dit heeft mogelijk een effect op de gelijkheid van middelen tussen het Openbaar Ministerie en de verdediging (*equality of arms*).

Tenslotte hebben wij aandacht besteed aan de vraag wat de privacyrisico's zijn van mogelijk toekomstige uitbreiding van gebruik van de Raffinaderij. Hierbij moet bijvoorbeeld gedacht worden aan *predictive policing* gebaseerd op *data mining* en andere vormen van Big Data-analyse. Een dergelijke uitbreiding brengt diverse risico's met zich mee die sowieso een andere insteek vergen dan de huidige insteek van het Raffinaderij concept. De huidige insteek draait in de kern om de beantwoording van concrete recherche-vragen in plaats van dat gezocht wordt naar onontdekte patronen of verbanden in politiegegevens.

Risicobeperkende maatregelen

Om de bovengenoemde risico's te adresseren, zijn diverse technische en organisatorische maatregelen genomen binnen het Raffinaderij project. Allereerst is het van belang om te vermelden dat de Raffinaderij enkel gegevens ontsluit uit bestaande politiebronnen en dat de Raffinaderij reeds bestaande recherche- en analyse-werkzaamheden vereenvoudigt en versnelt. Het grote verschil ligt in het feit dat de Raffinaderij de voorbereidingshandelingen (zoals het combineren en verrijken van data) die de opsporingsambtenaar of analist vroeger handmatig moest doen automatiseert, waardoor de opsporingsambtenaar of analist zich kan richten op het daadwerkelijke recherche- en analysewerk. De controle-mechanismen uit de Wpg die op deze handelingen van toepassing zijn en de implementatie daarvan binnen de politie zijn onverkort op de Raffinaderij van toepassing. Naast deze algemene compliance maatregelen zijn voor de Raffinaderij specifieke maatregelen genomen.

Een eerste Raffinaderij-specifieke waarborg is logging van alle handelingen. Om de herkomst en het gebruik van de data te kunnen traceren is elk data element terug te voeren op de originele bron. Alle handelingen die vervolgens met de data worden gedaan door een specifieke gebruiker worden gelogd, zodat stap voor stap terug te voeren is wat een analist of rechercheur heeft gedaan en hoe deze tot een bepaalde conclusie is gekomen.

Om de vertrouwelijkheid van de data te waarborgen is authenicatie en autorisatie systeem ingericht binnen de Raffinaderij. Dit systeem is gebaseerd op het politie autorisatiemodel. Het autorisatiemodel is rol- en attribuut gebaseerd. Dit betekent dat gebruikers alleen die data elementen kunnen zien waartoe zij gemachtigd zijn.

Belangrijkste waarborg lijkt echter een gedegen bewustzijn binnen het Raffinaderij team te zijn dat er wordt gewerkt met een krachtig instrument waarmee verantwoordelijk moet worden omgesprongen. Bewustzijn over de privacyrisico's en de risico's voor de integriteit van de opsporing zorgen er voor dat gewaakt wordt voor 'datahonger' en 'mission- en function creep'. Hiermee is niet alleen de privacy gediend, maar ook de integriteit van de opsporing.

Het is daarom sterk aan te bevelen om dit bewustzijn goed te borgen binnen de bredere politieorganisatie mocht besloten worden om de Raffinaderij operationele status te geven. Training en bewustwording over de mogelijkheden, onmogelijkheden en risico's van de Raffinaderij-werkwijze zijn daar belangrijk onderdelen van. Daarnaast zijn compliance en governance maatregelen, zoals het aanstellen van een specifieke Functionaris Gegevensbescherming voor de Raffinaderij, het doen van privacy impact assessments voor nieuwe toepassingen en het voeren van een duidelijke registratie van verwerkingen zeer wenselijk.

Conclusie

De Raffinaderij brengt ontegenzeggelijk (privacy)risico's mee, maar deze zijn – in ieder geval voor wat betreft de pilotfase waarin de Raffinaderij zich nu bevindt - afdoende geadresseerd om te kunnen spreken van een verwerking die een toereikende wettelijke basis heeft en voldoet aan de eisen van proportionaliteit en subsidiariteit. De nieuwe tooling, toepassingsgebieden en werkwijzen leveren geen nieuwe (privacy)vraagstukken op die tot een andere conclusie nopen dan die van de PIA uit 2013 waarin eenzelfde conclusie werd getrokken.

Indien besloten wordt Raffinaderij verder te implementeren in de politieorganisatie (waardoor het gebruik en de gebruikersgroep groter wordt) is het van belang een aantal aanvullende risicobeperkende maatregelen te treffen.

Inhoudsopgave

5.1.2.h

1 Inleiding

In onze samenleving worden veel data gegenereerd. Dit gebeurt niet alleen op sociale media en internet, ook overheden en bedrijven genereren veel data. Deze ontwikkeling wordt aangeduid met de term *Big Data*. Big Data betreft de verzameling en analyse van grote hoeveelheden, heterogene data. Deze datasets zijn zo groot dat de technologie die nodig is om deze data te analyseren tot voor kort niet bestond.[2] Big Data-analyses bieden kansen voor de politie. De data kunnen aanwijzingen, sporen of andere belangrijke informatie bevatten die van belang zijn voor de opsporing. Daar staat tegenover dat de stortvloed aan data ook een bedreiging kan zijn voor de opsporing. *Information overload*, het niet meer wijs kunnen worden uit de beschikbare gegevens, kan ertoe leiden dat belangrijke aanwijzingen of sporen niet of te laat worden ontdekt.

Het is de uitdaging om effectief en efficiënt om te gaan met de beschikbare gegevens binnen de politie. Binnen de Nationale politie (verder: de politie) wordt daarom op dit moment gewerkt aan het concept 'Raffinaderij'. De Raffinaderij is géén tool maar een werkwijze waarmee ruwe data worden opgewerkt tot bruikbare informatie en kennis. Een parallel kan worden gelegd met een olieraffinaderij: in een olieraffinaderij wordt ruwe olie opgewerkt tot verschillende bruikbare eindproducten. De Raffinaderij is een concept dat een nieuwe werkwijze introduceert voor informatiegestuurde opsporing die wordt ondersteund door integrale analyse-instrumenten waarin gestructureerde en ongestructureerde (Big) data uit diverse bronnen in samenhang kunnen worden geanalyseerd.

Het concept Raffinaderij (hierna: Raffinaderij) is veelbelovend en mogelijk zelfs noodzakelijk voor het succes van de opsporing. Er zijn echter ook risico's verbonden aan het gebruik en de inzet van de Raffinaderij. Deze risico's liggen primair op het gebied van de privacy van de burger. Meer specifiek ligt de vraag voor welke effecten het gebruik van de Raffinaderij op de privacy van de burger heeft en hoe deze eventuele risico's en negatieve effecten voorkomen of ondervangen kunnen worden. Bij de beantwoording van deze vraag speelt het juridisch kader voor de bescherming van persoonsgegevens een zeer belangrijke rol.

[2] Sloan & Warner 2013, pp. 19-20.

5.1.2.h

1.1 Doel van de PIA

In 2012-2013 heeft 5.1.2.h een Privacy Impact Assessment (PIA) gedaan voor de Proeftuinfase van de Raffinaderij. De proeftuin is, na een (positieve) evaluatie, uitgebreid tot een bredere operationele pilot die tot eind 2017 loopt. In 2017 dient wederom de afweging te worden gemaakt óf, en zo ja op welke manier het Raffinaderij concept na 2017 wordt voortgezet. Hiertoe wordt een Business Case opgesteld door 5.1.2.h

De politie vindt het belangrijk dat ten behoeve van de Business Case en de besluitvorming over het vervolg van Raffinaderij de PIA uit 2013 wordt herijkt.

Dit is allereerst noodzakelijk omdat de Raffinaderij pilot geëvolueerd en opgeschaald is en nu in het hele land wordt gebruikt in onderzoeken op het gebied van liquidaties (en de voorbereiding daarvan) en op het gebied van contra-terrorisme, extremisme en radicalisering (CTER).

Ten tweede is het juridisch kader dat van toepassing is op de Raffinaderij aan het veranderen. Op Europees niveau is Richtlijn 2016/680/EG[3] aangenomen, die de Wet politiegegevens aanpast. Daarnaast zijn op nationaal niveau voorstellen voor de modernisering van Boek 2 van het Wetboek van Strafvordering gedaan en buigt de Eerste Kamer zich momenteel over de Wet Computercriminaliteit III.

Tenslotte is de maatschappelijke aandacht voor het gebruik van data analyse binnen de openbare orde en veiligheidssector toegenomen. Zo is onder andere door de Wetenschappelijke Raad voor het Regeringsbeleid in het rapport '*Big Data in een Vrije en Veilige Samenleving*' kritisch geflecteerd op data analyse systemen zoals de Raffinaderij.

In deze PIA wordt beoordeeld hoe het huidige gebruik van de Raffinaderij (en het gebruik dat voor de komende jaren wordt voorzien) zich verhoudt tot het juridisch kader waarbinnen de politie opereert. Dit kader bestaat met name uit de Grondwet, databeschermingswetgeving in de vorm van de Wet politiegegevens en de Europese Richtlijn 2016/680, politiewetgeving en het strafvorderlijk kader (Wetboek van

[3] Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens. De Richtlijn dient voor 6 mei 2018 geïmplementeerd te zijn.

Strafvordering en – waar relevant - de Wet Computercriminaliteit III).

Het doel van de PIA is om tot een systeem te komen waarmee het opsporingsbelang en het beschermen van de rechten van burgers beide optimaal geregeld zijn. Hiervoor is het noodzakelijk in beeld te brengen wat de (verwachte) juridische en maatschappelijke grenzen van de toepassing van de Raffinaderij zijn.

1.2 Methodologie

Deze PIA identificeert en analyseert de mogelijke privacyrisico's van de Raffinaderij anno 2017.

1. Het doen van een legitimiteitstoets en het maken van een inschatting van de risico's van de huidige wijze van gebruik (een update van de PIA uit 2013) en advies over de daarbij benodigde privacy verhogende en risicobeperkende maatregelen;
2. Een legitimiteitstoets en inschatting van de risico's (op hoofdlijnen) van mogelijke toekomstige toepassing en wijze van gebruik.

De legitimiteitstoets en risico analyse zijn gebaseerd op interviews, literatuurstudie en jurisprudentie analyse.

Meer specifiek wordt in deze PIA update een antwoord gezocht op de volgende vragen:

1. Leveren wijzigingen in gebruikte tooling en technologie nieuwe privacyvraagstukken op?
2. Leveren aangepaste werkwijzen en methoden nieuwe privacyvraagstukken op?
3. Leveren aangepaste toepassingsgebieden nieuwe privacyvraagstukken op? L SEP

Bij de keuze voor de rapportage over de privacyrisico's is ervoor gekozen de PIA rapportage uit 2013 (groten)deels te herschrijven. Dit heeft het praktische voordeel dat de PIA 2017 zelfstandig kan worden gelezen zonder dat telkens op de PIA 2013 teruggegrepen hoeft te worden.

1.3 Leeswijzer

Deze rapportage is opgebouwd uit 13 hoofdstukken.

Hoofdstuk 2 gaat dieper in op het doel en de scope van deze PIA.

In hoofdstuk 3 wordt het concept Raffinaderij en de positie daarvan binnen de politieorganisatie kort toegelicht. In hoofdstuk 4 wordt vervolgens dieper ingegaan op de organisatorische en technische aspecten van de Raffinaderij.

In hoofdstuk 5 wordt een algemeen beeld gegeven van het juridisch kader dat van toepassing is op de Raffinaderij. Het gaat dan met name over het grondrecht op privacy. Bij het gebruik van gegevens in het kader van de Raffinaderij maken we een onderscheid tussen het *verzamelen* van gegevens (waarbij naast de Wet politiegegevens primair het Wetboek van Strafvordering relevant is) en het verder *verwerken* van politiegegevens (waarop de Wet politiegegevens van toepassing is). In hoofdstuk 6 gaan we dieper in op het juridisch kader voor het verzamelen van politiegegevens, in hoofdstuk 7 op het juridisch kader voor het verwerken van politiegegevens.

Op basis van de informatie uit de hoofdstukken 5 tot en met 7 doen wij in de hoofdstukken 8 en 9 de legitimiteitstoets voor wat betreft de verwerking van politiegegevens binnen de Raffinaderij. In hoofdstuk 8 kijken we naar de juridische grondslag voor het verwerken van de gegevens, in hoofdstuk 9 kijken we naar de invulling van de materiële compliance eisen.

In hoofdstuk 10 gaan wij in op de (privacy)risico's die de Raffinaderij kan opleveren. In hoofdstuk 11 worden deze risico's vertaald naar mogelijke gevolgen voor de betrokkenen en de politie. In hoofdstuk 12 worden de reeds genomen (en te nemen) risicobeperkende maatregelen besproken.

We besluiten de PIA met een algemene conclusie in hoofdstuk 13.

In de appendix bij dit rapport is een risico register opgenomen dat de geïdentificeerde risico's en risicobeperkende maatregelen in het kort beschrijft.

2 Opdrachtbeschrijving

2.1 Achtergrond

De Raffinaderij is een voorziening die het mogelijk maakt om grote hoeveelheden politiegegevens in samenhang te ontsluiten, analyseren, verrijken en de resultaten daarvan te visualiseren. Door data uit verschillende (politie)bronnen met elkaar te combineren, kunnen verbanden worden ontdekt tussen schijnbaar niet aan elkaar gerelateerde gebeurtenissen. Anderzijds kunnen hypothesen gebaseerd op verbanden die er in werkelijkheid niet zijn in een vroeg stadium worden ontkracht.[4]

De Raffinaderij kan daarmee het beste omschreven worden als een werkwijze die een rechercheur en een analist beter in staat stelt om met behulp van geautomatiseerde gegevensverwerking onderzoek te doen. De werkwijze behelst de gezamenlijke inzet van verschillende geavanceerde informatie-analyse-toepassingen. In de Raffinaderij is het mogelijk om op een effectieve en efficiënte manier grote hoeveelheden (on)gestructureerde data procesmatig te verwerken. De technologie die wordt gebruikt, maakt het ontsluiten, verrijken, analyseren en visualiseren van deze data mogelijk.

Het bovenstaande betekent dat een rechercheur en een analist door middel van de Raffinaderij zijn of haar onderzoeks- of analysevragen beter kan beantwoorden. [5]

2.2 Doel van de Raffinaderij

De overkoepelende doelstelling van de Raffinaderij is om de veiligheid te vergroten door betere opsporing en intelligence, dat wil zeggen het in stand houden van een zekere informatiepositie die vervolgens aangewend kan worden om concreet te handhaven. Meer specifiek zijn de volgende twee doelstellingen aan te wijzen:

- Het vergroten van de effectiviteit en de efficiëntie van de politie door het leveren van een bijdrage aan de Informatie Gestuurde Opsporing;

[4] De Vries 2016, p. 255.

[5] Een voorbeeld van een dergelijke rechercheonderzoeksvraag is de vraag wie een bepaalde liquidatie heeft gepleegd of wie opdracht tot een liquidatie heeft gegeven. Daarnaast kan de Raffinaderij worden gebruikt om een groter, overkoepelend probleem te stoppen. Zo kan de Raffinaderij worden ingezet om het aantal liquidaties terug te dringen of om de directe gevolgen voor de samenleving van dergelijke liquidaties te beperken.

- Het proces van waarheidsvinding in de opsporing versnellen en verbeteren door op een meer effectieve manier met grote hoeveelheden ongestructureerde data om te gaan.

Inbreuken op de rechtsorde door bepaalde vormen van zware criminaliteit kunnen worden voorkomen of op effectievere wijze worden aangepakt wanneer de politie een toereikende informatiepositie heeft.

2.3 Afbakening Privacy Impact Assessment

2.3.1 Algemeen

Een juridische analyse van de Raffinaderij is complex. Dit heeft er mee te maken dat de Raffinaderij eerder een werkwijze is dan een concreet afgebakend (software)product. Een complicerende factor is het feit dat de werkwijze inhoudt dat verschillende technische componenten gezamenlijk worden gebruikt om informatie te verwerken die afkomstig is uit verschillende bronnen. Deze informatie is vervolgens ingewonnen met behulp van uiteenlopende (opsporings)methoden, mogelijk ten behoeve van uiteenlopende doelen.

Een PIA is gericht op het identificeren en adresseren van risico's voor de *informationele privacy* van betrokkenen. Het primaire toetsingskader voor deze PIA is daarmee de Wet politiegegevens. Echter, de juridische en maatschappelijke vraagstukken die bij het gebruik van de Raffinaderij spelen, beperken zich niet noodzakelijk tot de informationele privacy. Ook het recht op een eerlijk proces (6 EVRM) kan bijvoorbeeld beïnvloed worden door gegevensverwerking door de politie. Om die reden maken wij in deze PIA waar mogelijk een onderscheid tussen risico's gerelateerd aan ***privacy- en gegevensbescherming*** en risico's gerelateerd aan de ***bredere mensenrechtelijke aspecten*** van informatie-gestuurde opsporing met behulp van de Raffinaderij.

2.3.2 Focus: opsporingsonderzoek en verkennend onderzoek

De opsporing maakt onderdeel uit van het proces van informatiegaring. Dit proces omvat verschillende typen van onderzoek. De Memorie van Toelichting bij de Wet bijzondere opsporingsbevoegdheden[6] maakt hierbij onderscheid tussen:

1. Het opbouwen en in stand houden van een zekere informatiepositie door
   a. Het opslaan, bewerken, gebruiken en analyseren van gegevens; of

[6] *Kamerstukken II* 1996–1997, 25 403, nr. 3.

   b. Het vergaren van gegevens door de toepassing van niet-ingrijpende middelen;
2. Het verkennend onderzoek; en
3. Het opsporingsonderzoek.

Deze onderzoeken zijn primair neergelegd in Titel IVA en Titel V van het Wetboek van Strafvordering (Sv).

In deze rapportage onderzoeken wij de privacy impact van de inzet van de Raffinaderijwerkwijze in het verkennend- en het opsporingsonderzoek in Nederland. Hierbij kijken wij hoofdzakelijk naar het huidige gebruik van de Raffinaderij: het gericht verwerken van gegevens op basis van concrete onderzoeks- en analysevragen.

Daarbij is het uitgangspunt dat de Raffinaderij wordt ingezet als een werkwijze binnen een opsporingsonderzoek zoals bedoeld in artikel 132a Sv. Daar gaat het meer specifiek om de mogelijkheid om de Raffinaderij in te zetten binnen klassieke onderzoeken, 'Titel IVA onderzoeken' en/of binnen 'Titel V onderzoeken' van het Wetboek van Strafvordering. Een 'Titel IVA onderzoek' betreft een onderzoek naar een verdachte van een misdrijf zoals omschreven in artikel 67 Sv. Een 'Titel V onderzoek' behelst de opsporing naar het beramen of plegen van ernstige misdrijven in georganiseerd verband, daaronder begrepen onderzoeken naar terroristische misdrijven (Titel VB). Daarnaast wordt de mogelijkheid om de Raffinaderij te gebruiken in het kader van verkennende onderzoeken, zoals bedoeld in artikel 126gg Sv, onderzocht (Titel VE). In het kader van deze onderzoeken en de bijbehorende opsporingsbevoegdheden kan de politie persoonsgegevens verzamelen die al dan niet als bewijs kunnen dienen. Op de *verzameling* van deze gegevens is primair het Wetboek van Strafvordering van toepassing.

In deze PIA zullen wij ons met name richten op het type 2 en 3 van het onderzoek: het verkennend onderzoek en het opsporingsonderzoek. Dit neemt niet weg dat type 1 van het onderzoek, het opbouwen en in stand houden van een zekere informatiepositie, op indirecte wijze de revue zal passeren in deze PIA. Dit heeft er mee te maken dat het opbouwen en in stand houden van een informatiepositie in het belang is van de handhaving van de rechtsorde.

5.1.2.h

2.3.3 Focus: verzamelen, verwerken, geautomatiseerd vergelijken en in combinatie doorzoeken van gegevens

Primair heeft deze PIA betrekking op de volgende aspecten waartoe de Raffinaderij tijdens het opsporingsonderzoek wordt ingezet:

1. Het verzamelen van (politie)gegevens uit diverse bronnen;
2. Het verwerken van deze gegevens. Hierbij wordt gebruik gemaakt van technische toepassingen om bruikbare informatie uit de ruwe data te destilleren;
3. Het geautomatiseerd vergelijken en in combinatie doorzoeken van de (politie)gegevens evenals het leggen van verbanden tussen deze gegevens en het in context plaatsen van deze gegevens.

De *verwerking* van persoonsgegevens door de politie wordt primair gereguleerd door de Wet politiegegevens (Wpg). Voor wat betreft de verwerking van persoonsgegevens in het kader van de hierboven genoemde opsporingsonderzoeken zijn twee artikelen van belang. Artikel 9 Wpg biedt de grondslag om onderzoek te doen in verband met de handhaving van de rechtsorde in een bepaald geval. Op grond van artikel 10 Wpg kunnen politiegegevens worden verwerkt om inzicht te krijgen in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde.

2.3.4 Focus: werkwijze van Raffinaderij

In deze rapportage wordt een PIA uitgevoerd op de werkwijze van de Raffinaderij. De Raffinaderij wordt momenteel ingezet voor opsporingsonderzoeken naar liquidaties, contra-terrorisme, extremisme en radicalisering (CTER) en in het onderzoek naar de vliegramp MH17. In het kader van deze analyse plaatsen wij uitdrukkelijk de inzet van de Raffinaderij in onderzoeken naar liquidaties en contra-terrorisme binnen de scope van dit onderzoek. De inzet van de Raffinaderij in het kader van de onderzoeken naar de vliegramp MH17 valt weliswaar (deels) binnen de scope van deze PIA maar zal gezien het specifieke en uitzonderlijke karakter niet uitgebreid aan de orde komen. Het onderzoek naar MH17 is niet direct representatief voor het type onderzoeken dat normaliter binnen de Raffinaderij plaats moet gaan vinden.

5.1.2.h

2.3.5 Focus: Datamining, geautomatiseerde besluitvorming en predictive policing

In de Raffinaderij wordt (nog) geen gebruik gemaakt van datamining technieken ten behoeve van geautomatiseerde besluitvorming of *predictive policing* (waar voorspellingen worden gedaan over toekomstige misdrijven en andere risico's). Het is de vraag of de Raffinaderij in de toekomst hiertoe überhaupt wordt ingezet. Met het oog op de toekomstbestendigheid van deze PIA besteden wij wel reeds aandacht aan dit onderwerp, ook al ligt de nadruk op de huidige toepassing.

2.3.6 Focus: Samenwerkingsverbanden en samenwerkingspartners

De politie werkt in steeds grotere mate samen met andere overheden en andere partners. Hiertoe zullen in de toekomst vermoedelijk samenwerkingsverbanden worden opgezet. Binnen deze samenwerkingsverbanden en met de partners zullen in toenemende mate gegevens worden gedeeld. In deze PIA zal dit aspect in beperkte mate en enkel waar relevant worden aangestipt. Achtergrond van deze keuze is dat de omgang met samenwerkingsverbanden niet een specifiek Raffinaderij vraagstuk is.

2.3.7 Buiten scope

Buiten de scope van deze PIA valt de analyse van:

- De inzet van de Raffinaderij ter uitvoering van de dagelijkse politietaak, zoals voortvloeit uit artikel 3 Politiewet juncto artikel 8 Wpg. Het valt ook sterk te betwijfelen of de Raffinaderij hier ooit wordt ingezet, omdat de toegevoegde waarde voor het uitvoeren van verwerkingen in het kader van de dagelijkse politietaak beperkt is gezien het specialistische karakter.
- Het juridisch kader met betrekking tot samenwerking met buitenlandse autoriteiten. De kern van dit juridisch kader staat in artikel 552i Sv en de Aanwijziging inzake de informatie-uitwisseling in het kader van de wederzijdse rechtshulp in strafzaken. Onderzoeken naar georganiseerde criminaliteit in het algemeen, en *high tech crime* in het bijzonder, kennen vaak grensoverschrijdende aspecten en gegevensuitwisselingen. Op dit moment wordt Raffinaderij (nog) niet ingezet in de samenwerking met buitenlandse (opsporings)diensten. Mocht in de toekomst worden overwogen om de Raffinaderij in te zetten in het kader van samenwerking met buitenlandse autoriteiten, bevelen wij een vervolgonderzoek naar dit onderwerp aan.

3 De Raffinaderij

3.1 Omschrijving

Zoals in het voorgaande hoofdstuk al kort werd aangestipt, kan het concept Raffinaderij het beste omschreven worden als een werkwijze die rechercheurs en analisten in staat stelt om met behulp van geautomatiseerde gegevensverwerking onderzoek te doen. Door de inzet van geavanceerde informatieanalyse-toepassingen wordt het mogelijk om op een effectieve en efficiënte wijze grote hoeveelheden (on)gestructureerde politiegegevens in samenhang te ontsluiten, analyseren, verrijken en de resultaten daarvan te visualiseren.

De Raffinaderij valt binnen de politie in het Business Intelligence domein. Business Intelligence wordt daarbij gedefinieerd als het geheel van processen, producten, hulpmiddelen en organisatorische inrichting ten behoeve van het geautomatiseerd verzamelen, integreren en veredelen van gegevens en het analyseerbaar maken, presenteren en distribueren van informatie.[7]

Hoewel in de Raffinaderij technische mogelijkheden kunnen worden gebouwd die *data mining*, *profiling* en *predictive policing* mogelijk maken, wordt de Raffinaderij momenteel expliciet niet voor deze verwerkingen ingezet. In de Raffinaderij worden veel gegevens geladen (*Big Data*) maar aan de analyse ligt altijd een specifieke, concrete recherchevraag ten grondslag.

3.2 De Raffinaderij als operationele pilot

In 2011 is in de *Holitna*-zaak onderzoek gedaan naar het netwerk van Robert M., die hoofdverdachte was in een omvangrijke kinderpornozaak in Amsterdam. Rechercheurs van de Landelijke Eenheid werden tijdens dit onderzoek geconfronteerd met enorme hoeveelheden gegevens op de computer van een van de verdachten. Mede hieruit ontstond de behoefte aan een werkwijze en een ondersteunende Business Intelligence voorziening die de politie beter in staat stelt om grote hoeveelheden data snel te ontsluiten, betekenis te geven en te analyseren. Bestaande expertise en ontwikkelde tools zijn ingezet om uit deze (on)gestructureerde hoeveelheid data voor de opsporing en vervolging bruikbaar materiaal te vinden. Dit heeft geleid tot de ontwikkeling van de Business Intelligence voorziening Raffinaderij, eerst in de vorm van een 'proeftuin', vervolgens als operationele pilot.

[7] Business Intelligence Strategie 2012.

De Raffinaderij is vervolgens in testfase bij verschillende onderzoeken gebruikt door de Landelijke Recherche, als onderdeel van de Landelijke Eenheid (zie PIA 2013).

De Raffinaderij is nu een operationele pilot en heeft projectstatus. Inmiddels is het gebruik van de Raffinaderij uitgebreid naar liquidatieonderzoeken (in 2014), CTER (in 2015) en het onderzoek naar het neerhalen van MH17 (in 2016). De Raffinaderij wordt op het moment van schrijven van deze PIA rapportage ingezet op diverse (grote) onderzoeken. De infrastructuur is landelijk beschikbaar en wordt gebruikt door zowel de Recherche als de Informatieorganisatie van de politie.

3.2.1 Betrokken partijen vanuit de opsporing

Op het moment van schrijven van deze rapportage gebruiken de politie en het Openbaar Ministerie de Raffinaderij in het kader van onderzoeken. Binnen de politie zijn alle eenheden betrokken. Binnen de eenheden zijn specifiek de recherchetak en de informatie-organisatietak betrokken. Bij het Openbaar Ministerie zijn het Landelijk Parket, zaaksofficieren en informatieofficieren betrokken in het kader van strafrechtelijke onderzoeken in de Raffinaderij.

Afhankelijk van het doel van een onderzoek kunnen ook andere partijen betrokken worden in het onderzoek en eventueel de Raffinaderij gebruiken. Bijvoorbeeld, wanneer de Raffinaderij ingezet wordt ter ondersteuning van onderzoeken in het kader van contra-terrorisme kan een medewerker van de Koninklijke Marechaussee, die onderdeel uitmaakt van de contra-terrorisme infocel, onderzoek doen met de Raffinaderij. Deze onderzoeken worden opgeslagen in SummIT. Een ander voorbeeld betreft een onderzoek door de Rijksrecherche naar corruptie. Wanneer dit onderzoek 'gedraaid wordt' in de Raffinaderij krijgt een medewerker van de Rijksrecherche de mogelijkheid om met de Raffinaderij te werken.

3.2.2 Toeleveranciers technologie

Zoals reeds uit het bovenstaande blijkt, is de Raffinaderij geen op zichzelf staand stuk software. De Raffinaderij is veel meer een werkwijze waarbij gebruik wordt gemaakt van verschillende tools, die deels door de politie zelf ontwikkeld zijn en deels afgenomen worden van externe softwareleveranciers. Eén van de belangrijkste externe softwarepakketten waar op dit moment (deels) mee wordt gewerkt, is Palantir.[8] Palantir is een analyse- en visualisatie tool en vormt als het ware de 'gebruikersvoorkant' van de

[8] www.palantir.com.

Raffinaderij. Daarnaast bedenkt de politie zelf op welke manier data wordt ontsloten, geïntegreerd, doorzoekbaar gemaakt, gevisualiseerd enzovoorts en ontwikkelt zij hiertoe zelf software en tools.[9] Nieuwe functionaliteiten worden op een zodanige manier geïntegreerd met de Palantir schil dat gebruikers niet merken dat het in feite gaat om een combinatie van tools.

[9] Vanaf de start van de Raffinaderij zijn hiertoe drie ontwikkelaars ingehuurd die vast onderdeel uitmaken van het Raffinaderijteam. Omdat de Raffinaderij een tijdelijke pilot betreft, konden geen formatieplaatsen worden gecreëerd.

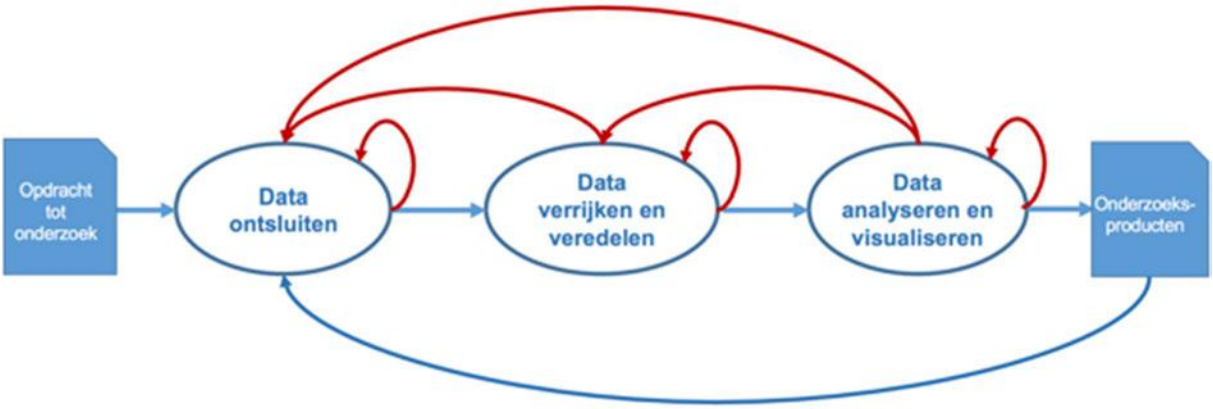
4 Technische werking en gebruik Raffinaderij

4.1 Inleiding

De Raffinaderij, en haar werkwijze, kan worden opgedeeld in drie fasen.

1. Het ontsluiten van gegevens;
2. Het verrijken van gegevens; en
3. Het analyseren en visualiseren van gegevens.

Hierbij moet worden opgemerkt dat deze verschillende fasen niet altijd helemaal na elkaar plaatsvinden. Tijdens de fase waarin informatie en gegevens geanalyseerd worden, kan blijken dat meer of andere gegevens noodzakelijk zijn en ontsloten moeten worden.



1. Ontsluiting van gegevens

In de eerste fase worden (politie)gegevens uit verschillende (politie)bronnen (zoals bijvoorbeeld SummIT) ontsloten ten behoeve van gebruik in de Raffinaderij. Dit betreft onder andere informatie verkregen uit bakens, processen-verbaal of IP-taps.

2. Verrijken van gegevens

Tijdens het opsporingsonderzoek gebruiken de rechercheurs en analisten de verschillende politiegegevens die in het onderzoek beschikbaar komen in samenhang met gegevens uit andere bronnen (bijvoorbeeld gegevens uit getuigenverhoren en processen-verbaal). Er ontstaat meer context doordat de beschikbare informatie uit het onderzoek verrijkt wordt met overige hiervoor beschikbare politiegegevens. Deze verrijking vindt deels geautomatiseerd plaats, bijvoorbeeld wanneer een geolocatie wordt toegevoegd aan een adres of wanneer een adres wordt toegevoegd aan een geolocatie. Zowel de waarde van de informatie, door een betere duiding, als de contouren van een onderzoek worden duidelijker.

3. Analyseren en visualiseren van gegevens

De laatste stap in het onderzoeksproces is het maken van een analyse nadat bepaalde (ongestructureerde) informatiecomponenten in een bepaalde context zijn geplaatst. Op basis van de beschikbare politiegegevens in het onderzoek wordt hierbij in feite een beeld of een reconstructie gevormd van hetgeen is gebeurd.

Analyseren van de beschikbare informatie maakt altijd onderdeel uit van de opsporingsprocessen. Dit kost echter veel tijd en menselijke capaciteit, zeker nu de hoeveelheid beschikbare data exponentieel toeneemt. De mogelijkheden om met geautomatiseerde gegevensverwerking en vergelijking dergelijke analyses uit te voeren, ondersteunt de rechercheur en de analist bij zijn of haar werkzaamheden en versterkt hem of haar in de mogelijkheden.
Met behulp van visualisatiemogelijkheden in de Raffinaderij wordt informatie op een toegankelijke manier gepresenteerd. Bovendien wordt de informatie beter doorzoekbaar en raadpleegbaar gemaakt voor de individuele medewerker. Visualisatie van gegevens is een belangrijk gereedschap in de strijd tegen '*information overload*', een stortvloed aan informatie.

Analyse en visualisatie van gegevens kunnen deels samenvallen wanneer verschillende bronnen in het kader van een opsporingsonderzoek worden ingezet. Bijvoorbeeld, wanneer bijzondere opsporingsmiddelen worden ingezet om de auto van een verdachte te volgen met behulp van een baken, de telefoon van een verdachte af te tappen (telefoontaps) én het internetverkeer van de verdachte te onderscheppen. In dat geval worden er drie verschillende technische acties uitgevoerd. De technische werking van deze acties is dusdanig verschillend dat de analist de verzamelde gegevens op drie verschillende manieren aangeleverd krijgt en veel tijd kwijt is om zijn of haar weg in deze data te vinden. Met behulp van visualisaties kan op eenvoudige wijze de relatie tussen verschillende entiteiten worden getoond (netwerkvisualisatie), kunnen gegevens op een tijdlijn worden geplaatst en kunnen gegevens op een kaart worden geplot. Op basis van deze visualisatie kan de data beter geanalyseerd worden door de analist en kan de opsporing efficiënter en sneller verlopen.

