M.I. Fedorova
R.M. te Molder
M.J. Dubelaar
S.M.A. Lestrade
T.F. Walree

Strafvorderlijke gegevensverwerking

Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden

RADBOUD UNIVERSITY PRESS

Strafvorderlijke gegevensverwerking

Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden

M.I. Fedorova
R.M. te Molder
M.J. Dubelaar
S.M.A. Lestrade
T.F. Walree

Strafvorderlijke gegevensverwerking
Een verkennende studie naar de relevante gezichtspunten bij de normering van het verwerken van persoonsgegevens voor strafvorderlijke doeleinden

Uitgegeven door RADBOUD UNIVERSITY PRESS
Postbus 9100, 6500 HA Nijmegen
www.radbouduniversitypress.nl | www.ru.nl/radbouduniversitypress
radbouduniversitypress@ru.nl

Ontwerp omslag en binnenwerk: Textcetera, Den Haag
Drukwerk: Pumbo.nl

ISBN: 9789083178998
DOI: http://doi.org/10.54195/KEDT3176
Versie: 2022-11 (gecorrigeerde tweede versie)

Gratis te downloaden via: www.radbouduniversitypress.nl

Opdrachtgever: Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

RADBOUD
UNIVERSITY
PRESS

Inhoudsopgave

Lijst met afkortingen

AA	Ars Aequi
AP	Autoriteit Persoonsgegevens
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
A-G	Advocaat-Generaal
AVG	Algemene Verordening Gegevensbescherming
BVerfG	Bundesverfassungsgericht
CTIVD	Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten
DD	Delikt & Delinkwent
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag voor de Rechten van de Mens
FG	functionaris gegevensbescherming
GDA	geautomatiseerde data-analyse
HvJ EU	Hof van Justitie van de Europese Unie
HGEU	Handvest van de Grondrechten van de Europese Unie
MIVD	Militaire Inlichtingen- en Veiligheidsdienst
m.nt.	met noot
MvA	Memorie van Antwoord
MvT	Memorie van Toelichting
NJB	Nederlands Juristenblad
OOG	onderzoeksopdrachtgericht
OvJ	Officier van Justitie
par.	paragraaf/paragraph
Polw.	Politiewet
R-C	rechter-commissaris
r.o.	rechtsoverweging
StPO	Strafprozessordnung
TIB	Toetsingscommissie Inzet Bevoegdheden
Wiv	Wet op de inlichtingen- en veiligheidsdiensten
Wpg	Wet politiegegevens
WvSv	Wetboek van Strafvordering

Woord vooraf

De digitalisering van de maatschappij heeft de mogelijkheden tot het vergaren van persoonsgegevens door de politie aanzienlijk doen toenemen. Door inbeslagname of het hacken van geautomatiseerde werken of grote digitale-gegevensdragers komt informatie steeds vaker in bulk bij de politie terecht en ook kunnen gegevens thans in toenemende mate met elkaar worden gecombineerd dankzij geavanceerde technologieën om zodoende nieuwe informatie te ontsluiten. De Nederlandse wetgever ziet zich geconfronteerd met nieuwe vragen omtrent de normering van het onderzoeken van gegevens ten behoeve van de opsporing. Met deze verkennende studie beogen wij de wettelijke waarborgen bij strafvorderlijke vergaring van gegevens in samenhang te bezien met waarborgen die gelden voor de daaropvolgende (verdere) verwerking van die gegevens. Daartoe inventariseren we in dit onderzoek welke eisen en waarborgen het Europese recht stelt aan de normering van de (verdere) verwerking van gegevens voor strafvorderlijke doeleinden. Voorts putten we bij het onderzoek inspiratie uit ervaringen met de Wiv 2017 en het recht in België, Duitsland en Noorwegen, wat handvatten biedt om de wijze van normeren en de inrichting van een wettelijke regeling nader te doordenken.

Dit onderzoek is verricht in opdracht van het Wetenschappelijk Onderzoeks- en Documentatiecentrum (WODC) binnen de gelederen van de vaksectie Strafrecht & Criminologie, verbonden aan het Onderzoekscentrum Staat en Recht (SteR) en Interdisciplinary Research Hub on Digitalisation and Society (iHub) aan de Radboud Universiteit.

Zonder de bijstand van anderen hadden wij dit onderzoek niet kunnen uitvoeren. Onze dank gaat allereerst uit naar alle experts die tijd hebben gevonden om hun ervaringen te delen en met ons van gedachten te wisselen. Prof. Bart Jacobs, prof. Piet Hein van Kempen en prof. Frederik Zuiderveen Borgesius bedanken wij voor het secuur en kritisch doorlezen van delen van het rapport. Bijzonder erkentelijk zijn wij student-assistent Noah Koch voor alle werkzaamheden – o.a. bronnenonderzoek, notuleren, transcriberen van interviews, bronnenlijst samenstellen, voetnotenapparaat ordenen – die hij in het kader van dit onderzoek heeft verricht. Onze dank gaat voorts uit naar Joske Wein, die als student-assistent betrokken was bij het verzamelen van met name de Duitstalige bronnen en collega Ruben Aksay voor het meekijken met Noorse bronnen.

Onze dank gaat ten slotte ook uit naar de leden van de begeleidingscommissie, bestaande uit voorzitter prof. mr. Göran Sluiter (Universiteit van Amsterdam); mr. Willemien de Jongste (WODC); prof. mr. Jan-Jaap Oerlemans (Universiteit Utrecht; CTIVD); dr. Bart van der Sloot (Tilburg University); mr. drs. Jacob Struyker Boudier (Ministerie van Justitie en Veiligheid). De kritische reflectie van en discussie met de commissie alsmede het commentaar van de commissieleden op conceptversies van dit onderzoeksrapport hebben een waardevolle bijdrage daaraan geleverd.

Dit onderzoek is afgerond op 15 juli 2022; de in voetnoten vermelde websites waren op die datum toegankelijk. In deze tweede gecorrigeerde druk is in voetnoot 537 (en de bijbehorende zin) een tekstuele wijziging aangebracht. Deze correctie werkt op generlei wijze door in de uitkomsten van het onderzoek.

Masha Fedorova, Ruben te Molder, Marieke Dubelaar, Sjarai Lestrade en Tim Walree*

Nijmegen, november 2022

* Prof. mr. M.I. (Masha) Fedorova, hoogleraar straf(proces)recht, Strafrecht & Criminologie, Onderzoekscentrum Staat en Recht (SteR), Radboud Universiteit; mr. R.M. (Ruben) te Molder, promovendus bij Strafrecht & Criminologie, Onderzoekscentrum Staat en Recht en Interdisciplinary research hub on digitalization and society (iHub), Radboud Universiteit; prof. mr. M.J. (Marieke) Dubelaar, hoogleraar straf(proces)recht, Strafrecht & Criminologie, Onderzoekscentrum Staat en Recht, Radboud Universiteit; dr. mr. S.M.A. (Sjarai) Lestrade, universitair hoofddocent straf(proces)recht), Strafrecht & Criminologie, Onderzoekscentrum Staat en Recht, Radboud Universiteit; en dr. mr. T.F. (Tim) Walree, universitair docent burgerlijk recht, Onderzoekscentrum Onderneming & Recht, en Interdisciplinary research hub on digitalization and society (iHub), Radboud Universiteit.

1 Inleiding

Deze studie is gericht op het onderzoeken van gegevens ten behoeve van de opsporing en heeft als centrale vraag welke eisen voortvloeien uit internationale regelgeving voor de normering van gegevensverwerking en op welke wijze een wettelijke regeling ter zake kan worden ingericht. Daarbij ligt de focus op verwerkingshandelingen bestaande uit het doen van onderzoek aan reeds verzamelde strafvorderlijke gegevens dan wel gegevens die in de verschillende politiesystemen aanwezig zijn.[1] Aanleiding voor deze studie vormen de plannen van de wetgever om de huidige wettelijke regeling aan te passen en bevoegdheden ter gegevensverwerking die thans zijn gelegen in het Wetboek van Strafvordering (WvSv) en de Wet politiegegevens (Wpg) te herschikken en waar nodig aan te passen. Om de wijze van normeren nader te doordenken, is bovendien gekeken naar de ervaringen met de Wet op de inlichtingen- en veiligheidsdiensten 2017 (Wiv 2017) waarin bevoegdheden ter vergaring en (verdere) verwerking in één wet zijn geregeld. Voorts is een verkennende studie verricht in een aantal naburige landen om te bezien op welke wijze de eisen die voortvloeien uit het Europese en internationale recht aldaar zijn vertaald naar de wettelijke regelingen en hoe deze regelingen zijn ingericht.

1.1 Achtergrond en aanleiding

1.1.1 Vergaren versus verwerken

Het vergaren van gegevens ten behoeve van het ophelderen van strafbare feiten vormt van oudsher een belangrijk onderdeel van het takenpakket van de politie.[2] Deze gegevens kunnen door middel van uiteenlopende opsporingsmethoden worden verzameld. Door de digitalisering van de maatschappij zijn de mogelijkheden tot het vergaren van persoonsgegevens verder toegenomen. In het kader van de lopende wetgevingsoperatie inzake de modernisering van het WvSv is uitvoerig gediscussieerd over de vraag hoe de bevoegdheden tot het vergaren van

1 Zie voor een nadere terminologische duiding paragraaf 1.4.

2 Onder persoonsgegevens verstaan wij conform art. 1 onder b Wpg alle informatie over een geïdentificeerd of een identificeerbare natuurlijke persoon. Voor het leesgemak duiden wij persoonsgegevens ook wel aan als gegevens.

(persoons)gegevens wettelijk moeten worden genormeerd. De vergaring van deze gegevens vormt immers snel een inbreuk op het recht op privacy en als dat het geval is, moet hiervoor een wettelijke basis bestaan met voldoende waarborgen tegen misbruik. Thans ligt er een conceptvoorstel voor een nieuw WvSv met daarin een aantal nieuwe bevoegdheden ter *vergaring* van (persoons)gegevens.

Een onderwerp dat binnen de strafvorderlijke context vooralsnog minder aandacht heeft gekregen, betreft de *verwerking* van de reeds vergaarde (persoons)gegevens. In de praktijk vergaren de opsporingsautoriteiten niet alleen gegevens, zij nemen deze gegevens ook regelmatig over in de politiesystemen om deze later al dan niet met behulp van geavanceerde *data science* technieken te doorzoeken, te ordenen, te analyseren of in verband te brengen met andere gegevens. Alle handelingen die met gegevens worden verricht nadat deze zijn vergaard, worden binnen strafvordering niet meer gerekend tot de 'vergaring', maar aangeduid als de 'verwerking' van gegevens.[3] Zeker in de huidige gedigitaliseerde maatschappij waarin steeds meer gegevens en geavanceerde data-analyse technologieën voorhanden zijn, heeft de politie steeds meer mogelijkheden om gegevens die reeds in de politiesystemen aanwezig zijn, met elkaar te combineren en zodoende een min of meer volledig beeld van iemands privéleven te krijgen.

Daar komt bij dat politie ook steeds vaker grote datasets in handen krijgt waarin nadere zoekacties kunnen worden uitgevoerd, zonder dat er op het moment van verkrijging reeds van een op het individu of een groep toegesneden verdenking sprake hoeft te zijn. Zo heeft de politie recent toegang gekregen tot miljoenen heimelijke berichten die op verschillende servers – zoals die van Ennetcom, PGPSafe, EncroChat en Sky Global – waren opgeslagen, op basis waarvan reeds honderden verdachten zijn aangehouden. Met name voor grote hoeveelheden, in bulk verkregen gegevens geldt doorgaans dat de gegevens op zichzelf niet zoveel zeggen, maar relevant worden wanneer de politie deze gegevens nader analyseert, visualiseert of in verband brengt met andere gegevens. Daarmee verplaatst het zwaartepunt van de door de overheid gemaakte privacy-inbreuk van de vergaring van gegevens veeleer naar de (verdere) verwerking van die gegevens.

1.1.2 Gebrekkige wettelijke normering

Hoewel de verwerking van persoonsgegevens door de recente ontwikkelingen nadrukkelijker dan voorheen onderdeel is geworden van het politieke en

3 Zie in deze zin onder meer *Rapport Commissie Koops* 2018; Schermer 2017.

wetenschappelijke debat[4], is de bestaande wettelijke regeling nog niet aangepast aan deze nieuwe realiteit, waarbij 1) in toenemende mate gegevens met elkaar worden gecombineerd via geavanceerde technieken en 2) informatie steeds vaker in bulk bij de politie terechtkomt door inbeslagname van grote gegevensdragers; door het hacken van servers of door systematische observatie/registratie zoals het geval is bij de inzet van ANPR (*automatic number plate recognition,* automatische kentekenplaatherkenning). Dat laatste leidt tot allerlei vragen in de praktijk ten aanzien van het verwerken van de vergaarde informatie. Zo is in eerdergenoemde zaken er steeds voor gekozen om de rechter-commissaris – "mogelijk zelfs ten overvloede" of als "extra waarborg" – in te schakelen voor het nader vastleggen van kaders voor het benutten van de vergaarde datasets.[5] Daarbij heeft de rechter-commissaris bepaald op welke wijze de gegevens mogen worden geanalyseerd (onder meer de mogelijke zoeksleutels en de bescherming van het verschoningsrecht en de verifieerbaarheid en reproduceerbaarheid van gegevens) en onder welke voorwaarden gegevens ter beschikking mogen worden gesteld voor andere opsporingsonderzoeken (steeds niet anders dan na voorafgaande toestemming van de rechter-commissaris).[6] De wet voorziet hier echter niet in.[7] In dit verband rijst dan ook de vraag of hiervoor een wettelijke regeling moet komen.