5.1.2.h

4.2 Gebruik ICT-middelen en oplossingen per fase

Voor de verschillende fasen in de Raffinaderij worden verschillende (software)componenten gebruikt. In de onderstaande paragrafen geven wij een overzicht van de gebruikte componenten.

4.2.1 Ontsluiten van (politie)bronnen ten behoeve van verwerking binnen de Raffinaderij

Gegevens worden door de politie verzameld in het kader van de uitvoering van de politietaak (handhaving, openbare orde en opsporing van strafbare feiten). Deze gegevens worden in diverse politiesystemen opgeslagen. Deze politiesystemen dienen als bronnen voor de Raffinaderij. Gegevens worden in de Raffinaderij beschikbaar gemaakt om daar relevante sporen en aanwijzingen in te vinden. Hiertoe wordt gebruik gemaakt van verschillende technische hulpmiddelen om de data te importeren zoals bijvoorbeeld RabbitMQ, Rsync, Vertica en Jenkins. Veelgebruikte bestandsformaten zijn JSON en CSV. Dit is geen uitputtend overzicht van hulpmiddelen om informatie digitaal te verzamelen. In de toekomst kunnen bovendien nieuwe of andere hulpmiddelen worden ingezet.

4.2.2 Verrijken, analyseren en visualiseren

In essentie is de Raffinaderij een omgeving waar beschikbare, ongelijksoortige informatiebronnen op eenvoudige wijze in combinatie met elkaar doorzoekbaar gemaakt kunnen worden. De basis *user interface*, data-integratie-/visualisatie techniek en logging-functionaliteiten worden op dit moment afgenomen van Palantir. De politie ontwikkelt daar weliswaar een eigen functionaliteit 'tegenaan', maar de gebruiker van de Raffinaderij merkt daar niets van en ziet slechts de Palantir-schil/front-end. Dit maakt Palantir één van de belangrijkste bouwstenen van de Raffinaderij.

4.3 Informatiebronnen

Kern van de Raffinaderij is het kunnen analyseren van grote hoeveelheden (ongestructureerde) data om daarmee betere opsporing mogelijk te maken en een tastbare bijdrage te kunnen leveren aan de veiligheid. Deze data zijn afkomstig uit verschillende bronnen binnen en buiten de politie. Zij worden ontsloten met behulp van de tools en technische toepassingen die zijn beschreven in paragraaf 4.2. Deze bronnen betreffen openbare bronnen, zoals publiekelijk beschikbare informatie op het internet, gesloten bronnen, zoals de data van bedrijven en publieke instanties, informatie en gegevens die zijn verkregen van een verdachte of van een persoon die mogelijk betrokken is bij het plegen van misdrijven in georganiseerd verband.

Wanneer de politie ten behoeve van opsporingsonderzoeken gegevens verzamelt uit de bovengenoemde bronnen, dan slaat zij deze op in haar eigen politiebronnen (zoals bijvoorbeeld SummIT). De Raffinaderij put uit deze politiebronnen.

Hieronder is een overzicht opgenomen van bronnen die momenteel in meer of mindere mate ontsloten (kunnen) worden in Raffinaderij. Afhankelijk van het (type) onderzoek in kwestie is bepaalde data wel of niet beschikbaar of voorhanden en ontstaan nieuwe behoeften.

1. Bronnen binnen de politie- en justitieketen

- ANPR van de politie / iTrechter
- Basis Voorziening Handhaving (BVH)
- Digitale Communicatie Sporen (DCS)
- Hansken (was Xiraf)
- Politie-antecedenten (voormalige HKS)
- Reliant / ORCA
- SummIT

2. Opsporingspartners

- FIU – verdachte transacties
- LIV – gestolen voertuigen

3. *Openbare bronnen (OSINT)*

- Primair sociale netwerksites, zoals Facebook, Twitter en Instagram

4. Bronnen uit de private sector (gesloten)

- ANPR van ARS / VIALIS
- (Gevorderde) gegevens uit specifieke opsporingsonderzoeken (opgeslagen in de politiebronnen onder 1)

6. Verdachten en overige betrokkenen

- Gegevens uit specifieke opsporingsonderzoeken (opgeslagen in de hierboven genoemde politiebronnen)

5.1.2.h

4.4 Gebruik van open source intelligence (OSINT)

In het kader van opsporingsonderzoeken wordt ook steeds meer *open source intelligence* (OSINT) ingezet. Doordat het gebruik van OSINT aan belang binnen de opsporing wint, en ook binnen Raffinaderij pilots worden gedraaid met tools waarmee openbare internetgegevens kunnen worden geanalyseerd, hebben wij ervoor gekozen om deze methode apart te bespreken.

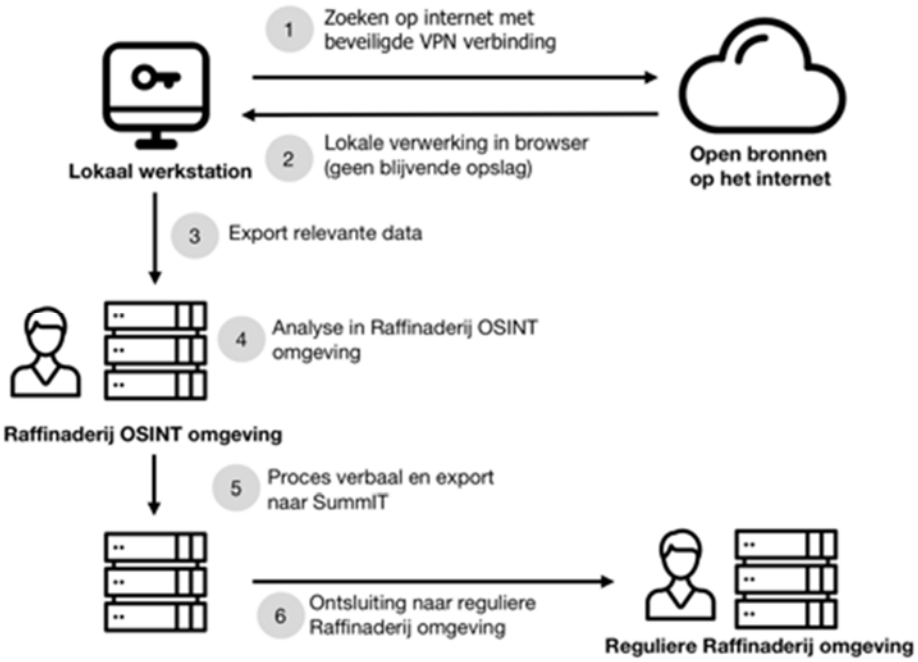
Vanuit deze PIA gezien is er ten aanzien van OSINT binnen Raffinaderij een tweedeling te maken:

a) OSINT als informatiebron voor de politie

OSINT data kan als gewone 'bron' van informatie voor de gehele opsporing worden gezien. Er bestaan verschillende OSINT-afdelingen binnen de politie die OSINT gebruiken in verschillende tools ten behoeve van de verschillende politietaken. Bij events kan bijvoorbeeld Twitter worden gemonitord ten behoeve van de handhaving. OSINT kan bovendien worden ingezet in opsporingsonderzoeken op het internet. Hier is de politie wel afhankelijk van de toestemming van de officier van justitie om OSINT in te mogen zetten. Wanneer bevindingen van belang zijn voor een onderzoek, zullen de bevindingen worden vastgelegd in SummIT. Via SummIT zijn de bevindingen vervolgens raadpleegbaar in de Raffinaderij.

b) OSINT in het kader van de Raffinaderij

Momenteel wordt in het kader van de Raffinaderij een proces en een omgeving ontwikkeld waarmee gebruikers op eenvoudige, veilige maar ook 'vluchtige' wijze bepaalde OSINT-data kunnen filteren en analyseren. Dit proces vindt niet in de omgeving van de Raffinaderij zelf plaats. Wanneer de eerste analyses van de OSINT-data zijn gemaakt, kunnen de gebruikers deze data vervolgens 'binnenhalen' en opslaan in de politieomgeving van de Raffinaderij voor verdere analyses (zie afbeelding).



In het kader van deze PIA zal met name aandacht worden besteed aan het gebruik van OSINT in het kader van de Raffinaderij zelf.

Bij Raffinaderij wordt voor CTER-onderzoeken door een aantal medewerkers gebruik gemaakt van de Raffinaderij OSINT omgeving. Deze omgeving is gescheiden van de reguliere Raffinaderij-omgeving.

Doel van de inzet van OSINT is om verbindingen te leggen, verbindingen te verklaren, verbanden in kaart te brengen en een algeheel beeld van een persoon of van een netwerk te krijgen. Bij de toepassing van OSINT wordt informatie die op het open internet beschikbaar is verzameld. Hierbij moet gedacht worden aan informatie die beschikbaar is op sociale media.

De informatie die veelal wordt ingewonnen met behulp van OSINT zijn metadata. Metadata betreft data over data. Metadata zijn, met andere woorden, gegevens die karakteristieken van bepaalde gegevens beschrijven. Op sociale netwerken wordt in kaart gebracht wat er op een profiel van een persoon te vinden is. Ook als een profiel niet openbaar is of wanneer de inhoud van berichten niet toegankelijk is, levert de algemene informatie, de vrienden of volgers die iemand heeft, met wie/wat/waar de persoon op de foto staat, wie foto's leuk vindt of wie er op foto's reageert, van welke groepen een persoon lid is, de politie al waardevolle inzichten op. De metadata stelt de politie in staat om bijvoorbeeld relaties

tussen personen te bepalen en om verbindingen te leggen tussen personen onderling, tussen personen en organisaties en tussen organisaties onderling. Hiertoe worden visualisatietools ingezet om verbindingen echt te visualiseren. Met behulp van OSINT kan de onderzoeker van de politie de sociale omgeving van een persoon opbouwen en in kaart brengen.

De politie gebruikt Raffinaderij OSINT om in het kader van een onderzoek personen of groepen te observeren en netwerken in kaart te brengen. Door een gericht onderzoek te doen naar een persoon danwel een criminele of terroristische groep of organisatie is het mogelijk om de gegevensverwerking en het aantal betrokken subjecten beperkt te houden. In Raffinaderij OSINT wordt er gericht onderzoek gedaan en worden relaties en verbanden die worden opgebouwd van tevoren en gedurende het onderzoek steeds doordacht. Met behulp van Raffinaderij OSINT wordt dus niet ongericht allerlei data die op het internet te vinden is naar binnen gehaald en *gecrawld* om vervolgens een verband in al die gegevens te vinden. Raffinaderij OSINT wordt ook expliciet niet gebruikt om met personen te corresponderen of te communiceren.

4.5 Mogelijke toekomstige inzet Raffinaderij: Big Data-analyses

De inzet van de Raffinaderijmethode kan op verschillende manieren worden uitgebreid. Bijvoorbeeld door de Raffinaderij in te zetten op meer toepassingsgebieden of thema's[10] of door de gebruikersgroep uit te breiden naar andere doelgroepen dan rechercheurs en analisten.

Een andere mogelijke uitbreiding ligt op het terrein van andere data-analyse methoden. In deze paragraaf bespreken wij de mogelijkheid om met behulp van de Raffinaderij meer geavanceerde Big Data-analyses (meer specifiek *data mining)*.[11] Met behulp van *machine learning* kunnen clusters en patronen in de data worden gevonden die zonder een dergelijke analyse onopgemerkt zouden blijven.[12] Deze inzichten kunnen vervolgens worden gebruikt om voor toekomstige data profielen te maken op basis waarvan geautomatiseerde besluitvorming kan plaatsvinden (*profiling*).

De Raffinaderij maakt momenteel geen gebruik van technieken als *data mining, profiling* en geautomatiseerde besluitvorming. Het is echter van belang om in deze PIA stil te staan

[10] Bijvoorbeeld voor onderzoeken naar mensenhandel, kinderporno of grootschalige fraudezaken.

[11] Rubinstein 2013, p. 74; Hildebrandt 2008, p. 18.

[12] Sloan & Warner 2013, pp. 19-20.

5.1.2.h

bij deze toepassing omdat de Raffinaderij dergelijke toepassingen wel zou kunnen faciliteren in de toekomst.

5 Juridisch kader privacy en bescherming persoonsgegevens algemeen

In specifieke situaties kan het verwerken van grote hoeveelheden data door de politie op gespannen voet komen te staan met de bescherming van de persoonlijke levenssfeer van personen. Het recht op bescherming van de persoonlijke levenssfeer wordt ook wel aangeduid als het recht op (informationele) privacy. De informationele privacy is een species van het recht op privacy en heeft betrekking op informatie over een bepaalde persoon.

In dit hoofdstuk wordt op hoofdlijnen het juridisch kader beschreven voor legitieme inbreuken op de persoonlijke levenssfeer en daaruit voortvloeiende verwerkingen van persoonsgegevens binnen de opsporing.

De basis van dit juridische kader is het grondrecht op bescherming van de persoonlijke levenssfeer van burgers. Dit recht op privacy is onder meer vastgelegd in het Handvest van Grondrechten van de Europese Unie (Handvest), artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) en artikel 10 van de Nederlandse Grondwet maar ook in artikel 12 van de Universele Verklaring van de Rechten van de Mens en in artikel 17 van het Verdrag inzake Burgerrechten en Politieke Rechten.

In de Raffinaderij heeft het grondrecht op privacy grofweg twee dimensies:

- Ten behoeve van de opsporing worden gegevens *verzameld*. Hiervoor moet een rechtmatige grondslag zijn op basis van de Wet politiegegevens en de gegevens moeten in lijn met strafvorderlijke regels worden verzameld.
- Vervolgens worden de gegevens verder *verwerkt* van persoonsgegevens in het kader van een strafrechtelijk onderzoek. Op deze verdere verwerking is de Wet politiegegevens van toepassing.

Bovendien speelt het maatschappelijk belang van transparantie van overheidshandelen mee, zoals onder meer is neergelegd in de Wet Openbaarheid Bestuur.

5.1 Het grondrecht op privacy

Het grondrecht op privacy heeft zich ontwikkeld tot een positief en een negatief recht. Het recht op privacy als een negatief recht betekent dat de staat zich zo veel mogelijk dient te onthouden van inmenging in het privéleven van haar burgers.[13] Het positieve recht op privacy vloeit voort uit enkele van de eerdere genoemde internationale verdragen en wetten. Uit deze bepalingen vloeit de positieve verplichting van staten voort om de negatieve privacy van burgers te waarborgen. Dit betekent met andere woorden dat de staat het recht op privacy van de burger wettelijk moet beschermen en moet garanderen dat de burger dit recht effectief kan uitoefenen.[14] Om te kunnen waarborgen dat een individu zijn recht op privacy effectief kan uitoefenen, kan een staat verplicht worden om actief op te treden. In dat geval kan de staat verplicht worden om (wettelijke) maatregelen te treffen die het individu beschermen tegen inbreuken. Daarnaast kan de staat effectieve middelen ter beschikking stellen aan het individu zodat deze zich tegen inbreuken kan beschermen.[15]

Het recht op bescherming van de persoonlijke levenssfeer is neergelegd in artikel 8 EVRM. Uit het tweede lid van dit artikel blijkt dat het recht op privacy geen absoluut recht is: er mogen inbreuken op dit recht worden gemaakt wanneer dit bij wet is geregeld en het noodzakelijk is in een democratische samenleving ten behoeve van gerechtvaardigde doelen zoals de opsporing van strafbare feiten.

Het eerste element dat relevant is voor de opsporing is dat de inbreuk noodzakelijk moet zijn. Het betreft hier proportionaliteits- en subsidiariteitstoets. De wet die de inbreuk legitimeert, moet vervolgens voldoen aan zekere kwaliteitsvereisten. Zo moet de wet- en regelgeving voor burgers vrij toegankelijk zijn.[16] Ook moet de inbreuk voldoende voorzienbaar zijn op basis van de wet.[17] De wet moet daarom voldoende specifiek geformuleerd zijn om het individu de mogelijkheid te geven om zijn of haar gedrag hieraan

---

[13] Helberger 2013, p. 152.

[14] Van der Helm 2009, p. 19.

[15] Van der Helm 2009, p. 19.

[16] EHRM 26 april 1979, A 30 (*Sunday Times),* r.o. 30. Net als in de hieronder genoemde uitspraak *Handyside* is deze uitspraak gedaan in de context van het recht op vrijheid van meningsuiting. De doctrine is echter eveneens van toepassing op het recht op privacy.

[17] EHRM 7 december 1976, nr. 5493/72 (*Handyside t. Verenigd Koninkrijk*). Deze uitspraak is gedaan in de context van het recht op vrijheid van meningsuiting maar de doctrine is eveneens van toepassing op het recht op privacy.

aan te passen en om willekeur van de overheid te voorkomen.[18] Deze eis van voorzienbaarheid is met name van belang in de context van de technologie de veranderende technologie. De inbreuken op de persoonlijke levenssfeer kunnen groter worden doordat technologie steeds geavanceerder en indringender wordt. Doordat de technologie zich continu ontwikkelt en verandert, is het des te belangrijker dat er een nauwkeurige omschrijving en afbakening van de toepassingen van bevoegdheden bestaat.[19] Uit het bovenstaande volgt dat een belangenafweging moet worden gemaakt. Daarbij moet bijvoorbeeld het opsporingsbelang van de politie worden afgewogen tegen het belang van de burger.

In de Nederlandse Grondwet is het recht op privacy verankerd in artikel 10. Dit artikel vereist dat de persoonlijke levenssfeer van burger geëerbiedigd en beschermd wordt. In de artikelen 11 tot en met 13 van de Grondwet zijn specifieke privacy-rechten opgenomen, namelijk het recht op de onaantastbaarheid van het lichaam, het recht op privésfeer van een woning en het briefgeheim. Voor wat betreft privacy-schendingen in het kader van de strafrechtelijke handhaving van de rechtsorde heeft de Hoge Raad in het arrest *Zwolsman* bepaald dat een specifieke wettelijke grondslag nodig is wanneer meer dan geringe inbreuken op de persoonlijke levenssfeer plaatsvinden.[20] Dit betekent dat artikel 3 Politiewet, dat de algemene taakstelling van de politie bevat, niet als basis kan dienen voor de toepassing van opsporingsmethoden die een meer dan geringe inbreuk op de persoonlijke levenssfeer tot gevolg hebben.

Het doel van de bescherming van de privacy van burgers in de context van de verzameling en verwerking van gegevens door politie is om de machtsbalans tussen burgers en de overheid te bewaken. Net als andere grondrechten, zoals de vrijheid van meningsuiting of het recht op gelijke behandeling, vloeit het recht op privacy voort uit de behoefte om het belang van de burger te beschermen tegen machtsmisbruik en willekeur. Het belang van de burger om zijn of haar recht op privacy beschermd te zien, dient te worden afgewogen tegen het maatschappelijke belang van de openbare orde en veiligheid.

---

[18] EHRM 13 november 2012, nr. 24029/07 (*MM t. Verenigd Koninkrijk*) en EHRM 24 april 1990, nr. 11105/84).

[19] Zie onder andere: EHRM 24 april 1990, A 176 A (*Kruslin t. Frankrijk*), EHRM 24 april 1990, A 176 B *(Hüvig vs Frankrijk)*, EHRM 16 februari 2000, nr. 27798/95 (*Amman t. Zwitserland)* en EHRM 21 juni 2011, nr. 30194/09 (*Shimovolos t. Rusland*).

[20] Hoge Raad 19 december 1995, *NJ* 1996.

5.1.2.h

5.1.1 Het recht op informationele privacy

Het recht op informationele privacy is een species van het recht op privacy. Het kan gedefinieerd worden als "*the claim of individuals (..) to determine for themselves when, how and to what extend information about them is communicated to others*".[21] Privacy omvat in deze lezing het recht om bepaalde feiten die betrekking hebben op het persoonlijke leven van een individu geheim te houden. Het is aan het individu om zelf in alle vrijheid te beslissen welke informatie hij over zichzelf met anderen wil delen.[22] Het individu heeft met andere woorden medeweten en zeggenschap over de verzamelde, opgeslagen en (eventueel) aan derden geopenbaarde informatie die tot hem of haar herleidbaar is.

Het recht op informationele privacy wordt voor wat betreft het gebruik van persoonsgegevens binnen de politie gewaarborgd door de Wet politiegegevens.

5.2 Verzamelen versus verwerken van persoonsgegevens

Voor de uitvoering van haar taken verwerkt de politie persoonsgegevens (politiegegevens). Het juridisch kader voor de verzameling en het verder verwerken van deze gegevens wordt gevormd door de Politiewet, het Wetboek van Strafvordering en de Wet politiegegevens. Grofweg valt een onderscheid te maken tussen het kader voor het *verzamelen* van gegevens (artikel 3 Politiewet en het Wetboek van Strafvordering) en het binnen de politie *verder verwerken* van politiegegevens (Wet politiegegevens).

In de context van het verzamelen van gegevens is de aard van het onderzoek en de 'inbreukmakendheid' van de daarbinnen gebruikte bevoegdheden het primaire aanknopingspunt. Er wordt daarbij onderscheid gemaakt tussen:

1. Onderzoeken waarbij voor het vergaren van gegevens geen gebruik wordt gemaakt van ingrijpende middelen (inclusief het verkennend onderzoek) en;
2. 'Titel IVA' en 'Titel V' onderzoeken waarbij zwaardere, bijzondere opsporingsbevoegdheden mogen worden gebruikt.[23] 'Titel IVA' onderzoeken zijn gericht op een concrete verdachte, de 'Titel V' onderzoeken op het verkrijgen van inzicht in georganiseerde misdaad die een ernstige inbreuk op de rechtsorde oplevert (Titel V), dan wel terrorisme (Titel VB).

---

[21] Westin 1967, p. 7. Het concept informationele privacy wordt aan Alan Westin toegeschreven, hoewel Westin deze term zelf niet gebruikt.

[22] Borking 2010, p. 22.

[23] Beijer 2004.

De juridische context van het verzamelen van gegevens sluit maar in beperkte mate aan op het onderscheid dat wordt gehanteerd bij het verwerken van persoonsgegevens binnen de politie. In de Wet politiegegevens wordt een onderscheid gemaakt tussen het verwerken van persoonsgegevens ter uitvoering van de dagelijkse politietaak (artikel 8 Wpg) en de gerichte verwerking van persoonsgegevens (artikel 9 en 10 Wpg). Bij de gerichte verwerking gaat het om het onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (artikel 9 Wpg) en inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (artikel 10 Wpg). Bij deze laatste categorie moet allereerst gedacht worden aan het werk van de Teams Criminele Inlichtingen, maar ook aan de 'thematische' verwerkingen die plaatsvinden binnen de politie.[24]

In de volgende twee hoofdstukken gaan wij nader in op de juridische kaders voor het verzamelen en verwerken van politiegegevens.

[24] Volgens *Kamerstukken II* 2005-2006, 30 327, nr. 3, p. 12: "Tevens is gerichte gegevensverzameling in deze zin aan de orde bij de opbouw van een informatiepositie over ernstige bedreigingen van de rechtsorde, zoals terroristische activiteiten, die niet vallen binnen het werkgebied van en de criteria die gelden voor de criminele inlichtingen eenheid (CIE) of de regionale inlichtingen dienst (RID), maar die – omdat zij een zwaarwegend maatschappelijk probleem vormen – wel vergen dat gegevens kunnen worden verwerkt over personen die betrokken kunnen zijn bij die handelingen die zouden kunnen wijzen op activiteiten die een ernstige bedreiging van de rechtsorde vormen."

6 Juridisch kader verzamelen (politie)gegevens

In dit hoofdstuk wordt het juridisch kader voor de *verzameling* van politiegegevens door de politie toegepast op de werkwijze van de Raffinaderij. Politiegegevens mogen alleen worden verzameld voor gerechtvaardigde doeleinden. De verzameldoelen worden gespecificeerd in de artikelen 8 tot en met 13 van de Wpg. In zijn algemeenheid kunnen we daarbij stellen dat het Wetboek van Strafvordering zich primair richt op de rechtmatige verkrijging van politiegegevens voor zover het gaat om politiegegevens die in het kader van een strafrechtelijk onderzoek zijn verzamend. De Wet politiegegevens ziet vervolgens toe op de verdere *verwerking* van deze gegevens (zie hoofdstuk 7).[25]

Alvorens wij dit wettelijke kader kunnen toepassen op de Raffinaderij dient duidelijk te zijn in welke context en in welk soort onderzoeken de Raffinaderij wordt ingezet. Hiervoor is het allereerst noodzakelijk om te bepalen op basis van welke *grondslag* de Raffinaderij wordt toegepast.

6.1 Grondslagen verzameling (politie)gegevens

De politie is belast met de handhaving van de rechtsorde en het verlenen van hulp aan hen die deze behoeven. De politie voert deze taak uit onder gezag van de officier van justitie. Deze taak omvat het opsporen van strafbare feiten (artikel 3 Politiewet juncto artikel 141 Wetboek van Strafvordering). Om haar politietaak goed uit te kunnen voeren, heeft de politie voldoende informatie nodig. Dit betekent niet dat er ongelimiteerd gegevens mogen worden verwerkt, er dient aan de eisen van proportionaliteit en subsidiariteit te worden voldaan.[26]

Wanneer de politie gegevens verzamelt voor de uitvoering van haar taken, dan moet hiervoor een wettelijke basis zijn. Dit omdat het verzamelen en opslaan van persoonsgegevens van personen een inbreuk op de persoonlijke levenssfeer is.[27] De wettelijke basis voor het verzamelen en verder verwerken van persoonsgegevens voor opsporingsdoeleinden kan primair worden gevonden in de artikelen 8, 9 en 10 van de Wet Politiegegevens juncto artikel 3 Politiewet. Daar waar persoonsgegevens worden verzameld

[25] Dit neemt niet weg dat op grond van artikel 126dd Sv voor sommige bijzondere opsporingsmiddelen een speciale regeling bestaat waarbij het Wetboek van Strafvordering een lex specialis is ten opzichte van de Wpg.

[26] *Kamerstukken II* 1996-1997, 25 403, nr. 3, p. 9.

[27] EHRM 6 juni 2006, nr. 62332/00 (*Segerstedt-Wiberg en anderen t. Zweden*).

met behulp van opsporingsbevoegdheden die een meer dan geringe inbreuk op de persoonlijke levenssfeer maken is echter een specifieke(re) wettelijke basis nodig. Deze worden gevonden in de regelingen omtrent de dwangmiddelen en de bijzondere opsporingsbevoegdheden.

6.1.1 De opsporing van strafbare feiten

De wettelijke basis voor het maken van meer dan geringe inbreuken op de persoonlijke levenssfeer van de verdachte zijn te vinden in het Wetboek van Strafvordering. Het strafvorderlijk juridisch kader is een belangrijk fundament om de privacy impact van de Raffinaderij te beoordelen. Immers, een groot deel van de persoonsgegevens die in het kader van de Raffinaderij worden verwerkt, moeten conform het strafvorderlijk kader zijn verzameld. Dit neemt overigens niet weg dat de gegevens ook via een ander kader verzameld kunnen worden.

Het proces van informatiegaring is een belangrijk onderdeel van het opsporingsonderzoek zoals bedoeld in artikel 132a Sv. De basisactiviteit van dit proces is het opbouwen en in stand houden van een goede informatiepositie, in het belang van de strafrechtelijke handhaving van de rechtsorde. Daarnaast kan een aantal andere typen van onderzoek worden onderscheiden. De Memorie van Toelichting bij de Wet Bijzondere Opsporingsbevoegdheden (Wet BOB) maakt daarbij onderscheid tussen:

1. Het opbouwen en in stand houden van een zekere informatiepositie;[28] door
   a. Het opslaan, bewerken, gebruiken en analyseren van gegevens, of
   b. Het vergaren van gegevens door de toepassing van niet-ingrijpende middelen;[29]
2. Verkennend onderzoek; en
3. Opsporingsonderzoek (zoals bedoeld in Titel IV, IVA, V en VB Sv).

Deze drie typen onderzoek kunnen gelijktijdig plaatsvinden.[30]

De hierboven genoemde soorten onderzoeken kunnen worden aangemerkt als grondslagen die van belang zijn in het kader van de Raffinaderij. Het betreft het verkennend

---

[28] De Memorie van Toelichting bij de Wet BOB voegt hieraan toe dat het opbouwen en in stand houden van een zekere informatiepositie personen betreft die geregistreerd staan in het register zware criminaliteit, volgens *Kamerstukken II* 1996-1997, 25 403, nr. 3, p. 9.

[29] Onder niet-ingrijpende middelen wordt verstaan het ogen en oren openhouden. Zulke niet-ingrijpende middelen worden vaak niet in de wet geregeld omdat zij geen inbreuk op de privacy maken, volgens *Kamerstukken II* 1996-1997, 25 403, nr. 3, p. 8.

[30] *Kamerstukken II* 1996-1997, 25 403, nr. 3, p. 9.

onderzoek ter voorbereiding van de opsporing (Titel VE Sv), het opsporingsonderzoek naar aanleiding van een vermoeden van het plegen van een strafbaar feit (klassiek opsporingsonderzoek en 'Titel IVA' onderzoek), het opsporingsonderzoek naar ernstige misdrijven, beraamd of gepleegd in georganiseerd verband (Titel V Sv) en het opsporingsonderzoek gericht tegen terroristische misdrijven (Titel VB Sv). Deze grondslagen zullen hieronder nader worden toegelicht.

6.1.1.1 Het opbouwen en in stand houden van een zekere informatiepositie

In de Memorie van Toelichting bij de Wet BOB geeft de wetgever aan dat het opsporingsonderzoek als bedoeld in artikel 132a Sv gezien kan worden als onderdeel van een meeromvattend proces van informatiegaring. De basisactiviteit van dit proces van informatiegaring is het opbouwen en in stand houden van een goede informatiepositie.[31] Hieruit kan worden afgeleid dat het verzamelen en verwerken van gegevens ten behoeve van deze informatiepositie (*intelligence*) formeel geen onderdeel uitmaakt van het opsporingsonderzoek, maar daar wel onlosmakelijk mee is verbonden. We kunnen stellen dat het *intelligence* werk van de politie het voorportaal is van opsporing. De grondslag voor het intelligence werk van de politie ligt in artikel 10 Wpg. De Wpg geeft geen bevoegdheden tot het vergaren van gegevens aan de politie, wel kunnen gegevens verkregen uit opsporingsonderzoek, verkennend onderzoek, of de toepassing van niet-ingrijpende middelen worden gebruikt voor de *intelligence* taak.

6.1.1.2 Verkennend onderzoek (Titel VE Sv)

Het verkennend onderzoek is bedoeld ter voorbereiding op de opsporing. De officier van justitie kan bevelen dat opsporingsambtenaren een onderzoek instellen wanneer aanwijzingen bestaan dat binnen een groep personen misdrijven worden beraamd of gepleegd die gezien hun aard of samenhang met andere misdrijven een ernstige inbreuk op de rechtsorde opleveren. Doel van dit onderzoek is de voorbereiding van opsporing. De regels omtrent het verkennend onderzoek zijn neergelegd in Titel VE, en meer specifiek in artikel 126gg Sv.[32]

Het verkennend onderzoek maakt dus geen onderdeel uit van het opsporingsonderzoek, maar gaat aan het opsporingsonderzoek vooraf en dient aldus ter voorbereiding op het opsporingsonderzoek. Het verkennend onderzoek valt onder de strafrechtelijke handhaving

---

[31] *Kamerstukken II* 1996–1997, 25 403, nr. 3, p. 8.

[32] Het betreft hier misdrijven zoals omschreven in artikel 67 lid 1 Sv.

van de rechtsorde. Het is echter niet toegestaan opsporingsbevoegdheden in te zetten om gegevens te verzamelen in het kader van een verkennend onderzoek.

Er lijkt echter wel ruimte te bestaan om politiegegevens die in het kader van andere opsporingsonderzoeken zijn verzameld te gebruiken voor een verkennend onderzoek. Artikel 126dd lid 1 Sv spreekt namelijk van de mogelijkheid om politiegegevens te gebruiken voor een ander 'strafrechtelijk onderzoek' dan waartoe de bevoegdheid tot vergaring van gegevens voor was uitgeoefend. Er wordt dus niet gesproken van een 'opsporingsonderzoek'. Deze bepaling is in de literatuur geïnterpreteerd als een mogelijkheid om gegevens uit andere onderzoeken in het kader van een verkennend onderzoek te gebruiken.[33]

Als deze interpretatie wordt gevolgd, dient ervoor te worden gewaakt dat niet op grote schaal politiegegevens, die zijn verkregen met behulp van bijzondere opsporingsbevoegdheden, alsnog worden verstrekt aan en verder worden verwerkt in een verkennend onderzoek waar deze bijzondere opsporingsbevoegdheden niet mogen worden toegepast. Dit heeft er mee te maken dat artikel 126dd Sv uitdrukkelijk niet bedoeld is om de strikte regels omtrent de inzet van bijzondere opsporingsbevoegdheden en de verkrijging van politiegegevens in andere onderzoeken te omzeilen. Dit artikel laat, met andere woorden, geen ruimte voor standaard bulkverstrekkingen. Naast het verstrekken van BOB-gegevens in het kader van een opsporingsonderzoek kunnen deze gegevens ook worden verstrekt ten behoeve van de *intelligence* taak van de politie (artikel 10 lid 1 onder b van de Wpg jo artikel 126dd lid 1 onder b Sv) hiervoor geldt eenzelfde redenering als voor het gebruik binnen (verkennende) onderzoeken. Doorgifte van politiegegevens in het kader van artikel 126dd Sv is daarom ook alleen mogelijk wanneer de officier van justitie dit voldoende onderbouwt en motiveert.

Naast het algemene artikel 126gg Sv bestaan er specifieke bepalingen ten aanzien van het verkennend onderzoek bij terroristische misdrijven. Ten eerste biedt artikel 126hh Sv de Officier van Justitie de mogelijkheid om bij een persoon (of een publieke en particuliere instanties), waarvan redelijkerwijs wordt vermoed dat hij of zij toegang heeft tot een gegevensbestand dat in het kader van de bestrijding van terrorisme van belang is, het bestand te vorderen. De Officier van Justitie kan dergelijke gegevensbestanden slechts vorderen na machtiging door de rechter-commissaris. De toepassing van de bevoegdheid

[33] Blom 2007.

is gebonden aan nauwe voorwaarden en is omgeven met strikte waarborgen voor een zorgvuldige omgang met persoonsgegevens.[34] Daarnaast kan de Officier van Justitie op grond van artikel 126ii Sv bepaalde identificerende gegevens van een persoon vorderen, onder meer bij de aanbieders van een openbaar telecommunicatienetwerk (lid 2).

6.1.1.3 Opsporingsonderzoek naar aanleiding van een vermoeden van het plegen van strafbaar feit

In het kader van een opsporingsonderzoek dat is gestart naar aanleiding van het vermoeden van het plegen van een strafbaar feit kunnen opsporingsbevoegdheden worden ingezet en kan informatie worden verzameld. Indien gebruik gemaakt wordt van bijzondere opsporingsbevoegdheden is er sprake van een 'Titel IVA' onderzoek.

6.1.1.4 Onderzoek naar ernstige misdrijven beraamd of gepleegd in georganiseerd verband (Titel V Sv)

Met inwerkingtreding van de Wet Bijzondere opsporingsbevoegdheden (Wet BOB) is een vernieuwd en ruimer opsporingsbegrip geformuleerd. Bovendien is de strafvordering niet meer gebonden aan de materiële eisen van de verdenking zoals bedoeld in artikel 27 Sv.[35] Dit betekent dat gegevens verzameld mogen worden met behulp van de toepassing van de bijzondere opsporingsbevoegdheden, zoals bedoeld in Titel V Sv, ten behoeve van een onderzoek waarbij een redelijk vermoeden bestaat dat in georganiseerd verband ernstige misdrijven worden beraamd of gepleegd.

6.1.1.5 Opsporing van terroristische misdrijven (Titel VB Sv)

Het doel van het opsporingsonderzoek naar terroristische misdrijven is om in een zo vroeg mogelijk stadium op te treden ter voorkoming van terroristische aanslagen. Daarom is het sinds de introductie van de Wet ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven voor de inzet van bijzondere opsporingsbevoegdheden bij terrorisme niet nodig om een redelijk vermoeden van een strafbaar feit te hebben. Het bestaan van een aanwijzing voor dergelijke misdrijven is

---

[34] De persoonlijke levenssfeer van de betroffen personen dient zo veel mogelijk te worden gewaarborgd (lid 3). Wanneer deze bewerking is voltooid, ziet de officier van justitie erop toe dat uitsluitend de gegevens die het resultaat zijn van de bewerking en van betekenis zijn voor het onderzoek voor het onderzoek verder worden verwerkt (lid 5 sub a). Deze gegevens mogen alleen worden verwerkt voor de opsporing van terroristische misdrijven (lid 6). Resultaten die niet van betekenis zijn voor het onderzoek, moeten worden vernietigd (lid 5 sub b).

[35] Cleiren 2000.

voldoende.[36] De Wet ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven is neergelegd in Titel VB Sv. Titel VB Sv maakt het dus mogelijk om bij aanwijzingen van terroristische misdrijven bijzondere opsporingsbevoegdheden in te zetten. Zo is stelselmatige observatie, stelselmatige inwinning van informatie, opnemen en onderzoek van communicatie en het vorderen van gegevens onder omstandigheden mogelijk.

6.2 Bevoegdheden verzamelen gegevens (gecategoriseerd naar bron)

Om gegevens binnen de Raffinaderij te mogen verwerken, moeten zij eerst rechtmatig zijn verzameld. De grondslagen voor het verzamelen van gegevens worden gegeven in de Wpg. Welke gegevens daadwerkelijk verzameld mogen worden onder welke omstandigheden wordt grotendeels bepaald door het Wetboek van Strafvordering, omdat dit wetboek de regelingen bevat voor het verzamelen van gegevens waarbij een meer dan geringe inbreuk op de persoonlijke levenssfeer wordt gemaakt.

Om te bepalen of gegevens rechtmatig verzameld zijn, is het onderscheid dat is gemaakt naar de verschillende typen strafrechtelijke onderzoeken van belang. Het is dus van belang om na te gaan of een onderzoek een 'Titel IVA' 'Titel V' of een verkennend onderzoek betreft. Dit onderscheid bepaalt ook welke (bijzondere) opsporingsbevoegdheden mogen worden toegepast in de verschillende onderzoeken.

Met betrekking tot het verzamelen van gegevens voor een opsporingsonderzoek of een verkennend onderzoek bestaan verschillende soorten opsporingsbevoegdheden. Met behulp van deze bevoegdheden kan de politiegegevens verkrijgen uit verschillende bronnen. Deze bevoegdheden tot het verzamelen van gegevens categoriseren wij grofweg naar de bron waarop zij betrekking hebben.

6.2.1 Openbare bronnen

Het raadplegen en bekijken van openbare bronnen op incidentele basis vormt slechts een geringe inbreuk op de persoonlijke levenssfeer. Als zodanig kan volstaan worden met een relatief algemene wettelijke basis (artikel 3 Politiewet) om deze inbreuk te legitimeren. Wanneer er sprake is van systematische analyse en vastlegging van gegevens dan is sprake

[36] *Kamerstukken II* 2004/05, 30 164, nr. 3, p. 9.

van een meer dan geringe inbreuk op de persoonlijke levenssfeer en is een specifiekere wettelijke basis noodzakelijk.[37]

Of er bij open bronnen onderzoek sprake is van stelselmatigheid is, wordt beoordeeld aan de hand van elementen als duur, intensiteit en frequentie.[38] Bij het gebruik van openbare bronnen in de opsporing zal eerder sprake zijn van stelselmatigheid wanneer de observatie geautomatiseerd is. Het is een verschil of sporadisch een profiel wordt bekeken, of grote hoeveelheden gegevens (bijvoorbeeld een hele Twitter-tijdlijn) worden binnengehaald ten behoeve van analyse in de Raffinaderij.

Voor wat betreft het gebruik van openbare bronnen in het kader van de opsporing van strafbare feiten (al dan niet met behulp van de Raffinaderij) zal, zeker wanneer de gegevens worden opgeslagen, doorgaans sprake zijn van een meer dan geringe inbreuk op de persoonlijke levenssfeer die een meer specifieke wettelijke basis behoeft dan artikel 3 Politiewet. Een specifieke wettelijke basis voor open bronnen onderzoek ontbreekt momenteel echter nog in Nederland. Om inbreuken te legitimeren, wordt momenteel aangesloten bij de regeling van artikel 126g Sv. Wanneer in het kader van de uitvoer van de politietaak stelselmatig openbare bronnen worden geraadpleegd, dan wordt een opsporingsonderzoek gestart waarbinnen de toepassing van deze bevoegdheid mogelijk is. Deze regeling is echter geschreven voor de fysieke wereld.

Om deze reden is in het consultatievoorstel voor de vaststellingswet voor het Boek 2 van het nieuwe Wetboek van Strafvordering [39] een specifieke opsporingsbevoegdheid opgenomen voor het open bronnen onderzoek: de stelselmatige vastlegging van persoonsgegevens uit open bronnen (8.2.4). Deze bepaling luidt als volgt:

1. *In geval van verdenking van een misdrijf waarop naar de wettelijke omschrijving gevangenisstraf van een jaar of meer is gesteld, kan de officier van justitie bevelen*

[37] Zie in dit kader onder meer EHRM 6 juni 2006, nr. 62332/00 (*Segerstedt-Wiberg en anderen t. Zweden*), par. 72 en EHRM 4 mei 2000, nr. 28341/95 (*Rotaru t. Roemenië*).

[38] Zie onder andere de volgende uitspraken van de Hoge Raad 21 maart 2000, 112845, ECLI:NL:HR:2000:AA5254, ECLI:NL:HR:AL8449, HR 1 juli 2014, 13/04699, ECLI:NL:HR:2014:1569.

[39] Ministerie van Justitie, Memorie van Toelichting: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek, raadpleegbaar via: https://www.rijksoverheid.nl/documenten/kamerstukken/2017/02/07/memorie-van-toelichting-vaststellingswet-boek-2-van-het-nieuwe-wetboek-van-strafvordering-het-opsporingsonderzoek.

dat een opsporingsambtenaar stelselmatig, met een technisch hulpmiddel, persoonsgegevens uit open bronnen vastlegt.

2. *Het bevel tot stelselmatige vastlegging van persoonsgegevens uit open bronnen wordt gegeven voor een periode van ten hoogste drie maanden. De geldigheidsduur kan telkens voor een periode van ten hoogste drie maanden worden verlengd.*
3. *Bij of krachtens algemene maatregel van bestuur worden regels gegeven omtrent:*
    a. *de autorisatie van de opsporingsambtenaren die kunnen worden belast met de uitvoering van het bevel, bedoeld in het eerste lid;*
    b. *de geautomatiseerde vastlegging van gegevens over de uitvoering van het bevel, bedoeld in het eerste lid.*

De wetgever onderkent in het wetsvoorstel dat door de inzet van dergelijke technieken sneller dan voorheen een min of meer volledig beeld kan worden verkregen van bepaalde aspecten van de persoonlijke levenssfeer van een betrokkene. In deze open bronnen staan niet alleen feitelijke gegevens maar deze bronnen bevatten ook informatie die betrekking heeft op bijvoorbeeld het gedrag, gevoelens, meningen en sociale contacten van een persoon. Daarbij stelt de wetgever dat de inbreuk op de persoonlijke levenssfeer beperkt is bij niet-stelselmatige vastlegging van gegevens. Dit wordt anders wanneer het onderzoek in open bronnen zo intensief en diepgaand is dat een min of meer volledig beeld van bepaalde aspecten van het persoonlijke leven van een persoon ontstaat. In dat geval is een uitdrukkelijke wettelijke grondslag vereist.

Ten aanzien van de stelselmatige observatie overweegt de wetgever dat:

> *"stelselmatige observatie ziet op het stelselmatig volgen van een persoon of stelselmatig diens aanwezigheid of gedrag waarnemen. Hoewel open bronnen indicaties kunnen bevatten voor de aanwezigheid of het gedrag van een persoon (bijvoorbeeld met foto's of berichten op sociale media) neemt de opsporingsambtenaar niet zelf het gedrag of de aanwezigheid van de persoon waar."*

Daarmee heeft het volgen of waarnemen een "real-time" element in zich. De wetgever vervolgt dat:

"de aanwezigheid, het gedrag of de bewegingen van de persoon in geval van stelselmatige observatie "realtime" [worden] gevolgd of waargenomen en daarmee feitelijk vastgesteld, al dan niet met behulp van een technisch hulpmiddel."[40]

Voorts is in het wetsvoorstel de mogelijkheid opgenomen om stelselmatig gegevens vast te leggen door middel van openbare bronnen onderzoek binnen de context van een verkennend onderzoek (9.1). Hiermee wordt de onduidelijkheid die nu bestaat bij het gebruik van open bronnen binnen de Raffinaderij (en het politiewerk in den brede) weggenomen.

6.2.2 Verzameling gegevens private sector (gesloten bronnen)

Gegevens die bij een derde zijn opgeslagen en relevant zijn in het kader van een strafrechtelijk onderzoek kunnen door de politie worden gevorderd. Het staat de politie niet vrij om de gegevens op te vragen, er moet een vordering worden overlegd. Wel kan een bedrijf of overheid op grond van artikel 9 juncto artikel 43 Wbp zelfstandig besluiten om de gegevens vrijwillig te verstrekken. Hierbij is wel van belang dat de verstrekking daadwerkelijk vrijwillig is en dat er geen (indirecte) druk is op de private actor. Voor de private actor geldt dat artikel 43 Wbp een uitzonderingsgrond is om het doelbindingsprincipe te doorbreken. Op het moment dat er een meer permanente samenwerking ontstaat (bijvoorbeeld in de vorm van een publiek-private samenwerking) dan moet gekeken worden of er een rechtsgrondslag beschikbaar is voor deze uitwisseling (bijvoorbeeld artikel 8 sub f Wbp / artikel 6 lid 1 sub f AVG).

6.2.3 Verzameling van gegevens bij andere opsporingsdiensten en toezichthouders

De politie kan gegevens verstrekt krijgen van andere bijzondere opsporingsdiensten maar ook van bijvoorbeeld toezichthouders. In het kader van de Raffinaderij worden gegevens gebruikt vanuit bijvoorbeeld de FIU. De specifieke verstrekkingsgronden voor deze instanties hebben hun basis in de materiewetten op basis waarvan ze zijn opgericht. Het voert te ver om al deze gronden te bespreken. In het kader van de Raffinaderij is met name relevant dat gegevens die rechtstreeks van derden worden verkregen, danwel vanuit samenwerkingsverbanden, rechtmatig verzameld en gedeeld zijn. Verwerkingen en verstrekkingen zonder grondslag kunnen ook een negatieve impact hebben op de Raffinaderij.

[40] Ministerie van Justitie, Memorie van Toelichting: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek, pp. 58-60.

5.1.2.h

6.2.4 Verzameling van gegevens bij de verdachte en/of diens omgeving

Diverse bevoegdheden uit het Wetboek van Strafvordering zijn direct gericht op het verzamelen van gegevens bij de verdachte welke een meer dan gering inbreuk maken op de persoonlijke levenssfeer. Hieronder worden enkele veelgebruikte bevoegdheden beschreven.

6.2.4.1 Inbeslagname (Titel IV, derde afdeling) en doorzoeking ter vastlegging van gegevens (Titel IV, zevende afdeling)

Op grond van artikel 94 Sv kunnen gegevensdragers (smartphones, computers, USB sticks et cetera) in beslag worden genomen en kan daaraan onderzoek worden gedaan. Momenteel worden deze voorwerpen ge-imaged en ingelezen, verwerkt, opgeslagen in Hansken. Hansken is primair de 'bron' van data. Rechercheurs kunnen (in Hansken) zoeken naar informatie uit hun eigen onderzoek. De Raffinaderij heeft een koppeling met Hansken waardoor ook in Raffinaderij gewerkt kan worden met (een deel van) de data. Met betrekking tot de inbeslagname moet rekening worden gehouden met een recente uitspraak van de Hoge Raad waarin werd geoordeeld dat de politie na inbeslagname niet ongelimiteerd het inbeslaggenomen voorwerp (*in casu* een smartphone) mag onderzoeken. De Hoge Raad oordeelde dat opsporingsambtenaren bevoegd zijn om, zonder tussenkomst van een officier van justitie of een rechter-commissaris, een smartphone te onderzoeken wanneer de inbreuk op de persoonlijke levenssfeer van de gebruiker beperkt is.[41] Een inbreuk is beperkt wanneer een gering aantal gegevens wordt geraadpleegd. Een onderzoek kan daarentegen onrechtmatig zijn wanneer dat onderzoek zo verstrekkend is dat een min of meer compleet beeld is verkregen van bepaalde aspecten van het persoonlijke leven van de gebruiker van de smartphone. Dit kan het geval zijn wanneer alle gegevens op de mobiele telefoon worden onderzocht met gebruikmaking van technische hulpmiddelen. Een vermoeden van een dergelijke inbreuk ontstaat wanneer de politie een (volledig) inzicht verkrijgt in contacten, oproepgeschiedenis, berichten en foto's door onderzoek aan de mobiele telefoon en/of de bijbehorende SIM-kaart.[42]

---

[41] Het arrest gaat alleen over onderzoek aan voorwerpen die door opsporingsambtenaren zelfstandig in beslag zijn genomen. De situatie van een doorzoeking door een Officier van Justitie of een rechter-commissaris valt buiten het bereik van dit arrest. Dat blijkt uit hetgeen wordt overwogen in rechtsoverweging 2.8 en uit de opsomming van de relevante wetsartikelen in rechtsoverweging 2.4.

[42] HR 4 april 2017, 15/03882, ECLI:NL:HR:2017:584.

5.1.2.h

6.2.4.2 Afluisteren telecommunicatie

Het afluisteren van telecommunicatie, bijvoorbeeld via een klassieke tap of een IP tap, is op grond van artikel 126m Sv (Titel IVA) of artikel 126t Sv (Titel V) mogelijk. De uitgewerkte tapverslagen (ongestructureerde data) en de begin- en de eindpaal worden geregistreerd in SummIT en die data is op die manier beschikbaar in Raffinaderij.

Het tapsysteem zelf (Orca) registreert echter veel meer metadata dan in SummIT wordt gezet (bijvoorbeeld tussenliggende paallocaties). Vanuit opsporingsperspectief kan die data interessant zijn, bijvoorbeeld ten behoeve van de locatie-bepaling. De Raffinaderij kan die data *near real-time* ontsluiten. Daarbij moet echter niet uit het oog worden verloren dat de grondslag waarop de data verkregen wordt, overeenstemt met het doel waarvoor de gegevens vervolgens voor worden gebruikt. Het is mogelijk dat er in geval van *near real-time* ontsluiting van locatiegegevens sprake is van stelselmatige observatie, hetgeen een andere, bijzondere opsporingsbevoegdheid is.

6.2.4.3 Overig data verzameld met behulp van (bijzondere) opsporingsbevoegdheden

Naast de bovenstaande voorbeelden kan met behulp van (bijzondere) opsporingsbevoegdheden ook nog op andere gronden dan wel kan andere informatie worden verzameld. Zoals bijvoorbeeld de (reis)bewegingen van personen op basis van bakendata die wordt verzameld op grond van een bevel stelselmatige observatie (artikel 126g e.v. Sv), of communicatiegegevens die zijn opgenomen met behulp van een technisch hulpmiddel (artikel 126l e.v. Sv). Het voert voor deze PIA te ver om in te gaan op al deze verschillende gegevensbronnen, maar de kern is gelijk: het gaat om politiegegevens die verzameld zijn op grond van een specifieke (bijzondere) opsporingsbevoegdheid.

6.3 Nieuwe bevoegdheden: Wet Computercriminaliteit III

Ten tijde van het schrijven van dit rapport ligt in de Eerste Kamer het wetsvoorstel[43] betreffende de Wet Computercriminaliteit III ter behandeling. Dit wetsvoorstel heeft wijzigingen van het Wetboek van Strafrecht en van het Wetboek van Strafvordering tot oogmerk. Het doel van deze wetgeving is om de opsporing en vervolging van computercriminaliteit te verbeteren en te versterken door deze aan te passen aan de technologische ontwikkelingen op het internet en het gebruik van computers voor communicatie en opslag en verwerking van gegevens. Hiertoe krijgen opsporingsdiensten meer bevoegdheden. Zo kunnen zij onder omstandigheden op afstand computers, mobiele telefoons, servers, clouddiensten, gegevensdragers en andere communicatieapparatuur

[43] *Kamerstukken II* 2015-2016, 34372, nr. 3.

5.1.2.h

('geautomatiseerd werken') binnendringen en kunnen zij software voor de opsporing van ernstige vormen van criminaliteit plaatsen. Bij zeer ernstige misdrijven, zoals deelname aan een terroristische organisatie (artikel 140a WvSr) en doodslag (artikel 287 WvSr) of moord (artikel 289 WvSr), kunnen opsporingsambtenaren naast het aftappen van communicatie (artikel 126l of artikel 126m Sv) of het doen van stelselmatige observaties (artikel 126g Sv) ook gegevens veiligstellen of ontoegankelijk maken (artikel 126nba juncto artikel 126zpa Sv).

6.4 Herziening Wetboek van Strafvordering (modernisering Strafvordering)

Het Wetboek van Strafvordering heeft sinds 1926 weinig structurele verandering gezien. De wereld waarop het Wetboek van Strafvordering van toepassing is, heeft echter een grote digitaliseringsslag gemaakt. Tegenwoordig geschiedt veel in de samenleving op digitale wijze en gebeurt slechts weinig nog op papier, zo ook in de opsporing door de politie. Met de modernisering van het Wetboek van Strafvordering wordt gepoogd om aan te sluiten bij deze veranderingen.[44] De taken, bevoegdheden en werkzaamheden worden effectiever en efficiënter verricht, nieuwe werkwijzen worden gerealiseerd en functionarissen, burgers en andere belanghebbenden krijgen een betere informatiepositie. Aan de andere kant beoogt de modernisering van het Wetboek van Strafvordering om administratieve lasten en fouten in de registratie terug te dringen. Opsporingsbevoegdheden worden bijgesteld en aangescherpt, onder meer ten aanzien van de verwerking van informatie. De wetgeving moet op deze manier toegankelijker worden voor de burger en de rechtspraktijk, zodat de politie adequaat kan reageren op strafbaar gedrag en het nemen van onjuiste beslissingen kan worden voorkomen. Al met al probeert de wetgever om het Wetboek van Strafvordering zo te moderniseren dat de bevoegdheden, instrumenten en werkzaamheden passen in deze digitale tijd en effectief ingezet kunnen worden in de opsporing.

In februari 2017 zijn boek 1 (strafvordering in het algemeen) en boek 2 (het opsporingsonderzoek) van de Herziening Wetboek van Strafvordering in consultatie gegaan. De hierop volgende boeken 3 tot en met 8 zullen in de loop van 2017 in consultatie gaan.

[44] Daarnaast is een belangrijk doel het stroomlijnen van het strafproces en het 'opschonen' van het Wetboek van Strafvordering.

In het kader van de Raffinaderij is met name boek 2 (het opsporingsonderzoek) relevant. Dit boek bevat de regeling van het opsporingsonderzoek en de bijbehorende opsporingsbevoegdheden en bevat onder meer een regeling van de inbeslagname van gegevensdragers en het gebruik van bijzondere opsporingsbevoegdheden.[45]

Het ziet er naar uit dat met de modernisering van het Wetboek van Strafvordering geen ingrijpende stelselwijzigingen plaats zullen vinden die, hetgeen beschreven in deze PIA, in aanzienlijke mate zouden treffen. Veeleer gaat het om een stroomlijningen van het huidige systeem van het voorbereidend onderzoek. Wel zijn er punten die voor het functioneren van de Raffinaderij relevant kunnen zijn. Het gaat dan met name over de nieuwe regeling van het verkennend onderzoek.

Relevante wijzigingen met het oog op de Raffinaderij zijn:

1. De algemene beginselen van doelbinding (*détournement de pouvoir*) en proportionaliteit en subsidiariteit worden direct gecodificeerd.
2. Het verruimen van de mogelijkheden om binnen een verkennend onderzoek opsporingsbevoegdheden toe te passen die een meer dan geringe inbreuk kunnen maken op de persoonlijke levenssfeer (meer specifiek open bronnen onderzoek).
3. Het onderscheid tussen 'gewone' en 'bijzondere' opsporingsbevoegdheden komt te vervallen. In plaats daarvan komt een regeling voor 'heimelijke bevoegdheden'.
4. Het is onduidelijk of de regelingen van artikel 126cc Sv en 126dd Sv blijven bestaan en zo ja, in welke vorm.

Ad 1) Doelbinding, proportionaliteit en subsidiariteit
Door het direct vastleggen van deze beginselen wordt het belang van deze uitgangspunten onderstreept. Hoewel dit niet tot wezenlijk andere uitkomsten voor het gebruik van de Raffinaderij leidt, is het goed om deze beginselen als uitgangspunt voor het handelen in het oog te houden.

Ad 2) Aanpassing verkennend onderzoek

[45] Ministerie van Justitie, Memorie van Toelichting: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek. Deze wetsvoorstellen zijn raadpleegbaar via: https://www.rijksoverheid.nl/actueel/nieuws/2017/02/07/modernisering-van-het-wetboek-van-strafvordering-vordert-gestaag.

In de praktijk is slechts een enkele keer een verkennend onderzoek uitgevoerd. De noodzaak van het verkennend onderzoek wordt door opsporingsinstanties echter wel onderschreven. Om die reden wil de wetgever de mogelijkheden voor de toepassing van het verkennend onderzoek uitbreiden. Meer in het bijzonder wordt gekeken naar de mogelijkheid om in het kader van een verkennend onderzoek stelselmatig persoonsgegevens uit open bronnen vast te leggen en om geautomatiseerde gegevensbestanden van de overheid bij het verkennend onderzoek te kunnen betrekken.[46] De Raffinaderij zou bij uitstek een middel zijn om deze nieuwere, uitgebreidere vorm van verkennend onderzoek te faciliteren. Op het verkennend onderzoek is de Wpg van toepassing. Relevant is dat de wetgever voor het verkennend onderzoek het algemene uitgangspunt, dat politiegegevens binnen de politieorganisatie voor andere taken beschikbaar moeten kunnen zijn, buiten werking laat. Op grond van artikel 15 lid 2 Wpg juncto artikel 2:13 Bpg moeten verzoeken tot het delen van gegevens uit een verkennend onderzoek geweigerd kunnen worden, omdat het bij een verkennend onderzoek een omvangrijke groep van personen betreft ten aanzien van wie geen verdenking is van betrokkenheid bij ernstige strafbare feiten.[47]

Ad 3) Onderscheid gewone en bijzondere opsporingsbevoegdheden

Het onderscheid tussen gewone en bijzondere opsporingsbevoegdheden komt in het nieuwe wetboek te vervallen. In plaats daarvan komen er 'gewone' en 'heimelijke' bevoegdheden. In beginsel zou dit voor de Raffinaderij weinig verschil moeten maken, ware het niet dat onduidelijk is wat de status is van het (her)gebruik van BOB-gegevens (zie ad 4).

Ad 4) (Her)gebruik BOB-gegevens

Relevant voor de Raffinaderij is dat vooralsnog onduidelijk is hoe in het nieuwe Wetboek wordt omgegaan met de regeling van artikel 126cc Sv en 126dd Sv. Momenteel worden in deze artikelen grenzen gesteld aan het hergebruik van BOB-gegevens binnen de politie. In het nieuwe voorstel voor Boek 2 wordt weliswaar verwezen naar artikel 126cc Sv in het nieuwe artikel 2.8.2.9.1 Sv, maar de artikelen 126cc Sv en 126dd Sv zelf komen verder niet terug in het voorstel.

---

[46] Ministerie van Justitie, Memorie van Toelichting: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek, p. 62.

[47] Ministerie van Justitie, Memorie van Toelichting: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek, p. 268.

7 Juridisch kader verwerken politiegegevens

In dit hoofdstuk wordt het wettelijk kader voor de verwerking van politiegegevens uiteengezet. Hierop is primair de Wet politiegegevens van toepassing. De Wpg zal op 25 mei 2018 worden vervangen door de implementatiewet van de Richtlijn 2016/680/EG.[48]

7.1 Wet politiegegevens

Het gebruik van persoonsgegevens binnen de politieorganisatie wordt primair gereguleerd door de Wet politiegegevens (Wpg) en het daarbij horende Besluit politiegegevens (Bpg). Voor wat betreft het verwerken van persoonsgegevens in het kader van de Raffinaderij moet dus aansluiting worden gezocht bij de Wpg. De Autoriteit Persoonsgegevens (verder: AP) is aangewezen als toezichthouder op de naleving van deze wet (artikel 35 Wpg).

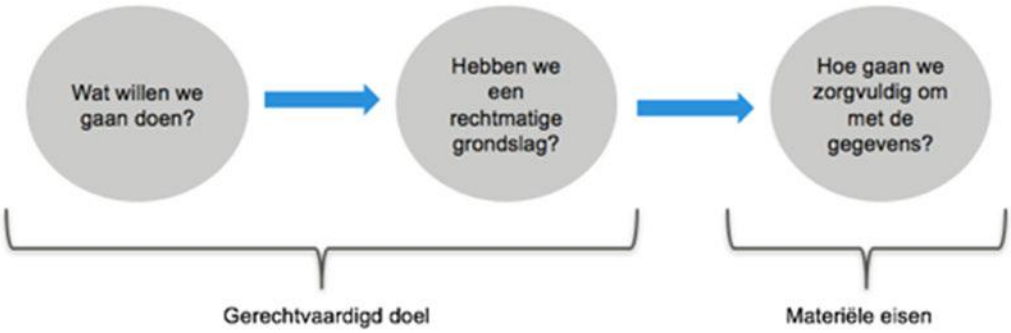
De Wpg is van toepassing op de verwerking van politiegegevens die in een bestand zijn opgenomen of bestemd zijn om in een bestand te worden opgenomen (artikel 2 Wpg).[49] De handelingen die plaatsvinden met gegevens in het kader van de Raffinaderij kunnen worden aangemerkt als verwerkingen in de zin van de Wpg. Artikel 1 onder c Wpg definieert verwerkingen namelijk als elke handeling met betrekking tot politiegegevens. Zoals reeds geconcludeerd in de PIA uit 2013 kunnen de verwerkte gegevens in het kader van de Raffinaderij worden aangemerkt als politiegegevens.

Blijkens artikel 3 lid 1 Wpg is het verwerken van politiegegevens slechts toegestaan voor zover de verwerking noodzakelijk is bij of krachtens de wet geformuleerde doeleinden. Dit betekent met andere woorden dat voor een verwerking een bij wet geformuleerd doel en een bijbehorende wettelijke grondslag moet bestaan. Vervolgens dient te worden voldaan aan de materiële vereisten van de Wpg (zie hiervoor hieronder). Deze doeleinden zijn te vinden in de artikelen 8 tot en met 13 Wpg.

---

[48] Ten tijde van het schrijven van deze rapportage was nog geen (concept)versie van de implementatietekst beschikbaar. Om die reden hanteren wij de richtlijn als uitgangspunt.

[49] De Memorie bij de Wet politiegegevens (*Kamerstukken II* 2005-2006, 30 327, nr. 3) stelt dat de definitie van het begrip 'bestand' aansluit bij de definitie van het begrip 'bestand' uit de Wet bescherming persoonsgegevens (p. 30). Een bestand is 'elk gestructureerd geheel van persoonsgegevens die volgens bepaalde criteria toegankelijk zijn'. De Memorie van Toelichting bij de Wbp geeft aan dat verwerkingen in een bestand zowel geautomatiseerd als niet geautomatiseerd kunnen zijn (zie p. 53).



7.1.1 Soorten politiegegevens

Een politiegegeven wordt in artikel 1 sub a Wpg gedefinieerd als:

> "*elk persoonsgegeven dat in het kader van de uitoefening van de politietaak wordt verwerkt*."

Persoonsgegevens zijn in artikel 1 sub a Wet bescherming persoonsgegevens gedefinieerd als:

> *"alle gegevens betreffende geïdentificeerde of identificeerbare natuurlijk personen."*

Een persoon is *geïdentificeerd* wanneer uit de aard van de gegevens rechtstreeks de identiteit van een persoon kan worden bepaald. Een voorbeeld hiervan is (de combinatie van) de voornaam, achternaam en geboortedatum van een persoon.

Een persoon is *identificeerbaar* wanneer de identiteit van een persoon aan de hand van de gegevens niet direct is vast te stellen, maar dat deze herleidbaar is door een combinatie van andere gegevens. Identificeerbaarheid dient daarbij ruim te worden opgevat.[50] Een kenteken is bijvoorbeeld niet noodzakelijkerwijs een persoonsgegevens maar de identiteit kan mogelijk worden herleid wanneer het kenteken wordt gekoppeld aan de RDW kentekendatabase. De identificeerbaarheid van een persoon is afhankelijk van de gegevens en van de verantwoordelijke die de gegevens verwerkt. Wanneer de verantwoordelijke zonder veel inspanning de identiteit van een persoon kan achterhalen, is er sprake van persoonsgegevens. Aangezien de politie meer middelen ter beschikking heeft om een persoon te identificeren en identificatie daarmee geen onevenredige inspanning vergt, zal over het algemeen sneller worden aangenomen dat een gegeven een persoonsgegeven is

[50] Zie in dit kader bijvoorbeeld HvJ 19 oktober 2016, C-582/14 (*Breyer*).

en daarmee een politiegegeven is wanneer dit gegeven in een politiebestand is opgenomen.

Het begrip persoonsgegeven stamt uit een tijd voor 'Big Data'. Dit maakt de beoordeling of en wanneer er sprake is van een persoonsgegeven lastig. In de context van Big Data is het namelijk vaak niet op voorhand te zeggen of iets een persoonsgegeven is of niet. Daarom is het onder omstandigheden moeilijk om te bepalen of een dataset persoonsgegevens bevat. Veelal zal dit bepaald moeten worden door de koppeling die tussen de losse data in de bestanden tot stand kan worden gebracht.

Politiegegevens mogen alleen worden verwerkt voor zover dit noodzakelijk is voor een goede uitvoering van de politietaak (artikel 3 Politiewet).

7.1.1.1 Gevoelige persoonsgegevens

Naast gewone persoonsgegevens bestaan er in de Wpg ook gevoelige gegevens. Deze gegevens leveren naar hun aard een groter privacy-risico voor de betrokkene op. In artikel 5 Wpg worden gevoelige gegevens[51] gedefinieerd als:

> '*politiegegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven, alsmede persoonsgegevens betreffende het lidmaatschap van een vakvereniging*'.

De verwerking van deze gegevens mag slechts plaatsvinden voor zover dit voor het doel van de verwerking onvermijdelijk is. Aangezien er in het kader van de Raffinaderij grote hoeveelheden data worden verwerkt, is het niet ondenkbaar dat het daarbij ook om gevoelige persoonsgegevens gaat. Dit is in het bijzonder het geval voor contra-terrorisme onderzoeken waarbij godsdienstige overtuiging een relevante factor kan zijn in het onderzoek (jihadisme).

7.1.1.2 Grondslagen verwerking van politiegegevens

Artikel 3 Wpg regelt de noodzakelijkheid, rechtmatigheid en doelbinding van verwerkingen van politiegegevens. Zoals reeds hierboven omschreven, is de verwerking van politiegegevens slechts toegestaan voor zover de verwerking noodzakelijk is bij of

[51] Hierbij moet worden opgemerkt dat de persoonsgegevens die in het kader van de Wpg als gevoelige persoonsgegevens worden bestempeld onder het regime van de Wet bescherming persoonsgegevens als bijzondere persoonsgegevens worden bestempeld (art. 16 Wbp).

5.1.2.h

krachtens de wet geformuleerde doeleinden. Deze doeleinden staan vermeld in artikel 8 tot en met 13 Wpg.

Een verdere verwerking van politiegegevens is alleen mogelijk wanneer de nieuwe verwerking niet onverenigbaar is met het doel waarvoor de gegevens zijn verkregen. Met andere woorden, de Wpg moet uitdrukkelijk voorzien in de mogelijkheid om de politiegegevens verder te verwerken voor dat specifieke doel.

In het kader van de Raffinaderij zijn drie doelen voor de verwerking van persoonsgegevens relevant:

- Ten eerste kunnen persoonsgegevens worden verwerkt in het kader van de uitvoering van de dagelijkse politietaak zoals bedoeld in artikel 8 Wpg. Dit betreft de niet-gerichte verwerking van politiegegevens;
- Een tweede doel is de gerichte verwerking van politiegegevens, zoals bedoeld in artikel 9 en 10 Wpg. Daarvan is sprake als de politie overgaat tot de verwerking van grote hoeveelheden persoonsgegevens, bijvoorbeeld in het kader van een onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval (artikel 9 Wpg) en voor verwerkingen met het oog op het verkrijgen van inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde (artikel 10 Wpg);
- Een derde doel waar politiegegevens voor mogen worden verwerkt, is wanneer er sprake is van een verdere verwerking. Dit is onder meer neergelegd in de artikelen 11 en 13 Wpg. Zoals hierboven al beschreven, is de verdere verwerking van politiegegevens aan strikte regels gebonden.

7.1.2 Materiële eisen Wpg

Uit artikel 3 lid 2 Wpg volgt dat voor de verwerking geldt dat politiegegevens slechts mogen worden verwerkt voor zover zij rechtmatig zijn verkregen en de gegevens moeten , gelet op het doel waarvoor de gegevens zijn verzameld, toereikend, terzake dienend en niet bovenmatig zijn.

Naast deze algemene eis van rechtmatigheid bestaan er in de Wpg ook inhoudelijke eisen aan de wijze waarop met persoonsgegevens wordt omgegaan. Daarbij kan gedacht worden aan eisen die betrekking hebben op de vertrouwelijkheid, beveiliging, datakwaliteit, transparantie en de invulling van de rechten voor betrokkenen. Bovendien geldt voor bepaalde doeleinden dat de herkomst van de gegevens en de wijze van verkrijging van

deze gegevens vermeld moet worden. In Hoofdstuk 9 gaan wij specifiek in op de materiële eisen die aan de verwerking van politiegegevens wordt gesteld in het kader van de Raffinaderij.

De vraag of het verwerken van politiegegevens in het kader van de Raffinaderij legitiem is, hangt af van de vraag of de verwerking noodzakelijk is voor een of meer in de wet geformuleerde doeleinden en de vraag hoe de gegevens verwerkt worden. Dit laatste moet in overeenstemming zijn met de inhoudelijke eisen. Beide elementen moeten vervuld worden zodat er sprake is van een legitieme gegevensverwerking in het kader van de Raffinaderij. In deze PIA zullen wij in Hoofdstuk 8 beide aspecten afzonderlijk bespreken.