De regels die er wel zijn voor wat betreft de verwerking zijn thans ook over verschillende wetten verspreid. Zo is in het WvSv primair de vergaring ten behoeve van lopend onderzoek geregeld, maar zijn er ook enkele verwerkingsbepalingen opgenomen, terwijl de Wpg juist in teken staat van de (verdere) verwerking, maar daarin onder omstandigheden ook een grondslag wordt gevonden voor

4 Zie onder meer *Rapport Commissie Koops* 2018, p. 25-48; Schermer 2017, p. 207-216; Stevens e.a. 2021, p. 234-245; Dubelaar, Fedorova & Te Molder 2021, p. 53-81.

5 Zie bv. Rb. Midden-Nederland 17 juni 2021, ECLI:NL:RBMNE:2021:2570 en Rb. Amsterdam 3 juli 2021, ECLI:NL:BRAMS:2021:3825.

6 Zie bijvoorbeeld zaken in het zogeheten Tandem-onderzoek waarin miljoenen versleutelde berichten die zich in Canada bevonden in beslag zijn genomen: Rb. Amsterdam 19 april 2018, ECLI:NL:RBAMS:2018:2504; Rb. Amsterdam 7 december 2018, ECLI:NL:RBAMS:2018:8698; Rb. Rotterdam 9 juni 2020, ECLI:NL:RBROT:2020:11875 en enkele zaken waarin met behulp van de Franse autoriteiten servers van Encrochat zijn gehackt: Rb. Oost-Brabant 25 maart 2021, ECLI:NL:RBOBR:2021:1272; Rb. Oost-Brabant 8 juli 2021, ECLI:NL:RBOBR:2021:3249; Rb. Midden-Nederland 17 juni 2021, ECLI:NL:RBMNE:2021:2570; Rb. Amsterdam 14 september 2021, ECLI:NL:RBAMS:2021:5460. Met betrekking tot Sky Global (Sky ECC) zie bv. Rb. Midden-Nederland 17 juni 2021, ECLI:NL:RBMNE: 2021:2570. Zie ook Dubelaar, Fedorova & Te Molder 2021, p. 73-74.

7 Het ter beschikking stellen van gegevens aan andere onderzoeken is thans geregeld in art. 126dd WvSv en deze bepaling bevat als eis dat een Officier van Justitie hier toestemming voor moet geven.

het doen van nader onderzoek. In de Wet justitiële en strafvorderlijke gegevens (Wjsg) is de verwerking van persoonsgegevens door andere autoriteiten zoals het Openbaar Ministerie geregeld. Bij aanvang van dit onderzoek had de wetgever het plan opgevat om een nieuwe gegevensverwerkingswet te ontwerpen die de huidige Wpg en de Wjsg zou incorporeren.[8] Daarbij zouden de huidige artikelen 126cc-dd WvSv die gaan over de (verdere) verwerking voor wat betreft enkele bijzondere opsporingsbevoegdheden in het gemoderniseerde WvSv komen te vervallen. De gedachte daarbij was dat de vergaring van gegevens het beste in het WvSv zou kunnen worden geregeld en de verwerking ervan in de nieuwe gegevensverwerkingswet. De vraag is evenwel of beide activiteiten zich wel op deze wijze laten scheiden en wat de mogelijke implicaties zijn van een dergelijke separate normering. Inmiddels is duidelijk geworden dat er (op korte termijn) geen geheel nieuwe gegevensverwerkingswet gaat komen. Maar de vraag naar wat nu waar moet worden geregeld is nog wel aan de orde, nu in het voorstel voor het gemoderniseerde WvSv thans niets is geregeld omtrent de verdere verwerking van gegevens.

1.1.3 Inrichting nieuwe regeling

Bij het nader vormgeven van een nieuwe regeling of het aanpassen van de bestaande regelingen in het WvSv en de Wpg doet zich in elk geval een aantal complicaties voor. De eerste complicatie is gelegen in het samenkomen van twee rechtsgebieden, te weten strafvordering en gegevensbeschermingsrecht die op andere principes en beginselen zijn gestoeld. Hierbij is van belang dat in het WvSv op een andere manier invulling wordt gegeven aan rechtsbescherming dan de huidige Wet politiegegevens. Waar het in strafvordering gaat om het identificeren en bestraffen van de werkelijk schuldige aan een strafbare gedraging (en het vrijwaren van de onschuldige), is de verwerking van (vooralsnog) de politiegegevens voornamelijk ingegeven door het stroomlijnen van de gegevenshuishouding van het justitiële apparaat in het kader van een fatsoenlijke bescherming van de (individuele) privacybelangen.

Een tweede complicatie die met het voorgaande samenhangt, is dat er veel onduidelijkheid bestaat over de eisen en waarborgen die in Europees verband worden gesteld aan verwerking van persoonsgegevens. Dat speelt vooral bij gegevens die in bulk zijn verkregen of reeds in politiesystemen liggen opgeslagen, waar de jurisprudentie de ontwikkelingen in de praktijk volgt. De jurisprudentie van het EHRM en het Hof van Justitie EU op dit thema ontwikkelt zich in rap tempo,

8 Memorie van Toelichting (ambtelijke versie 2020), p. 228. Zie voorts over het voornemen de Wpg en de Wjsg samen te voegen: *Kamerstukken II* 2013/14, 33 842, nr. 2, p. 3.

waarbij een systematisch overzicht van de geldende eisen en beperkingen ontbreekt. Ook over de eisen die voortvloeien uit de EU Richtlijn 2016/680 bestaat onduidelijkheid.[9] Zo kent de richtlijn veel open begrippen die in het kader van opsporing nadere uitwerking behoeven en waarvan niet op voorhand duidelijk is op welke wijze een en ander zijn beslag moet krijgen in een wettelijke regeling.

Samenvattend kan worden gesteld dat zowel ten aanzien van de inhoud van de normering (de toepasselijke eisen en waarborgen inzake het gebruik van gegevens) als voor wat betreft de wijze van normering (hoe kan dit op een inzichtelijke wijze worden geregeld?) de nodige vragen zich opwerpen. Deze vragen zijn niet uniek voor de strafvorderlijke context, ze komen ook terug in de context van het inlichtingenwerk dat zijn wettelijke basis vindt in de Wiv 2017. Daarom zal eveneens naar inzichten op basis van de ontwikkeling van deze wetgeving worden gekeken. Tevens is Nederland niet het enige land dat zich met deze nieuwe realiteit en de daaruit voortvloeiende vragen geconfronteerd ziet, hetgeen reden vormt een blik over de grens te werpen om te bezien hoe deze thematiek elders geregeld is dan wel opgepakt wordt. Welke keuzes worden gemaakt en wat zijn mogelijke implicaties voor de rechtsbescherming?

1.2 Vraagstelling

Het voorgaande leidt tot de volgende onderzoeksvragen.

1. Waar liggen de juridische knelpunten in het huidige wettelijke kader ter zake van het doen van onderzoek aan vergaarde (persoons)gegevens voor strafvorderlijke doeleinden?
2. Welke eisen en waarborgen stellen relevante Europeesrechtelijke rechtsbronnen aan de normering van het verwerken van (persoons)gegevens voor strafvorderlijke doeleinden?
3. Welke voor deze normering relevante gezichtspunten kunnen worden ontleend aan de Wiv 2017 en het recht in België, Duitsland en Noorwegen?

De eerste onderzoeksvraag betreft het in kaart brengen van het huidige wettelijke kader en het nader exploreren van de knelpunten zoals die onder meer door recente ontwikkelingen aan het licht zijn gekomen. Vervolgens wordt bij de tweede onderzoeksvraag geanalyseerd welke eisen het Europese recht stelt ten aanzien

9 Zie onder meer Stevens e.a. 2021, p. 240; Winter e.a. 2020, p. 23.

van het normeren van strafrechtelijk onderzoek aan reeds verzamelde gegevens. De Nederlandse regeling moet immers aan de internationale standaarden voldoen. De focus ligt primair bij Europeesrechtelijk rechtsbronnen. Deze bronnen geven overigens vooral richting ten aanzien van de inhoud van de normering en niet zo zeer de vorm of de wijze waarop de regeling wordt ingericht. Inspiratie ten aanzien van de inhoud én de wijze waarop een regeling kan worden vormgegeven wordt voorts opgedaan door kennis te nemen van de inzichten die zijn verkregen bij de ontwikkeling van de Wiv 2017 en het recht in naburige landen, zoals dat tot uitdrukking komt in de derde onderzoeksvraag. De Wiv 2017 en het recht in naburige landen bieden weliswaar geen normatieve aanknopingspunten of richtsnoeren, maar er kunnen mogelijk wel lessen worden getrokken uit de wijze waarop in andere contexten en in andere landen met de geconstateerde knelpunten wordt omgegaan en hoe de regelingen vervolgens zijn ingericht. Deze verkenning dient dan ook vooral ter inspiratie en reflectie.

1.3 Focus en afbakening

De kern van dit onderzoek ziet op onderzoek van gegevens voor strafvorderlijke doeleinden. De term onderzoek wordt hierbij als overkoepelende term gebezigd voor allerlei handelingen met betrekking tot reeds vergaarde gegevens ter realisering van strafvorderlijke doelen (waarheidsvinding of opbouwen van een informatiepositie). Onderzoek van gegevens omvat dan ook verschillende handelingen. Vanuit analytisch oogpunt is het nuttig om onderscheid te maken tussen twee verschillende vormen van onderzoek.

1) Onderzoek met als doel om gegevens te ontsluiten voor de opsporing
Een opsporingsbevoegdheid wordt ingezet om informatie te vergaren die kan worden gebruikt voor het proces van waarheidsvinding tijdens de opsporing of tijdens de zitting. Soms is direct gebruik van de gegevens niet mogelijk, omdat een opsporingsbevoegdheid zodanig veel gegevens oplevert dat eerst nader moet worden onderzocht wat de gegevens inhouden. In deze gevallen moet dus onderzoek plaatsvinden voordat de vergaarde gegevens daadwerkelijk voor operationele doeleinden kunnen worden benut.

2) Onderzoek met als doel het opbouwen van een informatiepositie – los van een concreet opsporingsonderzoek

In sommige gevallen zullen de opsporingsautoriteiten reeds vergaarde informatie ook willen onderzoeken om – los van concrete opsporingsonderzoeken – een informatiepositie op te bouwen. Zo kan het bijvoorbeeld nuttig zijn om gegevens die in de systemen van de politie aanwezig zijn bij elkaar te brengen om zo informatieproducten te genereren, bijvoorbeeld om nader inzicht te krijgen in de omvang van een crimineel samenwerkingsverband.

In deze focusbepaling ligt een aantal belangrijke afbakeningen besloten. Dit onderzoek is niet in de eerste plaats gericht op de daadwerkelijke vergaring van gegevens en de wijze waarop dat is genormeerd.[10] Het accent ligt op de fase daarna. In de tweede plaats betreft dit onderzoek het gebruik van gegevens voor *strafvorderlijke doeleinden*. Dit houdt in dat het onderzoek gericht moet zijn op het aan het licht brengen van strafbare feiten, ook al bestaat nog geen concreet zicht op deze feiten. Het begrip strafvorderlijke doeleinden is breder dan het vergaren van bewijs of de opsporing van reeds begane strafbare feiten. De politie is immers de afgelopen decennia steeds pro-actiever gaan werken; het optreden is in toenemende mate gericht op het in kaart brengen en doorgronden van criminele netwerken en organisaties die wellicht strafbare feiten plegen of zullen gaan plegen.[11] Ook het opbouwen van een informatiepositie met als doel om zicht te krijgen op reeds gepleegde of nog te plegen strafbare feiten, rekent de politie tot haar taak.[12] Het gebruik van gegevens voor buiten strafvordering gelegen doelen zoals de handhaving van de openbare orde valt hiermee buiten het bereik van dit onderzoek. In de derde plaats ligt de nadruk op specifieke verwerkingshandelingen gericht op kennisvermeerdering. Daarbij valt te denken aan het combineren of verrijken van gegevens. Anders gezegd: het onderzoek is gericht op verwerkingshandelingen die moeten bijdragen aan het versterken van de informatiepositie van de politie in het algemeen, dan wel het ophelderen en bewijzen van concrete strafbare feiten in het bijzonder. Meer 'klassieke' verwerkingshandelingen zoals de regels inzake het

10 De vergaring van gegevens is geregeld in het WvSv en de Polw. 2012.

11 Dit komt onder meer tot uitdrukking in de mogelijkheid tot het verrichten van een verkennend onderzoek op grond van art. 126gg WvSv waarmee de politie probeert zicht te krijgen op sectoren van de samenleving waarbinnen misdrijven worden beraamd of gepleegd en in de mogelijkheden die het WvSv biedt om informatie te vergaren zonder dat reeds sprake is van een verdenking van een concreet strafbaar feit (bijvoorbeeld bij aanwijzingen van terrorisme). Daar komt bij dat de politie ook inlichtingen verzamelt op basis van de algemene taakstelling zoals neergelegd in art. 3 Polw. 2012. Zie voorts Van den Eeden e.a. 2021, p. 84 waar wordt geconstateerd dat de politie in relatie tot cybercriminaliteit zich ook meer wil toeleggen op het opbouwen van een informatiepositie.