7.2 Europese Richtlijn verwerking politiegegevens

Op 27 april 2016 zijn twee stukken wetgeving gepubliceerd. Enerzijds de Richtlijn 2016/680/EC betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten (Richtlijn).[52] Anderzijds de Verordening 2016/679 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (Algemene Verordening Gegevensbescherming).[53]

Met name de Richtlijn is relevant voor de werkzaamheden die in het kader van de Raffinaderij worden uitgevoerd. De Richtlijn regelt de wijze waarop onder meer de politie om moet gaan met politiegegevens. De Richtlijn zal dan ook op een aantal punten tot wijziging van de huidige Wet politiegegevens leiden. Momenteel implementeert de Nederlandse wetgever deze Richtlijn. Pas wanneer de Richtlijn is geïmplementeerd, kan met zekerheid worden gezegd hoe de Wpg precies gewijzigd is en wat de definitieve

[52] Richtlijn (EU) 2016/680 van het Europese Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad.

[53] Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

invloed is op de Raffinaderij. Desalniettemin is het van belang om nu al stil te staan bij de (mogelijke) wijzigingen die uit de Richtlijn voortvloeien. Deze zullen hieronder worden besproken.

7.2.1 Categorieën betrokkenen (artikel 6 Richtlijn)

De verschillende categorieën van betrokkenen moeten worden gespecificeerd. De Richtlijn maakt onderscheid tussen verdachten, veroordeelden, getuigen en anderszins betrokkenen.

7.2.2 Datakwaliteit (artikel 7 Richtlijn)

Er moeten gradaties in de juistheid en betrouwbaarheid van gegevens worden aangebracht. Zo dienen politiegegevens die op feiten zijn gebaseerd zo veel mogelijk te worden onderscheiden van politiegegevens die op een persoonlijk oordeel gebaseerd zijn. Daarnaast is de inspanningsverplichting opgenomen dat de politie alle redelijke maatregelen neemt om te voorkomen dat onjuiste, onvolledige of niet meer actuele gegevens worden doorgestuurd of op een andere manier beschikbaar worden gesteld. Hiertoe wordt de kwaliteit van de gegevens, voor zover haalbaar, gecontroleerd voordat de gegevens worden doorgestuurd of beschikbaar worden gesteld. Wanneer blijkt dat toch onjuiste persoonsgegevens zijn doorgezonden of wanneer persoonsgegevens onrechtmatig zijn verstuurd, wordt de ontvanger hierover geïnformeerd. De gegevens worden dan in ieder geval gerectificeerd of gewist.

7.2.3 Informatieplicht (artikel 13 Richtlijn)

Op basis van de Richtlijn krijgt de politie een informatieplicht op basis waarvan zij betrokkenen dient te informeren over gegevensverwerkingen die de betrokkenen betreffen. Deze informatieplicht sluit aan op hetgeen is bepaald in de Algemene verordening gegevensbescherming. Blijkens het derde lid van dit artikel dient de politie in ieder geval informatie ter beschikking te stellen over:

- De identiteit en de contactgegevens van de verantwoordelijke;
- In voorkomend geval de contactgegevens van de functionaris voor de gegevensbescherming;
- De doeleinden van de verwerking waarvoor de persoonsgegevens zijn bestemd; en
- De rechten van de betrokkenen.

De politie kan deze informatieplicht blijkens artikel 13 lid 3 Richtlijn uitstellen, beperken of achterwege laten voor zover en zolang een dergelijke maatregel in een democratische samenleving, met inachtneming van de grondrechten en de legitieme belangen van de natuurlijke persoon, een noodzakelijk en evenredig maatregel is om:

- Belemmering van officiële of gerechtelijke onderzoeken of procedures te voorkomen;
- Nadelige gevolgen voor de voorkoming, opsporing, het onderzoek en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen te voorkomen;
- De openbare veiligheid te beschermen;
- De nationale veiligheid te beschermen;
- De rechten en vrijheden van anderen te beschermen.

Of er sprake is van een uitzonderingssituatie, zoals bedoeld in voornoemd artikel, en de informatieplicht buiten toepassing kan worden gelaten, dient in elk specifiek geval goed beoordeeld te worden. Lidstaten kunnen wettelijke maatregelen treffen om verwerkingscategorieën aan te wijzen die geheel of gedeeltelijk onder één van de punten van lid 3 vallen (lid 4). Met andere woorden, lidstaten kunnen wettelijke categorieën vaststellen waarvoor de informatieplicht uitgesteld, beperkt of achterwege gelaten wordt.

7.2.4 Registerplicht (artikel 24 Richtlijn) en bijhouden logbestanden (artikel 25 Richtlijn)

Op grond van artikel 24 van de Richtlijn is de politie verplicht om een register van alle verwerkingen bij te houden. Deze verplichting kan worden gezien als een uitbreiding van de protocolplicht zoals deze nu al in artikel 32 Wpg bestaat. Artikel 24 van de Richtlijn bepaalt dat *in casu* de politie in twee hoedanigheden registers moeten bijhouden.

- Ten eerste als (verwerkings)verantwoordelijke: een register van alle categorieën van onder haar verantwoordelijkheid vallende verwerkingen.
- Daarnaast als bewerker: een register van alle categorieën van verwerkingen die zij heeft verricht namens andere verantwoordelijken.

Wanneer de politie als verantwoordelijke optreedt, dient het onderstaande in het register te worden opgenomen:

- De naam en de contactgegevens van de verantwoordelijke, van de eventuele gezamenlijke verantwoordelijken en van de functionaris voor gegevensbescherming;
- De verwerkingsdoeleinden;
- De categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden bekendgemaakt, met inbegrip van ontvangers in derde landen of internationale organisaties;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- In voorkomend geval het gebruik van profilering;

5.1.2.h

- In voorkomend geval de categorieën van doorgiften van persoonsgegevens aan een derde land of een internationale organisatie;
- En aanwijzing betreffende de rechtsgrondslag van de verwerking, met inbegrip van doorgiften, waarvoor de persoonsgegevens bestemd zijn;
- Indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van persoonsgegevens moeten worden gewist;
- Indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

Verwerkt de politie gegevens ten behoeve van een andere organisatie, en handelt zij daarmee als bewerker, dient het register het onderstaande te bevatten:

- De naam en de contactgegevens van de bewerker of bewerkers en van iedere verantwoordelijke namens wie de verwerker handelt en, in voorkomend geval, van de functionaris voor gegevensbescherming;
- De categorieën van verwerkingen die namens iedere verantwoordelijke zijn uitgevoerd;
- Indien van toepassing, doorgiften van persoonsgegevens aan derde landen of een internationale organisatie indien daartoe door de verantwoordelijke uitdrukkelijke instructies zijn gegeven, met inbegrip van de vermelding van dat derde land of de internationale organisatie;
- Indien mogelijk, een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

De politie is daarnaast verplicht om logbestanden bij te houden van bepaalde verwerkingen die geschieden. Deze logs worden uitsluitend gebruikt om te controleren of de verwerking van persoonsgegevens rechtmatig is, voor interne controle, ter waarborging van de integriteit en de beveiliging van de persoonsgegevens en voor strafrechtelijke procedures (artikel 25 Richtlijn).

7.2.5 PIA en Voorafgaande raadpleging (artikel 27 en 28 Richtlijn)

Wanneer een bepaalde verwerking extra risicovol voor de rechten en vrijheden van burgers is, dient een *privacy impact assessment* te worden uitgevoerd voordat met de verwerking wordt aangevangen (artikel 27 Richtlijn). Onder omstandigheden moet ook een voorafgaande raadpleging (voordat met de verwerking wordt begonnen) bij de toezichthoudende autoriteit geschieden (artikel 28 Richtlijn). Dat is het geval als uit de PIA

5.1.2.h

blijkt dat een verwerking een hoog risico met zich meebrengt en indien de verantwoordelijke geen maatregelen neemt om het risico te beperken of wanneer de aard van de verwerking een hoog risico voor de rechten en vrijheden van betrokkenen oplevert. Dit laatste is in het bijzonder het geval wanneer gebruikt wordt gemaakt van nieuwe technologieën.

7.2.6 Gegevensbescherming door ontwerp en standaardinstellingen (artikel 20 Richtlijn)

Uitgangspunt bij de ontwikkeling van politie systemen is dat reeds bij het ontwerp rekening wordt gehouden met privacybescherming. Dit is het beginsel van *Privacy by Design and by Default*. Privacybeschermende maatregelen kunnen zowel technisch als organisatorisch van aard zijn.

7.2.7 Meldplicht datalekken (artikel 30 en 31 Richtlijn)

Er wordt een specifieke meldplicht datalekken bij overheidsinstanties gecreëerd (artikel 30 Richtlijn). Wanneer een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, dient de verantwoordelijke binnen 72 uur de toezichthouder te informeren over dit incident, tenzij het niet waarschijnlijk is dat de inbreuk een risico voor de rechten en vrijheden van de betrokkene met zich meebrengt. De verantwoordelijk verstrekt de volgende informatie aan de toezichthouder:

- Aard van de inbreuk, waar mogelijk de categorieën en het aantal betroffen betrokkenen en de categorieën en aantal betroffen persoonsgegevens;
- Naam van de Functionaris Gegevensbescherming of een ander contactpunt van informatie;
- De waarschijnlijke gevolgen van de inbreuk in verband met persoonsgegevens; en
- De voorgestelde of getroffen maatregelen om de (nadelige) gevolgen van het incident te beperken.

Wanneer de toezichthouder na het verstrijken van de 72 uur wordt geïnformeerd, dient de verantwoordelijke de vertraging te motiveren en onderbouwen.

De genoemde meldplicht is een afgezwakte variant van de meldplicht datalekken die gecreëerd is in de Algemene Verordening Gegevensbescherming.

Wanneer de inbreuk waarschijnlijk een hoog risico voor de rechten en vrijheden van de betrokkene met zich meebrengt, informeert de verantwoordelijke de betrokkene over de inbreuk zonder onnodige vertraging (artikel 31 Richtlijn).

7.2.8 Functionaris voor de Gegevensbescherming (artikel 32 – 34 Richtlijn)

Artikel 32 van de Richtlijn schrijft voor dat de verwerkingsverantwoordelijke een Functionaris voor de Gegevensbescherming (FG) aanwijst.
Diegene heeft als taak (zie artikel 34):

- Om de verantwoordelijke en diens werknemers te informeren en adviseren;
- Toe te zien op de naleving van de Richtlijn en andere gegevensbeschermings-bepalingen, inclusief het toewijzen van verantwoordelijkheden, bewustmaking en opleiding van het personeel;
- Om te adviseren ten aanzien van PIAs en toezien op de uitvoering van de PIAs;
- Om samen te werken met de toezichthoudende autoriteiten; en
- Om op te treden als contactpunt voor de toezichthouder, onder meer voor wat betreft de voorafgaande raadpleging.

Het is belangrijk dat de FG tijdig en naar behoren wordt betrokken bij aspecten die verband houden met de bescherming van persoonsgegevens.

In verband met de taken en bevoegdheden van de FGs verwijzen wij naar de Richtlijnen betreffende FGs van de Artikel 29 Werkgroep.[54]

7.2.9 Doorgifte aan derde landen of internationale organisaties (artikel 35 – 40 Richtlijn)

De doorgifte van gegevens aan derde landen of internationale organisaties en gegevensexporten worden aan strengere eisen en voorwaarden gebonden (artikel 35 – 40 Richtlijn).[55]

---

[54] WP29 2016. Weliswaar zijn de richtlijnen primair gericht op FGs die worden aangesteld onder de Algemene Verordening Gegevensbescherming, desalniettemin zijn deze richtlijnen ook relevant voor FGs die worden aangesteld onder deze Richtlijn, voor zover het overeenkomstige bepalingen betreft.
[55] Paragraaf 3 Wpg ziet op de verstrekking van politiegegevens aan anderen dan de politie en de Koninklijke Marechaussee. Deze paragraaf bevat slechts een artikel dat van toepassing zijn op de verstrekking van gegevens aan organisaties buiten Nederland, te weten art. 17 Wpg. Voor het overige bevat onder meer de Wpg artikelen die eisen stellen aan de verstrekking aan opsporingsambtenaren en gezagsdragers (art. 16 Wpg), verstrekking aan politie en gezagsdragers Bonaire, Sint Eustatius en Saba (art. 17a Wpg) en verstrekking aan derden structureel (art. 18 Wpg), incidenteel (art. 19 Wpg) en structureel voor een samenwerkingsverband (art. 20 Wpg). De Richtlijn daarentegen bevat meer verschillende bepalingen ten aanzien van doorgiften, onder meer op basis van adequaatheidsbesluiten (art. 36 Richtlijn), op voorwaarde van passende waarborgen (art. 37 Richtlijn) en doorgifte aan ontvangers in derde landen (art. 39 Richtlijn).

Op grond van artikel 35 lid 1 Richtlijn moet doorgifte van gegevens aan derde landen of internationale organisaties noodzakelijk zijn voor de opsporing, vervolging en voorkoming van misdrijven. Gegevens mogen alleen doorgegeven worden aan een verwerkingsverantwoordelijke die zelf ook een bevoegde autoriteit is. De lidstaat van waaruit de persoonsgegevens komen, moet *toestemming* gegeven hebben voor doorgifte. Hiervan mag alleen worden afgeweken ingeval van acute of ernstige bedreiging voor openbare veiligheid of fundamentele belangen, en indien toestemming niet tijdig verkregen kan worden (lid 2). In het geval dat de bevoegde autoriteit toestemming verleent, neemt deze alle relevante factoren mee zoals de ernst van het strafbare feit, het doel van de doorgifte en het niveau van bescherming van het land van de ontvanger (art. 35 lid 1 sub e).

Artikel 36 Richtlijn betreft de doorgifte van politiegegevens aan derde landen en internationale organisaties wanneer de Europese Commissie een adequaatheidsbesluit heeft genomen. In dat geval is geen specifieke toestemming nodig. Artikel 37 Richtlijn maakt de doorgifte mogelijk zonder een adequaatheidsbesluit wanneer passende waarborgen voor de bescherming van persoonsgegevens zijn getroffen en deze waarborgen zijn getoetst. Artikel 38 Richtlijn bevat de regels op grond waarvan het mogelijk is om gegevens te verstrekken aan derde landen of internationale organisaties waar geen passend beschermingsniveau bestaat. In artikel 39 Richtlijn worden regels gegeven voor situaties waarin de ontvanger van de gegevens in een derde land gevestigd is, maar *geen* bevoegde autoriteit is. Dit artikel is niet van toepassing op internationale overeenkomst tussen lidstaten en derde landen op het gebied van justitiële samenwerking in strafzaken en politiële samenwerking.

Artikel 40 verplicht de Commissie en de lidstaten om zich actief in te zetten om, ten aanzien van derde landen en internationale organisaties, de samenwerking en procedures op dit gebied te ontwikkelen, verbeteren en bevorderen.

7.2.10 Toezichthouder en sancties

De AP is de toezichthouder op de naleving van de Richtlijn. De huidige taken van de toezichthouder zullen flink worden uitgebreid. Zo heeft de AP onder meer het houden van toezicht op naleving van de Richtlijn tot taak, zij heeft een adviesrol aan onder meer de wetgever, verantwoordelijken en bewerkers, een onderzoeksbevoegdheid, een informatierol en er kunnen klachten bij haar worden ingediend (artikel 46 Richtlijn). Bovendien worden

5.1.2.h

er eisen gesteld aan de onafhankelijkheid van de toezichthouder en gelden er algemene voorwaarden voor de leden van de toezichthoudende autoriteit (artikelen 42 en 43 Richtlijn).

De AP heeft de bevoegdheid om corrigerende maatregelen te treffen, zoals:

- Het waarschuwen van de verantwoordelijke en bewerker wanneer een voorgenomen verwerking mogelijk in een inbreuk op de Richtlijn resulteert;
- Verantwoordelijke of verwerker de opdracht te geven om verwerkingen aan te passen door gegevens te rectificeren of te wissen;
- Het opleggen van een (tijdelijk) verwerkingsverbod (artikel 47 Richtlijn).

Lidstaten stellen zelf de straffen vast die van toepassing zijn op inbreuken op de Richtlijn. Bovendien moeten de lidstaten alle nodige maatregelen treffen om ervoor te zorgen dat de regels worden nageleefd. Deze maatregelen moeten doeltreffend, evenredig en afschrikkend zijn (artikel 57 Richtlijn).

8 Legitimiteit gebruik gegevens binnen de Raffinaderij

Zoals in de voorgaande hoofdstukken is uiteengezet, bestaan er twee juridische kaders voor de verzameling en de verwerking van gegevens. Er bestaat een zekere mate van overlap tussen deze twee kaders. De politie mag enkel gegevens verzamelen wanneer daar een rechtmatige grondslag voor is in de Wet politiegegevens. Daar waar het verzamelen van deze gegevens een meer dan geringe inbreuk op de persoonlijke levenssfeer vormt, is een specifiekere wettelijke grondslag noodzakelijk. Deze grondslagen zijn te vinden in het Wetboek van Strafvordering en allen gekoppeld aan de context van het strafrechtelijk onderzoek.

In dit hoofdstuk wordt de legitimiteit van de verzameling en de verwerking van politiegegevens binnen de Raffinaderij getoetst aan de vereisten uit de Wet politiegegevens. De materiële vereisten uit deze wet worden in hoofdstuk 9 behandeld.

Om te kunnen vaststellen of er sprake is van het legitiem verzamelen en verwerken van politiegegevens in de Raffinaderij dient allereerst te worden bepaald wie de verantwoordelijke is voor de gegevensverwerkingen in de Raffinaderij. Vervolgens moet voor de beoogde verwerking worden vastgesteld of er sprake is van een gerechtvaardigd doel (waarvoor een wettelijke grondslag bestaat voor de verwerking van de politiegegevens). De verwerkingen in het kader van de Raffinaderij (en waaraan wij in deze PIA aandacht besteden), zijn het delen van gegevens binnen de politieorganisatie en het geautomatiseerd vergelijken en in combinatie zoeken van politiegegevens.

8.1 Verantwoordelijkheid

Wanneer politiegegevens worden gebruikt in het kader van de Raffinaderij moet worden vastgesteld wie verantwoordelijk is voor de verwerking.

Op grond van artikel 1 sub f onder 1 Wpg is de korpschef verantwoordelijk voor de Raffinaderij en de gegevens die in de context van de Raffinaderij worden verwerkt. De Politiechefs van de Eenheden zullen voor verwerkingen binnen hun eenheid als eerste aanspreekpunt fungeren op grond van de (onder)mandaatregeling.[56] De Politiechef van Amsterdam is de houder van de BI-portefeuille waaronder de Raffinaderij valt.

[56] Mandaatbesluit Politie 2017.

5.1.2.h

Daarnaast wijst het hierboven genoemde artikel 1 sub f Wpg het College van procureurs-generaal, als verantwoordelijke voor de Rijksrecherche aan onder 2, en onder 3 de Minister van Defensie als verantwoordelijke voor de Koninklijke Marechaussee aan.

Ook het Openbaar Ministerie heeft een rol bij het gebruik van de politiegegevens binnen de Raffinaderij. Het Openbaar Ministerie heeft namelijk zeggenschap over het gebruik en het delen van politiegegevens in het kader van strafrechtelijke onderzoeken.

8.2 Verwerkingsdoelen en grondslagen

Nu helder is wie de verantwoordelijke is voor de gegevensverwerking moet vervolgens worden vastgesteld of sprake is van een gerechtvaardigd doel voor de verwerking. Zoals in hoofdstuk 6 al is beschreven, worden de grondslagen voor *verzameling* of *verkrijging* van de politiegegevens gevonden in de Titels IVA en V van het Wetboek van Strafvordering (Sv) en in de artikelen 8, 9 en 10 Wpg. Op de *verdere verwerking* van politiegegevens ziet vervolgens enkel de Wet politiegegevens. Deze wet stelt regels aan het beheer van gegevens die door de politie worden verwerkt bij de uitvoering van de politietaak. De politie heeft tot (overkoepelende) taak om te zorgen voor de daadwerkelijke handhaving van de rechtsorde. Daarnaast moet zij hulp bieden aan hen die deze behoeven (artikel 3 Politiewet 2012).

De Wpg bepaalt dat politiegegevens alleen mogen worden verwerkt wanneer zij rechtmatig zijn verkregen (artikel 3 lid 2 Wpg). Dit betekent dat gegevens die niet rechtmatig zijn verzameld in beginsel niet mogen worden gebruikt in het kader van de Raffinaderij. Om te kunnen bepalen of er sprake is van een gerechtvaardigd doel voor de verwerking is het van belang nader te kijken naar:
a) het doel van de verwerking in Raffinaderij;
b) de noodzakelijkheid van de verwerking; en
c) of de verzamelde politiegegevens toereikend, ter zake dienend en niet bovenmatig zijn.

8.2.1 Doel van de gegevensverwerking in het kader van de Raffinaderij

Gegevensverwerking door de politie moet noodzakelijk zijn voor het bereiken van door de wetgever geformuleerde legitieme doelen (artikel 3 lid 1 Wpg). De gegevens mogen alleen voor het doel worden verwerkt waarvoor zij zijn verkregen, tenzij de Wpg anders bepaalt. De doelen waarvoor de politiegegevens verder kunnen worden verwerkt, staan limitatief opgesomd in de artikelen 8 tot en met 13 Wpg. In het kader van de Raffinaderij zijn de doelen die zijn neergelegd in de artikelen 8 tot en met 11 en artikel 13 Wpg relevant. Deze zullen hieronder nader worden toegelicht.

8.2.1.1 Niet-gerichte verwerking: Dagelijkse politietaak (artikel 8 Wpg)

Artikel 8 Wpg regelt de verwerking van politiegegevens in het kader van de uitvoering van de dagelijkse politietaak (zoals bedoeld in artikel 3 Politiewet 2012). Deze verwerkingen vinden plaats in het kader van het basispolitiewerk.[57] De verwerkingen die in het kader van de uitvoering van de dagelijkse politietaak worden uitgevoerd, betreffen niet-gerichte verwerkingen. Voor deze taak wordt de Raffinaderij niet gebruikt, wel kunnen mogelijk gegevens die zijn verzameld zijn op basis van deze taak worden ingelezen in de Raffinaderij.

8.2.1.2 Gerichte verwerking: Handhaving openbare rechtsorde in een bepaald geval (artikel 9 Wpg)

In artikel 9 Wpg is de verwerking van politiegegevens in het kader van de handhaving van de openbare rechtsorde in een bepaald geval jegens bepaalde personen neergelegd. Er is, met andere woorden, sprake van een gerichte verwerking. Politiegegevens kunnen op deze grondslag worden verwerkt voor onderzoeken die plaatsvinden in het kader van opsporingsonderzoeken.[58]

8.2.1.3 Gerichte verwerking: Inzicht in betrokkenheid bij misdrijven (artikel 10 Wpg)

Artikel 10 Wpg regelt de verwerking van persoonsgegevens die tot doel hebben om inzicht te krijgen in de betrokkenheid van personen bij het beramen of plegen van misdrijven. Uit de Memorie van Toelichting bij de Wpg volgt dat het uit de praktijk blijkt dat de verwerking van gegevens over verdachte en onverdachte personen noodzakelijk kan zijn zodat de politie een informatiepositie kan opbouwen om zicht te kunnen krijgen en behouden op ontwikkelingen en verschijnselen die een ernstige bedreiging van de rechtsorde vormen. Er wordt geprobeerd om een beeld te krijgen van de betrokkenheid van personen bij bepaalde ernstige handelingen of misdrijven door middel van omvangrijke en gerichte gegevensverzamelingen. Dit betreft een min of meer permanent proces van analyse en leidt tot het vastleggen van gegevens over veelal nog onverdachte personen. Op basis van deze informatiepositie kan besloten worden om over te gaan tot een operationeel opsporingsonderzoek, dan wel om operationele maatregelen in de sfeer van de openbare orde te treffen.[59] Nadere analyse van deze politiegegevens kan leiden tot een nieuw opsporingsonderzoek (artikel 9 Wpg). Ook kan besloten worden tot operationele maatregelen in de sfeer van de openbare orde.[60]

---

[57] *Kamerstukken II* 2005-2006, 30 327, nr. 3, p. 38.

[58] *Kamerstukken II* 2005-2006, 30 327, nr. 3, p. 43.

[59] *Kamerstukken II* 2005-2006, 30 327, nr. 3, p. 12.

[60] *Kamerstukken II* 2005-2006, 30 327, nr. 3, pp. 46-47.

8.2.1.4 Verdere verwerking: Geautomatiseerd vergelijken en in combinatie zoeken (artikel 11 Wpg)

De wet biedt de mogelijkheid om de gegevens die zijn verwerkt ten behoeve van een bepaald onderzoek (artikel 9 Wpg) of voor een doel uit artikel 10 Wpg, te vergelijken met gegevens die zijn verwerkt in een ander onderzoek. Bovendien kunnen politiegegevens op basis van artikel 11 lid 4 Wpg in combinatie met elkaar worden verwerkt. Er is hier sprake van een verdere verwerking van politiegegevens.
Omdat deze verwerkingen risico's voor de bescherming van de persoonlijke levenssfeer tot gevolg kunnen hebben, zijn deze vormen van verwerking gebonden aan strikte regels.[61] In par. 8.2.3 zal hier nader op worden ingegaan.

Als de Raffinaderij als instrument of werkwijze wordt ingezet, dan is er per definitie sprake van het geautomatiseerd vergelijken of het in combinatie doorzoeken van politiegegevens. Lid 4 van artikel 11 Wpg maakt het mogelijk om politiegegevens, die worden verwerkt op grond van de artikelen 8 tot en met 10 Wpg in combinatie met elkaar te verwerken. Dit betekent dat de politie politiegegevens – binnen de grenzen van de Wpg – mag doorzoeken, combineren, verrijken enzovoorts. Artikel 11 Wpg is daarmee een belangrijke wettelijke basis voor een deel van de verwerkingen die in het kader van de Raffinaderij, en in samenhang met de artikelen 8 tot en met 10 Wpg, plaatsvinden.

8.2.2 Ondersteunende taken (artikel 13 Wpg)

Politiegegevens mogen alleen voor een ander doel worden verwerkt wanneer de Wpg daarin uitdrukkelijk voorziet. Artikel 13 Wpg biedt een dergelijke mogelijkheid: politiegegevens van artikel 8, 9 en 10 Wpg mogen verder worden verwerkt ten behoeve van de ondersteuning van de politietaak. De wet noemt vijf aspecten die vallen onder het bereik van deze ondersteunende taak, namelijk:

- Het vaststellen van eerdere verwerkingen ten aanzien van eenzelfde persoon of zaak, onder meer ter bepaling van eerdere betrokkenheid bij strafbare feiten;
- Het ophelderen van strafbare feiten die nog niet herleid konden worden tot een verdachte;
- Identificatie van personen of zaken;
- Het onder de aandacht brengen van personen of zaken met het oog op het uitvoeren van een gevraagde handeling dan wel met het oog op een juiste bejegening van personen;
- Het uitvoeren van taken ten dienste van de justitie.

[61] Van der Bel, van Hoorn & Pieters 2013, pp. 67-68.

5.1.2.h

Het is daarbij aan de verantwoordelijke, de korpschef, om te bepalen welke gegevens voor verdere verwerking in aanmerking komen.

8.2.3 Noodzakelijk, toereikend, ter zake dienend en niet bovenmatig

Wanneer het doel van de gegevensverwerking is bepaald (zoals genoemd in de artikelen 8 tot en met 13 Wpg), moet vervolgens beoordeeld worden of de verwerking noodzakelijk is om dat doel te vervullen. Daarnaast moet worden bepaald in hoeverre de daarvoor verzamelde politiegegevens toereikend, ter zake dienend en niet bovenmatig zijn (artikel 3 Wpg). Bij de toetsing hiervan, zijn de eisen van proportionaliteit en subsidiariteit leidend. Het beginsel van proportionaliteit houdt in dat de verwerking van de persoonsgegevens noodzakelijk is om het doel te bereiken of te vervullen. Op grond van het beginsel van subsidiariteit kan het middel niet op een andere, minder ingrijpende manier worden bereikt.

In het kader van de Raffinaderij dienen opsporingsambtenaren en analisten zich af te vragen welke gegevens zij nodig hebben om een opsporingsvraag te beantwoorden. Wanneer blijkt dat een opsporingsvraag met minder gegevens kan worden beantwoord, dient dit te gebeuren. Bovendien moeten deze gegevens ook relevant zijn voor de beantwoording van de opsporingsvraag. Met name van belang is om 'fishing expeditions' te voorkomen. Een voorbeeld van een fishing expedition is bijvoorbeeld het zonder concrete aanleiding of verdenking combineren van grote hoeveelheden gegevens om te kijken of er een interessant verband gevonden kan worden.

Hetzelfde geldt voor de inzet van middelen of tools: kan een opsporingsvraag worden beantwoord door een ander middel of een andere tool in te zetten die een minder grote inbreuk op de privacy van de betrokkene heeft? Het voorgaande betekent dat een opsporingsambtenaar of analist niet toegang tot alle data krijgt omdat deze toch beschikbaar zijn of omdat deze gegevens mogelijk relevant kunnen zijn.
Wanneer een analist of opsporingsambtenaar toegang wil tot persoonsgegevens of gebruik wil maken van bepaalde middelen of tools, zal men steeds moeten nagaan of dit nodig is voor de beantwoording van de recherchevraag of dat die vraag beantwoord kan worden met minder gegevens of door de inzet van minder ingrijpende middelen of tools.

Dit betekent dat de vraag of het verwerken van politiegegevens in het kader van de Raffinaderij legitiem is, afhangt van de omstandigheden van het geval.

5.1.2.h

8.3 Delen van gegevens binnen de Politie en tussen onderzoeken

Binnen de politie en tussen de politie en onder andere de Koninklijke Marechaussee kunnen politiegegevens worden gedeeld. De mogelijkheid om deze gegevens te delen, vloeit voort uit artikel 15 Wpg. Dit artikel voorziet in een ruim verstrekkingsregime.

De verantwoordelijke is op grond van artikel 15 Wpg verplicht om politiegegevens ter beschikking te stellen aan daartoe (overeenkomstig artikel 6 lid 2 Wpg) geautoriseerde personen binnen de politieorganisatie, die deze gegevens nodig hebben voor de uitvoering van hun taak. Deze gegevensdeling moet strikt noodzakelijk zijn met het oog op de uitvoering van de politietaak.[62]

De verplichting tot het ter beschikking stellen van politiegegevens sluit aan bij de verplichtingen in de artikelen 10 en 11 Politiewet 2012. Op grond van deze artikelen moeten alle ambtenaren die belast zijn met een politietaak elkaar wederkerig de nodige hulp bieden en voortdurend samenwerken ter uitvoering van die taak. Wanneer dat nodig is voor een goede uitvoering van politietaak, kan alleen in bijzondere gevallen worden afgeweken van deze verplichting tot ter beschikking stelling van politiegegevens.

Ten behoeve van de uitvoering van de strafrechtelijke handhaving van de rechtsorde moet de officier van justitie, als leider van het opsporingsonderzoek, te allen tijde zeggenschap kunnen uitoefenen over de verwerking van politiegegevens. In het verlengde hiervan is het daarom zeer wenselijk dat de officier van justitie nauw wordt betrokken bij het besluit om politiegegevens al dan niet te delen.

8.3.1 Het gebruik van politiegegevens uit andere lopende of afgesloten onderzoeken

Hoewel artikel 126cc Sv stelt dat bepaalde politiegegevens moeten worden vernietigd nadat het betreffende onderzoek is afgerond, maakt artikel 126dd Sv het mogelijk om deze verplichting tot vernietiging van politiegegevens te doorbreken.
Het gaat daarbij om politiegegevens die zijn verkregen door observatie met behulp van een technisch hulpmiddel dat signalen registreert, het opnemen van telecommunicatie of het vorderen van gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot deze gebruiker.

De officier van justitie kan bepalen dat deze politiegegevens onder voorwaarden ook in andere strafrechtelijke onderzoeken kunnen worden gebruikt, te weten:

[62] Zoals bedoeld in paragraaf 2 Wpg.

1. Binnen een ander strafrechtelijk onderzoek dan waartoe de opsporingsbevoegdheid is uitgeoefend; en
2. Om inzicht te krijgen in de betrokkenheid van personen bij misdrijven en handelingen zoals bedoeld in artikel 10 lid 1 sub a en b Wpg (TCI en Themaverwerkingen).

De komst en de inzet van de Raffinaderij maakt deze bevoegdheid extra relevant. Politiegegevens uit verschillende onderzoeken kunnen met behulp van de Raffinaderij op technische wijze namelijk gemakkelijk worden gecombineerd.

8.3.2 Gebruik TCI-gegevens[63]

Criminele-inlichtingen zijn volgens artikel 1 sub f van het Besluit Verplichte Politiegegevens:

> "*gegevens die in aanmerking komen voor verwerking op grond van artikel 10 eerste lid onderdeel a van de Wet politiegegevens.*"

Deze TCI-gegevens mogen worden verwerkt om inzicht te krijgen in strafbare feiten. Deze gegevens mogen echter niet als bewijs dienen. Wanneer een TCI beschikt over relevante en operationeel te gebruiken informatie, de zogenoemde CI-informatie, zal zij deze informatie door middel van een proces-verbaal verstrekken aan de chef van de meest gerede opsporingsdienst. Het leidende uitgangspunt is dat het Openbaar Ministerie de plicht heeft om de rechter te voorzien van alle informatie die redelijkerwijs van belang kan zijn voor de beoordeling van een strafzaak. Het Openbaar Ministerie zal CI-informatie enkel gebruiken om een redelijk vermoeden van schuld, zoals bedoeld in artikel 27 Sv, te bepalen en vervolgens een onderzoek te starten. CI-informatie dient in dat geval als startinformatie. Daarnaast kan CI-informatie in een lopend onderzoek richting geven. CI-informatie dient dan als sturingsinformatie. In deze situaties wordt CI-informatie niet als bewijs gebruikt omdat de afschermingsbelangen van informanten daaraan in de weg staan.[64] Het bewijs zal moeten worden gevonden in de resultaten van het onderzoek waarin de CI-informatie een rol heeft gespeeld. Deze praktijk is door Nederlandse en Europese rechtspraak

[63] Teams criminele inlichtingen, voorheen criminele inlichtingen eenheden (CIEs). Waar wij spreken van TCI gegevens doelen wij op criminele-inlichtingen in de zin van artikel 1 onder f van het Besluit verplichte politiegegevens.

[64] Hier moet worden opgemerkt dat momenteel geen informanten informatie in de Raffinaderij wordt ontsloten. Indien dergelijke informatie wel wordt ontsloten in de Raffinaderij is dit een belangrijk punt om rekening mee te houden.

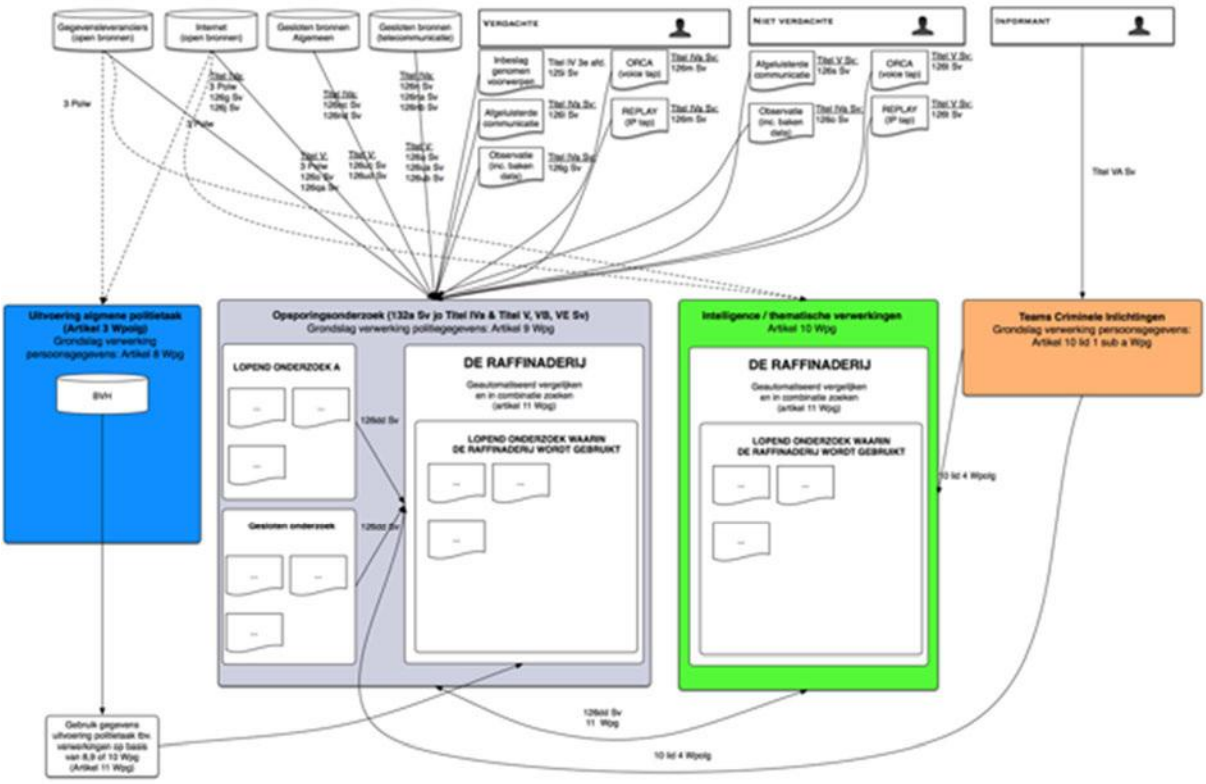
erkend.[65] Zodat er sprake is van een bewezenverklaring moet de informatie worden 'opgevolgd' door voldoende tactische en toetsbare informatie die de verdenking bevestigt. Als twijfel ontstaat over de CI-informatie moet zij getoetst worden op de rechtmatigheid van verkrijging en verdere verwerking.

In het kader van de Raffinaderij is het daarom van belang om vast te stellen wanneer politiegegevens worden gebruikt voor de opsporing of wanneer zij voor de bewijsvoering worden gebruikt. De CI-gegevens kunnen zéér gevoelig zijn. Gevolg van de openbaarmaking van deze gegevens kan bijvoorbeeld informanten mogelijk compromitteren. Daarom is er een strenger regime van toepassing wanneer deze gegevens te verstrekt worden (artikel 7 en artikel 8 lid 2 Besluit Verplichte Politiegegevens). Voor de Raffinaderij is het van belang dat binnen de politie het besef bestaat dat het mengen van 'CI-gegevens' en 'gewone gegevens' tot problemen kunnen leiden in onderzoeken. Dit risico speelt met name wanneer deze data worden gebruikt ter verrijking van andere data. Daarom is het van belang dat vastgesteld kunnen worden welke gegevens waar vandaan afkomstig zijn zodat duidelijk is waar deze gegevens al dan niet voor gebruikt kunnen worden.

[65] EHRM 20 november 1989, NJ 1990, 245 (*Kostovski*), r.o. 44; EHRM 4 juli 2000, EHRC 2000, 71; HR 14 september 1992, NJ 1993, 83; HR 18 januari 1999, *NJ* 1999, 253.

5.1.2.h

8.4 Schematische weergave Raffinaderij binnen het huidige juridische kader



8.5 Verzamelen versus verwerken: wrijving in het juridisch kader voor gegevensverwerking

De Wet politiegegevens en het Wetboek van Strafvordering sluiten qua systematiek niet (naadloos) op elkaar aan. In de PIA Raffinaderij 2013 is dit ook reeds geconstateerd. De WRR signaleert in haar rapport *Big Data in een vrije en veilige samenleving*[66] hetzelfde en concludeert vervolgens dat de privacy waarborgen primair in de verzamelfase zitten, maar in veel mindere mate in de fase van de analyse en het gebruik. Het verzamelen van gegevens kent door het strafvorderlijk kader veel juridische waarborgen (bijvoorbeeld een machtiging van de officier van justitie en de toets van de Rechter-commissaris in een aantal gevallen). Dit geldt in veel mindere mate voor de verdere verwerking van persoonsgegevens in het kader van de analyse en het gebruik binnen de politieorganisatie. Dit is een potentieel risico voor de privacy (en andere rechten) van betrokkenen alsmede voor de integriteit van onderzoeken.

Afbeelding 1 – WRR: Big Data-proces in fasen[67]

Het betreft hier niet zozeer een specifiek risico van de Raffinaderij, als wel een breder vraagstuk aangaande de informatie-huishouding van de politie en de inrichting van ons strafproces- en gegevensbeschermingsrecht. Vanuit het perspectief van deze PIA is dit dan

[66] WRR 2016.

[67] WRR 2016, p. 39.

ook geen probleem dat hier direct geadresseerd kan worden. Met de Raffinaderij wordt binnen de grenzen van de wet geopereerd, maar werkwijzen zoals de Raffinaderij rechtvaardigen misschien een meer fundamentele herijking van het juridisch kader voor de gegevensverwerking door de politie.

De regulering van de opsporing vindt plaats in de context van het voorbereidende onderzoek. Het gaat hierbij om een (min of meer) concrete zaak waarbij er een verdenking bestaat (Titel IV en IVA Sv), een redelijk vermoeden dat misdrijven in georganiseerd verband worden beraamd of gepleegd, dan wel om aanwijzingen voor een terroristisch misdrijf (Titel V en VB Sv).

De regulering van het gebruik van politiegegevens kent een ander vertrekpunt, namelijk het concrete doel waartoe de politiegegevens verwerkt. Dit kan een gerichte verwerking zijn met het oog op de strafrechtelijke handhaving van de rechtsorde in een concreet geval (artikel 9 Wpg), maar ook de verwerking van politiegegevens ten behoeve van het verkrijgen van inzicht in de betrokkenheid van personen bij het plegen of beramen van ernstige misdrijven (artikel 10 Wpg). Artikel 10 Wpg betreft de verwerking van politiegegevens voor 'intelligence' doeleinden: het in stand houden van een zekere informatiepositie die vervolgens aangewend kan worden om concreet te handhaven.

> *"Op basis van de informatiepositie kan worden besloten tot een operationeel opsporingsonderzoek, dan wel tot operationele maatregelen in de sfeer van de openbare orde."*[68]

Wanneer binnen de politie op grote schaal gegevens worden verwerkt (zoals binnen de Raffinaderij), dan wordt het onderscheid tussen intelligence en opsporing steeds vager. Gegevens worden bijvoorbeeld verzameld in het kader van een opsporingsonderzoek. Deze gegevens worden vervolgens gebruikt voor intelligence doeleinden en daarna weer "teruggegeven" (al dan niet verrijkt) aan een concreet opsporingsonderzoek, waar de gegevens kunnen worden gebruikt als bewijs. Het onderscheid tussen intelligence en opsporing wordt in die zin door technologieën en werkwijzen als de Raffinaderij arbitrair omdat de intelligence analyses herhaald kunnen worden binnen een concreet opsporingsonderzoek waar zij als bewijs kunnen dienen. Intelligence en opsporing putten dus uit dezelfde bronnen.

---

[68] *Kamerstukken II* 2005–2006, 30 327, nr. 3, p. 12.

5.1.2.h

Enerzijds is dit een goede zaak omdat de politie hierdoor vele malen effectiever en efficiënter wordt, maar deze praktijk roept wel de vraag op ten aanzien van de omgang met deze schaalvergroting en wat voor effect onrechtmatig verkregen bewijs heeft dan wel veroorzaakt in dat geheel.

8.5.1 Grotere privacyschending door onderling in verband gebrachte gegevens?

Het eerste vraagstuk dat de grootschalige gegevensverwerking oproept, is de weging van eventuele privacy-inbreuken. De proportionaliteit en subsidiariteit van de toepassing van opsporingsbevoegdheden worden nu getoetst op het moment van de toepassing (dus bij het verzamelen van de gegevens). Hierbij gaat het om *checks* van buiten de politie-organisatie (namelijk bij de officier van justitie of de rechter-commissaris).

Voor de onderlinge combinatie en het hergebruik van gegevens binnen de politie-organisatie moet de bevoegd functionaris (meestal de teamleider) toestemming geven. Dit betreft echter een vrij marginale privacytoets die enkel gericht is op de gegevens uit het eigen onderzoek en het hergebruik daarvan in een andere context. Het kan evenwel zijn dat een persoon in meerdere onderzoeken voorkomt (als verdachte, maar mogelijk ook anderszins als betrokkene) en dat op basis van de combinatie van de gegevens en de analyses die daarmee worden gedaan een zeer compleet beeld van deze persoon ontstaat. Dit kan een grotere privacy-inbreuk opleveren dan de gelegitimeerde inbreuken in de verzamelfase. De som van de inbreuken is als het ware meer dan de delen. Momenteel wordt hier in samenhang niet op getoetst. Als dit zou gebeuren dan ligt het in de rede dat dit analoog aan de verzamelfase wordt gedaan door een officier van justitie of misschien zelfs wel een rechter-commissaris. In zekere zin vindt een dergelijke toets wel plaats in het kader van artikel 11 lid 4 Wpg. Op grond van dit artikel kan het bevoegd gezag bepalen dat politiegegevens die verwerkt zijn op grond van de artikelen 8, 9 of 10 Wpg in combinatie met elkaar kunnen worden verwerkt. Het doel hiervan is om vast te stellen of verbanden bestaan tussen deze gegevens. Wanneer dergelijke verbanden bestaan, kunnen deze gegevens verder worden verwerkt na instemming van de daartoe bevoegde functionaris. Het betreft hier evenwel een minder onafhankelijke toets, daar de bevoegde functionaris onderdeel is van de politie.

5.1.2.h

8.5.2 Omgang met onrechtmatig verkregen bewijs

Met het oog op de bewijsvoering is het een belangrijk aandachtspunt om op te merken dat de gegevensverwerking, de informatie en het bewijs in belangrijke mate sequentieel zijn. Dit geldt niet alleen voor de Raffinaderij maar voor het gehele strafprocesrecht. Dit betekent dat een vervolgstap in het opsporingsproces veelal gebaseerd zal zijn op eerder verkregen bewijs en eerder verrijkte informatie. Wanneer in een eerdere schakel in de keten een strafvorderlijke fout is gemaakt, bijvoorbeeld doordat bijzondere opsporingsbevoegdheden onjuist of onrechtmatig zijn toegepast, kan dit van invloed zijn op de houdbaarheid van de daarop gebaseerde bewijsmiddelen. Dit is de leer van de *fruits of the poisonous tree*. Als uiterste consequentie kunnen bewijsmiddelen die gebaseerd zijn op eerdere schakels worden uitgesloten. Dit vraagstuk is in het kader van de Raffinaderij zeer relevant omdat politiegegevens in de Raffinaderij met elkaar gecombineerd kunnen worden. Daarbij kunnen juist verkregen en eventueel onjuist verkregen gegevens worden vermengd. Het is mogelijk lastig om terug te voeren welk deel van de gegevens nog wel gebruikt mag worden en welke gegevens niet meer gebruikt mogen worden. Door de omstandigheden van het geval kan een rechter zich vervolgens genoodzaakt zien om het gehele bewijsmiddel uit te sluiten.

Gegevens die verzameld zijn in het kader van een voorbereidend onderzoek worden opgeslagen in de politiesystemen en worden hiermee automatisch politiegegevens die, afhankelijk van de grondslag die daarvoor is, verder mogen worden verwerkt ten behoeve van de politietaak. In zoverre het BOB-bevoegdheden betreft, mogen de gegevens enkel voor andere onderzoeken of voor de artikel 10 Wpg taak worden gebruikt op het moment dat er toestemming is van de officier van justitie. Als deze toestemming er is, dan zijn deze gegevens daarmee buiten de context van het originele onderzoek rechtmatig beschikbaar. Mocht tijdens de terechtzitting blijken dat de gegevens in het originele onderzoek onrechtmatig zijn verkregen en hier de zware sanctie van de bewijsuitsluiting aan wordt verbonden, dan zijn de gegevens niet meer beschikbaar voor dat concrete onderzoek. Dit wil echter niet zeggen dat de gegevens ook gewist zijn uit de systemen en/of niet meer worden gebruikt in andere onderzoeken waarvoor toestemming was verleend of worden gebruikt als intelligence (en later weer als bewijs in een andere zaak).

De vraag is welk gevolg een dergelijk vormverzuim bij de verzameling van gegevens heeft, wanneer deze gegevens binnen de Raffinaderij worden gebruikt voor een ander onderzoek.

Artikel 359a Sv creëert de mogelijkheid voor de rechter om aan vormverzuimen in het

strafrechtelijke vooronderzoek strafprocesrechtelijke 'sancties' te verbinden. Uit de bewoording van dit artikel lijkt te volgen dat artikel 359a Sv uitsluitend betrekking heeft op het voorbereidend onderzoek tegen de verdachte ten aanzien van het aan hem tenlastegelegde feit waarover de rechter die in artikel 359a Sv wordt bedoeld, moet oordelen. Dit betekent dat artikel 359a Sv niet van toepassing is indien het verzuim is begaan buiten het verband van dit voorbereidend onderzoek. Ook wordt de verdachte niet beschermd tegen vormverzuimen die gemaakt zijn wanneer de geschonden norm niet ziet op het belang van de verdachte (*Schutznorm*).[69]

De mogelijkheid dat gegevens die onrechtmatig zijn verkregen in een onderzoek tegen de verdachte (of een onderzoek waar de verdachte in voorkwam, maar niet als (hoofd)verdachte) gebruikt worden in het kader van een ander onderzoek tegen dezelfde verdachte, wordt met toepassingen als de Raffinaderij steeds groter. Het is de vraag of daarom op de langere termijn de beperkingen van 359a Sv en de *Schutznorm* houdbaar blijven.[70] In extreme gevallen kan onrechtmatig bewijs zelfs 'witgewassen' worden: door de mogelijkheid om gegevens over onderzoeken heen te gebruiken kan een onrechtmatig verkregen stuk bewijs toch nog dienst bewijzen tegen de verdachte in een andere zaak.

[69] De *Schutznorm* is het relativiteitsvereiste. De *Schutznorm* vereist dat gekeken wordt welk belang het geschonden voorschrift beoogt te beschermen en in hoeverre dit belang betrekking heeft op de verdachte, volgens Corstens 2014, p. 826.

[70] Zie in dit kader onder andere, NJ 2004, 376 en ECLI:NL:GHARL:2013:607.

9 Materiële eisen verwerking persoonsgegevens

Zoals in hoofdstuk 7 al werd aangestipt, stelt de Wpg naast de algemene eisen van rechtmatigheid ook inhoudelijke eisen aan de wijze waarop met persoonsgegevens wordt omgegaan. Dit zijn de zogenoemde materiële eisen. Daarbij kan gedacht worden aan eisen die betrekking hebben op de vertrouwelijkheid, beveiliging, datakwaliteit, transparantie en de invulling van de rechten van betrokkenen.

9.1 Materiële eisen

Deze materiële eisen stellen eisen aan een zorgvuldige verwerking van gegevens binnen de politie. In het kader van deze PIA belichten wij de meest relevante materiële eisen. Wij staan hier met name stil bij de eisen zoals deze nu bestaan in de Wet politiegegevens. Daar waar de Richtlijn 2016/680 een verandering teweeg brengt, zullen wij dit vermelden.

9.1.1 Data kwaliteit

Zowel uit de Wpg als uit de Richtlijn volgt dat politiegegevens juist en nauwkeurig dienen te zijn (artikel 4 lid 1 Wpg en artikel 4 lid 1 sub d Richtlijn). Gegevens die onjuist of onvolledig zijn, dienen te worden verbeterd, aangevuld of gewist.

Artikel 7 Richtlijn maakt bovendien onderscheid tussen persoonsgegevens die op feiten zijn gebaseerd en persoonsgegevens die op een persoonlijk oordeel zijn gebaseerd. Vervolgens moeten maatregelen worden getroffen om ervoor te zorgen dat persoonsgegevens die onjuist, onvolledig of niet meer actueel zijn niet meer worden doorgezonden of beschikbaar worden gesteld. Bevoegde autoriteiten dienen, voor zover mogelijk, hiervoor de kwaliteit van de gegevens te controleren voordat gegevens worden doorgezonden of beschikbaar worden gesteld. Voor zover dat mogelijk is wordt bij de doorzending de nodige aanvullende informatie toegevoegd zodat de ontvangende instantie in staat is om de juistheid, volledigheid en betrouwbaarheid van de gegevens te beoordelen en de mate van actueelheid vast te stellen (lid 2). Wanneer blijkt dat onjuiste persoonsgegevens zijn doorgezonden of gegevens onrechtmatig zijn verzonden, dient de ontvanger hiervan direct te worden geïnformeerd. De persoonsgegevens worden dat gerectificeerd of gewist (lid 3).

In de Raffinaderij wordt gewerkt met veel gegevens die uit verschillende originele bronnen afkomstig zijn. Er dienen derhalve controles op de kwaliteit plaats te vinden. In principe vindt de validatieslag van deze gegevens plaats bij het verzamelen en vastleggen van gegevens in de bronsystemen. Hierbij zijn fouten of onvolledigheden uiteraard niet

uitgesloten. Analisten en rechercheurs dienen zich daarom bewust te zijn van mogelijke 'doorwerkfouten' wanneer zij gebruik maken van de mogelijkheden van de Raffinaderij. Deze doorwerkfouten kunnen het gevolg zijn van onjuiste, onvolledige of niet meer actuele c.q. verouderde informatie die uit het bronsysteem komt. Daarbij is het goed om op te merken dat het combineren en verrijken van gegevens in de Raffinaderij het aan de andere kant juist ook mogelijk maakt om fouten en onvolledigheden in de brondata eenvoudiger te signaleren. Wanneer blijkt dat gegevens onjuist zijn, is het van belang om stil te staan bij de vraag op welke manier ervoor wordt gezorgd dat de gegevens vervolgens goed in het originele bronsysteem komen te staan. Hiervoor kan het noodzakelijk zijn om bestaande processen te bekijken of hiertoe nieuwe processen te creëren. Ook is het van belang dat processen bestaan om ervoor te zorgen dat de ontvanger van onjuiste informatie wordt geïnformeerd en dat deze persoonsgegevens worden gerectificeerd of gewist.

9.1.2 Beveiliging

Uit artikel 4 lid 3 Wpg en artikel 29 Richtlijn vloeit de verplichting voort dat de verantwoordelijke passende technische en organisatorische maatregelen treft om de politiegegevens te beveiligen. Onder de nieuwe Richtlijn is bovendien een meldplicht datalekken gecreëerd waardoor overheidsinstanties, waaronder de politie, een inbreuk in verband met persoonsgegevens onverwijld moeten melden bij de toezichthouder (artikel 30 Richtlijn). Onder omstandigheden zal de betrokkene ook moeten worden geïnformeerd over de inbreuk (artikel 31 Richtlijn).

De Raffinaderij draait vanuit het beveiligde rekencentrum van de politie op 'eigen' servers binnen het Digitale Transferium. De servers hebben geen directe verbinding met het internet. Analisten en opsporingsambtenaren kunnen alleen die gegevens inzien en analyseren die relevant zijn voor hun eigen onderzoek.

Deze personen kunnen de Raffinaderij vanaf de eigen werkplek benaderen. Om toegang te kunnen krijgen, dienen deze personen allereerst geautoriseerd te zijn (zie par. 9.1.3) en accounts voor verschillende lagen te hebben. De inlogprocedure loopt vervolgens als volgt:

1. De analist of opsporingsambtenaar logt in op de algemene omgeving van de politie;
2. Vervolgens logt de analist of opsporingsambtenaar in op het digitaal transferium;
3. Vanuit het digitaal transferium kan de analist of opsporingsambtenaar vervolgens inloggen op de Raffinaderij.

9.1.3 Autorisaties

Artikel 6 Wpg vereist dat de verantwoordelijke een systeem van autorisaties onderhoudt dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid. Politiegegevens mogen slechts worden verwerkt door ambtenaren van de politie die daartoe zijn geautoriseerd en voor zover deze autorisatie strekt (lid 2). Ook kunnen personen die geen ambtenaar van de politie zijn, worden geautoriseerd om politiegegevens te verwerken ter uitvoering van de politietaak waarmee zij belast zijn (lid 4). De eisen die aan de autorisaties worden gesteld, worden nader gespecificeerd in het Besluit Politiegegevens. Uit de Wpg en het Besluit volgt dat alleen die (opsporings)ambtenaren die aan een onderzoek zijn toegewezen en specifiek met dit onderzoek zijn belast toegang mogen krijgen tot de gegevens binnen dat onderzoek.[71] De regels omtrent autorisaties zijn neergelegd in de goedgekeurde visie van het Autorisatiemodel voor de Nederlandse Politie die uit juli 2011 dateert.[72] Het autorisatiemodel voor de Raffinaderij is gebaseerd op dit model en de implementatie daarvan in SummIT.

9.1.4 Geheimhoudingsplicht

Op grond van artikel 7 Wpg rust er een (afgeleide) geheimhoudingsplicht op degene aan wie politiegegevens ter beschikking zijn gesteld met betrekking tot die gegevens die worden verwerkt in het kader van de taken van de politie. De geheimhoudingsplicht kan alleen worden doorbroken wanneer een wettelijk voorschrift verplicht tot het verstrekken van politiegegevens of wanneer de politietaak tot verstrekking noodzaakt in bijzondere gevallen.

Gezien de schaal waarop verwerkingen geschieden en het belang dat met de Raffinaderij gemoeid is, is het van belang dat de geheimhoudingsplichten goed worden gewaarborgd.

Ambtenaren die bij de Raffinaderij betrokken zijn en in aanraking komen met politiegegevens hebben een screening ondergaan [73] en, waar nodig, een

[71] Artikel 2:4 Besluit politiegegevens ten aanzien van themaverwerking ernstige misdrijven en artikel 2:5 Besluit politiegegevens voor wat betreft de TCI-verwerkingen. De categorieën van ambtenaren die in aanmerking kunnen komen voor de autorisaties in het kader van de voorgenoemde onderzoeken, worden aangewezen in overeenstemming met de officier van justitie, blijkt uit artikel 2:6 Besluit politiegegevens.

[72] Expertgroep Autorisatiemodel Nederlandse Politie 2011.

[73] Er zijn verschillende screeningsniveaus. Medewerkers hebben minimaal een P-screening. Afhankelijk van de gevoeligheid van het werk, de positie en/of de omvang en de gevoeligheid van informatie waar een medewerker toegang toe heeft, zal een A-screening vereist zijn.

5.1.2.h

geheimhoudingsverklaring ondertekend.[74] Dit geldt zowel voor gebruikers uit de operatie als voor medewerkers uit het Raffinaderij-team en medewerkers die betrokken zijn bij de diverse IT-tools. Ambtenaren die de Raffinaderij gebruiken voor onderzoeken hebben alleen toegang tot de gegevens die van belang zijn voor hun eigen onderzoek of voor de uitvoering van de politietaak waarmee zij belast zijn.

9.1.5 Dataminimalisatie

Op grond van artikel 3 lid 2 Wpg mogen niet meer politiegegevens worden verwerkt dan noodzakelijk is voor het doel waarvoor de gegevens worden verwerkt. Deze verplichting volgt eveneens uit artikel 4 lid 1 sub c Richtlijn: gegevens dienen toereikend, ter zake dienend en niet bovenmatig te zijn voor het doel waarvoor zij worden verwerkt.

Met behulp van de Raffinaderij worden relevante gegevens uit bronbestanden ontsloten en geanalyseerd. Ervan uitgaande dat wordt voldaan aan het systeem van autorisaties hebben medewerkers van een opsporingsteam in de Raffinaderij toegang tot bronnen en gegevens die ze normaal gesproken, in de bronsystemen, ook tot hun beschikking hebben in het kader van onderzoeken. Door de Raffinaderij te gebruiken in het kader van een onderzoek krijgt een opsporingsteam dus niet toegang tot meer of andere gegevens. Wel biedt de Raffinaderij hen de mogelijkheid om op andere manieren 'slim gebruik te maken' van alle data omdat de gegevens in combinatie met elkaar kunnen worden verwerkt.
Hierdoor ontstaat het risico dat opsporingsambtenaren door de beschikbaarheid van de Raffinaderij en haar mogelijkheden, geneigd kunnen zijn om zo veel mogelijk gegevens in een onderzoek te betrekken, in de hoop dat zij met behulp van de Raffinaderij een relevant verband vinden. Medewerkers hebben die neiging normaalgesproken (zonder IV-middelen als de Raffinaderij) minder omdat ze dan veel te lang bezig zijn om al die gegevens door te nemen of te verwerken. Een dergelijk gebruik van de Raffinaderij staat op gespannen voet met het beginsel van dataminimalisatie.

[74] Ambtenaren van de politie hebben de eed of belofte afgelegd. Medewerkers die niet in dienst zijn bij de politie, maar tijdelijk voor de politie werkzaam zijn, bijvoorbeeld door externe inhuur, hebben een geheimhoudingsverklaring ondertekend.

5.1.2.h

9.1.6 Toezicht

De Wpg belicht meerdere mogelijkheden voor het houden van toezicht om een zorgvuldige verwerking van politiegegevens te borgen.

Intern toezicht

Op grond van artikel 33 Wpg rust op de Korpschef van de politie, als verantwoordelijke, de plicht om regelmatig privacy audits te laten uitvoeren. De uitkomsten van deze audit moeten worden overlegd aan de AP.

De verantwoordelijke moet op grond van artikel 34 Wpg ook een Privacyfunctionaris aanstellen die er namens de verantwoordelijke op toeziet dat de verwerking van politiegegevens in overeenstemming met de wet geschiedt. Daarnaast kent de Wpg de mogelijkheid om een Functionaris Gegevensbescherming (FG) aan te stellen (artikel 30 Wpg). Anders dan de privacyfunctionaris heeft een Functionaris Gegevensbescherming een onafhankelijke positie en vervult degene naast de AP een vorm van extern toezicht.

Onder de Richtlijn wordt de FG een verplichte functie binnen de politie (artikelen 32 tot en met 34 Richtlijn). Op het moment van schrijven is het nog onduidelijk of de functie van de FG onder de Richtlijn vergelijkbaar is met de Privacyfunctionaris of de Functionaris Gegevensbescherming.

9.1.6.1 Extern toezicht - Autoriteit persoonsgegevens

De Autoriteit Persoonsgegevens is de toezichthouder op de verwerking van politiegegevens door de politie (artikel 35 Wpg).[75] De AP heeft de bevoegdheid om ambtshalve of op verzoek van een belanghebbende een onderzoek in te stellen naar de manier waarop gegevens worden verwerkt (artikel 60 Wet bescherming persoonsgegevens, Wbp). De AP heeft een toezichthoudende taak op grond van artikel 35 leden 1 en 2 Wpg jo artikel 60 lid 1 Wbp en zij kan handhavend optreden.

De AP moet gehoord worden wanneer het voornemen bestaat om gevoelige gegevens op te nemen in een nieuw bestand. Daarnaast moet de aard van de verwerking, in het bijzonder wanneer nieuwe technologieën, mechanismen of procedures specifieke risico's met zich meebrengen voor de fundamentele rechten van de betrokkene, in het bijzonder

[75] De Autoriteit Persoonsgegevens is ingesteld op grond van artikel 51 van de Wet bescherming persoonsgegevens. In deze wet zijn haar taken en bevoegdheden neergelegd.

5.1.2.h

het recht op bescherming van de persoonlijke levenssfeer (artikel 35 lid 4 Wpg).

Kijkend naar de Raffinaderij is helder dat er met behulp van de Raffinaderij mogelijk gevoelige persoonsgegevens worden verwerkt. Bovendien bestaat de Raffinaderij uit nieuwe technologieën, mechanismen of procedures die specifieke risico's met zich meebrengen. De Raffinaderij biedt de politie de mogelijkheid om effectiever invulling te geven aan haar reeds bestaande bevoegdheden die voortvloeien uit de Politiewet, het Wetboek van Strafvordering en de Wet politiegegevens. De extra risico's voor de bescherming van de fundamentele rechten van de betrokkene spelen met name door de schaalvergroting die door de Raffinaderij mogelijk is. Wel is het de vraag of de Raffinaderij als een nieuw bestand moet worden aangemerkt, of dat het slechts een tool is om reeds bestaande bestanden beter te ontsluiten.

Het is mogelijk dat het werken met de Raffinaderij wordt aangemerkt als een verwerking zoals bedoeld in artikel 13 Wpg. Deze Raffinaderij ondersteunt de politie bij de uitvoering van haar politietaak. Hiertoe worden persoonsgegevens betreffende eenzelfde persoon geautomatiseerd vergeleken en verder verwerkt (lid 3). Wanneer artikel 13 Wpg van toepassing is, dan moet schriftelijk worden vastgelegd voor welk specifiek doel de gegevens verder worden verwerkt, de categorieën van personen en de categorieën gegevens die verder worden verwerkt en de termijn waarbinnen de verdere verwerking wordt beëindigd (lid 4).

De AP blijft zeer waarschijnlijk toezichthouder op de verwerking van politiegegevens door de politie, ook na de inwerkingtreding van de Richtlijn (artikel 41 lid 3 Richtlijn). Dit is echter afhankelijk van de Nederlandse implementatie van deze Richtlijn. Op het moment van het schrijven van deze rapportage is deze implementatiewet nog niet gepubliceerd.

9.1.6.2 Protocolplicht

Op de verantwoordelijke rust een protocolplicht, zo volgt uit artikel 32 Wpg. Op grond van deze protocolplicht dient de politie onder meer de verstrekking van gegevens maar ook de geautomatiseerde vergelijking of combinatie en de hernieuwde verwerking van gegevens vast te leggen. Door de verstrekking van gegevens vast te leggen, kan achteraf de gegevensuitwisseling van politiegegevens worden gecontroleerd. Wanneer de Politie niet aan deze verplichting voldoet, kan de AP een bestuurlijke boete opleggen (artikel 35 lid 3 Wpg).

5.1.2.h

Onder de Richtlijn wordt de protocolplicht die op de politie rust, aangescherpt. Zo dient de politie een uitgebreid register van verwerkingen (artikel 24 Richtlijn) en logbestanden over de verschillende vormen van verwerkingen bij te houden (artikel 25 Richtlijn).

9.1.7 Bewaartermijnen

In de artikelen 8 tot en met 10 Wpg is bepaald wanneer gegevens moeten worden verwijderd. Daarnaast beoogt artikel 14 Wpg te voorzien in een beperkte periode waarin de verwijderde politiegegevens worden bewaard ten behoeve van de afhandeling van klachten en de verantwoording van verrichtingen. Als algemene regel geldt voor gegevens die worden verwijderd op grond van de artikelen 9 en 10 Wpg dat zij moeten worden verwijderd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor zij zijn verwerkt. Gegevens die worden verwijderd, zijn dus niet langer toegankelijk voor operationele doeleinden maar zij worden niet onmiddellijk vernietigd. Deze gegevens worden als het ware apart gezet om er voor te zorgen dat de operatie geen toegang meer heeft tot deze gegevens. In bijzondere gevallen kunnen de gegevens opnieuw beschikbaar komen voor operationeel gebruik.

In de Raffinaderij worden gegevens verwerkt die afkomstig zijn uit bronsystemen. Daarbij is het uitgangspunt dat deze bronsystemen (moeten) voldoen aan de regels omtrent verwijdering uit de artikelen 8 tot en met 10 Wpg. Zodra de bewaartermijn is afgelopen en de gegevens niet meer toegankelijk mogen zijn voor operationele doeleinden zal ook in de Raffinaderij niet meer met deze gegevens worden gewerkt.

Uit de privacy audit politie 2015, over de jaren 2011 tot en met 2014 bleek dat de bewaartermijnen van de gegevens als een van de risicogebieden bestempeld werd en dat zij een onvoldoende scoorde.[76] In het daaropvolgende verbeterplan werd aangekondigd dat de politie eind 2019 "*grotendeels maar nog niet volledig*" aan de wettelijke privacyregels zal voldoen.[77]

9.1.8 Rechten van de betrokkenen

De betrokkene heeft het recht op inzage in de politiegegevens die hem of haar betreffen (artikel 25 Wpg).
Dit recht wordt in de Richtlijn uitgebreid (artikel 14 Richtlijn). Wanneer de betrokkene zijn recht op inzage uitoefent, wordt hij geïnformeerd over:

[76] Minister van Veiligheid & Justitie 2015.

[77] Gegevensautoriteit Nationale Politie 2016, p. 3.

5.1.2.h

- Het doel en de rechtsgrondslag van de verwerking;
- Welke categorieën persoonsgegevens worden verwerkt;
- De ontvangers van de persoonsgegevens;
- Indien mogelijk de bewaartermijn;
- Zijn recht op rectificatie en verwijdering van de gegevens en de mogelijkheid om een klacht in te dienen bij de toezichthouder (artikel 16 en 17 Richtlijn); en
- Alle beschikbare informatie over de oorsprong van de gegevens (artikel 14 Richtlijn).

Onder strikte voorwaarden kan het recht op inzage worden beperkt (artikel 15 Richtlijn).

In de Raffinaderij worden enkel gegevens uit bronbestanden verwerkt waarover een onderzoeksteam normaal gesproken ook zou beschikken. De procedures voor inzage van de verzamelde persoonsgegevens gaan daarom via de normale wegen die daarvoor beschikbaar zijn.

5.1.2.h

10 (Privacy)risico's Raffinaderij

Hieronder wordt een overzicht gegeven van de risico's die verbonden zijn aan het gebruik van de Raffinaderij. Daarbij wordt eerst ingegaan op de risico's die (onzorgvuldige) verwerking van persoonsgegevens met zich mee kunnen brengen. In hoofdstuk 11 wordt vervolgens stil gestaan bij de gevolgen voor de burger (de betrokkene) en voor de politie wanneer de risico's zich daadwerkelijk manifesteren.

Bij het bespreken van deze risico's moet worden aangetekend dat, hoewel het hier een *Privacy Impact Assessment* betreft, de risico's die de gegevensverwerkingen binnen de Raffinaderij met zich mee kunnen brengen soms andere mensenrechtelijke implicaties hebben dan alleen beperkingen of consequenties voor het recht op privacy. Hierbij kan bijvoorbeeld worden gedacht aan het recht op een eerlijk proces. Ook signaleren wij risico's die kunnen ontstaan ondanks dat volledig in lijn met het Wetboek van Strafvordering en de Wet politiegegevens wordt gehandeld. Het betreft in onze ogen nieuwe risico's die nog niet door de wetgever zijn onderkend.