12 De politie gaat daarin dus minder reactief te werken dan vroeger. Zij gaat zelf actief op zoek naar organisaties en groepen waarbinnen mogelijk strafbare feiten worden gepleegd of beraamd.

opslaan van gegevens van een getuige, het gebruik van vingerafdrukken of gegevens afkomstig van DNA-onderzoek vallen (grotendeels) buiten het bestek van deze studie.[13] Bij de variëteit van verwerkingshandelingen en het brede verwerkingsbegrip wordt hieronder nader stilgestaan.

1.4 Terminologie

Verwerkingshandelingen

Uit het voorgaande wordt duidelijk dat de focus ligt op het verrichten van onderzoek aan reeds vergaarde gegevens. Het proces van vergaring en de daaraan verbonden wettelijke en jurisprudentiële waarborgen is dus niet zelfstandig object van onderzoek, maar wordt uitsluitend bezien in relatie tot het proces van (verdere) verwerking van die gegevens. Terminologisch ligt daar evenwel een complicatie. Vanuit gegevensbeschermingsrechtelijk oogpunt kan het onderscheid tussen vergaring en verwerking tot verwarring leiden, nu het vergaren of verzamelen van gegevens binnen de Wpg wordt gezien als een vorm van verwerking. In de Wpg wordt namelijk onder de verwerking van gegevens simpelweg elke handeling verstaan die met gegevens kan worden verricht.[14] Als voorbeelden van verwerkingshandelingen worden in artikel 1 onder c Wpg genoemd 'het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, afschermen of vernietigen van politiegegevens'. De Wpg gaat dus uit van een breed verwerkingsbegrip. Vanuit die terminologie bezien betreft dit onderzoek in feite de *verdere* verwerking van gegevens. Om terminologische verwarring zoveel mogelijk te vermijden zal in het vervolg van deze studie met de term *verwerking* in beginsel worden verwezen naar het bredere concept. Gaat het om (alle) handelingen die op de vergaring volgen, dan wordt gesproken van *het gebruik* of *verdere verwerking* van gegevens. Dit onderzoek gaat echter specifiek over het uitvoeren van onderzoek aan reeds vergaarde gegevens voor strafvorderlijke doelen, hetgeen meerdere verwerkingshandelingen kan omvatten.

13 Termijnen voor opslag en dergelijke komen alleen aan de orde voor zover rechtstreeks relevant voor de operationele praktijk.

14 Een dergelijk breed verwerkingsbegrip is ook terug te vinden in art. 4 lid 2 AVG en in art. 1 onder f Wiv 2017.

Gegevens

Ook het begrip gegevens vraagt om nadere toelichting, mede in relatie tot de focus van dit onderzoek. Er is veel variëteit in gegevens die ten behoeve van de opsporing worden verzameld en verder verwerkt. In dit onderzoek richten wij ons primair op persoonsgegevens waarbij de definitie uit de Wpg wordt aangehouden. Het gaat om gegevens die betrekking hebben op identificeerbare of geïdentificeerde, individuele natuurlijke personen.[15] Niet-persoonsgegevens zoals bijvoorbeeld informatie over een plaats-delict vallen daarmee buiten het bereik van dit onderzoek. In dit rapport zullen wij de begrippen gegevens en persoonsgegevens als synoniemen hanteren. De keuze voor de focus op persoonsgegevens is ingegeven doordat juist voor dit type gegevens nadere waarborgen noodzakelijk zijn in het licht van het recht op bescherming van persoonsgegevens en het recht op privacy. Tegelijk constateren wij dat de definitie van persoonsgegevens nauwelijks bijdraagt aan de afbakening van dit onderzoek. In het kader van de opsporing verzamelen en verwerken de opsporingsautoriteiten nu eenmaal een groot aantal zeer verschillende soorten persoonsgegevens van verschillende typen personen (verdachten, getuigen, aangevers). Een bijzonder punt van aandacht in dit onderzoek vormen zogenaamde bulkgegevens, waartoe dit onderzoek overigens niet is beperkt. Onder bulkgegevens worden in dit onderzoek gegevens verstaan die zich bevinden in bulkdatasets. Voor de term bulkdataset zoeken wij aansluiting bij de terminologie zoals die ook wordt gebruikt in artikel 1 onder a van de Tijdelijke regeling verwerking bulkdatasets Wiv 2017, namelijk 'een omvangrijke gegevensverzameling waarbij het merendeel van de gegevens betrekking heeft op organisaties en/of personen die geen onderwerp van onderzoek zijn [..] en dat ook niet worden'.

Normering

In voorgaande is nader stilgestaan bij het object van onderzoek namelijk de activiteit van het verrichten van 1) onderzoek aan 2) gegevens voor 3) strafvorderlijke doeleinden. De vraag daarbij is hoe die activiteit *genormeerd* moet worden en wat dat betekent voor de inrichting van een nieuwe wettelijke regeling. Met het begrip normeren in strafvorderlijke context doelen we op het stellen van normen aan bepaald strafvorderlijk optreden met als doel het sturen van het gedrag van

15 Art. 1 onder b Wpg. De definitie van "gegevens" in het gemoderniseerde WvSv is "iedere weergave van feiten, begrippen of instructies, op een overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken", art. 2.1.1 nieuw Sv.

overheidsfunctionarissen.[16] Wij richten ons daarbij op het normeren door de wetgever in de vorm van formuleren van nadere regels dan wel richtinggevende beginselen. Omdat de activiteit van normeren onlosmakelijk verbonden is met het houden van toezicht op de naleving van de normen, zal ook daaraan aandacht worden besteed.

1.5 Methodologie

1.5.1 Toelichting per onderzoeksvraag

Het onderzoek ten behoeve van de *eerste onderzoeksvraag* naar de vormgeving van en de problemen in het huidige juridische kader heeft bestaan uit een deskresearch naar wetgeving, parlementaire documentatie, jurisprudentie, beleidsdocumenten en wetenschappelijke commentaren. Aan de hand van die bronnen zijn de verschillende regelingen die op de verwerking van gegevens binnen de context van de opsporing en hun onderlinge verhouding van toepassing zijn in kaart gebracht. Tevens is gekeken naar de vraag welke knelpunten daarbij in de jurisprudentie en literatuur zijn geconstateerd voor wat betreft de inrichting van de regelingen en de inhoud van de normering. Bij de analyse van de mogelijke gebreken in het juridisch kader is tevens aandacht besteed aan mogelijke alternatieven voor de huidige regeling zoals die tot uitdrukking komen in de plannen van de wetgever in het kader van de modernisering van het WvSv. Om de huidige regeling beter te doorgronden en zicht te krijgen op de problemen in de praktijk zijn voorts interviews met 19 professionals gehouden met diverse wetenschappelijke dan wel beroepsmatige achtergronden. Bij de selectie van respondenten en de methode van interviews wordt hieronder nader stilgestaan.

Ter beantwoording van de *tweede onderzoeksvraag* naar het Europeesrechtelijk kader zijn verschillende rechtsbronnen bestudeerd. Allereerst is in kaart gebracht welke eisen de EU Richtlijn 2016/680 ofwel de *Law Enforcement Directive* stelt aan het gebruik van in de opsporing verkregen gegevens. Voorts is relevante jurisprudentie van het EHRM inzake het recht op privacy zoals neergelegd in artikel 8 EVRM en het Hof van Justitie EU inzake artikel 7 en 8 HGEU bestudeerd. Bij deze analyse is aansluiting gezocht bij secundaire literatuur die nader inzicht verschaft in deze regelgeving en jurisprudentie. Daarbij valt bijvoorbeeld te denken aan wetenschappelijke commentaren, openbare onderzoeksrapporten, toelichtingen en andere beleidsdocumenten. Bij beantwoording van de tweede onderzoeksvraag is

16 Zie over normering meer uitgebreid Samadi 2020, p. 22 e.v.

geen aandacht besteed aan de Conventie 108+ nu dit verdrag voor wat betreft het in dit onderzoek centraal gestelde onderwerp grotendeels overlapt met de Richtlijn 2016/680 en bovendien nog niet in werking is getreden. Ook wordt in dit onderzoek geen aandacht besteed aan de (mogelijk) normerende werking die van artikel 6 EVRM uitgaat ten aanzien van onderzoek aan gegevens.[17]

Aan de *derde onderzoeksvraag* ligt een vergelijkende methode ten grondslag. Er is in dit verband gekeken naar de Wiv 2017 en naar de regelingen in enkele naburige landen. Zowel de interne rechtsvergelijking met de Wiv 2017 als de verkennende externe rechtsvergelijking met het buitenland heeft plaatsgevonden aan de hand van een deskstudie aangevuld met interviews. Bij de deskstudie naar de Wiv 2017 is gekeken naar de wet zelf, de parlementaire geschiedenis, literatuur en de bevindingen van de commissie Jones-Bos die de Wiv 2017 recent heeft geëvalueerd. Voor wat betreft de verkennende rechtsvergelijking met het buitenland is gekozen voor een drietal landen, te weten België, Duitsland en Noorwegen. Dat onderzoek berust op deskresearch aangevuld met interviews met respondenten uit de drie verschillende landen. Bij de selectie van landen en respondenten wordt in het vijfde hoofdstuk nader stilgestaan.

De centrale onderzoeksbevindingen zijn besproken in een zogeheten *expertmeeting* waaraan een drietal wetenschappers met verschillende achtergronden en een drietal politieambtenaren met ervaring met strafvordering en de Wpg deelnamen.[18] Doel van deze expertmeeting was te reflecteren op de resultaten van het onderzoek en de lessen die daaruit vallen te trekken met het oog op de aanpassing van de bestaande wettelijke regeling.

1.5.2 Nadere toelichting op de interviews

Naast een deskresearch zijn als gezegd in het kader van dit onderzoek ook interviews gehouden met respondenten in Nederland, België, Duitsland en Noorwegen. Er is gesproken met professionals uit de strafrechtspraktijk die te maken hebben met gegevensverwerking alsmede met wetenschappers die ervaring hebben opgedaan met op strafvorderlijke gegevensverwerking toepasselijke regelgeving,

17 Over art. 6 EVRM in relatie tot onderzoek van grote hoeveelheden gegevens is reeds een en ander geschreven. De vraag is immers hoe de uit art. 6 EVRM voortvloeiende verdedigingsrechten kunnen worden verwezenlijkt als met behulp van allerlei technieken grote hoeveelheden gegevens worden onderzocht. Zie onder meer Schermer & Oerlemans 2020; Galič 2021; Dubelaar, Fedorova & Te Molder 2021. Zie voorts ook HR 28 juni 2022, ECLI:NL:HR:2022:900.

18 Deze expertmeeting is gehouden op 15 juni 2022. Zie bijlage voor de lijst met deelnemers.

dan wel een bijzondere expertise hebben op het gebied van gegevensverwerking en/of strafvordering. In totaal is met negentien respondenten gesproken.

Voor wat betreft de Nederlandse rechtspraktijk is gesproken met een senior rechter, een Officier van Justitie, een lid van de politie, een strafrechtadvocaat, een adviseur bij de afdeling bestuursondersteuning van de AIVD die zich bezighoudt met de herziening van de Wiv 2017 en twee (beleids)medewerkers van de AP. Daarnaast zijn ook experts op het gebied van de Europees (privacy en gegevensbeschermings)recht en Richtlijn 2016/680 geïnterviewd. Ten aanzien van de respondenten uit het buitenland is zowel gesproken met wetenschappers die zich bezighouden met de thematiek van het normeren van gegevensverwerking in het strafrecht als met ervaringsdeskundigen die in hun dagelijkse werk van doen hebben met gegevensverwerking ten behoeve van strafrechtelijk onderzoek. Zowel in België, Duitsland als Noorwegen zijn drie verschillende respondenten geïnterviewd. Een lijst met geïnterviewde personen is opgenomen in Bijlage I bij dit onderzoek.

De interviews dienden enerzijds ter verkenning van de uitgangspunten van de normering van het verwerken van persoonsgegevens, anderzijds is beoogd met de interviews een zo volledig mogelijk beeld te krijgen met name ook omtrent de inhoud en wijze van normering van gegevensverwerking in het buitenland. De interviews zijn gehouden met één of twee respondenten tegelijkertijd, en hebben zowel fysiek als digitaal plaatsgevonden. Bij elk interview waren steevast twee en soms drie onderzoekers aanwezig. Ieder interview is vervolgens teruggeluisterd door een student-assistent die de gesprekken heeft getranscribeerd.

De interviews waren kwalitatief van aard en vonden semigestructureerd plaats op basis van een topiclist die steeds is aangepast op basis van de expertise en/of functie van de desbetreffende respondent. De keuze voor semigestructureerde interviews is gebaseerd op meerdere, vooraf geformuleerde onderwerpen/vragen die bij (bijna) alle respondenten aan bod dienden te komen, terwijl tevens ruimte diende te bestaan voor het doorvragen/uitdiepen van onderwerpen als de antwoorden van respondenten daartoe aanleiding gaven. Er is voor kwalitatieve interviews gekozen vanwege het verkennende karakter van het te verrichten onderzoek en vanwege de relevantie van de eigen opvattingen van de respondenten over de verwerking van persoonsgegevens voor de opsporing.

1.6 OPBOUW VAN HET RAPPORT

Het rapport is als volgt opgebouwd: in het tweede hoofdstuk wordt het bestaande wettelijk kader uiteengezet waarbij tevens aandacht wordt besteed aan de voorlopige plannen van de wetgever om de regeling aan te passen. Aan het slot van dit hoofdstuk worden enkele aandachts- of knelpunten benoemd die volgen uit het nationale kader en die richting geven aan het vervolg van het onderzoek. Zij vormen als het ware 'de bril' van waaruit naar de andere contexten wordt gekeken. In het derde hoofdstuk wordt het relevante Europeesrechtelijk kader besproken en geanalyseerd. Zoals zal blijken, is de jurisprudentie ten aanzien van strafvorderlijke gegevensverwerking volop in ontwikkeling. Voorts zijn er ten aanzien van de Richtlijn 2016/680 de nodige interpretatievragen. In het vierde hoofdstuk wordt vervolgens gekeken naar de ervaringen met de Wiv 2017 en in het vijfde hoofdstuk naar de ervaringen in de drie vergelijkingslanden. In die hoofdstukken wordt besproken op welke wijze in de Wiv 2017 en de vergelijkingslanden invulling is gegeven aan Europeesrechtelijke eisen en waarborgen en welke keuzes aldaar zijn gemaakt voor wat betreft de inrichting en de inhoud van de respectieve regelingen. Daarbij is tevens aandacht besteed aan de vraag in hoeverre die regelingen naar tevredenheid functioneren. In het zesde (slot)hoofdstuk worden de lijnen bij elkaar gebracht en wordt nader gereflecteerd op de bevindingen uit de eerdere hoofstukken met het oog de inrichting van een nieuwe regeling en de keuzes die in dit verband voorliggen.

2 Het huidige en het gemoderniseerde wettelijke kader voor onderzoek aan gegevens voor strafvorderlijke doeleinden

2.1 Inleiding

Dit hoofdstuk biedt een antwoord de volgende deelvraag: *Waar liggen de knelpunten in het huidige wettelijke kader voor wat betreft het doen van onderzoek aan reeds vergaarde (persoons)gegevens voor strafvorderlijke doeleinden?* Daartoe wordt uiteengezet hóe de normering van opsporingsonderzoek aan reeds verkregen gegevens thans is genormeerd. Daarbij gaat de aandacht in het bijzonder uit naar twee wetten: de Wet politiegegevens (Wpg) en het Wetboek van Strafvordering (WvSv). Allereerst wordt in paragraaf 2.2 stilgestaan bij de vraag welke onderwerpen in welke wetten zijn geregeld en waarom daarvoor is gekozen. Daarna wordt in paragraaf 2.3 nader stilgestaan bij de wijze van normering in deze wetten. Bij deze bespreking ligt het zwaartepunt op de wettelijke systematiek, beginselen en uitgangspunten. Ook zal aandacht worden besteed aan de wijze waarop toezicht wordt uitgeoefend op de uitvoering van deze wetten. Normering is immers zoals eerder aangegeven nauw verweven met toezicht.[19] Ter afsluiting van dit hoofdstuk volgt in paragraaf 2.4 een overzicht van de belangrijkste knelpunten die voortvloeien uit het huidige juridische kader inzake onderzoek aan reeds verkregen gegevens ten behoeve van de opsporing.

2.2 Structuur wet- en regelgeving

In het huidige juridische kader zijn twee wetten in het bijzonder van belang voor de normering van het doen van onderzoek aan gegevens ten behoeve van strafvorderlijke doeleinden: de Wet politiegegevens (Wpg) en het Wetboek van Strafvordering (WvSv). In het hiernavolgende wordt stilgestaan bij de vraag welke onderwerpen in welke wetten zijn geregeld, waarom daarvoor is gekozen en hoe deze wetten zich tot elkaar verhouden.

19 Zie hoofdstuk 1, onder terminologie.

2.2.1 Wet politiegegevens (Wpg)

Van belang voor de normering van het opsporingsonderzoek aan in de opsporing verkregen persoonsgegevens is ten eerste de Wpg. De reikwijdte van de Wpg volgt uit artikel 2 Wpg dat kort gezegd bepaalt dat de wet van toepassing is op de verwerking van politiegegevens. Politiegegevens zijn persoonsgegevens die worden verwerkt in het kader van de politietaak als bedoeld in artikel 3 en artikel 4 Politiewet 2012 (Polw. 2012).[20] Een van deze taken betreft de daadwerkelijke handhaving van de rechtsorde, waaronder de opsporing van strafbare feiten is te scharen.

Voor de definitie van *persoonsgegevens* is in de Wpg aansluiting gezocht bij de definitie in het algemene persoonsgegevensbeschermingsrecht: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.[21] Van persoonsgegevens is dus sprake als deze een persoon identificeren of herleidbaar naar hem of haar zijn. Zo is een telefoonnummer als zodanig geen persoonsgegeven, maar wel als een telefoonnummer is te herleiden tot een concreet persoon of samen met een naam wordt verwerkt.[22]

Onder *verwerken* wordt verstaan elke bewerking of elk geheel van bewerkingen met betrekking tot politiegegevens of een geheel van politiegegevens.[23] De Wpg geeft in artikel 1, onder c, een niet-uitputtende lijst van voorbeelden: "verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, samenbrengen, met elkaar in verband brengen, afschermen of vernietigen". Het begrip verwerken heeft dus betrekking op het gehele proces dat een persoonsgegeven doormaakt vanaf het moment dat het is verzameld tot aan het moment van vernietiging.[24]

Mede vanwege het brede bereik van de Wpg is deze wet ook van toepassing op het reguleren van onderzoek aan reeds vergaarde gegevens voor strafvorderlijke doeleinden. Tegelijkertijd is deze wet niet enkel op deze activiteiten toegesneden. De Wpg is veeleer te beschouwen als een wet waarin is geregeld hoe de politie met persoonsgegevens moet omgaan, ongeacht hoe zij deze gegevens heeft verkregen. Daarnaast ziet de Wpg niet alleen op het verwerken van gegevens voor strafvorderlijke doeleinden, ook het verwerken van gegevens verkregen in het

20 Artikel 1, onder a, Wpg.
21 Artikel 1, onder b, Wpg.
22 HvJ EG 6 november 2003, C-101/01, ECLI:EU:C:2003:596 (*Lindqvist*), par. 24.
23 Artikel 1, onder c, Wpg.
24 De definitie van verwerken in de Wpg komt dus overeen met de definitie van verwerken in artikel 4, onderdeel 2, AVG. Zie hierover Kranenborg & Verhey 2018, p. 111-112.

kader van de openbare ordetaak van de politie is in de Wpg geregeld. Niettemin bevat de Wpg wel een aantal belangrijke bepalingen over onder meer het hergebruik van gegevens die in de opsporing zijn vergaard voor andere doelen en het opbouwen van een informatiepositie.

2.2.2 Wetboek van Strafvordering (WvSv)

Naast de Wpg is ook het WvSv van belang voor de normering van het opsporingsonderzoek aan gegevens. Voor een goed begrip van deze bepalingen moet worden bedacht dat het gebruik van gegevens in beginsel ligt besloten in de bevoegdheid tot vergaring. Aan het gebruik of de verwerking van gegevens is dan ook relatief weinig aandacht besteed in strafvordering. In het WvSv is een aantal bepalingen neergelegd, waarin specifiek eisen worden gesteld aan de verwerking van gegevens die met bepaalde opsporingsmethoden zijn verkregen. Anders dan in de Wpg het geval is, zijn deze bepalingen steeds gekoppeld aan een aantal specifieke opsporingsbevoegdheden. Het gaat om een bonte verzameling bepalingen die in de loop van de jaren, in het kader van verschillende wetgevingsoperaties aan het WvSv zijn toegevoegd:[25]

- Artikel 125n WvSv stelt eisen aan het bewaren en vernietigen van gegevens die zijn vastgelegd tijdens een doorzoeking.26
- Artikel 126nb WvSv, vierde lid, stelt eisen aan het bewaren en vernietigen van gegevens die zijn verkregen met het bevel tot nummeridentificatie.27
- Artikel 126cc/dd WvSv stellen eisen aan het bewaren, vernietigen en gebruiken van gegevens die met enkele bijzondere opsporingsbevoegdheden zijn verkregen.28
- Artikel 126jj WvSv stelt eisen aan het bewaren, vernietigen en raadplegen van ANPR-gegevens die op basis van dit artikel zijn verkregen.[29]

25 Het WvSv bevat meer bepalingen over de verwerking van gegevens, bijvoorbeeld over het verwerken van DNA, foto's of vingerafdrukken. Deze onderwerpen vallen echter buiten het bereik van dit onderzoek.

26 Deze bepaling is het resultaat van de Wet Computercriminaliteit I (*Stb.* 1993, 33) en II (*Stb.* 2006, 300).

27 Ingevoerd in het kader van de Wet wijziging van bepalingen met betrekking tot de verwerking van persoonsgegevens (*Stb.* 2001, 180).

28 Ingevoerd in het kader van de Wet bijzondere opsporingsmethoden (*Stb.* 2000, 32).

29 Ingevoerd in het kader van de Wet vastleggen en bewaren van kentekengegevens door de politie (*Stb.* 2017, 462).

In het kader van dit onderzoek zijn in het bijzonder de artikelen 126cc/dd WvSv van belang. Anders dan in de overige bevoegdheden is in deze artikelen een meer algemene regeling getroffen voor het bewaren, vernietigen en hergebruiken van gegevens die met enkele bijzondere opsporingsbevoegdheden zijn verkregen. Het gaat om de volgende opsporingsbevoegdheden: observatie met behulp van een technisch hulpmiddel, het opnemen van vertrouwelijke communicatie, het opnemen van communicatie of het vorderen van gegevens.

Artikel 126cc WvSv bevat een regeling voor de bewaring en vernietiging van gegevens die met eerdergenoemde bevoegdheden zijn verkregen. Uit artikel 126cc WvSv volgt kort gezegd dat de gegevens die zijn verkregen met de inzet van bijzondere opsporingsbevoegdheden worden bewaard zolang de zaak niet is geëindigd. Als de zaak wel is geëindigd, dienen de gegevens binnen twee maanden te worden vernietigd. Artikel 126cc WvSv geeft invulling aan het zogeheten doelbindingsbeginsel, inhoudende dat gegevens die met bijzondere opsporingsbevoegdheden zijn verkregen in beginsel alleen mogen worden gebruikt voor het specifieke onderzoek waarvoor ze zijn verkregen.[30]

Tegelijkertijd is in artikel 126dd WvSv erkend dat zogeheten doelafwijkend gebruik van gegevens die met de eerdergenoemde bevoegdheden zijn verkregen onder omstandigheden mogelijk is. Op basis van deze bepaling kan de Officier van Justitie bepalen dat de gegevens voor een ander strafrechtelijk onderzoek kunnen worden gebruikt dan waartoe de bevoegdheid is uitgeoefend of voor het opbouwen van een informatiepositie als bedoeld in artikel 10, eerste lid, onderdelen a en b Wpg. De strekking van artikel 126dd WvSv is beperkt. Het doel van deze bepaling is voorschrijven wanneer de elders gebruikte gegevens moeten worden vernietigd.[31]

2.2.3 Verhouding tussen Wet politiegegevens en Wetboek van Strafvordering

Uit het voorgaande volgt dat onderzoek van gegevens die in de opsporing zijn verkregen in zowel de Wpg als WvSv, aan nadere regels is onderworpen. Opvallend hieraan is dat de wetgever in sommige gevallen de noodzaak heeft gezien om onderzoek van gegevens niet in de Wpg, maar in het WvSv te regelen. Kennelijk kon de Wpg in deze gevallen niet volstaan als juridisch kader. Het WvSv staat dan ook in een specialis-verhouding tot de Wpg. In dit verband rijst wel de vraag waarom de wetgever specifiek voor deze opsporingsbevoegdheden en dwangmiddelen de noodzaak heeft gezien om een van de Wpg afwijkende regeling voor de

30 Zie over het doelbindingsbeginsel uitgebreid hoofdstuk 3.

31 *Kamerstukken II* 1996/97, 25403, nr. 3, p. 88.

verwerking van verkregen gegevens te ontwikkelen. Deze vraag klemt temeer indien wordt bedacht dat de wetgever meermaals kenbaar heeft gemaakt dat de vergaring van gegevens in het WvSv moet worden geregeld en de (verdere) verwerking in de Wpg.[32]

Deze vraag laat zich echter niet gemakkelijk beantwoorden, omdat de wetgever deze vraag nooit expliciet onder ogen heeft gezien. Voor een aantal van de verwerkingsbepalingen in het WvSv is keuze voor plaatsing in het WvSv niet verwonderlijk, nu deze bepalingen dateren van voor de inwerkingtreding van de Wpg. Maar ook in het kader van de verwerkingsbepalingen die ná de inwerkingtreding van de Wpg aan het WvSv zijn toegevoegd, is de wetgever nooit expliciet ingegaan op de vraag waarom in het WvSv soms een van de Wpg afwijkende regeling is ontwikkeld. Illustratief is hier de memorie van toelichting van de Wpg. Hierin wordt weliswaar opgemerkt dat in het WvSv ten aanzien van bepaalde gegevens die met enkele bijzondere opsporingsbevoegdheden zijn verkregen van de Wpg afwijkende regels gelden, zonder nader toe te lichten waarom hiervoor is gekozen.[33] De verhouding tussen de Wpg en het WvSv lijkt dus niet het resultaat te zijn van een algemeen uitgangspunt, maar veeleer van verschillende maatschappelijke, politieke en juridische ontwikkelingen.