10.1 (Data)Governance

Een goede (data)governance is van essentieel belang in het kader van de Raffinaderij. Hieronder wordt verstaan het zorgdragen voor de juiste verwerking van en een zorgvuldige omgang met persoonsgegevens bij gebruikmaking van de Raffinaderij. Omdat de Raffinaderij uit veel bronnen put en het gebruik van de Raffinaderij een specifieke 'mindset' vraagt, is specifieke borging en sturing binnen de politie daarop noodzakelijk. Omdat de Raffinaderij op dit moment nog de status van pilot heeft, is de inbedding van die sturing binnen de politie begrijpelijkerwijs beperkt. Dit risico wordt in de praktijk opgevangen door de huidige projectleiders van de Raffinaderij (5.1.2.e en 5.1.2.e). De projectleiders hebben een hoog privacybewustzijn en borgen op dit moment ook dat de Raffinaderij niet wordt misbruikt. Wanneer deze projectleiders wegvallen, ontstaat het risico dat ook het privacybewustzijn dat specifiek is benodigd voor de Raffinaderij in de governance verdwijnt. Wanneer de Raffinaderij wordt opgenomen in de bredere organisatie is het daarom van groot belang dat de (data)governance wordt ingericht in lijn met dit hoge privacybewustzijn dat specifiek is gericht op de werking van de Raffinaderij. In hoofdstuk 12 doen wij hiertoe enige aanbevelingen.

5.1.2.h

10.2 Risico's beheer gegevens

Wanneer niet goed wordt omgegaan met het beheer van de gegevens kunnen in het kader van de Raffinaderij risico's ontstaan op het gebied van:

- Traceerbaarheid herkomst en gebruik data (de herkomst van data is goed geregeld in de Raffinaderij);
- Vermenging van data; en
- Vluchtigheid en verandering in bronbestanden;

Deze risico's zullen hieronder worden toegelicht.

10.2.1 Traceerbaarheid herkomst en gebruik data

In de Raffinaderij worden grote hoeveelheden gegevens verwerkt die uit verschillende databronnen afkomstig zijn. Met het oog op de effectiviteit en integriteit van de opsporing is het van belang dat de data die in de Raffinaderij worden verwerkt traceerbaar zijn. Dit betekent dat moet kunnen worden herleid hoe de Raffinaderij en de rechercheur of analist tot een bepaalde uitkomst, het 'eindproduct', zijn gekomen. Wanneer dit niet mogelijk is, is onduidelijk hoe conclusies en acties tot stand zijn gekomen en daarmee is de opsporing niet langer controleerbaar.

Een belangrijk element hierbij is om allereerst de herkomst van gegevens duidelijk te maken (*data provenance)*. De controleerbaarheid van de totstandkoming van het bewijs is van groot belang daar waar politiegegevens worden gebruikt voor de bewijsvoering. De traceerbaarheid van gegevens en het gebruik van de politiegegevens door analisten en mogelijke derden (*event logging*) moet gewaarborgd zijn om op deze wijze de *chain of custody* te bewaren.

10.2.2 Vermenging van data

In het verlengde van het risico op onvoldoende traceerbaarheid van de herkomst en het gebruik van data ligt het risico op vermenging van data. De Raffinaderij biedt de mogelijkheid om politiegegevens te verrijken en combineren. Politiegegevens worden in de Raffinaderij niet inhoudelijk veranderd, noch worden politiegegevens toegevoegd aan de bronbestanden. Wel kan het verrijken en combineren van de politiegegevens uit de bronbestanden nieuwe data of informatie opleveren. Deze informatie is daarmee opgebouwd uit de politiegegevens uit bronbestanden of uit de interpretatie van deze data. Dit is op zichzelf geen probleem, maar het wordt problematisch wanneer dit proces

5.1.2.h

oncontroleerbaar wordt. Door de vermenging van deze data groeit ook het risico op ongewilde openbaarmakingen. Dit kan gebeuren doordat data met een hoge risicoclassificatie vermengd kan raken met data met een lagere risicoclassificatie. Er is sprake van een risicovolle vermenging van data wanneer gegevens onjuist zijn verkregen (zie par. 8.5.2 ten aanzien van de *fruits of the poisonous tree*-doctrine). Een ander voorbeeld van een risicovolle verwerking betreft de vervaging tussen *intelligence* en opsporing (zoals uiteengezet in par. 8.5).

10.2.3 Vluchtigheid en verandering in bronbestanden

Een eigenschap van data is dat zij veranderen, verouderen en verdwijnen. Als dit niet accuraat wordt doorgevoerd in gegevensverwerkingen dan levert dat een risico op. Dit speelt des te meer bij grootschalige informatieverwerking. Aangezien de Raffinaderij politiegegevens uit onderliggende bronnen verkrijgt, is het van belang om controle te houden op de inhoud en de accuraatheid van de politiegegevens in deze bronbestanden en de verwerking en doorwerking daarvan in de Raffinaderij.

10.2.4 Gegevenskwaliteit

Wanneer gegevens niet de juiste kwaliteit hebben, bijvoorbeeld omdat ze incorrect of verouderd zijn, dan levert dit een risico op voor de effectiviteit van de opsporing én de privacy van de betrokkenen.

10.3 Schaalvergroting

De Raffinaderij maakt effectieve informatieverwerking mogelijk in het kader van de opsporing op een schaal die eerder niet te realiseren viel. Deze nieuwe mogelijkheden om gegevens uit verschillende bronnen en onderzoeken te combineren, is een grote kans voor de opsporing maar het kan ook leiden tot ongewenste schaalvergroting.

Doordat het huidige juridische kader en de daarbij horende waarborgen momenteel nog niet toegespitst zijn op al deze nieuwe mogelijkheden wordt door de schaalvergroting het risico op privacy-inbreuken voor burgers groter. De huidige wet- en regelgeving stelt momenteel weinig grenzen aan het geautomatiseerd vergelijken van politiegegevens of aan het combineren van data, behalve voor wat betreft de algemene eis van dataminimalisatie. Dit heeft mogelijk tot gevolg dat de capaciteiten van de politie geen gelijke tred houden met de benodigde *check and balances*.

5.1.2.h

Een ander risico van schaalvergroting is dat in de publieke perceptie het beeld kan ontstaan dat de politie gebruik maakt van allerlei technieken en methodes die te vergelijken zijn met de programma's van bijvoorbeeld de CIA en NSA.

De schaalvergroting doet zich voor op vier aspecten:

- Opbouw historie;
- Datahonger;
- Mission- en function creep; en
- Samenwerkingsverbanden.

Deze vier aspecten zullen hieronder nader worden toegelicht.

10.3.1 Opbouw historie

Een belangrijk aspect van digitale gegevensverwerking is dat historische data even eenvoudig geraadpleegd en doorzocht kan worden als recente data.
Hiermee wordt de privacy impact van het verzamelen van gegevens door de politie per definitie groter dan het geval was in het tijdperk vóór de introductie van voorzieningen als Raffinaderij. Gegevens werden toen bewaard op allerlei lokale systemen, harde schrijven en daarnaast grotendeels op papier. Dit had tot gevolg dat oude documenten en bestanden op een gegeven moment lastiger (of niet meer) raadpleegbaar en doorzoekbaar waren, simpelweg omdat een dossier alleen fysiek beschikbaar was, omdat een bestand lokaal was opgeslagen of alleen beschikbaar was in een specifiek daarvoor gebouwd register.

De introductie van de Raffinaderij en andere, geavanceerde, informatiesystemen heeft gevolgen voor de levensduur van een politiegegeven. Wanneer de gegevens 'technisch' langer en makkelijker toegankelijk worden, neemt de druk op privacy steeds verder toe. Zelfs wanneer de wettelijke bewaartermijnen *an sich* niet langer worden. De wet kent enkele wettelijk vastgelegde bewaartermijnen die niet zomaar veranderen. Toch kan in de praktijk een zekere erosie plaatsvinden van de waarborgen die de wettelijke bewaartermijnen bieden. Dit komt onder andere doordat, bijvoorbeeld in opsporingsonderzoeken, de bewaartermijnen deels afhankelijk zijn van het feit of de politiegegevens nog "nodig zijn voor het doel waarvoor zij zijn verkregen".[78] En die periode kan aanzienlijk zijn:

[78] Artikel 9 Wpg.

- In geval het opsporingsonderzoek heeft geleid tot een vervolging is verwijdering pas aan de orde op het moment dat de rechter ten aanzien van de zaak onherroepelijk heeft beslist;
- Als een zaak niet is opgelost, wordt het onderzoek veelal wel voortgezet maar op een minder intensief niveau. De gegevens kunnen in dat geval nodig blijven voor het vervolg van het onderzoek en voor het geval nieuwe aanknopingspunten worden ontdekt of zich aandienen. Dit laatste is bijvoorbeeld het geval als bij een ander onderzoek gegevens bekend worden die betrekking hebben op dit onderzoek. De gegevens blijven dan doorgaans nodig voor het doel van het onderzoek tot uiterlijk het moment waarop de feiten, waar het onderzoek zich op richt, zijn verjaard.[79]

De toenemende mogelijkheden van *data mining* en de toenemende hoeveelheid digitale sporen die de politie verzamelt, resulteert in een toenemende kans dat er relevante verbanden gevonden kunnen worden tussen gegevens. Hierdoor kan de wens ontstaan om gegevens voor onbepaalde tijd te bewaren omdat zij in de toekomst mogelijk nog relevant gaan worden voor een *data mining* exercitie.

Tenslotte kan de relevantie van historische gegevens worden verlengd door deze in te brengen in andere (lopende) onderzoeken of aan te wenden voor de intelligence taak van artikel 10 Wpg.

10.3.2 Datahonger

De wens om een gepleegd strafbaar feit op te lossen, kan resulteren in het feit dat steeds meer gegevens in een onderzoek betrokken en ingebracht worden. Met name in zaken waar geen concrete aanwijzingen bestaan of waar zaken 'vastzitten', kan de neiging ontstaan om op grote schaal extra gegevensbronnen aan het onderzoek, en dus in de Raffinaderij, toe te voegen in de hoop alsnog een aanwijzing of aanknopingspunt te vinden. Daardoor neemt de kans op een 'bijvangst' toe. Deze zogenoemde *fishing expeditions* of *data dredging* zijn risicovol voor de privacy van betrokkenen omdat de link tussen de politiegegevens en het daadwerkelijk onderzoek steeds vager wordt. Bovendien zijn er in de grote hoeveelheden data altijd wel (sterke en minder sterke) correlaties tussen variabelen te vinden die niets met elkaar te maken hebben.[80]

---

[79] *Kamerstukken II* 2005-2006, 30 327, nr. 3, pp. 16-17.

[80] WRR 2016, p. 83.

10.3.3 Mission- en function creep

De doelbinding is een belangrijk principe in het gegevensbeschermingsrecht. Op grond van dit principe mogen gegevens slechts worden verwerkt voor een duidelijk omschreven doel en moeten zij in principe binnen dezelfde context worden verwerkt. Dit betekent dat de doelen voor de verwerking niet gaandeweg de verwerking mogen verschuiven of geheel mogen wegvallen. Zolang het doel waarvoor informatie wordt verwerkt helder blijft, kan men controleren in hoeverre de gegevens die worden verwerkt daadwerkelijk noodzakelijk zijn en ter zake dienen voor het vervullen van het doel. Daarnaast kan beoordeeld worden in hoeverre de hoeveelheid gegevens die worden verzameld in een bepaald onderzoek proportioneel is en of de hoeveelheid data niet bovenmatig is.

Het doelbindingsprincipe wordt onder druk gezet door de introductie van Business Intelligence voorzieningen in het opsporingsproces. *Data mining* heeft bijvoorbeeld als kenmerk dat de analyses beter worden naarmate er meer gegevens worden gebruikt. Door middel van *data mining* kunnen verbanden worden ontdekt die in papieren dossiers en met het blote oog vermoedelijk niet aan het licht zouden komen. Die verbanden kunnen voor onderzoeken van doorslaggevend belang blijken of de ontdekte verbanden kunnen aanleiding zijn om het zwaartepunt in een onderzoek te verschuiven. Wanneer dat gebeurt, komt de doelbinding onder druk te staan. Immers, een onderzoek naar een specifieke verdachte mag niet zomaar of gaandeweg veranderen in een verkennend onderzoek naar een bepaald fenomeen of strafbaar feit en visa versa. De verleiding om politiegegevens voor een ander doel of een ander onderzoek te gebruiken, zal in de praktijk groot zijn – simpelweg omdat de gegevens beschikbaar zijn en omdat er technische mogelijkheden zijn om snel en effectief de gegevens te verwerken c.q. te analyseren.

In de Raffinaderij is het risico op 'function creep' en 'mission creep' aanwezig. Dit betreft het fenomeen dat systemen zowel qua functionaliteiten als qua toepassingsgebieden steeds verder worden uitgebreid. Zonder dat er een nieuw toetsings- of wegingsmoment door de politie tegenover staat. Daarom is het van belang dat de politie weerstand biedt tegen de verleiding om zich binnen onderzoeken te laten leiden door de technologische mogelijkheden in plaats van door de juridische kaders.

10.3.4 Samenwerkingsverbanden

De kans bestaat dat in de toekomst samenwerkingsverbanden met andere overheidsinstanties worden gezocht. Daarbij kan gedacht worden aan instanties als de FIOD, Douane, AIVD of MIVD.

5.1.2.h

De Wet politiegegevens stelt duidelijke kaders aan de incidentele en structurele verstrekking van gegevens door de politie aan derden. Ondanks de nieuwe mogelijkheden die de Raffinaderij technisch gezien biedt voor informatie-uitwisseling, is het van belang dat de eisen van de Wpg als basis voor de verwerking en verstrekking van politiegegevens worden nageleefd. Met andere woorden, wanneer de politie politiegegevens met derden, bijvoorbeeld in samenwerkingsverbanden, deelt, dient er specifiek aandacht te worden besteed aan de vereisten omtrent deze gegevensuitwisseling.

Een samenwerkingsverband kan tot gevolg hebben dat gegevensbestanden uit andere dan politiebronnen en –domeinen worden toegevoegd en verwerkt in het kader van de Raffinaderij. Bovendien neemt de schaal van verwerking verder toe en bestaat het risico dat traditionele 'schotten' (van technische en juridische aard) tussen de verschillende organisaties verdwijnen waardoor waarborgen voor de bescherming van de persoonlijke levenssfeer van de betrokkenen minder worden.

10.4 Beveiligingsincidenten en datalekken

De beveiliging van de politiegegevens wordt steeds belangrijker omdat deze gegevens op grote schaal worden opgeslagen, gekoppeld en geanalyseerd. Naarmate er meer bronnen worden ontsloten in de Raffinaderij, de Raffinaderij breder ingezet gaat worden (op meer thema's en/of op meer onderzoeken) en meer personen toegang krijgen tot de Raffinaderij, neemt de kans op en de impact van datalekken en beveiligingsincidenten toe. Dit risico speelt ook wanneer meer gegevens uit databronnen in de Raffinaderij worden ingeladen. Ook de impact van een mogelijk incident kan hierdoor toenemen.

Doordat grote hoeveelheden de politiegegevens in en via de Raffinaderij beschikbaar zijn, worden de nodige eisen gesteld aan de beveiliging. Wanneer de beveiliging van de Raffinaderij niet op orde is, zouden deze gegevens beschikbaar kunnen worden voor onbevoegden. Door een datalek kunnen bijvoorbeeld grote hoeveelheden zeer gevoelige informatie op straat kunnen komen te liggen.

5.1.2.h

10.5 Inzet externe leveranciers

Op het moment van schrijven van deze rapportage wordt gewerkt met Palantir, een Amerikaanse software-oplossing. Samenwerking met externe leveranciers heeft als mogelijk risico dat derden (uit een vreemde mogendheid) toegang krijgen tot de data.

10.6Transparantie en controleerbaarheid

Omdat met behulp van de Raffinaderij gigantische hoeveelheden gegevens worden geanalyseerd, is het voor een buitenstaander moeilijk te doorgronden hoe gegevens worden gecombineerd, verbanden worden gelegd enzovoorts. Dit roept vragen op met betrekking tot de reproduceerbaarheid en herleidbaarheid van opsporingshandelingen. Transparantie in de zin van controleerbaarheid is een noodzakelijke voorwaarde voor een eerlijk proces. Het is dan ook van belang dat alle handelingen goed gelogd worden en dat er een duidelijke *chain of custody* bestaat die ook kan worden gecontroleerd.

Een andere aspect dat speelt in het kader van transparantie en controleerbaarheid is de informatie asymmetrie tussen politie en OM en de verdediging. Daar waar de politie het vraagstuk van *information overload* kan adresseren door gebruik te maken van de Raffinaderij is het de vraag hoe de verdediging hiermee om moet gaan. Zij hebben immers niet dezelfde mogelijkheden en kennis als de politie van de Raffinaderij. Dit bemoeilijkt de taak van de verdediging om de juistheid van de Raffinaderij analyses te controleren en betwisten.

10.7Risico's van mogelijke uitbreiding inzet Raffinaderij

Op het moment van schrijven van deze rapportage is er een discussie gaande met betrekking tot de vraag voor welke type of soort opsporingsonderzoeken of verwerkingen de Raffinaderij in de toekomst gebruikt kan worden. De mogelijkheden de Raffinaderij lijken onbegrensd. Er moeten echter duidelijke keuzes worden gemaakt voor wat betreft de inzet van de Raffinaderij.

Het gebruik van de Raffinaderij kan op twee manieren worden uitgebreid. Enerzijds door de Raffinaderij in te zetten voor meer soorten opsporingsonderzoeken. Anderzijds zou het in potentie mogelijk zijn om de Raffinaderij in te zetten voor *predictive policing* (op basis van *data mining* en *profiling*). Uitbreiding brengt bepaalde risico's met zich mee. Hieronder zal nader hierop worden ingegaan.

5.1.2.h

10.7.1 Uitbreiding naar andere opsporingsonderzoeken

Op dit moment wordt de Raffinaderij gebruikt voor onderzoeken ten aanzien in het kader van liquidaties, contraterrorisme en MH17. Het is mogelijk dat de politie in de toekomst de Raffinaderij wil inzetten voor andere vormen van zware criminaliteit of ondermijning.[81] Dergelijke uitbreiding van het gebruik van de Raffinaderij kan de risico's beschreven in dit hoofdstuk vergroten (omdat de kans toeneemt of het gevolg groter is).

10.7.2 Het gebruik van de Raffinaderij voor predictive policing

Daarnaast is een uitbreiding van het gebruik van de Raffinaderij mogelijk doordat de Raffinaderij wordt ingezet voor *data mining* en *profiling* met als doel *predictive policing* mogelijk te maken. De Raffinaderij wordt op dit moment niet ingezet voor dit doel. De technische mogelijkheden hiertoe bestaan echter wel. Daarom wordt er op deze plaats aandacht besteed aan de mogelijke risico's van deze vorm van (Big) data analyse.

Net als voor wat betreft de uitbreiding van het gebruik van de Raffinaderij naar andere opsporingsonderzoeken blijven de risico's die in de voorgaande paragrafen zijn beschreven onverkort bestaan. Daarnaast zorgen deze vormen van big data analyse voor risico's met een specifieke impact op de betrokkene. Dit wordt apart besproken in het volgende hoofdstuk.

[81] Hierbij kan gedacht worden aan mensenhandel, grootschalige drugshandel, kinderporno, wapenhandel, ontvoeringen van kinderen enzovoorts.

5.1.2.h

11 Impact bij manifestatie privacyrisico's

In dit hoofdstuk wordt ingegaan op de mogelijke effecten voor zowel de burger als voor de politie indien onzorgvuldig wordt omgegaan met de privacy van betrokkenen of als zich de risico's uit het voorgaande hoofdstuk voordoen.

Hoewel deze rapportage een Privacy Impact Assessment behelst en wij de werkwijze van de Raffinaderij primair toetsen aan het kader van het recht op privacy van de burger, vinden wij het van groot belang om stil te staan bij het feit dat een manifestatie van privacyrisico's gevolgen kan hebben voor andere belangrijke fundamentele rechten van de burger.

Daarnaast willen wij hier benadrukken dat niet alle gevolgen zich daadwerkelijk zullen voordoen wanneer onzorgvuldig met de privacy van een betrokkene wordt omgegaan of wanneer zich een privacyrisico manifesteert.

11.1Impact op de burger

De burger kan zich geconfronteerd zien met meerdere gevolgen of effecten wanneer een van de privacyrisico's, zoals beschreven in hoofdstuk 10, zich manifesteert. Deze gevolgen hebben niet alleen effect op het recht op privacy van de burger, een manifestatie van deze risico's kan ook gevolgen hebben op andere, fundamentele rechten van de burger.

11.1.1 Onvrijwillige en ongewenste openbaarmaking

Bij elke gegevensverwerking bestaat het risico dat gegevens in de handen vallen van (kwaadwillende) derden, bijvoorbeeld omdat gegevens kwijtraken of buit worden gemaakt. De mogelijke gevolgen daarvan voor de betrokkene zijn afhankelijk van de aard van de gegevens en de hoeveelheid gegevens die worden verwerkt. Naast aantasting van de privacy van de betrokkene (omdat het publiek mogelijk kennis kan nemen van de politiegegevens) kan het lekken van politiegegevens ook leiden tot misbruik, zoals fraude, identiteitsdiefstal of afpersing. Daarnaast kan verlies van gegevens leiden tot stigmatisering van de betrokkene of een bepaalde groep.

Het risico op ongewilde openbaarmaking neemt toe wanneer BI-voorzieningen onderlinge verbanden leggen tussen de verschillende politiegegevens waardoor verrijkte data met een diffuus karakter kunnen ontstaan. Hierdoor ontstaat informatie die deels uit vertrouwelijke informatie is opgebouwd, bijvoorbeeld informatie van informanten, en deels uit openbare informatie. Het risico op ongewilde openbaarmaking neemt toe naarmate het moeilijker is om terug te voeren welke data waar vandaan zijn gekomen en wat de status, in termen

van gevoeligheid en vertrouwelijkheid, is van de nieuwe informatie die uit deze data ontstaat. Dit risico speelt ook in de context van de Raffinaderij. Een voorbeeld hiervan is wanneer een verdachte in een rechtszaak wordt geconfronteerd met bewijs dat is verkregen uit of door middel van de Raffinaderij en waarin onverhoopt gegevens staan die voor de verdachte herleidbaar zijn tot een informant. De impact dat informatie herleidbaar is tot een informant is bij het huidige gebruik van de Raffinaderij beperkt doordat de Raffinaderij niet gebruik maakt van informatie van informanten. Indien informanten informatie in de toekomst wel gebruikt wordt, bestaat wel de kans dat informatie tot de informant herleidbaar is.

11.1.2 Aantasting persoonlijke autonomie

Het recht op privacy geeft de betrokkene een ruimte voor zichzelf waar hij of zij ongestoord zichzelf kan zijn. Deze ruimte vormt ook een barrière tegen onrechtmatige inmenging door anderen, zoals door de politie of de staat. Het recht op privacy biedt als het ware een schild tegen ongeremde machtsuitoefening door anderen en beschermt daarmee de autonomie van de betrokkene.

In hoeverre de Raffinaderij de persoonlijke autonomie van betrokkenen aantast, is niet eenduidig te zeggen. Dit is afhankelijk van het concrete gebruik van de Raffinaderij en de in acht genomen waarborgen zoals vastgelegd in het Europees Verdrag voor de Rechten van de Mens, het Handvest van de Grondrechten van de EU de Nederlandse Grondwet, de Richtlijn 2016/680, het Wetboek van Strafvordering en de Wet Politiegegevens.

In het algemeen kan wel worden gezegd dat hoe meer gegevens de politie verzamelt en vastlegt over de betrokkenen, hoe sterker de machtspositie van de politie wordt ten opzichte van haar burgers. Wanneer zich tegelijkertijd ook de data-analysemogelijkheden aan de kant van de politie sterk ontwikkelen, verschuift de machtsbalans verder richting de staat. Het belang om waarborgen ter bescherming van de privacy van betrokkenen te treffen, neemt dan verder toe.

In het verleden werd de hoeveelheid verwerkte data al snel beperkt door de grenzen die aan de opslagcapaciteit, de beschikbare capaciteit van medewerkers en de beschikbare tijd waarbinnen onderzoeken afgerond moesten worden. Deze waarborg uit het fysieke tijdperk dwong in de praktijk tot afbakening. Door (onder andere) de Raffinaderij valt deze waarborg in het informatietijdperk langzaam weg. Technische mogelijkheden worden onbegrensd. Het optreden van de politie wordt in potentie onbegrensd wanneer bijvoorbeeld *data mining* wordt uitgevoerd vanuit de visie dat hetgeen technisch mogelijk is met beschikbare data ook daadwerkelijk wordt gedaan. Dit kan afbreuk doen aan de

persoonlijke autonomie van de betrokkene, namelijk om te veranderen en om andere keuzes te maken dan die in het verleden.[82] Aantasting van de persoonlijke autonomie is met name een risico bij grootschalige verwerkingen en geautomatiseerde besluitvorming of geautomatiseerde vergelijking van persoonsgegevens.

11.1.3 Fair trial

Door de enorme verwerkingscapaciteit aan de kant van de politie en het Openbaar Ministerie wordt het voor de verdediging lastiger om toegang te krijgen tot het bewijsmateriaal dat door de politie en het Openbaar Ministerie is verkregen en verwerkt. Het risico bestaat dat de politie en het Openbaar Ministerie bewust of onbewust de verdediging 'onder papierwerk bedelven'. De verdediging beschikt immers niet over dezelfde geavanceerde analysemethoden en –middelen. Dit kan op gespannen voet staan met het recht op een eerlijk proces, zoals neergelegd in artikel 6 EVRM (*equality of arms*).

11.1.4 Rechtsonzekerheid door open en vage normen

In dit rapport is een aantal ontwikkelingen gesignaleerd waarvan de juridische situatie nog niet duidelijk is, bijvoorbeeld het terrein van OSINT (zie par. 4.4). Dit levert zowel voor de burger als voor de politie rechtsonzekerheid op, met name zolang er geen jurisprudentie bestaat of een gezaghebbende uitspraak door een minister is gedaan. Tot die tijd blijft het een interpretatie van de politie, het Openbaar Ministerie of betrokken externe privacyadviseurs in hoeverre een bepaalde handeling of werkwijze binnen de juridische kaders valt.

11.1.5 Onnauwkeurigheid

Bij de inzet van de Raffinaderij kunnen onnauwkeurigheden optreden, bijvoorbeeld wanneer gegevens van onschuldige burgers worden verwerkt en dit ten onrechte tot een verdenking leidt. Er is dan sprake van een zogenoemde 'vals positief'. Bij een valse positief geeft een uitkomst ten onrechte aan dat een bepaalde conditie aanwezig is.[83] Dit risico bestaat met name wanneer niet naar een concrete verdachte onderzoek wordt gedaan maar wanneer onderzoek wordt gedaan met behulp van risicoprofielen of naar groepen van betrokkenen.

Er geldt dan ook een verhoogd risico op 'doorwerkfouten' in het kader van gegevensverwerkingen binnen de Raffinaderij. Met andere woorden, dat er onjuiste gegevens verwerkt worden die niet (tijdig) zijn of worden gecorrigeerd of gewijzigd.

[82] WRR 2016, p. 89.

[83] WRR 2016, p. 84.

Wanneer die onjuiste gegevens vervolgens verwerkt worden in het kader van onderzoeken of complexe *data mining* processen kan dit ongewenste gevolgen hebben voor de betrokkene. Daarnaast bestaat het risico van vermenging van juiste met onjuiste gegevens wanneer gegevens die juist zijn, worden verrijkt met onjuiste gegevens. Daarmee ontstaat een nieuw data-element waarin juiste en onjuiste gegevens vermengd zijn. Analyses kunnen inmiddels zo snel worden gedaan worden dat verschillende feiten en data-elementen mogelijk al met elkaar gecombineerd zijn voordat de oorspronkelijke gegevens gerectificeerd kunnen worden. Voor de betrokkene betekent een dergelijke situatie ook dat een eventueel beroep op zijn of haar recht op herstel van onjuiste gegevens bemoeilijkt wordt indien de fouten nauwelijks meer traceerbaar zijn.

11.1.6 Gevolgen van een inbreuk op de beveiliging

De beveiliging van data is erg belangrijk doordat gevoelige data op grote schaal worden verzameld, opgeslagen, verrijkt en gekoppeld. Naarmate meer data uit meer bronnen worden gehaald en naarmate de Raffinaderij voor meer onderzoeken wordt ingezet, neemt het risico op datalekken en beveiligingsincidenten toe.[84]

Voor de burger betekent dit dat sprake kan zijn van onvrijwillige en ongewenste openbaarmaking van gegevens die hem of haar betreffen (zie par. 11.1.1). Omdat onbekend is waar gelekte gegevens terecht komen, is het goed mogelijk dat een betrokkene zich jaren na een dergelijk datalek geconfronteerd ziet met nadelige consequenties.

11.2Impact op de politie

Risico's die voortvloeien uit de onzorgvuldige omgang met politiegegevens bij het gebruik van de Raffinaderij hebben naast mogelijk negatieve gevolgen voor burgers ook hun weerslag op politie en justitie als geheel. In de onderstaande paragrafen zijn de afbreukrisico's voor de politie (en het Openbaar Ministerie) beschreven.

11.2.1 'Stuk gaan' zaken

Onzorgvuldig of onrechtmatig gebruik van de Raffinaderij kan er in resulteren dat een zaak voor de rechter 'stuk gaat'. Wanneer de verzameling van de politiegegevens op onrechtmatige wijze heeft plaatsgevonden, kan dit gevolgen hebben bij de terechtzitting. Het Openbaar Ministerie kan, als uiterste consequentie, niet ontvankelijk worden verklaard ten gevolge van grove vormverzuimen (artikel 359a lid 1 sub c Sv over de verzuim van

[84] WRR 2016, p. 87.

vormen in het voorbereidend onderzoek). Dit is echter uitzonderlijk.[85] Het ligt eerder in de lijn der verwachtingen dat bewijs wordt uitgesloten in een procedure, maar dit is afhankelijk van de omstandigheden van het geval (artikel 359a lid 1 sub b Sv).

Bewijsuitsluiting kan enkel worden toegepast wanneer een belangrijk (strafvorderlijk) voorschrift of rechtsbeginsel in aanzienlijke mate is geschonden door de onrechtmatige bewijsgaring.[86] In navolging van de jurisprudentie van het EHRM stelt de Hoge Raad dat een beroep op schending van artikel 8 EVRM (bescherming van de persoonlijke levenssfeer) niet automatisch ook een schending van artikel 6 EVRM (recht op een eerlijk proces) met zich meebrengt. Dit betekent dat ook al is bewijsmateriaal in strijd met artikel 8 EVRM verzameld, het gebruik van dat materiaal niet (zonder meer) leidt tot een oneerlijk proces.[87] Het zal dus afhangen van de omstandigheden van het geval of bewijsmateriaal, dat in het kader van de Raffinaderij op onzorgvuldige wijze is verzameld of verwerkt, wordt uitgesloten in een procedure. Hierbij moet worden opgemerkt dat de Raffinaderij zelf geen bewijs genereert. De Raffinaderij maakt het mogelijk om, op basis van bronbestanden, relevante gegevens en informatie te vinden in de grote hoeveelheden data die beschikbaar zijn. Vervolgens moeten de rechercheur en de analist de gevonden uitkomsten controleren en verifiëren.

Het stuk gaan van zaken is niet alleen een risico voor de procesgang, zij kan mogelijk ook de reputatie van de politie en het Openbaar Ministerie aantasten. Hierdoor kan de indruk bij het publiek worden gewekt dat onrechtmatig verkregen bewijs wordt 'witgewassen' door het (via omwegen) in een ander onderzoek te gebruiken.

11.2.2 Toezicht en hogere compliancekosten

De toezichthouder op de Wet politiegegevens de AP. De AP kan ambtshalve handhaven, bijvoorbeeld naar aanleiding van klachten van betrokkenen. Bovendien kan bestuursdwang volgen wanneer onregelmatigheden bij de verwerking van politiegegevens in het kader van de Raffinaderij worden geconstateerd.

Daarnaast kan de AP de verantwoordelijke die handelt in strijd met de Wpg een bestuurlijke boete opleggen (art. 35 lid 3 Wpg juncto Wbp). Onder de Richtlijn staat het lidstaten vrij

[85] Corstens 2014, p. 817 en pp. 828-829.

[86] HR 30 maart 2004, *NJ* 2004, 376 (Afvoerpijp) waarin algemene regels voor de toepassing van artikel 359a Sv worden gegeven en HR 19 februari 2013, ECLI:NL:HR:2013:BY5321, *NJ* 2013, 308.

[87] Corstens 2014, p. 831.

om zelf te bepalen op welke wijze naleving van de bepalingen wordt gehandhaafd (art. 46 lid 1 sub a Richtlijn).

Tot op heden heeft de AP, voor zover bekend, nog niet structureel gehandhaafd op non-compliance met de Wpg. Wel is door de Auditdienst Rijk een privacy audit Wpg gedaan in 2015. In deze audit scoorde de politie slecht voor wat betreft de naleving van de Wpg.[88]

Contact met de toezichthouder en verscherpt toezicht leiden over het algemeen tot hogere compliance kosten.

11.2.3 Terughoudendheid binnen de organisatie om gegevens te delen

Zoals hierboven is beschreven, kan een onzorgvuldige omgang met gegevens binnen de Raffinaderij ertoe leiden dat de rechter in specifieke gevallen gegenereerd bewijs uitsluit in strafzaken (zie par. 8.5.2 en par. 11.2.1). Wanneer er discussie ontstaat over de vraag of het verwerken van gegevens door middel van de Raffinaderij wel geheel conform de regels is, bijvoorbeeld omdat elementen van het bewijs gegenereerd zijn op basis van gegevens die niet op de juiste wijze zijn verzameld c.q. in het 'systeem' terecht zijn gekomen, bestaat de kans dat er binnen de politie en binnen het Openbaar Ministerie terughoudendheid ontstaat ten aanzien van het delen van informatie en het gebruik van de Raffinaderij.

Momenteel wordt er in de Raffinaderij geen CI-informatie (artikel 10 Wpg) of informanten-informatie (artikel 12 Wpg) opgeslagen. Indien dergelijke informatie in de toekomst wel in de Raffinaderij beschikbaar is, kan een dergelijke vrees om gegevens te delen in het kader van de Raffinaderij ook ontstaan wanneer gevoelige politiegegevens, zoals gegevens over informanten,[89] door een onbewuste combinatie bekend kunnen worden en binnen de Raffinaderij gemakkelijk toegankelijk zijn. Met name de TCIs kunnen terughoudender worden met het delen van gegevens.

11.2.4 Terughoudendheid bij derden om gegevens te delen

Derden die informatie aan de politie verstrekken, zoals bedrijven die vrijwillig gegevens afstaan of informanten,[90] kunnen terughoudender worden in het delen van informatie. Deze terughoudendheid kan ontstaan door de toenemende mogelijkheden van de politie om

[88] Auditdienst Rijk (2015), *Privacy Audit WPG politie*, 29 oktober 2015, kenmerk ADR 2015 1306.

[89] Deze problematiek spelt niet in het huidige gebruik van de Raffinaderij. De Raffinaderij verwerkt namelijk geen gegevens die afkomstig zijn van informanten.

[90] Deze problematiek speelt niet in het huidige gebruik van de Raffinaderij. De Raffinaderij verwerkt namelijk geen gegevens die afkomstig zijn van informanten.

personen aan informatie te koppelen, maar ook als gevolg van de wetenschap dat gegevens in diverse typen onderzoek gebruikt kunnen worden en dat gegevens in de toekomst beschikbaar blijven voor de politie. Dit risico kan versterkt worden wanneer sprake is van een ongewilde openbaarmaking, bijvoorbeeld door datalekken.