Uit de ratio van de verwerkingsbepalingen in het WvSv kan niettemin impliciet worden afgeleid dat het bieden van (meer) rechtsbescherming een belangrijk argument is geweest om in het WvSv een van de Wpg afwijkende regeling te ontwikkelen. De hierboven genoemde gegevensverwerkingsbepalingen die in het WvSv zijn opgenomen, bevatten immers steeds strengere en specifiekere normen dan de Wpg.[34] Illustratief zijn hier de bewaar- en vernietigingsregels die in de artikelen 125n WvSv, 126nb WvSv en 126cc WvSv zijn opgenomen. De bewaar- en vernietigingsregels in de Wpg zijn afhankelijk gesteld van het doel van de verwerking en deze doelen zijn soms wel erg ruim geformuleerd, met als gevolg dat de gegevens ook lang kunnen worden bewaard.[35] In het WvSv zijn de bewaar- en vernietigingsregels echter gekoppeld aan de vraag of de strafzaak is geëindigd (artikel 126cc WvSv) of dat de gegevens niet meer van belang zijn voor het onderzoek (artikel 125n en artikel 126nb, vierde lid, WvSv). Ook artikel 126dd WvSv vormt een

32 Zie onder meer *Kamerstukken II* 1996/97, 25403, nr. 3, p. 8; *Kamerstukken II* 2005/06, 30327, nr. 3, p. 3 en 25; *Kamerstukken II* 2012/13, 33542, nr. 3, p. 25. In de literatuur is dat ook breed gesignaleerd. Zie Mac Gillavry 2005, p. 405; Schermer 2017, p. 210; Rapport Commissie Koops 2018, p. 26.

33 *Kamerstukken II* 2005/06, 30327, nr. 3, p. 16.

34 Vgl. in dit verband ook *Rapport Commissie Koops* 2018, p. 59-60.

35 Zie onder meert art. 9 lid 4 Wpg en art. 10 lid 6 Wpg.

verzwaring ten opzichte van het regime in de Wpg. De Wpg kent ook verschillende normen voor doelafwijkend gebruik van gegevens, maar artikel 126dd WvSv is strenger. Voor doelafwijkend gebruik op basis van artikel 126dd WvSv is immers toestemming van de Officier van Justitie vereist, terwijl de Wpg doorgaans alleen eist dat een bevoegd functionaris die vaak werkzaam is bij de politie, toestemming geeft.[36]

2.2.4 Modernisering van het Wetboek van Strafvordering

Ter afsluiting is het goed nader stil te staan bij de plannen inzake de modernisering van het WvSv. In dit kader heeft de wetgever immers kenbaar gemaakt te willen terugkeren naar het uitgangspunt dat de vergaring in het WvSv moet worden geregeld en de verwerking in een specifieke gegevensverwerkingswet, vergelijkbaar met de Wpg. In het gepubliceerde conceptwetsvoorstel voor het nieuwe WvSv zijn de bepalingen over de verwerking van in de opsporing verkregen gegevens geschrapt.[37] De consequentie hiervan is dus ook dat de (recent veel toegepaste)[38] artikelen 126cc/dd WvSv zijn verwijderd. De minister is van plan de geschrapte bepalingen onder te brengen in een nieuwe gegevensverwerkingswet waarin de huidige Wpg en de Wjsg moeten opgaan.[39] Waarom de wetgever er vooralsnog voor kiest om deze bepalingen in deze nieuwe wet onder te brengen is onduidelijk. In 2018 heeft de commissie Koops bijvoorbeeld nog geadviseerd om het toepassingsbereik van de artikelen 126cc/dd WvSv uit te breiden.[40] De reden hiervoor is dat bij digitaal opsporingsonderzoek steeds vaker voorkomt dat gegevens worden vergaard die voor andere doelen van belang kunnen zijn dan het doel waarvoor de gegevens zijn vergaard.

Tegelijkertijd is ook het nieuwe WvSv vooralsnog niet geheel consequent in de uitwerking van het eerdergenoemde uitgangspunt. Artikel 2.7.39 nieuw WvSv voorziet immers onder meer in een regeling voor het uitvoeren van onderzoek aan

36 Art. 126dd lid 1 WvSv.

37 Het gaat om de artikelen 27a, 27b, 55c, 61a, 125m, 125n, derde lid, 126nb, vierde lid, 126cc, 126dd en 151a WvSv. Zie voorts conceptmemorie van toelichting (ambtelijke versie) 2020 voor het nieuwe WvSv, p. 228-229.

38 Zie onder meer Rb. Den Haag 20 januari 2021, ECLI:NL:RBDHA:2021:284; Rb. Zeeland-West-Brabant 24 februari 2021, ECLI:NL:RBZWB:2021:735; Rb. Amsterdam, 30 april 2021, ECLI:NL:RBAMS:2021:2161; Rb. Oost-Brabant 15 december 2021, ECLI:NL:RBOBR:2021:6861; Rb. Oost-Brabant 2 februari 2022, ECLI:NL:RBOBR:2022:312.

39 Memorie van Toelichting (ambtelijke versie 2020), p. 228, 532. Zie voorts over het voornemen de Wpg en de Wjsg samen te voegen: brief van de Minister van Veiligheid en Justitie van 23 juni 2014 (*Kamerstukken II* 2013/14, 33 842, nr. 2, p. 3).

40 *Rapport Commissie Koops* 2018, p. 60.

gegevens nádat deze zijn overgenomen.[41] Strikt genomen gaat het in artikel 2.7.39 nieuw WvSv aldus ook om handelingen die worden verricht, nadat de gegevens zijn vergaard.

2.3 WIJZE VAN NORMERING: UITGANGSPUNTEN, SYSTEMATIEK EN TOEZICHT

De Wpg en het WvSv kennen voor wat betreft de vergaring en verwerking van gegevens goeddeels dezelfde doestellingen. Enerzijds zijn deze wetten bedoeld om de opsporingsautoriteiten, in het bijzonder de politie, de ruimte te bieden om gegevens te vergaren en nader te verwerken. Anderzijds voorzien deze wetten in waarborgen, opdat de rechten en belangen van burgers worden beschermd. Aan deze doelstelling is echter in beide wetten op geheel andere wijze invulling gegeven. Daar waar de normering in de Wpg is te typeren als *principle based,* is in het WvSv gekozen voor een vorm van *rule based* normering. Ook de wijze waarop toezicht wordt uitgeoefend op de Wpg respectievelijk WvSv is wezenlijk anders. In deze paragraaf wordt nader ingegaan op de verschillen in normering en toezicht tussen de Wpg en het WvSv.

2.3.1 Wet politiegegevens: uitgangspunten, wettelijke systematiek en toezicht

2.3.1.1 Uitgangspunten en wettelijke systematiek

De verwerking van persoonsgegevens in de Wpg wordt eerst en vooral genormeerd door de algemene beginselen van gegevensverwerking: rechtmatigheid en behoorlijkheid, doelbinding, dataminimalisatie, juistheid van gegevens, opslagbeperking, integriteit en vertrouwelijkheid. Deze beginselen zijn neergelegd in de artikelen 3-4b Wpg. Deze artikelen brengen aldus een aantal normen tot uitdrukking waaraan elke gegevensverwerking door de politie moet voldoen. Veel van deze beginselen zijn in lijn met de Richtlijn 2016/680 nauwelijks gedefinieerd of nader uitgewerkt.[42]

Illustratief zijn hier de beginselen van noodzakelijkheid en behoorlijkheid. Hoewel het noodzakelijkheidsvereiste is neergelegd in artikel 3 lid 1 Wpg, keert dit vereiste als zodanig niet terug in de specifieke grondslagen op basis waarvan de politie gegevens mag verwerken. Niettemin dient het

41 Voor de leesbaarheid is hier de term 'computer' gebruikt, maar artikel 2.7.39 ziet op digitale-gegevensdragers en geautomatiseerde werken.

42 Zie nader hoofdstuk 3 over deze Richtlijn 2016/680.

noodzakelijkheidsvereiste wel steeds bij toepassing van de Wpg in overweging te worden genomen.[43] Ook het beginsel van behoorlijkheid heeft niet of nauwelijks aandacht gekregen.[44] In de wet noch in de memorie van toelichting is nader toegelicht wat dit beginsel inhoudt. De consequentie hiervan is dat onduidelijk is wat dit beginsel betekent en hoe de politie dit beginsel bij de toepassing van de Wpg in haar afwegingen moet betrekken.

Sommige beginselen hebben daarentegen wel meer uitwerking gekregen. Dat geldt in het bijzonder voor het doelbindingsbeginsel en de daarmee samenhangende beginselen van data-minimalisatie en opslagbeperking.[45] Het doelbindingsbeginsel bestaat uit twee componenten: doelspecificatie en doelbinding.[46] Dit beginsel verplicht er dus toe het doel van de verwerking te expliciteren en vervolgens schrijft het beginsel voor dat gegevens mogen worden verwerkt op een manier die niet onverenigbaar is met dit vooraf gegeven of geformuleerde doel.

De wetgever heeft op twee manieren nadere invulling gegeven aan het doelspecificatiebeginsel. Allereerst heeft de wetgever in de Wpg zelf een aantal doelen onderscheiden binnen de brede politietaak. In het kader van dit onderzoek zijn de volgende doelen van belang: 1) algemene politietaak (artikel 8 Wpg); 2) handhaving rechtsorde concreet geval (artikel 9 Wpg) en 3) het opbouwen van een informatiepositie (artikel 10 Wpg).[47] Het eerste doel dat is te vinden in artikel 8 Wpg, is bedoeld voor het verwerken van gegevens die in het kader van de dagelijkse politietaak zijn verkregen. Hierbij kan onder meer worden gedacht aan surveillance, eenvoudig recherche-/opsporingswerk en het handhaven van wetten en regels.[48] Voor de verwerking van gegevens die door middel van de in het WvSv geregelde opsporingsbevoegdheden zijn verkregen, zijn artikel 9 en 10 Wpg bedoeld. De reden voor het onderscheid tussen enerzijds artikel 8 Wpg en anderzijds artikel 9 en 10 Wpg is gelegen in de ernst van de privacy-inbreuk. Daar waar in het kader van artikel 8 Wpg gegevens worden verwerkt die weinig over iemands privéleven zeggen, gaat het in artikel 9 en 10 Wpg om gegevens die meer prijs kunnen geven over iemands privéleven.

---

43 *Kamerstukken II* 2005/06, 30327, nr. 3, p. 39, 45 en 55.

44 Ook in het Unierecht is dit beginsel nauwelijks geconcretiseerd. Zie daarover H3, § 3.2.1.1.

45 Zie over de relatie tussen de beginselen uitgebreid Koning 2020.

46 Zie hierover nader hoofdstuk 3.

47 In de literatuur worden de volgende doelen aangewezen: algemene politietaak (artikel 8 Wpg); handhaving rechtsorde concreet geval (artikel 9 Wpg); opbouwen informatiepositie (artikel 10 Wpg); beheer en controle van informanten (artikel 12 Wpg); ondersteuning van de politietaak (artikel 13 Wpg).

48 *Kamerstukken II* 2005/06, 30327, nr. 3, p. 38 (MvT).

Mede vanwege de ernst van de inbreuk op privacy heeft de wetgever - ten tweede - voor wat betreft artikel 9 en 10 Wpg in nadere doelspecificatie willen voorzien. Zo heeft de wetgever in het kader van artikel 9 bepaald dat de politie binnen een week nadat is begonnen met de verwerking nader moet specificeren wat het doel van de verwerking precies is. Binnen het brede doel – handhaving van de rechtsorde in een concreet geval – moet de politie dus nog een specifieker verwerkingsdoel formuleren en schriftelijk vastleggen. In artikel 10 Wpg heeft de wetgever voor een andere systematiek gekozen. In artikel 10 Wpg heeft de wetgever nader omschreven welke vormen van criminaliteit en over welke personen gegevens mogen worden verwerkt met als doel het opbouwen van een informatiepositie. Dit artikel verplicht de politie – anders dan artikel 9 Wpg – niet ertoe vooraf op te schrijven wat het doel van de verwerking is. Overigens lijkt de wetgever in de memorie van toelichting wel te suggereren dat ook bij toepassing van artikel 10 Wpg vooraf moet worden geëxpliciteerd wat het doel van de verwerking is.[49] De tekst van artikel 10 Wpg verplicht hier echter niet toe.

Dit vrij complexe systeem van doelbinding heeft de wetgever verder gecompliceerd door bij elk verwerkingsdoel in artikel 8, 9 en 10 Wpg te regelen dat (verder) doelafwijkend gebruik van de gegevens mogelijk is, indien dat noodzakelijk is voor andere doelen binnen de politietaak.[50] In de praktijk betekent dit dat de gegevens die voor het ene doel zijn verwerkt, bijvoorbeeld de opsporing van strafbare feiten (op grond van art. 9 Wpg), voor een ander doel kunnen worden verwerkt, bijvoorbeeld het opbouwen van een informatiepositie (op grond van art. 10 Wpg), zolang dat maar noodzakelijk is voor dat andere doel.[51] Voorts heeft de wetgever in artikel 11 Wpg een grondslag gecreëerd voor het zoeken in gegevens voor andere doelen dan waarvoor de gegevens zijn verkregen. Zo mag de politie op basis van bijvoorbeeld artikel 11 Wpg gegevens vergelijken en bepaalde data-analyses uitvoeren met gegevens die op basis van artikel 8, 9 en 10 Wpg zijn verwerkt, indien dat noodzakelijk is voor een onderzoek als bedoeld in artikel 9 Wpg of een verwerking als bedoeld in artikel 10 Wpg.