11.2.5 Politieke aandacht - Kamervragen

De politiek kan uit eigen beweging vragen stellen ten aanzien van de gegevensverwerkingen en het gegevensbeheer binnen de politie. Deze aandacht kan het gevolg zijn van berichtgeving in de media of volgen naar aanleiding van signalen uit de publieke opinie (zie par. 11.2.6) en mogelijk afbreuk doen aan het imago van de politie als organisatie en over de wijze waarop zij met politiegegevens omgaat. Overigens hoeft de aandacht niet per definitie negatief te zijn. Politieke druk kan ook leiden tot noodzakelijke aanpassingen in wetgeving en veranderingen binnen de politieorganisatie.

11.2.6 Perceptie en publieke opinie

De burger verwacht dat de politie zorgt voor hun veiligheid, de orde handhaaft, misdaad voorkomt en de gevolgen van misdaad zo veel mogelijk beperkt. Ook in het digitale tijdperk waarin we nu leven. Internet en het gebruik van sociale media zorgen er voor dat mensen tegenwoordig zelf goed en snel geïnformeerd zijn en zij verwachten dat de politie minimaal hetzelfde weet en daarop (pro)actief, snel en effectief optreedt en daarvoor adequate middelen ter beschikking heeft. Aan de andere kant heerst er bij de burger ook angst voor Big Brother-scenario's. Zeker nu er met de introductie van nieuwe technologieën, zoals camera-toezicht, tracking van devices, kentekenregistratie en *artificial intelligence* steeds meer mogelijk wordt. Ook wordt er vanuit de politiek steeds meer aandacht besteed aan de inzet van deze technologieën.[91]

De schandalen van de afgelopen jaren rondom de afluisterpraktijken van de NSA, zoals *PRISM*, *Boundless Informant* en *Upstream*, hebben ervoor gezorgd dat er veel publieke aandacht is gekomen voor de werkwijze en de informatieverwerking door zowel opsporings- als inlichtingen- en veiligheidsdiensten. In maart 2017 nog zijn tienduizenden geheime CIA-documenten over technieken voor bijvoorbeeld het hacken van aan het internet verbonden apparaten gelekt (misbruik van de zogenoemde *zero days*).[92] De

[91] Solon 2017.

[92] MacAskill, Thielman & Oltermann 2017. In de Tweede Kamer werden in maart 2017 kritische vragen over deze *zero days* gesteld, Beantwoording van de Kamervraag van leden Voortman (GL) en van Raak (SP) aan de Minister van Buitenlandse Zaken en de Minister van Binnenlandse Zaken

mogelijke impact van de in opspraak geraakte handelswijze van de (Amerikaanse) inlichtingendiensten moet niet worden onderschat. De onthullingen hebben in Europa geleid tot meerdere kritische en fundamentele uitspraken van hoge Europese rechters geleid. Zo is bijvoorbeeld de Safe Harbour overeenkomst die de Europese Commissie met de Verenigde Staten had afgesloten, afgeschoten. In de Nederlandse politiek worden ook steeds meer kritische vragen over de inzet van dergelijke technologieën gesteld.

Hoewel de context van de opsporing en het gebruik van Raffinaderij wezenlijk anders is dan die van de (in opspraak geraakte handelswijze van de) Amerikaanse Inlichtingendiensten moet de mogelijke impact van dergelijke ontwikkelingen niet worden onderschat. Niet in de laatste plaats omdat één van de centrale software componenten van de Raffinaderij, Palantir, ook door deze diensten wordt gebruikt.

Bovenstaande ontwikkelingen kunnen leiden tot een negatieve beeldvorming over de Raffinaderij. Wanneer de verdere uitbouw en de toepassing van de Raffinaderij niet (geheel) conform de wet gebeurt, zal in de publieke opinie een dergelijke inrichting of werkwijze (terecht) weerstand oproepen. Een (al dan niet terecht) beeld kan afbreuk doen aan de Raffinaderij en aan het imago van en het vertrouwen in de politie als geheel. Ook kan het vervolgens een weerslag hebben op de manier waarop rechters en advocaten omgaan met het bewijs dat door de politie is vergaard en gepresenteerd. Daarom is het belangrijk dat niet alleen wordt voldaan aan de juridische eisen maar dient de politie ook rekening te houden met de publieke opinie.

Bij continuering en implementatie van de Raffinaderij binnen de politie is de kans aanwezig dat via bijvoorbeeld een WOB-verzoek inzicht zal worden gevraagd in de werkwijze en de gang van zaken in de Raffinaderij. Natuurlijk zijn er bepaalde uitzonderinggronden opgenomen in de WOB waardoor in bepaalde gevallen het verstrekken van informatie kan worden geweigerd of beperkt (artikel 10 WOB), maar het kan gebeuren dat naar aanleiding van een WOB-verzoek openheid van zaken moet worden gegeven ten aanzien van de Raffinaderij. Dit brengt communicatie- en politieke risico's mee voor de politie.

---

en Koninkrijksrelaties aangaande het bericht dat de CIA kwetsbaarheden in met het internet verbonden apparaten misbruikt, d.d. 9 maart 2017, nummer 2017Z03599, beschikbaar via: https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2017Z03599&did=2017D07392.

5.1.2.h

11.3Impact van mogelijk toekomstig gebruik

Op het moment van schrijven van deze rapportage is er een discussie gaande met betrekking tot de vraag voor welke type en soort opsporingsonderzoeken of verwerkingen de Raffinaderij in de toekomst gebruikt zal en kan gaan worden. De mogelijkheden van de inzet van de Raffinaderij lijken onbegrensd. Er moeten echter duidelijke keuzes worden gemaakt voor wat betreft de inzet van de Raffinaderij.

Het gebruik van de Raffinaderij kan op twee manieren worden uitgebreid. Enerzijds kan de Raffinaderij worden ingezet voor meer soorten opsporingsonderzoeken, anderzijds is het mogelijk om de Raffinaderij in te zetten voor Big Data-analyses.

Uitbreiding brengt bepaalde risico's met zich mee. Hieronder zal daar nader op worden ingegaan.

11.3.1 Uitbreiding naar andere opsporingsonderzoeken

Zoals eerder beschreven, wordt de Raffinaderij op dit moment gebruikt voor onderzoeken ten aanzien in het kader van liquidaties, contraterrorisme en MH17. Het is mogelijk dat de politie in de toekomst de Raffinaderij wil inzetten voor andere vormen van zware criminaliteit of ondermijning.[93]

Dergelijke uitbreiding van het gebruik van de Raffinaderij heeft veel van de in de voorgaande paragrafen genoemde risico's tot gevolg. Sommige risico's zullen groter en urgenter worden doordat schaalvergroting plaatsvindt. Ook neemt het risico op datalekken automatisch toe naarmate er meer gegevens in de Raffinaderij gecombineerd worden of naarmate meer personen geautoriseerd zijn om toegang te krijgen tot de Raffinaderij en hier verwerkingen uit te voeren. Uitbreiding van het gebruik van de Raffinaderij voor andere opsporingsonderzoeken kan verschillende afbreukrisico's met zich meebrengen. Deze afbreukrisico's zullen zich bij een dergelijk gebruik van de Raffinaderij eerder manifesteren doordat potentieel op grotere schaal (gevoelige) politiegegevens worden verwerkt. Dit kan grote gevolgen hebben voor de rechten van de burger.

[93] Hierbij kan gedacht worden aan mensenhandel, grootschalige drugshandel, kinderporno, ontvoeringen van kinderen enzovoorts.

5.1.2.h

11.3.2 Het gebruik van de Raffinaderij voor Big Data-analyses

Daarnaast is een uitbreiding van het gebruik van de Raffinaderij mogelijk doordat de Raffinaderij wordt ingezet voor Big Data-analyses van politiegegevens. De Raffinaderij kan in theorie worden gebruikt voor *profiling*-doeleinden of geautomatiseerde besluitvorming.

In de publieke opinie en perceptie kan zo'n uitbreiding (of zelfs een veronderstelde uitbreiding) weerstand oproepen. De Raffinaderij wordt mogelijk gezien als een alwetende *Big Brother*. Dit kan leiden tot politieke aandacht, bijvoorbeeld in de vorm van Kamervragen. Ook kunnen dergelijke signalen aanleiding zijn voor de Autoriteit Persoonsgegevens om zich met de Raffinaderij bezig te houden en mogelijk toezicht te houden.

Daarnaast is het mogelijk dat er zowel binnen de politie als bij derde partijen een terughoudendheid ontstaat om gegevens te delen ten behoeve van de Raffinaderij. Tenslotte moet worden opgemerkt dat het gebruik van Big Data-analyses nog geen beproefde methode in een procedure voor de rechter is.

11.3.2.1 Gevolgen van gebruik Big Data-technieken (predictive policing)

De Raffinaderij zou technisch doorontwikkeld kunnen worden om Big data-analyses uit te voeren. Big Data-analyses kunnen dienen voor ondersteuning van (geautomatiseerde) besluitvorming. Ook zou de Raffinaderij dan ingezet kunnen worden om profielen van betrokkenen op te stellen. Deze technieken kunnen gebruikt worden om pro-actief op te sporen en aldus criminaliteit te voorkomen (*predictive policing*).

Het is van belang om op te merken dat er momenteel géén plannen bestaan om dergelijke analyses met behulp van de Raffinaderij uit te voeren. Dit neemt niet weg dat wij op deze plek stil willen staan bij de mogelijke risico's die een dergelijk gebruik opleveren, puur en alleen omdat de Raffinaderij de technische mogelijkheid biedt om zulke analyses te doen. Daarnaast is het van belang om op te merken dat het niet gezegd is dat de onderstaande risico's zich daadwerkelijk zullen manifesteren.

Big data-analyses en geautomatiseerde besluitvorming kunnen allerlei nadelige gevolgen voor de betrokkene hebben. Deels komen deze negatieve gevolgen overeen met de hierboven genoemde consequenties voor de betrokkene.

5.1.2.h

Het doel van *predictive policing* is op basis van historische data voorspellingen te doen over de toekomst. Wanneer de data echter incorrect of *biased* zijn, en deze vervolgens gecombineerd worden met andere gegevens, kan dit tot onjuiste uitkomsten leiden.[94] Wanneer aan deze uitkomsten vervolgens conclusies en acties worden verbonden, kan dit (zeer) nadelige gevolgen voor de betrokkene hebben. Een betrokkene kan bijvoorbeeld worden aangemerkt als verdachte in een zaak omdat hij in een bepaald profiel valt of zich in een bepaalde omgeving bevond terwijl hij of zij niets met de zaak te maken heeft. Daarom is het van belang dat niet blind op data vertrouwd wordt, noch dat blind gevaren wordt op de uitkomsten van dergelijke analyses.

Afhankelijk van de data die in de Raffinaderij verwerkt worden, kunnen analyses (in de toekomst) plaatsvinden dat met behulp van **zachte data**. Voorbeelden van dergelijke zachte data zijn data over online gedrag, normen en taalgebruik. Wanneer deze gegevens voor profiling worden gebruikt, vraagt dit om meer duiding en interpretatie. Immers, het gebruik van zachte gegevens in plaats van harde gegevens kan zonder een dergelijke duiding tot verkeerde conclusies leiden.[95]

Daarnaast kan **sociale stratificatie** plaatsvinden.[96] Dit betekent dat groepen in maatschappelijke lagen worden ingedeeld waar tussen ongelijkheid bestaat. Een dergelijke indeling kan een impact hebben op zowel de groepen als op de individuen in deze groepen. Groepen kunnen worden gediscrimineerd, bijvoorbeeld op etniciteit of religie. Sociale stratificatie wordt extra problematisch wanneer zij gebaseerd is op incorrecte data. Profielen en de op basis van profielen getrokken conclusies kunnen leiden tot **stigmatisering** van betrokkenen en groepen en zij kunnen leiden tot bevestiging van **stereotypes**. Het is voor een betrokkene zeer lastig om aan een dergelijk stereotype te ontkomen.[97] Daarbij kan het gebeuren dat een bepaalde conclusie over een groep klopt, maar dat de betrokkene in kwestie de uitzondering hierop is.[98] Daarnaast kan het gebeuren dat betrokkenen zich gaan gedragen naar de uitkomsten van bepaalde beslissingen en profielen. Er is dan sprake van **normalisatie**. Dit heeft een weerslag op de autonomie en de persoonlijke ontwikkeling van de betrokkene (zie par. 11.1.2).

---

[94] WRR 2016, p. 89.

[95] WRR 2016, p. 63.

[96] WRR 2016, p. 12.

[97] WRR 2016, p. 112 en Schermer 2013, p. 139.

[98] WRR 2016, p. 24.

Het gebruik van big data-analyses kan er ook toe leiden dat een individu beoordeeld wordt op basis van **probabilistische kennis**. Deze kennis wordt vergaard op basis van correlaties en interferenties en geeft aan wat individuen misschien zullen doen, in plaats van op basis van wat individuen daadwerkelijk hebben gedaan. Dit kan afbreuk doen aan de autonomie van de mens: dat hij of zij in staat is om te veranderen en om andere keuzes te maken dan die uit het verleden (zie par. 11.1.2).

Geautomatiseerde besluitvorming kan ten slotte ***chilling effects*** hebben. De betrokkene voelt zich niet meer vrij om zich te gedragen zoals hij of zij dat wenst. Daarom past hij of zij (onbewust) het gedrag aan. Het chilling effect kan daarmee eveneens grote gevolgen hebben op de autonomie van de betrokkene (zie par. 11.1.2).[99] Bovendien kan het zijn dat de betrokkene zich niet meer uitlaat zoals hij of zij dat wil. Daarmee beperkt de betrokkene zichzelf in zijn of haar recht op vrijheid van meningsuiting en in zijn of haar recht op keuzevrijheid. Dit kan er vervolgens toe leiden dat de democratische samenleving onder druk komt te staan.

11.3.2.2 Gebrek aan informatie en controle

Doordat de betrokkene op het moment van verzameling van de gegevens niet geïnformeerd wordt over de mogelijke doelen van de verdere verwerking kan de betrokkene zich geconfronteerd zien met gevolgen die als een totale verrassing komen en waarover hij geen controle heeft. Bovendien is het mogelijk dat de betrokkene niet begrijpt waar een bepaalde beslissing vandaan komt en dat hij zich niet tegen een dergelijke beslissing kan verweren.

Een gebrek aan informatie en een gebrek aan kennis over de besluitvorming heeft tot gevolg dat een betrokkene zich mogelijk niet kan verweren tegen beslissingen die over hem of haar worden genomen. Het risico bestaat dat door de inzet van Big data-technieken niet duidelijk is hoe de politie tot een bepaalde beslissing is gekomen. Daarnaast zal het veelvuldig voorkomen dat een betrokkene niet op de hoogte is dat bepaalde gegevens worden verwerkt, waar deze worden verwerkt, door wie de gegevens worden verwerkt en voor welke doeleinden de gegevens worden verwerkt. Hierdoor kan de betrokkene zich geconfronteerd zien met resultaten die hij of zij niet begrijpt en waar hij of zij zich maar moeilijk tegen kan verzetten. Dit heeft effectief een beperking van de persoonlijke autonomie en zeggenschap tot gevolg.

[99] WRR 2016, pp. 111-112.

5.1.2.h

11.3.2.3 Black box

In het verlengde van de voorgaande paragraaf, namelijk het gebrek aan informatie en controle, speelt het risico van de *Black Box.* Met behulp van de Raffinaderij wordt de betrokkene steeds transparanter voor de politie. De politie krijgt met de Raffinaderij de mogelijkheid om gegevens over de betrokkene te combineren. Hieruit kunnen allerlei conclusies worden getrokken en uitkomsten aan verbonden. Bovendien kan de combinatie van twee op zichzelf onschuldige gegevens leiden tot de creatie van een nieuw gegeven en tot gevoelige inzichten over de betrokkene.[100]

De technieken die achter deze besluitvorming schuilgaan, zijn meestal ondoorzichtig. Hierdoor wordt een *Black Box* gecreëerd: alleen de makers zijn bekend met de wijze van besluitvorming. Zij weten welke gegevens worden gecombineerd met welke indicatoren en wat de wegingsfactoren zijn. Ten gevolge hiervan wordt de besluitvorming onnavolgbaar. De betrokkene kan zich hierdoor geconfronteerd zien met uitkomsten die hij of zij niet begrijpt en waartegen hij zich mogelijk maar moeilijk kan verweren.[101] Ook het corrigeren van data en uitkomsten die mogelijk niet kloppen, is lastig.[102] Hierdoor ontstaat ook een spanningsveld met het recht op een eerlijk proces (zie par. 11.1.3).

[100] WRR 2016, p. 26.

[101] WRR 2016, pp. 70 en 93.

[102] WRR 2016, p. 29.

5.1.2.h

12 Risicobeperkende maatregelen en aanbevelingen

Om de manifestatie van de in hoofdstuk 10 genoemde risico's en de in hoofdstuk 11 beschreven impact daarvan zo veel mogelijk te voorkomen, zijn de volgende risicobeperkende maatregelen in het kader van de Raffinaderij relevant. Een deel van deze risicobeperkende maatregelen is reeds genomen, daar waar er aanbevelingen zijn, wordt dit toegelicht.

12.1 (Data) Governance

De belangrijkste waarborg voor privacybescherming en het voorkomen van afbreukrisico's bij het gebruik van de Raffinaderij is om zorg te dragen voor de juiste verwerking van politiegegevens. Daarvoor is het noodzakelijk om de data governance - de overstijgende werkwijze voor zorgvuldige omgang met gegevens - goed te regelen.

Hierbij moet aangesloten worden bij de bredere governance voor wat betreft de informatiehuishouding van de politie. Momenteel is de Raffinaderij nog een losstaand project en is de data governance de verantwoordelijkheid van de projectleiding. Gezien de uitgebreide kennis van de Raffinaderij en de specifieke data- en privacyvraagstukken worden risico's momenteel beperkt. Als en wanneer de Raffinaderij wordt ingebed in de bredere politieorganisatie, is het zaak dat deze expertise ook wordt geborgd. Daarnaast moet rekening worden gehouden met de specifieke context van de Raffinaderij. Hiervoor zijn de volgende zaken in het bijzonder relevant.

12.1.1 Compliance en audit functionaliteit met specifieke expertise op het gebied van de Raffinaderij

Het verdient aanbeveling om een specifieke Functionaris Gegevensbescherming aan te stellen voor de Raffinaderij (zie in dit kader ook artikel 32 en verder van Richtlijn 2016/680/EG). Deze persoon dient naast kennis van de relevante wetgeving ook specifieke expertise en ervaring te hebben op het werkterrein van de Raffinaderij: met andere woorden, het snijvlak van privacy, opsporing en BI- voorzieningen en ontwikkelingen.

5.1.2.h

12.1.2 Duidelijk intake proces in voor aansluiting nieuwe bronnen en uitbreiding van bestaande werkwijzen (DPIA)

Wanneer nieuwe informatiebronnen 'standaard' ontsloten worden of beschikbaar komen via de Raffinaderij,[103] wanneer de Raffinaderij wordt uitgebreid naar andere soorten onderzoek of Big Data-analyses worden uitgevoerd, is het zaak de 'privacy impact' hiervan te onderzoeken. Dit is in lijn met artikel 27 van Richtlijn 2016/680/EG die gegevensbeschermings-effectbeoordelingen (DPIAs) verplicht stelt. Met dit instrument kunnen in een vroeg stadium eventuele risico's worden geïdentificeerd. De aanbevelingen voor risicobeperkende maatregelen die voortvloeien uit dergelijke (D)PIAs kunnen worden geïmplementeerd in de techniek of de organisatie, waarmee ook voldaan wordt aan de eis van *Privacy by Design* en *Privacy by Default*.

12.1.3 Richt een duidelijke registratie van verwerkingen in, gericht op de Raffinaderij

Op grond van de protocolplicht (artikel 32 Wpg) moet de politie onder meer de geautomatiseerde vergelijking, het in combinatie verwerken, de hernieuwde verwerking en de verstrekking van gegevens vastleggen. Hiermee wordt zowel het interne als het externe toezicht mogelijk gemaakt. Deze protocolplicht wordt in de Richtlijn aangescherpt (artikel 24 Richtlijn). De politie dient daarom de Raffinaderij verwerkingen te registeren.

In het verlengde van het bovenstaande moet ook zorggedragen worden voor toereikende artikel 11 lid 4 Wpg autorisaties.

12.1.4 Draag zorg voor informatie- en privacybewustzijn

Momenteel wordt de Raffinaderij door een beperkte groep rechercheurs en analisten gebruikt. Wanneer de Raffinaderij breder wordt uitgerold, is het van belang dat de gebruikers zich bewust zijn van de mogelijke (privacy)risico's van de Raffinaderij. Omdat de Raffinaderij in feite een nieuwe werkwijze is, moeten gebruikers daar specifiek in worden getraind. Vanuit privacy perspectief zal daarbij de nadruk moeten liggen op de vraag welke impact de Raffinaderij als BI-voorziening op betrokkenen kan hebben en hoe risico's bij het gebruik kunnen worden geminimaliseerd. Specifieke aandacht moet in dit kader uitgaan naar zaken als doelbinding (het voorkomen *detournement du pouvoir*), noodzakelijkheid (proportionaliteit en subsidiariteit), data minimalisatie en de gegevenskwaliteit.

---

[103] Daarmee wordt bedoeld: het gaat niet om het ontsluiten van data of een 'nieuwe' bron ten behoeve van een specifiek onderzoek maar om het ontsluiten van nieuwe bronnen voor grote groepen gebruikers (via een zogenoemde reguliere 'pipeline' zoals die nu binnen de Raffinaderij voor bronnen als SummIT, DCS en BVH bestaat).

5.1.2.h

12.2 Risico's beheer gegevens

12.2.1 Registratie herkomst en logging gebruik data

De data binnen de Raffinaderij zijn traceerbaar naar de bron waaruit zij zijn verkregen omdat deze koppelingen geregistreerd worden. Op die manier is de herkomst van de data die worden gebruikt binnen analyses bekend. Binnen Palantir wordt daarnaast elke handeling met de data gelogd op gebruikersniveau. Hiermee wordt gegarandeerd dat het gebruik van de data traceerbaar is en dat voldaan kan worden aan de protocolplicht.

12.2.2 Logging & classificatie op attribuutniveau

Het risico op de vermenging van data is in de Raffinaderij geadresseerd door op attribuutniveau vast te leggen uit welke bron(nen) de data afkomstig is en wie toegang mag hebben tot welk 'stukje' data. Hiermee wordt voorkomen dat ongeautoriseerde gebruikers toegang krijgen tot een verkeerde combinatie van gegevens. Een deel blijft dan simpelweg onzichtbaar.

Voor degenen die wel toegang hebben tot alle data geldt dat zij zich bewust moeten zijn van het risico op vermenging van data. Met name wanneer zij hun resultaten naar buiten toe presenteren.

Verder is aan de 'bronkant' juiste classificatie van gegevens een randvoorwaarde om ongewenste vermenging te voorkomen. De Wpg maakt onderscheid tussen 'gewone' persoonsgegevens en 'gevoelige' persoonsgegevens. Deze laatste categorie gegevens betreffen gegevens die betrekking hebben op iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven en lidmaatschap van een vakvereniging. De verwerking van deze gegevens is alleen toegestaan in aanvulling op de verwerking van andere politiegegevens en voor zover dit voor het doel van de verwerking onvermijdelijk is.

In de aankomende Richtlijn vindt meer dataclassificatie plaats. Daar wordt onderscheid gemaakt naar gradaties van juistheid en betrouwbaarheid. In Artikel 7 Richtlijn bestaan enerzijds politiegegevens die op feiten zijn gebaseerd en anderzijds politiegegevens die op een persoonlijk oordeel zijn gebaseerd. Daarnaast maakt de Richtlijn in artikel 6 onderscheid tussen verschillende categorieën van betrokkenen. Het betreft daarbij verdachten, veroordeelden, slachtsoffers en anderszins betrokkenen. Deze verschillende aspecten en dit onderscheid dient bij de verwerking en classificatie van data binnen de

5.1.2.h

politie te worden aangebracht (en hier dient ook in de Raffinaderij rekening mee te worden gehouden).

Tenslotte moeten binnen de Raffinaderij de bestaande regelingen omtrent het coderen van informantengegevens worden meegenomen.

12.2.3 Frequente verversing data en rechtstreekse koppeling met de bron

Aangezien de Raffinaderij politiegegevens uit onderliggende bronnen verwerkt, is het van belang om controle te houden op de inhoud en de accuraatheid van de politiegegevens in deze bronbestanden en de verwerking en de mogelijke doorwerking daarvan in Raffinaderij.
Binnen de Raffinaderij wordt het risico geadresseerd door de data uit bronbestanden frequent te verversen en, waar mogelijk, rechtstreeks 'te praten' met een bron. Hierdoor worden eventuele datakwaliteitsproblemen die specifiek zijn voor Raffinaderij voorkomen.
De frequentie van de updates is afhankelijk van het specifieke soort bron en het exacte soort gebruik. Soms is realtime informatie nodig, in andere gevallen volstaat een dagelijkse of wekelijkse update.[104]

12.2.4 Data kwaliteit mechanismen

Datakwaliteit is niet alleen vanuit het opsporings- en vervolgingsperspectief relevant, maar ook vanuit privacy-perspectief van groot belang. De datakwaliteit kan bij de Raffinaderij op verschillende manieren in het geding zijn. Hiertoe zijn verschillende oplossingsrichtingen denkbaar.

12.2.4.1 Informeren

Een risicobeperkende maatregel voor mogelijke risico's gerelateerd aan datakwaliteit is dat analisten en opsporingsambtenaren bij gebruikmaking van de Raffinaderij worden geïnformeerd over het feit dat de data mogelijk niet actueel zijn en dat ten gevolge hiervan de datakwaliteit mogelijk onvoldoende is. Gebruikers worden bijvoorbeeld geïnformeerd over de kwaliteit van de data doordat vermeld is wanneer deze data is verzameld, uit welke bron zij stamt, wanneer zij is ingeladen enzovoorts.

12.2.4.2 Wijziging

Met betrekking tot wijzigingen van data (de correctie van data) dient er een terugmeld-procedure te bestaan naar de originele informatiebron. Hoewel het mogelijk is dat de

[104] Op het moment van schrijven worden bijvoorbeeld SummIT en DCS dagelijks geüpdate en komt informatie van taps realtime binnen.

gebruiker in Raffinaderij 'voor zichzelf of voor zijn analyse' bepaalde data in de eigen Raffinaderij 'werkset' verbetert, moet ervoor gewaakt worden dat wordt 'vergeten' om dergelijke verbeteringen door te voeren in de originele bron. Overigens is de *incentive* van gebruikers groot om de data in zo een geval in de bron aan te passen omdat op die manier de verbetering met een volgende update van de data automatisch beschikbaar komt in Raffinaderij.

12.2.4.3 Data integration en record linkage audit trail

Het relateren en modelleren van data en het koppelen van gegevenssets binnen de Raffinaderij vormt een specifiek aandachtspunt. Wanneer brondata in dit kader geïntegreerd of gelinkt wordt (*data integration / data fusion / record linkage*) moet duidelijk zijn hoe de data zijn samengevoegd, welke entiteiten zijn gekoppeld, op basis van welke logica dit is gebeurd enzovoorts. Deze stap – welke in de Raffinaderij plaatsvindt - moet daarom voor de gebruiker verifieerbaar en omkeerbaar zijn.

Het audit trail is één van de sterke punten van de Raffinaderij (meer specifiek van het product Palantir): elke handeling (koppeling entiteiten, samenvoegen datasets etcetera) wordt individueel gelogd op handeling, tijd en persoon.

Hiermee wordt ook meteen invulling gegeven aan een deel van de protocolplicht door onder meer de verstrekking van gegevens maar ook de geautomatiseerde vergelijking of combinatie en de hernieuwde verwerking van gegevens vast te leggen.

12.2.4.4 Bewaartermijnen

Politiegegevens moeten verwijderd worden wanneer zij niet langer noodzakelijk zijn voor het doel waarvoor zij zijn verzameld. Hiertoe heeft de Wpg in de artikel 8 lid 6, in artikel 9 lid 4 en in artikel 10 lid 6 regels gesteld voor wat betreft het bewaren van politiegegevens. Hoewel de Raffinaderij er voor kan zorgen dat gegevens langere tijd nuttig zijn, waardoor de bewaartermijn wordt verlengd, zijn specifieke risicobeperkende maatregelen voor wat betreft het bewaren van politiegegevens voor de Raffinaderij niet relevant, omdat in de Raffinaderij gegevens niet blijvend worden opgeslagen.

12.3 Schaalvergroting

Met behulp van de Raffinaderij kunnen allerlei informatiebronnen en gegevens effectief met elkaar gecombineerd worden op een manier die niet eerder is gerealiseerd. Het juridisch kader en de daarbij horende waarborgen zijn nog altijd (onbedoeld) toegespitst op de tijd waarin deze mogelijkheid nog niet bestond. Daarom dient het risico van schaalvergroting en datahonger nadrukkelijk in het achterhoofd gehouden te worden.

Bij het gebruik van de Raffinaderij dient extra aandacht te worden besteed aan de risico's van schaalvergroting. Dit is naast een kwestie van naleving van de wet en het goed inrichten van governance en autorisaties ook een kwestie van cultuur. Bij het trainen van medewerkers van de Raffinaderij dient naast de 'knoppenkennis' ook expliciet aandacht te worden besteed aan de risico's van schaalvergroting en het (onbedoeld) misbruik van gegevens.

12.3.1 Mission- en function creep

Het is van belang dat de politie weerstand biedt tegen de verleiding om zich binnen onderzoeken te laten leiden door de technologische mogelijkheden in plaats van door de juridische kaders.

Het risico op *mission-* en *function creep* kan worden verkleind door een duidelijke data governance structuur in te richten en een privacy functionaris of een Functionaris Gegevensbescherming aan te stellen. Bij de governance moet blijvend aandacht worden besteed aan de overkoepelende functionaliteit van de Raffinaderij en de impact die de Raffinaderijmethode heeft op de privacy van betrokkenen. Een effectieve manier om dit vorm te geven, is door bij het realiseren van nieuwe functionaliteiten of bij aansluiting van nieuwe informatiebronnen een Privacy Impact Assessment te doen. Hiermee kunnen snel de risico's ingeschat worden. Periodiek moet gekeken worden naar de Raffinaderijmethode als geheel (*full life cycle data protection*).

Verder moet overwogen worden om andere toetsings- en wegingsmomenten in te bouwen voor het gebruik van de Raffinaderij. Het gaat dan met name over de manier waarop de Raffinaderij wordt gebruikt. De neiging moet worden voorkomen om willekeurige bronnen en gegevens 'door de Raffinaderij te halen'. Voor elke recherchevraag moet gekeken worden of het gebruik proportioneel is en voldoet aan het subsidiariteitsvereiste. Hiertoe kunnen bijvoorbeeld toetsingsvragen en/of functieprofielen voor het gebruik worden opgesteld. Hierbij speelt ook het bewustzijn bij gebruikers van de Raffinaderij een rol.

5.1.2.h

12.3.2 Dataminimalisatie

Op grond van het beginsel van dataminimalisatie mogen niet meer politiegegevens worden verwerkt dan noodzakelijk voor het doel waarvoor de gegevens worden verwerkt. Ervan uitgaande dat wordt voldaan aan het systeem van autorisaties hebben medewerkers in Raffinaderij toegang tot bronnen en gegevens die ze normaal gesproken, in de bronsystemen, ook tot hun beschikking hebben. Door de Raffinaderij te gebruiken in het kader van een onderzoek krijgt een opsporingsteam uitdrukkelijk niet toegang tot meer of andere gegevens. Wel biedt de Raffinaderij hen de mogelijkheid om op andere manieren 'slim gebruik te maken' van alle data omdat de gegevens in combinatie met elkaar kunnen worden verwerkt.

Hierdoor ontstaat het risico dat opsporingsambtenaren en analisten door de beschikbaarheid van de Raffinaderij en haar mogelijkheden, geneigd kunnen zijn om zo veel mogelijk gegevens in een onderzoek te betrekken, in de hoop dat zij met behulp van de Raffinaderij een relevant verband vinden (zie ook paragraaf 10.3.2). Het is van belang om deze spanning met het beginsel van dataminimalisatie in het oog te houden en maatregelen te treffen om dit te voorkomen, niet alleen binnen de politie maar ook bij het Openbaar Ministerie. Hierbij kan gedacht worden passende autorisaties, maar ook om gegevens maar beperkt beschikbaar te stellen of maar beperkt zichtbaar te maken.

Daarnaast moet er sprake zijn van logging, monitoring en handhaving. Deze eerste functionaliteit is zeer uitgebreid in de Raffinaderij ingebouwd. Monitoring en handhaving moeten een onderdeel zijn van de compliance organisatie.

12.4 Beveiligingsincidenten en datalekken

Binnen de Raffinaderij zijn passende technische en organisatorische beveiligingsmaatregelen getroffen. Zo draait de Raffinaderij vanuit het beveiligde rekencentrum van de politie op 'eigen' servers binnen het Digitale Transferium. De servers hebben geen verbinding met internet. Een analyse van de van de veiligheidsmaatregelen en hun effectiviteit valt evenwel buiten de scope van deze PIA.

12.4.1 Authenticatie en autorisatie

Het Autorisatiemodel Politie[105] is leidend voor de manier waarop de autorisatietoekenning is geregeld in de politiesystemen. Kort gezegd wordt op basis van de functie en het proces waarin iemand werkzaam is bepaald welke autorisatierol (met bijbehorende rechten)

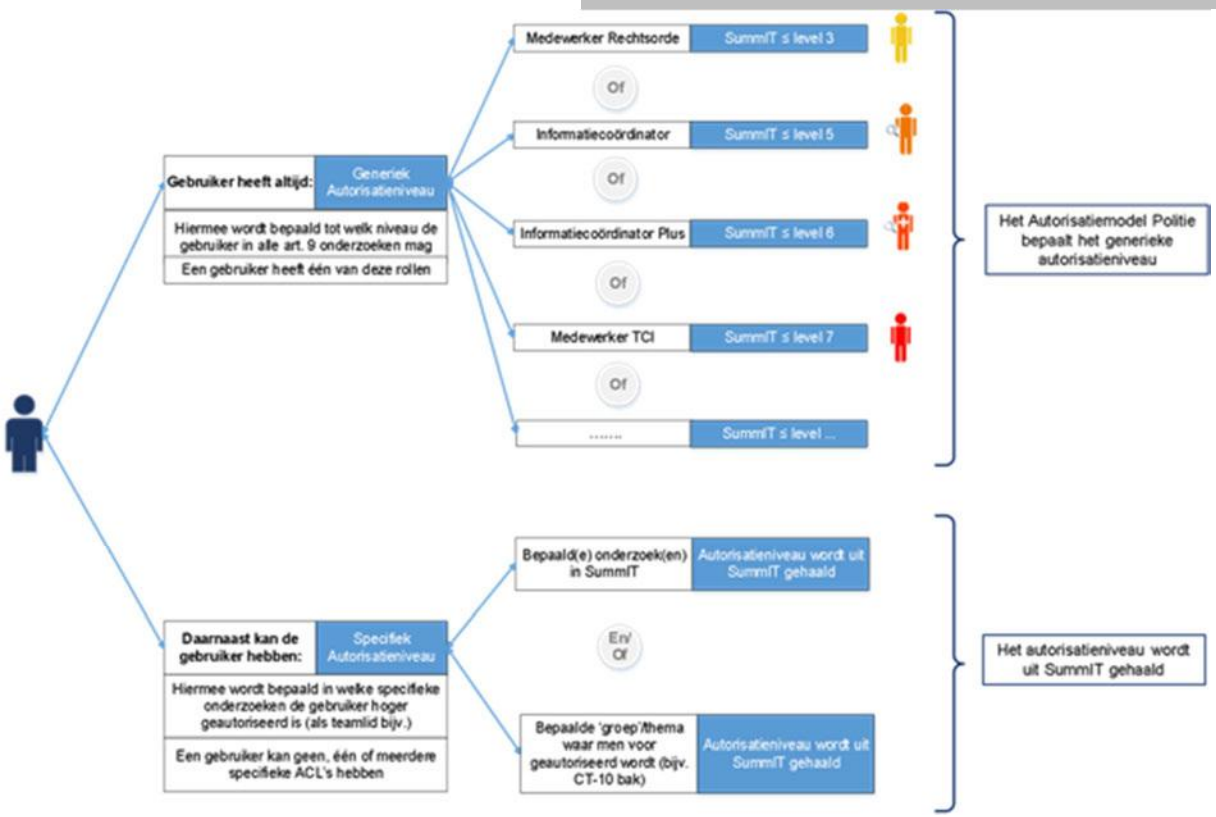
[105] Expertgroep Autorisatiemodel Nederlandse Politie 2011.

diegene krijgt. Voorwaarde voor het verkrijgen van een bepaalde autorisatierol is ook dat voldaan wordt aan bepaalde opleidings- en screeningeisen. In het algemeen geldt: naarmate de toegang tot informatie ruimer is, zijn de opleidings- en screeningseisen zwaarder.