Hoewel de wetgever in de Wpg veel aandacht heeft besteed aan doelbinding en de daarbij behorende mogelijkheden tot (verder) doelafwijkend gebruik,

49 Vgl. *Kamerstukken II* 2005/06, 30327, nr. 3, p. 4 en 10, waar wordt beschreven dat gerichte verwerking alleen toelaatbaar is indien van tevoren is beschreven wat het doel van de verwerking is.

50 Custers & Uršič 2016, p. 4-15, laten voor wat betreft de privaatrechtelijke context zien dat gegevens op verschillende manieren voor een ander doel kunnen worden verwerkt.

51 Zie ter illustratie een aantal recente zaken: Rb. Amsterdam 5 januari 2022, ECLI:NL:RBAMS:2022:131; Rb. Rotterdam 15 oktober 2021, ECLI:NL:RBROT:2021:10180; Rb. Zeeland-West-Brabant 6 juli 2021, ECLI:NL:RBZWB:2021:3406.

is opvallend dat de Wpg voor wat betreft de normering van het verwerken van gegevens vooral een algemeen kader schetst door de relevante beginselen te noemen, maar de uitwerking van deze beginselen vervolgens heeft overgelaten aan de politie zelf. In dit verband is niet alleen het eerdergenoemde artikel 9 lid 2 Wpg waarin de politie wordt opgedragen het doel van de verwerking nader te specificeren van belang, ook artikel 11 Wpg is hiervan een illustratie.

In plaats van dat artikel 11 Wpg precies voorschrijft wanneer de bepaling van toepassing is, kent deze bepaling brede begrippen zoals 'geautomatiseerd vergelijken' en 'in combinatie zoeken'. In de literatuur wordt artikel 11 Wpg aangewezen als grondslag voor het uitvoeren van complexe data-analyses,[52] maar bijvoorbeeld ook voor *predictive policing,*[53] waarbij door middel van data-analyse wordt ingeschat waar criminaliteit zal plaatsvinden of wie met een verhoogde waarschijnlijkheid strafbare feiten zal plegen. Het uitvoeren van data-analyses ten aanzien van gegevens die zijn overgenomen uit een inbeslaggenomen server of computer, verschilt echter wezenlijk van *predictive policing.* De vraag is dan ook artikel 11 Wpg wel voldoende is toegesneden op de verschillende manieren van data-analyse die voor uiteenlopende doelen kunnen worden uitgevoerd.

Een andere consequentie van het brede toepassingsbereik van de bepaling is dat toepassingsvoorwaarden vrij algemeen zijn geformuleerd.[54] Zo verwijst artikel 11 lid 4 Wpg naar 'bijzondere gevallen' zonder dat geheel duidelijk wordt wanneer daarvan sprake is.[55] Op deze manier lijkt de wetgever dus de ruimte te hebben geboden om – afhankelijk van de toegepaste methode – een afweging te maken tussen enerzijds het recht op privacy en anderzijds het belang van inzet van de methode.[56] Hier doet zich dan ook een belangrijk verschil voor met de normering in het WvSv.[57] In het WvSv is er immers voor gekozen om steeds zo precies mogelijk uit te schrijven op welke opsporingsmethode(n) de betreffende bevoegdheid ziet, waardoor ook de toepassingsvoorwaarden daarop zijn toegesneden.

52 Schermer 2017, p. 211.

53 Das & Schuilenberg 2018, par. 1. Overigens erkennen deze auteurs wel dat artikel 11 Wpg een magere grondslag is voor *predictive policing.*

54 De wetgever vond dit ook noodzakelijk omdat de bepaling zowel relevant is in het kader van de strafrechtelijke taken van de politie als de taken op het gebied van de openbare orde.

55 *Kamerstukken II* 2005/06, 30327, nr. 3, p. 66 bevat op dit punt wel enige aanwijzingen, maar laat nog steeds veel vragen open.

56 *Kamerstukken II* 2005/05, 30327, nr. 3, p. 38.

57 Vgl. in dit verband Stevens & Koops 2021, p. 705-709 die voor het nieuwe WvSv concluderen dat de regeling inzake de opsporing ook vooral de huidige stand van zaken codificeert en weinig open normen bevat.

2.3.1.2 Toezicht

De Wpg kent verschillende vormen van intern (niet-onafhankelijk) en extern (onafhankelijk) toezicht. Intern komt de privacyfunctionaris een belangrijke taak toe. Een privacyfunctionaris heeft als taak om adviezen te geven over de toepassing van de Wpg en toezicht te houden op de Wpg.[58] Zo is voor veel vormen van doelafwijkend gebruik toestemming nodig van de privacyfunctionaris.[59] Vaak is een privacyfunctionaris een politiefunctionaris die deskundig is op het gebied van het privacyrecht.[60] Extern houdt een zogeheten functionaris gegevensbescherming en de Autoriteit Persoonsgegevens (AP) toezicht op naleving van de Wpg. De functionaris gegevensbescherming (FG) beschikt over allerlei bevoegdheden die gelijkwaardig zijn aan de bevoegdheden in afdeling 5.2 Algemene wet bestuursrecht (Awb).[61] Naast deze functionarissen houdt de AP toezicht op de Wpg.[62] Deze autoriteit heeft handhavende en sanctionerende bevoegdheden.[63] Zo kan de AP een last onder dwangsom of een bestuurlijke boete opleggen. Opvallend is echter wel dat de AP veel minder toezichthoudende, adviserende en sanctionerende bevoegdheden heeft dan onder de Algemene verordening gegevensbescherming (AVG).[64] De AP heeft bijvoorbeeld geen bevoegdheid om verwerkingen stil te leggen of onrechtmatig verwerkte gegevens zelf te verwijderen. Verder is in de Wpg geregeld dat betrokkenen bij de AP klachten kunnen indienen.[65] Voor de uitoefening van dit klachtrecht en de toezichthoudende taak van de AP is het essentieel dat de politie bijhoudt op welke wijze zij gegevens verwerkt. In de Wpg zijn dan ook verschillende bepalingen te vinden die ertoe strekken dat de politie haar werkzaamheden documenteert of logt.[66] Verder komt aan betrokkenen het recht toe om inzage te vorderen in de gegevens die over hem/haar zijn verwerkt, maar onder omstandigheden kan dit recht op inzage worden afgewezen, bijvoorbeeld om te voorkomen dat een opsporingsonderzoek wordt doorkruist.[67]

58 Artikel 34 Wpg.
59 Kritisch hierover Schermer 2017, p. 211.
60 Groenhart in: *T&C Privacy- en gegevensbeschermingsrecht* 2020, commentaar op artikel 34 Wpg.
61 Artikel 36 Wpg.
62 Artikel 35 Wpg.
63 Zie artikel 35a Wpg respectievelijk artikel 35c Wpg.
64 Stevens e.a. 2021, p. 240-241. Zie voorts De Hert & Sajfert 2018, p. 251-252.
65 Artikel 31a Wpg.
66 Zie artikel 31d-33 Wpg.
67 Artikel 25 jo. 27 Wpg.

Naast bovenstaande toezichthouders krijgt ook de Officier van Justitie een rol toebedeeld in de Wpg.[68] De Officier van Justitie heeft immers het gezag over de opsporing en uit dien hoofde heeft hij ook in een aantal gevallen bepaalde zeggenschap over de verwerking van politiegegevens. Soms is dat in de Wpg bepaald (zie bijv. artikelen 11, 19 en 20 Wpg), maar vaker volgt dat uit de Aanwijzing Wet politiegegevens.[69]

2.3.2 Wetboek van Strafvordering: uitgangspunten, wettelijke systematiek en toezicht

2.3.2.1 Uitgangspunten en wettelijke systematiek

De wijze van normeren in het WvSv is echter geheel anders dan in de Wpg. In het WvSv is immers steeds zo precies mogelijk uitgeschreven in welke gevallen, op welke wijze, voor welke doelen en met inachtneming van welke waarborgen een bepaalde bevoegdheid mag worden toegepast. De keuze voor deze *rule based* benadering is in belangrijke mate het gevolg van het strafvorderlijke legaliteitsbeginsel (artikel 1 WvSv) dat voorschrijft dat strafvordering bij wet moet zijn voorzien. Tegelijkertijd wordt dit beginsel door zowel de wetgever als de Hoge Raad niet zo strikt toegepast dat elke methode of werkwijze waarmee gegevens voor de opsporing worden vergaard, moet berusten op een specifieke wettelijke grondslag. Alleen de methoden die 1) een meer dan beperkte inbreuk maken op grondrechten en/of 2) die zeer risicovol zijn voor de integriteit en beheersbaarheid van de opsporing, moeten worden voorzien van een wettelijke basis met bijbehorende waarborgen.[70] Dit uitgangspunt heeft ertoe geleid dat het huidige WvSv geen systematische beschrijving bevat van alle in de praktijk toegepaste opsporingsmethoden.[71] Opsporingsmethoden die niet of slechts in beperkte mate inbreuk maken op grondrechten en niet zeer risicovol zijn voor de integriteit en beheersbaarheid, worden gebaseerd op de algemene taakstelling van de politie (artikel 3 Politiewet in combinatie met artikelen 141/142 WvSv). Zo heeft de Hoge Raad in het verleden

68 Van der Bel e.a. 2020, p. 65.

69 Aanwijzing Wet politiegegevens en de rol van de Officier van Justitie, (*Stcrt.* 2018, 26060).

70 Zie onder meer *Kamerstukken II* 1996/97, 25403, nr. 3, p. 3 en 51; HR 19 december 1995, *NJ* 1996/249 m.nt. Schalken, r.o. 6.4.5; HR 20 januari 2009, ECLI:NL:HR:2009:BF5603, *NJ* 2009/225 m.nt. Borgers; HR 1 juli 2014, ECLI:NL:HR:2014:1569; HR 1 juli 2014, ECLI:NL:HR:2014:1562, *NJ* 2015/114/115 beide m.nt. Van Kempen.

71 Corstens 2021, p. 312. Ook in het gemoderniseerde WvSv wordt niet gestreefd naar een uitputtende wettelijke normering van de opsporing. Zie hierover Simmelink 2017, p. 324.

geoordeeld dat de inzet van bijvoorbeeld een IMSI-catcher, *stealth*-sms, lokfiets en -auto op artikel 3 Politiewet en artikelen 141/142 WvSv kunnen worden gebaseerd.[72]

De *rule based* normering is duidelijk te herkennen in de huidige bevoegdheden ter verwerking van gegevens die eerder in de opsporing zijn verkregen. Voor veel van deze bevoegdheden geldt dat precies is omschreven wat de aard en het doel van de bevoegdheid is, de gevallen waarin en de personen jegens wie de bevoegdheid mag worden gebruikt, de aanwijzing van de beslissingsbevoegde functionaris en de wijze van verslaglegging. Ter illustratie wordt hier gewezen op de eerdergenoemde artikelen 126cc/dd WvSv. Anders dan in de Wpg gebruikelijk is, is in deze artikelen precies vastgelegd in welke gevallen gegevens die met enkele bijzondere opsporingsmethoden zijn verkregen mogen worden bewaard (artikel 126cc WvSv) en voor welke andere doelen de gegevens kunnen worden verwerkt (artikel 126dd WvSv). Het voordeel van deze *rule based* benadering is dat voor zowel de burger als de opsporingsautoriteiten zelf meer duidelijkheid wordt geschapen over wat al dan niet is toegestaan. Uit dit samenstel van bepalingen volgt bijvoorbeeld duidelijk dat de wetgever heeft gekozen voor een 'enge' invulling van het doelbindingsbeginsel. Dat komt tot uitdrukking in de artikelen 126cc/dd WvSv waaruit volgt dat gegevens in beginsel alleen mogen worden gebruikt in het onderzoek waarin ze zijn vergaard en twee maanden na afloop van de zaak waarvoor ze zijn vergaard moeten worden verwijderd, waardoor de weg wordt afgesneden om ze nadien voor een ander doel te gebruiken. Een nadeel van deze enge invulling is inflexibiliteit. Zo is de vraag of bij deze enge uitleg van het doelbindingsbeginsel wel altijd voldoende rekening kan worden gehouden met de belangen van de opsporingsautoriteiten bij hergebruik van gegevens.