Ook in Raffinaderij is het autorisatiemodel politie doorgevoerd. De gegevens waartoe de gebruiker geautoriseerd is om mee te werken, wordt bepaald door een combinatie van:

1) Generiek autorisatieniveau: dat is het niveau waarmee de gebruiker volgens het Landelijk Autorisatiemodel Politie landelijk mag 'zoeken en speuren' (onder andere door gegevens die zijn verzameld op grond van artikel 9 Wpg);
2) Specifiek autorisatieniveau: dat is de autorisatie die de gebruiker in SummIT heeft gekregen op onderzoeksniveau (bijvoorbeeld als teamlid van onderzoek A, B en C).[106] De autorisatiewijzigingen binnen onderzoeken in SummIT werken automatisch door in Raffinaderij.

[106] Doorgaans heeft een medewerker als teamlid van een onderzoek een hoger autorisatieniveau dan het generieke niveau.



De autorisaties zijn op dataniveau doorgevoerd. Oftewel, er wordt gekeken naar het niveau waarop men in SummIT entiteiten, documenten, journaalmutaties enzovoorts heeft weggeschreven of geclassificeerd. Dat bepaalt uiteindelijk welke data men wel of niet ziet. De autorisaties werken ook door in de samenwerkingsomgeving van Raffinaderij (*collaboration*). Als een medewerker daar een analyse (en daarmee de onderliggende data) wil delen met een collega, zodat die collega daar verder mee kan werken in Raffinaderij, dan ziet die collega alleen díe data die hij of zij volgens zijn of haar eigen autorisatie mag zien.

12.4.1.1 Autorisaties van externen

De Raffinaderij heeft met verschillende externen te maken. Zo wordt gebruik gemaakt van de diensten van externe leveranciers (zoals op dit moment Palantir) en, waar nodig, ingehuurde medewerkers. De autorisatie van de externe medewerkers is afhankelijk van de taak die ze uitoefenen en wat daarvoor noodzakelijk is. Indien deze externe werknemers toegang nodig hebben tot politiegegevens in de Raffinaderij krijgen zij een A-screening en tekenen zij een geheimhoudingsverklaring. De (dagelijkse) aansturing en verantwoordelijkheid van diegenen ligt bij de (project)leiding van de Raffinaderij.

Daarnaast worden externen ingeschakeld om de systemen van de Raffinaderij te auditen of op andere wijze aan controle te onderwerpen. Ook deze personen dienen voldoende

gescreend te worden en een geheimhoudingsverklaring te tekenen alvorens zij de benodigde inzage krijgen in de Raffinaderij.

12.4.1.2 Nota bene: autorisatieniveaus in het licht van de Raffinaderij

Het Autorisatiemodel 2011 en de implementatie daarvan binnen bijvoorbeeld SummIT bieden een goede basis voor de bescherming van gegevens binnen de Raffinaderij. Echter, wanneer opsporingsambtenaren door nieuwe technologieën zoals de Raffinaderij meer mogelijkheden en middelen ter beschikking hebben om gegevens te verwerken, is het raadzaam om de 'rollen' periodiek te evalueren. Wanneer een bepaalde rol door voortschrijdende technologie ineens veel 'machtiger' wordt, is het raadzaam om het aantal personen met deze rol te beperken en/of de rol met meer waarborgen te bekleden. Dit is een punt dat met name in ogenschouw moet worden genomen als de Raffinaderij opschaalt qua gebruikersaantallen.

Om dit probleem te adresseren, kan bijvoorbeeld gedacht worden aan het 'uitbreiden' van het autorisatiemodel politie met (een) extra dimensie(s) waarbij ook rekening wordt gehouden met de hoeveelheid en soort data en soort bronnen die een persoon in combinatie met elkaar (geautomatiseerd) kan verwerken. Oftewel, er dient ook rekening te worden gehouden met danwel er dient onderscheid gemaakt te worden in de mate van privacygevoeligheid die bepaalde verwerkingen opleveren.

Een ander punt van aandacht betreft de binding van de autorisatie aan het doel van een bepaald onderzoek. De toegang tot gegevens wordt momenteel volgens het landelijk autorisatiemodel vastgesteld, in combinatie met de 'specifieke', vaak hogere, autorisatie die medewerkers in een bepaald onderzoek toegewezen kunnen krijgen. Dat kan betekenen dat wanneer opsporingsambtenaren of analisten in SummIT aan veel onderzoeken zijn toegevoegd, zij 'automatisch' bij de data van al die onderzoeken tot dat hogere niveau kunnen terwijl dat voor het onderzoek waar ze mee bezig zijn niet per se noodzakelijk is. Dit risico wordt groter wanneer autorisaties binnen onderzoeken door bevoegd functionarissen niet goed bijgehouden worden.

12.4.2 Meldplicht datalekken

Er dient een interne procedure meldplicht datalekken ingericht te worden die rekening houdt met de specifieke aspecten van de Raffinaderij. Wanneer binnen de politie reeds een procedure meldplicht datalekken bestaat, kan bij deze procedure aansluiting worden gezocht. Deze meldplicht dient vervolgens te worden geïmplementeerd.

Tenslotte dienen alle betrokken partijen zich er bewust van te zijn wanneer er sprake kan zijn van een datalek. Dit betekent dat de verschillende gebruikers van de Raffinaderij moeten weten wat een datalek is, zij moeten een mogelijk datalek kunnen herkennen en zij moeten in staat zijn om vervolgens de juiste acties ondernemen om het datalek zo snel mogelijk onder de aandacht te brengen van de verantwoordelijke.

12.5Inzet externe leveranciers

Het is van belang om goed stil te staan bij en zicht te houden op welke partijen toegang hebben tot welke politiegegevens, op de wijze waarop deze politiegegevens opgeslagen zijn en waar de gegevens staan opgeslagen. Dit is met name relevant wanneer buitenlandse partijen politiegegevens verwerken.

In het kader van de Raffinaderij zijn diverse maatregelen genomen om het risico van het werken met derden (meer specifiek Palantir) te verkleinen. Zo worden politiegegevens niet opgeslagen bij de leveranciers, maar enkel in het Digitaal Transferium. Daarnaast worden alle externe medewerkers gescreend en moeten zij geheimhoudingsverklaringen ondertekenen. Het is deze medewerkers ook niet toegestaan om eigen apparatuur en gegevensdragers mee te nemen. Tenslotte worden alle activiteiten van de externe medewerkers in realtime gemonitord. Naast deze direct op medewerkers gerichte maatregelen wordt ook gemonitord of data niet geëxfiltreerd worden uit het systeem.

12.6 Transparantie en controleerbaarheid

Er dient te worden gezorgd voor een duidelijk informatievoorziening richting de betrokkene en de politie moet transparant zijn over wat de Raffinaderijmethode precies behelst. Veel privacyzorgen kunnen geadresseerd worden door transparante communicatie. Om verkeerde beeldvorming te voorkomen, is het van belang om duidelijk te maken wat er wel en niet binnen de Raffinaderij gebeurt. Daarbij is het relevant om te vermelden dat de Raffinaderij veel waarborgen heeft getroffen die de privacy van betrokkenen moet beschermen, zoals het beperken van de inzet van de Raffinaderij tot bepaalde categorieën onderzoek, strenge autorisaties en een goede *audit trail* van gegevens. Ook adviseren wij om duidelijk te maken dat met behulp van de Raffinaderij expliciet geen Big Data-analyses, *predictive policing* en geautomatiseerde besluitvorming gebeurt. Daarnaast bevelen wij aan om met name transparant te zijn over het gebruik van externe software, zoals de software van Palantir.

5.1.2.h

12.6.1 Rechten van de betrokkene

Een specifiek onderdeel van transparantie en controleerbaarheid betreffen de rechten van de betrokkenen. In de Raffinaderij worden enkel gegevens (bronbestanden) verwerkt waarover een onderzoeksteam normaal gesproken ook zou beschikken. De procedures voor inzage gaan daarom via de normale wegen die daarvoor beschikbaar zijn. 5.1.2.h beveelt aan om de inroeping van de rechten van de betrokkene via de normale wegen te laten verlopen.

12.6.2 Controle en toezicht

Tenslotte is het van belang dat binnen de politieorganisatie wordt gecontroleerd en toezicht wordt gehouden op de naleving van alle bovenstaande elementen. 5.1.2.h beveelt aan dat er een specifieke Privacyfunctionaris of Functionaris Gegevensbescherming wordt aangesteld voor de Raffinaderij om toezicht te houden op de gegevensverwerkingen in het kader van de Raffinaderijmethode. Deze Functionaris Gegevensbescherming kan daarnaast een adviserende rol spelen en optreden als contactpunt voor de Autoriteit Persoonsgegevens.

12.7 Privacybaten

Het is van belang om te noemen dat met de huidige toepassing van de Raffinaderijmethode risico's, voor wat betreft de bescherming van persoonsgegevens, ook kunnen worden verkleind. De centrale architectuur van de Raffinaderij en de *logging* die erin wordt toegepast, zorgt ervoor dat er een hoge mate van controleerbaarheid en reproduceerbaarheid is op hetgeen met de data gebeurt in de Raffinaderij. Zo is bekend op welke wijze data door wie, op welk moment en waarom gecombineerd wordt. Daarnaast staat de kwaliteit van data hoog in het vaandel. Dit overzicht en deze controle bestaat buiten de Raffinaderij in de politieorganisatie in beperktere mate.

Naast het verkleinen van de risico's van de verwerking van politiegegevens door betere compliance maatregelen is er ook een direct voordeel voor de privacy (en andere grondrechten) van de betrokkene.

Omdat op grote schaal gegevens worden verwerkt binnen Raffinaderij zijn de mogelijkheden voor waarheidsvinding ook groter. Niet alleen kunnen meer data voor een completer beeld zorgen, ook is het door de effectievere en efficiënte werkwijze mogelijk om meer hypotheses te onderzoeken. Hierdoor kan een persoon juist uitgesloten worden als verdachte waardoor een minder grote inbreuk op de privacy van deze burgers

plaatsvindt. In een vroeg stadium kan, door het combineren van bronnen, namelijk worden vastgesteld of een burger iets met een bepaald misdrijf te maken heeft.[107]

Deze privacybaten dienen mee te worden gewogen in de totale beoordeling van de privacy impact van het gebruik van de Raffinaderij.

[107] Ter illustratie het volgende voorbeeld: indien bij het opvragen van verkeersgegevens rondom een plaats delict een bepaald telefoonnummer als 'interessant' naar voren zou komen wanneer alleen naar telecomdata zou worden gekeken, blijkt juist uit de combinatie met andere gegevens dat het betreffende telefoonnummer helemaal niet interessant is voor het onderzoek waardoor hier verder geen actie op wordt genomen.

13 Conclusies

Het concept Raffinaderij kan het beste worden omschreven als een werkwijze die rechercheurs en analisten in staat stelt om met behulp van geautomatiseerde gegevensverwerking onderzoek te doen. De Raffinaderij is daarbij geen *tool* maar veeleer een door data-analyse technologie ondersteunde werkwijze. Door de inzet van geavanceerde data-analyse technologieën wordt het mogelijk om op een effectieve en efficiënte wijze grote hoeveelheden (on)gestructureerde politiegegevens in samenhang te ontsluiten, analyseren, verrijken en de resultaten daarvan te visualiseren.

Omdat er sprake is van het gebruik van innovatieve technologieën die nieuwe, grootschalige verwerkingen van politiegegevens mogelijk maken, ontstaan er mogelijk nieuwe risico's voor de privacy van verdachten en andere betrokkenen. In deze *privacy impact assessment* zijn deze risico's geïdentificeerd en geanalyseerd. Het betreft een update van de PIA voor de Raffinaderij uit 2013.

13.1 Juridische grondslag

De juridische basis voor het verzamelen (en verder verwerken) van politiegegevens binnen de Raffinaderij moet gevonden worden in de artikelen 8 tot en met 13 Wpg. Omdat de Raffinaderij primair wordt ingezet voor *intelligence* doeleinden en voor specifieke opsporingsonderzoeken, en daarbij gebruik wordt gemaakt van het combineren en analyseren van verschillende datasets, zijn de belangrijkste grondslagen voor het gebruik van de Raffinaderij artikel 9 en 10 Wpg juncto artikel 11 Wpg.

De Raffinaderij wordt momenteel gebruikt voor grote en complexe zaken. Hiertoe worden gegevens uit diverse opsporingsonderzoeken (Titel IVA, Titel V en Titel VB Wetboek van Strafvordering onderzoeken) samengebracht in de Raffinaderij. Een voorwaarde voor het legitieme gebruik van de gegevens uit deze onderzoeken is dat zij op rechtmatige wijze zijn verzameld. Wanneer het verzamelen van deze gegevens een meer dan geringe inbreuk op de persoonlijke levenssfeer van de verdachte of andere betrokkenen vormt, is een specifieke wettelijke basis noodzakelijk. Deze basis moet worden gevonden in het Wetboek van Strafvordering (Sv), bijvoorbeeld in de regelingen omtrent de (bijzondere) opsporingsbevoegdheden. In zoverre de gebruikte gegevens zijn verzameld met behulp van de inzet van bijzondere opsporingsbevoegdheden, dient op grond van artikel 126dd Sv toestemming voor het hergebruik van deze gegevens in een ander onderzoek of voor intelligence doeleinden te worden gegeven door de officier van justitie.

5.1.2.h

Voor wat betreft de rechtmatigheid van de verwerking van politiegegevens levert de Raffinaderij ten opzichte van de vorige PIA geen nieuwe vraagstukken op. De Raffinaderij put alleen uit politiebronnen en verwerkt deze gegevens ter ondersteuning van het normale recherche- en analyseproces. Wanneer de gegevens die in de politiebronnen zijn opgeslagen legitiem zijn verzameld, geldt dat de verdere verwerking in de Raffinaderij rechtmatig is, zolang wordt voldaan aan de eisen van de Wpg. Indien onrechtmatig verkregen gegevens in deze bronnen aanwezig zijn, werkt dit uiteraard ook door in de Raffinaderij.

Nieuw ten opzichte van de PIA 2013 is dat nu ook open bronnen onderzoek (OSINT) wordt betrokken binnen de Raffinaderij werkwijze. Daar waar er sprake is van stelselmatigheid wordt het open bronnen onderzoek enkel gedaan op basis van de bevoegdheid tot stelselmatige observatie (artikel 126g Sv). Vanuit het perspectief van dataminimalisatie worden alleen die gegevens binnen de politieorganisatie gehaald die daadwerkelijk relevant zijn voor het onderzoek.
Op basis van het bovenstaande concluderen wij dat er in zijn algemeenheid een juridische grondslag is voor de verzameling en verdere verwerking van de politiegegevens in het kader van de Raffinaderij.

Een punt van aandacht richting de toekomst is de verhouding tussen het strafprocesrecht en het gegevensbeschermingsrecht. Zoals de WRR signaleert in haar studie naar Big Data in het veiligheidsdomein liggen de meeste waarborgen in de verzamelfase en niet in de analyse-fase (waar de Wet politiegegevens primair op ziet). Op de langere termijn werpt dit wellicht de vraag op of Wpg een voldoende wettelijke basis vormt ex. artikel 8 EVRM om inbreuken op de persoonlijke levenssfeer van de verdachte en andere betrokkenen te legitimeren. Het betreft hier echter niet zozeer een vraagstuk dat specifiek is voor de Raffinaderij, als wel voor de informatie-huishouding van de politie in zijn algemeenheid. Vanuit het perspectief van de PIA is dit dan ook niet een probleem dat direct geadresseerd kan worden. Met de Raffinaderij wordt binnen de grenzen van de wet geopereerd, maar werkwijzen zoals de Raffinaderij rechtvaardigen misschien een meer fundamentele herijking van het juridisch kader voor de gegevensverwerking door de politie in de toekomst.

5.1.2.h

13.2 Materiële eisen verwerking

Op grond van de Wpg moeten de verwerkingen binnen de Raffinaderij voldoen aan een aantal eisen. Het gaat daarbij om zaken als dataminimalisatie, datakwaliteit, geheimhouding, beveiliging en het invulling geven aan de rechten van de betrokkenen. Met alle genoemde eisen is voor zover mogelijk rekening gehouden binnen de Raffinaderij. Het betreft technische en organisatorische maatregelen. Deels gaat het om 'standaardprocedures' die bestaan binnen de politie waarbij geen specifieke aanpassingen noodzakelijk zijn voor de Raffinaderij. Op andere punten zijn er binnen de Raffinaderij specifieke (technische) maatregelen genomen. Hierbij kan met name gedacht worden aan zaken als het loggen van het gebruik van de politiegegevens. Op dit specifieke punt is de Raffinaderij zelfs meer 'privacybeschermend' dan de huidige politiepraktijk.

13.3 (Privacy)risico's Raffinaderij

Hoewel de Raffinaderij een krachtig middel is voor de opsporing, kan (verkeerd) gebruik van de Raffinaderij ook risico's met zich meebrengen. Deze liggen primair op het gebied van de privacy, maar ook andere grondrechten zoals het recht op een eerlijk proces kunnen in het geding komen.

Privacyrisico's kunnen onder andere ontstaan door gebrekkige (data)governance (wanneer de Raffinaderij niet goed wordt ingebed binnen de bredere politieorganisatie), gebrekkig beheer van gegevens, schaalvergroting en door beveiligingsincidenten. De impact die deze risico's (indien zij zich manifesteren) kunnen hebben op burgers zijn onder andere onvrijwillige en ongewenste openbaarmaking, aantasting van de persoonlijke autonomie en mogelijk in een inbreuk op het recht op een eerlijk proces. De mogelijke gevolgen van het manifesteren van deze risico's voor de politie zijn het 'stukgaan' van zaken, reputatieschade, handhaving door de toezichthouder, hogere compliancekosten en een grotere terughoudendheid binnen en buiten de politie om gegevens te delen.

Een specifiek risico, met name voor de politie zelf, betreft de samenwerking met externe leveranciers zoals Palantir. Binnen de Raffinaderij zijn voldoende maatregelen genomen om te voorkomen dat deze leveranciers onrechtmatig kennis kunnen nemen van politiegegevens. In de publieke opinie kan echter het gebruik van met name Palantir geassocieerd worden met de praktijken van de CIA en de NSA, hetgeen mogelijk negatief afstraalt op de politie.

5.1.2.h

Tenslotte hebben wij aandacht besteed aan de vraag wat de privacyrisico's zijn van mogelijk toekomstige uitbreiding van gebruik van de Raffinaderij. Hierbij moet bijvoorbeeld gedacht worden aan *predictive policing* gebaseerd op *data mining* en andere vormen van Big Data analyse. Dit brengt diverse risico's met zich mee. Hoe deze risico's zich kunnen manifesteren en welke risicobeperkende maatregelen dienen te worden genomen, is op dit moment echter niet concreet te zeggen. Een dergelijke uitbreiding brengt diverse risico's met zich mee die sowieso een andere insteek vergen dan de huidige insteek van het Raffinaderij concept. De huidige insteek draait in de kern om de beantwoording van concrete recherche-vragen in plaats van dat gezocht wordt naar onontdekte patronen of verbanden in politiegegevens.

13.4 Risicobeperkende maatregelen

Om de bovengenoemde risico's te adresseren zijn diverse technische en organisatorische maatregelen genomen. Daarnaast dienen een aantal aanvullende maatregelen genomen te worden, met name wanneer de Raffinaderij van de pilot- of projectfase naar een operationele status wordt gebracht. Binnen de huidige pilotfase van de Raffinaderij lijken de risico's toereikend geadresseerd te zijn door de genomen risicobeperkende maatregelen. Het betreft onder andere maatregelen op het gebied van beveiliging, (data)governance en de logging van gegevens en analyses binnen de Raffinaderij. De belangrijkste waarborg lijkt echter het gedegen bewustzijn binnen het Raffinaderij team te zijn dat er wordt gewerkt met een krachtig instrument waarmee verantwoordelijk moet worden omgesprongen. Bewustzijn over de privacyrisico's en de risico's voor de integriteit van de opsporing zorgen dat 'datahonger' en 'mission- en function creep' geen vat krijgen op de Raffinaderij.

Het is daarom sterk aan te bevelen om dit bewustzijn goed te borgen binnen de bredere politieorganisatie mocht besloten worden om de Raffinaderij operationele status te geven. Training en bewustwording over de mogelijkheden, onmogelijkheden en risico's van de Raffinaderij werkwijze zijn hier belangrijk onderdelen van. Daarnaast zijn ook compliance en governance maatregelen, zoals het aanstellen van een specifieke FG voor de Raffinaderij, het doen van privacy impact assessments voor nieuwe toepassingen en het voeren van een duidelijke registratie van verwerkingen zeer wenselijk.

5.1.2.h

13.5 Afsluitende beschouwing

De Raffinaderij brengt ontegenzeggelijk (privacy)risico's mee, maar deze zijn – in ieder geval voor wat betreft de pilotfase waarin de Raffinaderij zich nu bevindt - afdoende geadresseerd om te kunnen spreken van een verwerking die voldoet aan de eisen van proportionaliteit en subsidiariteit. De nieuwe tooling, toepassingsgebieden en werkwijzen leveren geen nieuwe privacyvraagstukken op die tot een andere conclusie nopen dan die van de PIA uit 2013.

Indien besloten wordt Raffinaderij verder te implementeren in de organisatie (waardoor het gebruik en de gebruikersgroep groter wordt) is het van belang een aantal aanvullende risicobeperkende maatregelen te treffen.

14 Literatuurlijst

WP29 2016
Article 29 Data Protection Working Party, 'Guidelines on Data Protection Officers ('DPOs')', WP 243, 13 December 2016, raadpleegbaar via: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf (beschikbaar in Engels)

Auditdienst Rijk 2015
Auditdienst Rijk, 'Privacy Audit WPG politie', 29 oktober 2015, kenmerk ADR 2015 1306

Beijer 2004
Beijer, A. et al., 'De Wet bijzondere opsporingsbevoegdheden – eindevaluatie', WODC 222, 2004

Van der Bel, van Hoorn & Pieters 2013
van der Bel, D., van Hoorn, A.M. & Pieters, J.J.T.M., 'Informatie en Opsporing – Handboek informatieverwerving, -verwerking en –verstrekking ten behoeve van de opsporingspraktijk', Kerckebosch / Studiecentrum Rechtspleging Utrecht: Zeist 2013

Blom 2007
Blom. T., 'Commentaar op artikel 126gg Sv onder H' in Cleiren, C.P.M., & Nijboer, J.F. (red.), 'Tekst en Commentaar Wetboek van Strafvordering', Deventer: Kluwer 2007

Borking 2010
Borking, J.J.F.M., 'Privacyrecht is code, Over het gebruik van Privacy Enhancing Technologies', Dissertatie Leiden 2010

Business Intelligence Strategie 2012
Business Intelligence Strategie, Programma Intelligence, juli 2012.

Cleiren 2000
Cleiren, C.P.M., 'Strafvordering in het algemeen', in: *Het Wetboek van Strafvordering Losbladig* (red. Melai, A. L., Groenhuijsen, M. S.), 2000, onder L

Corstens 2014
Corstens, G.J.M., 'Het Nederlandse strafprocesrecht', bewerkt door M.J. Borgers, Deventer: Kluwer 2014

Expertgroep Autorisatiemodel Nederlandse Politie 2011
Expertgroep Autorisatiemodel Nederlandse Politie, Autorisatiemodel voor de Nederlandse Politie – 'Autoriseren: zo doen we dat hier!' – visie op een landelijk autorisatiemodel voor de Nederlandse Politie, Opgesteld in opdracht van RKC / Portefeuillehouder Intelligence, juli 2011

Gegevensautoriteit Nationale Politie 2016
Gegevensautoriteit Nationale Politie, 'Verbeterplan Wet politiegegevens en Informatiebeveiliging', maart 2016, raadpleegbaar via: https://www.rijksoverheid.nl/documenten/rapporten/2016/05/27/tk-bijlage-verbeterplan-wet-politiegegevens-en-informatiebeveiligign

Helberger 2013
Helberger, N., 'Digital consumers and the law: towards a cohesive European framework', Alphen aan Den Rijn: Kluwer International Law

Van der Helm 2009
van der Helm, I., De privacybescherming van de zieke werknemer, dissertatie Uiversiteit Utrecht 2009

Hildebrandt 2008
Hildebrandt, M., 'Defining Profiling: A New Type of Knowledge?' In: Hildebrandt, M., & Gutwirth, S. (eds.), *Profiling the European Citizin*: *Cross Disciplinary Perspectives*, Dordrecht: Springer 2008 (p. 17-48)

Minister van Veiligheid & Justitie 2015
Kamerbrief van de Minister van Veiligheid & Justitie over privacy-onderzoeken politie met kenmerk 709105, d.d. 7 december 2015, p. 2, raadpleegbaar via: https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/07/tk-privacy-onderzoeken-politie

Knol & Zwenne 2015

Knol, P.C., & Zwenne, G.J., 'Tekst & Commentaar Telecommunicatie- en Privacyrecht', Deventer: Wolters Kluwer 2015

MacAskill, Thielman & Oltermann 2017
MacAskill, E., Thielman, S. & Oltermann, P., 'WikiLeaks publishes 'biggest ever leak of secret CIA documents', The Guardian, 7 maart 2017, beschikbaar via: https://www.theguardian.com/media/2017/mar/07/wikileaks-publishes-biggest-ever-leak-of-secret-cia-documents-hacking-surveillance.

Mandaatbesluit Politie 2017
Mandaatbesluit Politie januari 2017, beschikbaar via: https://www.politie.nl/binaries/content/assets/politie/documenten-algemeen/mandaten-en-regelingen/directie/mandaatbesluit-politie-januari-2017.pdf

Minister van Buitenlandse Zaken & Binnenlandse Zaken en Koninkrijksrelaties 2017
Beantwoording van de Kamervraag van leden Voortman (GL) en van Raak (SP) aan de Minister van Buitenlandse Zaken en de Minister van Binnenlandse Zaken en Koninkrijksrelaties aangaande het bericht dat de CIA kwetsbaarheden in met het internet verbonden apparaten misbruikt, d.d. 9 maart 2017, nummer 2017Z03599, beschikbaar via: https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2017Z03599&did=2017D07392

Rubinstein 2013
Rubinstein, I.S., 'Big Data: The End of Privacy or a New Beginning', International Data Privacy Law 2013 (Vol. 3, No. 2)

Schermer 2013
Schermer, B., 'Risks of Profiling and the Limits of Data Protection Law', in: Custers, B. c.s. (eds), *Discrimination & Privacy in the Information Society,* Berlin/Heidelberg: Springer 2013

Sloan & Warner 2013
Sloan, R.H. & Warner, R., 'Beyond Notice and Consent: Privacy, Norms and Consent', 2013 beschikbaar via: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2239099

Solon 2017
Solon, O., 'Facial recognition database used by FBI is out of control, House committee hears', The Guardian 27 maart 2017, beschikbaar via:

https://www.theguardian.com/technology/2017/mar/27/us-facial-recognition-database-fbi-drivers-licenses-passports

De Vries 2016
De Vries, I., 'Big Data' in: den Hengst, M., ten Brink, T. & ter Mors, J. (Politieacademie), *Informatiegestuurd politiewerk in de praktijk*, Deventer: Vakmedianet 2017 (pp. 249 - 262).

Westin 1967
Westin, A.F., 'Privacy and Freedom', London/Sydney/Toronto: The Bodly Head 1967

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

Wetgeving

Richtlijn (EU) 2016/680 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, en betreffende het vrije verkeer van die gegevens. De Richtlijn dient voor 6 mei 2018 geïmplementeerd te zijn

Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)

Kamerstukken II 1996–1997, 25 403, nr. 3.
Kamerstukken II 2004/05, 30 164, nr. 3
Kamerstukken II 2005-2006, 30 327, nr. 3
Kamerstukken II 2015-2016, 34 372, nr. 3

Ministerie van Justitie, Memorie van Toelichting: Vaststellingswet Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek, raadpleegbaar via:

https://www.rijksoverheid.nl/actueel/nieuws/2017/02/07/modernisering-van-het-wetboek-van-strafvordering-vordert-gestaag

Jurisprudentie

HvJ 8 april 2014, ECLI:EU:C:2014:23, gevoegde zaken C-293/12 en C-594/12 (*Digital Rights Ireland*)
HvJ 19 oktober 2016, C-582/14 (*Breyer*)
HvJ 21 december 2016, ECLI:EU:C:2016:970, gevoegde zaken C-203/15 en C-698/15 (Tele2 Sverige AB tegen Post- och telestyrelsen)

EHRM 7 december 1976, appl. no. 5493/72 (*Handyside vs. Verenigd Koninkrijk*)
EHRM 26 april 1979, A 30 (*Sunday Times)*
EHRM 20 november 1989, NJ 1990, 245 (*Kostovski*)
EHRM 24 april 1990, A 176 A (*Kruslin vs Frankrijk*)
EHRM 24 april 1990, A 176 B *(Hüvig vs Frankrijk)*
EHRM 24 april 1990, appl. no. 11105/84.
EHRM 16 februari 2000, appl. no. 27798/95 (*Amman vs. Zwitserland*)
EHRM 4 mei 2000, appl. no. 28341/95 (*Rotaru v. Romania*)
EHRM 4 juli 2000, EHRC 2000
EHRM 6 juni 2006, appl. no. 62332/00 (*Segerstedt-Wiberg and others v. Sweden*)
EHRM 3 april 2007, appl. no. 62617/00 (*Copland v. Verenigd Koninkrijk*)
EHRM 13 november 2012, appl. no. 24029/07 (*MM vs. Verenigd Koninkrijk*)
EHRM 21 juni 2011, appl. no. 30194/09 (*Shimovolos vs Rusland*)

HR 14 september 1992, NJ 1993, 83
HR 19 december 1995, *NJ* 1996
HR 18 januari 1999, *NJ* 1999, 253
Hoge Raad 21 maart 2000, 112845, ECLI:NL:HR:2000:AA5254
HR 30 maart 2004, *NJ* 2004, 376 (*Afvoerpijp*)
HR 20 april 2004, *NJ* 2004, 525, ECLI:NL:HR:AL8449
HR 19 februari 2013, ECLI:NL:HR:2013:BY5321, *NJ* 2013, 308
HR 1 juli 2014, 13/04699, ECLI:NL:HR:2014:1569
HR 4 april 2017, 15/03882, ECLI:NL:HR:2017:584

Gerechtshof Arnhem-Leeuwarden, 30 januari 2013 / KS 24-002363-10 30-1-13, ECLI:NL:GHARL:2013:607

Categorie	Beschrijving risico	Kans	Impact	Kans bij uitbreiding*	Impact bij uitbreiding*	Beschrijving impact op de burger	Beschrijving impact op de politie	Risicobeperkende maatregelen
(Data) governane	Zorgvuldige omgang met politiegevens binnen de Raffinaderij wordt niet geborgd.	L	H	H	H	Onrechtmatige of onzorgvuldige verwerking met als gevolg ongewenste openbaarmaking, aantasting persoonlijke autonomie, aantasting recht op een eerlijk proces, onnauwkeurigheid, veiligheid gegevens	Stukgaan zaken, toezicht en hogere compliancekosten, terughoudendheid om gegevens te delen, politieke aandacht, perceptie en negatieve publieke opinie.	- Data governance
Beheer gegevens	Traceerbaarheid herkomst en gebruik data niet gegarandeerd	L	H	L	H	Onrechtmatige of onzorgvuldige verwerking met als gevolg ongewenste openbaarmaking, aantasting recht op een eerlijk proces, onnauwkeurigheid, veiligheid gegevens	Stukgaan zaken, toezicht en hogere compliancekosten, terughoudendheid om gegevens te delen, politieke aandacht, perceptie en negatieve publieke opinie.	- Data governance - Data logging
Beheer gegevens	Vermenging van data	M	H	M	H			- Data governance - Data logging - Data classificatie - Data kwaliteit mechanismen - Autorisaties
Beheer gegevens	Vluchtigheid en verandering in bronbestanden	M	H	M	H			- Data governance - Data kwaliteit mechanismen
Beheer gegevens	Datakwaliteit	M	H	M	H			- Data governance - Data kwaliteit mechanismen
Schaalvergroting	Opbouw historie binnen de politie organisatie	M	M	M	H	Onrechtmatige of onzorgvuldige verwerking met als gevolg ongewenste openbaarmaking, aantasting persoonlijke autonomie, aantasting recht op een eerlijk proces, onnauwkeurigheid, veiligheid gegevens	Stukgaan zaken, toezicht en hogere compliancekosten, terughoudendheid om gegevens te delen, politieke aandacht, perceptie en negatieve publieke opinie.	- Data governance (met name bewustzijn)
Schaalvergroting	'Data honger'	L	H	H	H			- Data governance - Autorisaties
Schaalvergroting	Mission- en function creep	L	M	H	M			- Data governance - Autorisaties
Schaalvergroting	Samenwerkingsverbanden	L	M	H	M			- Data governance - Autorisaties
Beveiligingsincidenten en datalekken	Beveiligingsincidenten en datalekken	L	M	H	M	Onrechtmatige of onzorgvuldige verwerking met als gevolg ongewenste openbaarmaking, veiligheid gegevens	Toezicht en hogere compliancekosten, terughoudendheid om gegevens te delen, politieke aandacht, perceptie en negatieve publieke opinie.	- Data governance - Autorisaties - Meldplicht datalekken

** kans & impact bij uitbreiding geeft een indicatie wat het risico is (kans * gevolg) wanneer bij de opschaling van de Raffinaderij geen aanvullende risicobeperkende maatregelen (bijvoorbeeld op het gebied van governance) worden genomen ten opzichte van de pilot / projectfase.*