2.3.2.2 Toezicht

Binnen het strafvorderlijke kader hebben twee actoren – de rechter en het OM – een belangrijke toezichthoudende taak. Allereerst houdt de strafrechter toezicht op de rechtmatigheid van de opsporing. Op basis van artikel 359a WvSv heeft hij de mogelijkheid om aan onrechtmatigheden tijdens het voorbereidend onderzoek rechtsgevolgen te verbinden, zoals bewijsuitsluiting of niet-ontvankelijkheid van

72 Zie HR 1 juli 2014, ECLI:NL:HR:2014:1569; HR 1 juli 2014, ECLI:NL:HR:2014:1562, *NJ* 2015/114/115 beide m.nt. Van Kempen; HR 28 oktober 2008, 2009/224, ECLI:NL:HR:2008:BE9817; HR 6 oktober 2009, *NJ* 2009/503, ECLI:NL:HR:2009:BI7084; HR 11 november 2014, ECLI:NL:HR:2014:3142, *NJ* 2015/296, m.nt. Borgers. Zie voorts Fokkens & Kirkels-Vrijman 2009, p. 105-124; Borgers 2015.

het OM. In de praktijk is de toezichthoudende rol van de strafrechter echter beperkt. Een belangrijke reden hiervoor is dat veel zaken de strafrechter helemaal niet bereiken. Een andere reden hiervoor is vaste rechtspraak van de Hoge Raad inzake artikel 359a WvSv.[73] Deze rechtspraak heeft immers tot gevolg dat het niet-naleven van de Wpg in de regel niet tot enig rechtsgevolg in een concrete strafzaak hoeft te leiden. De lat voor de zwaardere sancties van niet-ontvankelijkheid en bewijsuitsluiting ligt in ieder geval hoog, zeker als geen strafvorderlijk zwaarwegende belangen zoals de bescherming van het recht op een eerlijk proces als bedoeld in artikel 6 EVRM worden geschonden.[74] De Wpg strekt vooral tot bescherming van het recht op privacy en een privacyschending wordt in strafvordering doorgaans niet gezien als een strafvorderlijk zwaarwegend belang.[75] De rechter heeft bij privacy-schendingen wel de mogelijkheid om strafvermindering toe te passen, maar ook daarvoor geldt dat dit vooral aan orde is bij de meer ernstige schendingen waarbij de verdachte ook concreet nadeel heeft geleden. In de huidige feitenrechtspraak over de vergaring en verwerking van crypto-data tekent zich ieder geval de lijn af dat de strafrechter doorgaans voorbijgaat aan verweren die zijn gestoeld op de Wpg. In dit verband wordt vaak overwogen dat niet aannemelijk is geworden dat de Wpg is geschonden en – als dat wel aannemelijk zou zijn – dat de rechtbank vragen over de Wpg niet hoeft te beantwoorden met het oog op de vragen in artikel 348/350 WvSv en/of het garanderen van een eerlijk proces.[76]

Naast de rechter wordt aangenomen dat ook het openbaar ministerie (OM) een toezichthoudende taak toekomt met betrekking tot de rechtmatigheid van de opsporing. De toezichthoudende taak is echter niet wettelijk vastgelegd.[77] Dat de Officier van Justitie een rol heeft bij het toezicht kan in de eerste plaats worden afgeleid uit de regeling van de opsporingsbevoegdheden die aan de Officier van Justitie een belangrijke rol toebedeelt. Voor de inzet van veel opsporingsbevoegdheden en dwangmiddelen is immers toestemming van de Officier van Justitie vereist.[78] Op deze wijze kan de Officier van Justitie bijdragen aan de rechtmatigheid van de opsporing. In de tweede plaats kan deze taak worden afgeleid uit

73 HR 1 december 2020, ECLI:NL:HR:2020:1890, *NJ* 2021/170 m.nt. Jörg.

74 HR 1 december 2020, ECLI:NL:HR:2020:1890, *NJ* 2021/170 m.nt. Jörg.

75 Luining, in: *Handboek Strafzaken* 2020, 18.8.

76 Zie onder meer Rb. Gelderland 20 oktober 2021, ECLI:NL:RBGEL:2021:5621; Rb. Gelderland 8 december 2021, ECLI:NL:RBGEL:2021:6584; Rb. Oost-Brabant 15 december 2021, ECLI:NL:RBOBR:2021:6861; Rb. Amsterdam 22 december 2021, ECLI:NL:RBAMS:2021:7553. Zie voor een andere benadering Rb. Amsterdam 30 september 2021, ECLI:NL:RBAMS:2021:5520.

77 Samadi 2020, p. 151 en 296.

78 Zie Samadi 2020, p. 297-303 over de praktijk hiervan.

het gezag dat hij uitoefent over de opsporing.[79] Vanuit dit gezag (en de daarmee verbonden notie van magistratelijkheid) kan het openbaar ministerie ook waken over de rechtmatigheid van de opsporing. In de praktijk zien officieren van justitie ook een toezichthoudende taak voor zichzelf weggelegd. De mate waarin ook daadwerkelijk toezicht wordt uitgeoefend is echter ook mede afhankelijk van de wijze waarop een individuele Officier van Justitie hieraan invulling geeft.[80]

2.4 Conclusie en aandachtspunten in de normering

In het voorgaande is stilgestaan bij de vraag hoe de normering van onderzoek aan gegevens in het huidige juridische kader is vormgegeven. In het licht van de ontwikkelingen op het gebied van de digitale opsporing is een aantal aandachtspunten in de normering aan te wijzen.[81] Vier punten verdienen in het bijzonder aandacht.

2.4.1 Vergaren en verwerken

Het eerste aandachtspunt betreft de keuze om de vergaring van gegevens zoveel mogelijk in het WvSv te regelen en de verwerking in de Wpg. Hoewel in de loop van de jaren verschillende bepalingen aan het WvSv zijn toegevoegd die betrekking hebben op de verwerking van in de opsporing verkregen gegevens, wil de wetgever deze bepalingen schrappen en onderbrengen in een nieuwe gegevensverwerkingswet. Nadere reflectie op deze keuze maar ook op eerdere keuzes om bepaalde vormen van gegevensverwerking juist wel in het WvSv te regelen, heeft echter niet of nauwelijks plaatsgevonden. Dat leidt in toenemende mate tot vragen op het gebied van wetgevingssystematiek; welke onderwerpen moeten in welke wet worden geregeld?

Ingevolge artikel 1 WvSv is het uitgangspunt dat de opsporing van strafbare feiten in het WvSv is geregeld. In dit licht bezien is de vraag of in het WvSv niet meer aandacht moet worden besteed aan de normering van het onderzoeken of analyseren van gegevens die in de opsporing zijn verkregen. Tegenwoordig vergaart de politie immers steeds grotere hoeveelheden gegevens die na vergaring vaak geen betekenis hebben en context ontberen. Nadat een nadere analyse heeft plaatsgevonden, wordt pas duidelijk op welke personen de gegevens betrekking

79 Artikel 148 WvSv. Zie nader Samadi 2020, p. 144-151.
80 Samadi 2020, p. 354.
81 Vgl. Schermer 2017, p. 207-211; *Rapport Commissie Koops* 2018, p. 26.

hebben en of de gegevens relevant materiaal bevatten. Thans voorziet het WvSv wel in enkele algemene bepalingen op het gebied van het opslaan, vernietigen en hergebruiken van gegevens die met enkele bijzondere opsporingsbevoegdheden zijn verkregen.[82] In het kader van de modernisering van het WvSv worden deze bepalingen geschrapt. Het gevolg hiervan is dat de verdere verwerking van grote hoeveelheden gegevens in het geheel buiten het WvSv wordt geregeld, maar de vraag is of dat wetssystematisch logisch is.

Andersom geldt ook dat de Wpg een bevoegdheid kent – artikel 11 Wpg – die op het eerste gezicht meer in het WvSv thuishoort. Deze bevoegdheid maakt het onder meer mogelijk om in het kader van een opsporingsonderzoek gegevens die reeds bij de politie aanwezig zijn te vergelijken of te combineren. Deze bevoegdheid voorziet aldus in een grondslag voor het doen van onderzoek aan gegevens die reeds in de systemen van de politie staan.

Kortom, hoewel het vergaren en verwerken van gegevens zich vaak wel van elkaar laten scheiden, is de vraag of dit onderscheid ook altijd moet worden doorgetrokken in de wettelijke normering.

2.4.2 Onderzoek van bulkgegevens

De inzet van (heimelijke) opsporingsbevoegdheden kan leiden tot bulkgegevens. Het in beslag nemen van een server of het hacken van een server kan er immers toe leiden dat bulkgegevens worden verkregen. In de context van strafvordering kunnen bulkgegevens worden gedefinieerd als een grote gegevensverzameling waarvan het merendeel betrekking heeft op personen die geen onderwerp van onderzoek zijn en dat ook nooit zullen worden.[83] Het begrip bulkgegevens is dus niet gerelateerd aan de wijze waarop gegevens zijn verkregen. Ook 'gerichte' vormen van gegevensvergaring zoals het in beslag nemen van een server kan ertoe leiden dat een grote gegevensverzameling wordt verkregen waarvan het merendeel betrekking heeft op personen die nooit onderwerp van strafrechtelijk onderzoek zullen zijn. Voorts is belangrijk om te benadrukken dat bulkgegevens een gradueel begrip is. Het percentage personen dat geen onderwerp van onderzoek is en dat ook nooit zal worden, kan van geval tot geval verschillen. Het verkrijgen van bulkgegevens ligt vanuit het oogpunt van het recht op privacy gevoeliger dan het verkrijgen van gegevens die wel te relateren zijn aan een of meer personen die

82 Artikelen 126cc/dd WvSv.

83 Deze definitie is gebaseerd op de definitie van bulkgegevens die voor de diensten wordt gebruikt. Zie over de definitie o.m. *Rapport Commissie Jones-Bos* 2020, p. 39. Zie voorts Galič 2022 over bulkgegevens in een strafvorderlijke context.

onderwerp van onderzoek zijn. Immers, met het verkrijgen van bulkgegevens komen gegevens over veel personen in de systemen van de politie te staan zonder dat voor elk van deze personen daarvoor een reden bestaat.

In het huidige WvSv is het onderzoek van verkregen bulkgegevens niet expliciet genormeerd.[84] In recente jurisprudentie is dan ook veel discussie ontstaan over de vraag of, en zo ja, op welke wijze onderzoek mag worden verricht aan bulkgegevens die door middel van de hackbevoegdheid zijn overgenomen in de systemen van de opsporingsautoriteiten.[85] Zo rijzen allerlei vragen over de wijze waarop die gegevensverwerking mag geschieden en welke waarborgen daarvoor gelden ten aanzien van de personen wier gegevens worden verwerkt. De verwerking kan bijvoorbeeld leiden tot een *fishing expedition* en vormt daarmee een risico voor de bescherming van het recht op privacy. Het gaat echter niet alleen om de waarborgen van een verdachte. Er spelen ook andere belangen, te weten de belangen van de samenleving als geheel. Kenmerkend voor bulkgegevens is immers dat daarin ook allerlei gegevens zijn vervat over personen die geen onderwerp van onderzoek zijn en dat ook nooit zullen worden.

2.4.3 Invulling van het doelbindingsbeginsel

Het derde aandachtspunt betreft de wijze waarop in de Wpg en het WvSv invulling is gegeven aan het doelbindingsbeginsel en daarmee ook de mogelijkheden tot doelafwijkend gebruik. In zowel de Wpg als het WvSv wordt onderzoek van in de opsporing verkregen gegevens eerst en vooral genormeerd door het doelbindingsbeginsel. Dit beginsel houdt in dat vergaarde gegevens in beginsel alleen mogen worden verwerkt voor het doel waarvoor ze zijn verkregen. Als dit doel is bereikt, dienen de gegevens te worden verwijderd. In de praktijk betekent dit dan ook dat gegevens die met de inzet van bijzondere opsporingsbevoegdheden zijn verkregen in beginsel alleen mogen worden gebruikt ten behoeve van het opsporingsonderzoek en het onderzoek ter zitting waarin de bevoegdheden zijn ingezet. Dit doel bepaalt dan ook wanneer de gegevens moeten worden vernietigd.[86]

84 Het gebruiken van gegevens voor andere doelen dan waarvoor de gegevens zijn verkregen is wel nader genormeerd in artikel 126dd WvSv.

85 Zie bijvoorbeeld Rb. Amsterdam 17 maart 2022, ECLI:NL:RBAMS:2022:1273; Rb. Limburg 26 januari 2022, ECLI:NL:RBLIM:2022:558; Rb. Noord-Holland 4 mei 2022, ECLI:NL:RBNHO:2022:3899.

86 Op verschillende plaatsen in het WvSv is deze gedachtegang te herkennen. Zie onder meer art. 125n en art. 126cc WvSv.

Tegelijkertijd is in zowel het WvSv als de Wpg erkend dat doelafwijkend gebruik mogelijk is.[87] Zo is in artikel 126dd WvSv bepaald dat gegevens die op basis van enkele bijzondere opsporingsbevoegdheden zijn verkregen voor andere strafrechtelijke onderzoeken mogen worden gebruikt. Ook de Wpg kent verschillende mogelijkheden tot doelafwijkend gebruik. Niet alleen is voor elk verwerkingsdoel bepaald dat gegevens voor andere doelen mogen worden verwerkt, artikel 11 Wpg bevat ook een meer algemene grondslag op basis waarvan politiegegevens met het oog op andere doelen nog eens bevraagd kunnen worden.[88]

In het licht van de mogelijkheden om gegevens centraal op te slaan en nader te verwerken lijkt de systematiek waarbij enerzijds doelbinding het uitgangspunt is en anderzijds mogelijkheden worden gecreëerd voor doelafwijkend gebruik onder druk komen te staan. Dat kan worden geïllustreerd aan de hand van de voorziening genaamd 'Raffinaderij'.[89] Dit is een voorziening die het mogelijk maakt om snel grote hoeveelheden politiegegevens te vergelijken en te combineren om zo tot nieuwe inzichten te komen. Zo kan informatie uit inbeslaggenomen telefoons of computers in samenhang worden geanalyseerd met tapverslagen, data van peilbakens en gegevens die uit het openbare bronnen afkomstig zijn. Het toepassen van de Wpg op een voorziening als Raffinaderij is niet eenvoudig, omdat niet steeds voorafgaand aan een verwerking is te bepalen wat het doel van de verwerking is. Het doel van Raffinaderij is het analyseren van gegevens om daaraan informatie te ontlenen, maar dat is wel heel algemeen.

Doelbinding en daarmee het beperken van de mogelijkheden tot doelafwijkend gebruik is een belangrijke waarborg voor zowel het recht op privacy als persoonsgegevensbescherming. Door vooraf te bepalen wat het doel van de verwerking is en alleen verwerkingen toe te staan die in overeenstemming zijn met dit doel wordt de gegevensverwerking inzichtelijk en kan misbruik worden voorkomen.[90] Als de gegevens niet meer nodig zijn om het doel te bereiken, moeten ze worden verwijderd. De vraag is dan ook hoe op een zinvolle wijze invulling kan worden gegeven aan doelbinding en doelafwijkend gebruik, waarbij zowel recht wordt gedaan aan het waarborgkarakter ervan alsook aan de werkbaarheid van de opsporing. Ter beantwoording van deze vraag zijn in het bijzonder het recht op

87 Ook in de *Richtlijn 2016/680* is dat erkend, zie hierover uitgebreid hoofdstuk 3.

88 Zie onder meer art. 8 lid 4, art. 9 lid 3, art. 10 lid 5 Wpg.

89 Zie voor een beschrijving van Raffinaderij: De Vries, 2017, p. 254-259. Deze voorziening is gestart als pilot maar wordt inmiddels landelijk toegepast door de politie, zo blijkt uit het jaarrapport van de politie over 2020. Beschikbaar via: https://www.politie.nl/binaries/content/assets/politie/onderwerpen/jaarverantwoording/2020/jaarverantwoording-politie-2020-inclusief-accountantsverklaring.

90 Zie over de ratio van het doelbindingsbeginsel onder meer Koning 2020, p. 71-78.

persoonsgegevensbescherming en het recht op privacy van belang, nu deze rechten eerst en vooral bepalen hoe precies het doel moet worden omschreven en in welke mate doelafwijkend gebruik is toegestaan.

2.4.4 Toezicht op gegevensverwerking

Een vierde aandachtspunt betreft – tot slot – het toezicht op de gegevensverwerking. In theorie houden verschillende, zowel interne als externe toezichtsorganen (AP, gegevensbeschermingsfunctionaris, privacyfunctionaris, OM, strafrechter) toezicht op de verdere verwerking van gegevens in de opsporing, maar het valt te betwijfelen of daadwerkelijk sprake is van effectieve rechtsbescherming, waarbij burgers adequaat zijn beschermd tegen misbruik en fouten. Voor wat betreft strafvorderlijk toezicht geldt immers dat de strafrechter (zeer) terughoudend is met het verbinden van rechtsgevolgen aan privacyschendingen, met als gevolg dat de rechter doorgaans niet uitvoerig controleert of de Wpg is nageleefd.[91] Ook de rol van het OM is op dit gebied beperkt. In het kader van de Wpg ligt dat wat anders. In theorie wordt op verschillende manieren zowel door interne als externe toezichthouders toezicht gehouden op naleving van de Wpg. Tegelijkertijd is ook hier de vraag of hier van effectief toezicht kan worden gesproken. Een probleem onder de Wpg is immers dat de verantwoordelijkheid voor naleving van de Wpg vooral bij de betrokkene zelf is neergelegd.[92] Een betrokkene kan een klacht indienen als hij van oordeel is dat de politie onrechtmatig gegevens heeft verwerkt, maar een betrokkene beschikt niet altijd over de benodigde informatie, bijvoorbeeld omdat de autoriteiten het recht op inzage beperken.[93] Bovendien doen zich hierbij ook praktische problemen voor, zoals onduidelijkheid over de vraag bij wie en op welke wijze en klacht moet worden ingediend en lange doorlooptijden.[94] Daarnaast heeft de AP ook mogelijkheden om zelfstandig toezicht uit te oefenen, maar de mogelijkheden hiertoe zijn – in vergelijking met de AVG – beperkt. De vraag is dan ook hoe toezicht op onderzoek van gegevens die in de opsporing zijn verkregen moet

91 Zie ter illustratie verschillende rechtbankzaken, waarin gevoerde verweren op basis van de Wpg steevast worden afgewezen: Rb. Gelderland 20 oktober 2021, ECLI:NL:RBGEL:2021:5612; Rb. Gelderland 8 december 2021, ECLI:NL:RBGEL:2021:6584; Rb. Oost-Brabant 15 december 2021, ECLI:NL:RBOBR:2021:6861; Rb. Amsterdam 22 december 2021, ECLI:NL:RBAMS:2021:7553.

92 Zie in een iets ander verband ook: Stevens e.a. 2021, p. 241.

93 Artikel 27 Wpg.

94 Vogiatzoglou e.a. 2020, p. 274-302.

worden geregeld, zodat een burger daadwerkelijk wordt beschermd tegen misbruik en andere fouten.

3 Europeesrechtelijk kader

3.1 Inleiding

In dit hoofdstuk wordt antwoord gegeven op de vraag welke eisen en waarborgen relevante Europese rechtsbronnen stellen aan de normering van onderzoek aan de in de opsporing verkregen gegevens. Daarbij wordt in het bijzonder ingegaan op de verplichtingen die staten hebben om het recht op gegevensbescherming en het recht op privacy te waarborgen. Deze rechten kunnen immers snel in het geding komen bij onderzoek aan gegevens voor strafvorderlijke doeleinden. Hierna wordt allereerst ingegaan op de EU-Richtlijn 2016/680, ofwel de '*Law Enforcement Directive*'. In deze richtlijn heeft de Uniewetgever nader invulling gegeven aan het recht op persoonsgegevensbescherming dat als zodanig alleen in artikel 8 van het Handvest van de Grondrechten van de Europese Unie (HGEU) is neergelegd. Daarna staat het recht op privacy centraal. Dit recht is zowel in artikel 7 HGEU als in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) erkend. Over de betekenis van het recht op privacy en de vereisten die een inbreuk op het recht op privacy kunnen rechtvaardigen in het kader van de opsporing heeft met name het Europees Hof voor de Rechten van de Mens (EHRM) zich uitgelaten. De laatste jaren neemt de jurisprudentie over artikel 7 en 8 HGEU in relatie tot de opsporing evenwel ook toe. In dit onderzoek is daarom ervoor gekozen om zowel in te gaan op de rechtspraak van het EHRM als van het Hof van Justitie EU (HvJ EU).

Een belangrijke kanttekening die met betrekking tot onderstaande analyse moet worden gemaakt is dat met dit onderzoek geen *toetsing* wordt beoogd waarbij wordt beoordeeld of een of meer specifieke opsporingsactiviteiten voldoen aan de eisen die het recht op gegevensbescherming of het recht op privacy stellen. De analyse in dit hoofdstuk heeft als doel in kaart te brengen welke eisen en waarborgen van belang zijn voor de inrichting van wetgeving op het gebied van onderzoek aan reeds vergaarde gegevens voor het nemen van strafvorderlijke beslissingen. De in dit hoofdstuk in kaart te brengen eisen en waarborgen dienen als normatief referentiekader, waarbinnen de wetgever regelgeving kan ontwikkelen.

3.2 RICHTLIJN 2016/680

Op 27 april 2016 komt binnen de EU de 'Law Enforcement Directive' tot stand (Richtlijn 2016/680).[95] De Richtlijn 2016/680 heeft als doel een alomvattend kader te creëren inzake de bescherming van persoonsgegevens bij het gebruik ervan door politie en strafrechtelijke autoriteiten, ongeacht of de betrokken personen getuige, slachtoffer of verdachte zijn. Enerzijds heeft de EU daarbij oog voor de bescherming van natuurlijke personen in verband met de verwerking van hun persoonsgegevens, anderzijds houdt de Uniewetgever rekening met de specifieke aard van het gebruik door politie en strafrechtelijke autoriteiten. Het doel dat de EU met deze Richtlijn 2016/680 voor ogen staat is bij te dragen aan het vergroten van het vertrouwen tussen de lidstaten en het versterken van een klimaat voor strafrechtelijke samenwerking tussen lidstaten van de EU en Schengenlanden. De richtlijn maakt onderdeel uit van de EU-hervormingsmaatregelen voor gegevensbescherming, naast de Algemene Verordening Gegevensbescherming (hierna: AVG) en de EU Verordening 2018/1725 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door instellingen, organen en instanties van de EU.

De Richtlijn 2016/680 regelt uitsluitend de verwerking van persoonsgegevens in het kader van de voorkoming, de opsporing en de vervolging van strafbare feiten. De focus van de richtlijn is op minimumharmonisatie van de regels in de verschillende lidstaten. Blijkens artikel 1, derde lid, Richtlijn 2016/680 kunnen lidstaten 'uitgebreide waarborgen' bieden voor de bescherming van persoonsgegevens.[96] In de Richtlijn 2016/680 staat een aantal kernpunten geformuleerd inzake het gebruik van gegevens. Lidstaten schrijven voor dat persoonsgegevens die door rechtshandhavingsautoriteiten worden verzameld:

a. op wettige en eerlijke wijze worden verwerkt;
b. uitsluitend voor welbepaalde, uitdrukkelijk omschreven en legitieme doeleinden worden verzameld en geheel in overeenstemming met deze doeleinden worden verwerkt;
c. toereikend, ter zake dienend en niet bovenmatig zijn in verhouding tot de doeleinden waarvoor zij worden verwerkt;
d. juist zijn en worden geactualiseerd waar nodig;
e. niet langer dan voor verwerkingsdoeleinden noodzakelijk is in een vorm worden bewaard die identificatie van de betrokkene mogelijk maakt;

95 *PbEU* 4.5.2016, L 119/89.

96 Zie ook Sajfert & Quintel 2019, I.4; Caruana 2017, p. 251 en252; Koning 2020, p. 53 en 54.

f. met gebruikmaking van passende technische of organisatorische middelen passend worden beschermd, waaronder ook de bescherming tegen ongeoorloofde of onrechtmatige verwerking.

Deze kernpunten staan in artikel 4, eerste lid, Richtlijn 2016/680 verwoord als relevante verwerkingsbeginselen. Het betreft onder meer het rechtmatigheidsbeginsel, het eerlijkheidsbeginsel, het doelbindingsbeginsel, het data-minimalisatiebeginsel, en het juistheidsbeginsel.

Bij de uitwerking van de verwerkingsbeginselen heeft de Uniewetgever een evenwicht gezocht tussen aan de ene kant individuele gegevensbescherming en aan de andere kant de belangen van de opsporing(sautoriteiten).[97] In de bovenstaande opsomming ontbreekt evenwel het transparantiebeginsel – dat wel in de AVG voorkomt.[98] De reden hiervoor is gelegen in de aard van de activiteiten van de autoriteiten waarmee de Richtlijn 2016/680 gemoeid is: (volledige) transparantie naar een betrokkene in een strafrechtelijke procedure is immers niet steeds mogelijk, omdat inzicht in en kennis van de betrokkene over de verwerking van diens persoonsgegevens de opsporing kan frustreren.[99]

Deze paragraaf is als volgt opgebouwd. Allereerst wordt ingegaan op de verwerkingsbeginselen van de Richtlijn 2016/680, nu deze beginselen eerst en vooral richtinggevend zijn voor de normering van de verwerking van de in de opsporing verkregen gegevens. Het doel van deze bespreking is het duiden van de verplichtingen die op staten rusten in verband met ververwerking van persoonsgegevens in de opsporing. In de analyse signaleren we daarnaast enkele problematische aspecten van deze beginselen. Vervolgens staan wij stil bij de vraag wat de Richtlijn 2016/680 op het gebied van toezicht op de verwerking van gegevens in het kader van opsporing vereist.

3.2.1 Verwerkingsbeginselen

3.2.1.1 Rechtmatigheid en eerlijkheid

Ingevolge artikel 4 lid 1 sub a Richtlijn 2016/680 dient de verwerking van persoonsgegevens rechtmatig en eerlijk te geschieden. Daarmee stelt deze bepaling de eis van een (verwerkings)grondslag voor het verwerken van persoonsgegevens door de opsporingsautoriteit. In elk ander geval is de verwerking van persoonsgegevens

97 De Hert & Papakonstantinou 2016, p. 9 en 11; Sajfert & Quintel 2019, I.4; FRA 2018, p. 283.
98 Dit in tegenstelling tot zijn equivalent in de AVG (in de categorie rechtmatigheid en behoorlijkheid). Zie ook De Hert & Sajfert 2021, p. 12; Sajfert & Quintel 2019, p. 21.
99 Zie ook Custers & Leiser 2019, p. 374.

onrechtmatig. In tegenstelling tot de AVG bestaat er onder de Richtlijn 2016/680 slechts één mogelijke verwerkingsgrondslag. Artikel 8 lid 1 Richtlijn 2016/680 bepaalt:

> *"De lidstaten zorgen ervoor dat verwerking alleen rechtmatig is indien en voor zover die verwerking noodzakelijk is voor de uitvoering door een bevoegde autoriteit van een taak voor de in artikel 1, lid 1, bedoelde doeleinden, en dat die verwerking gebaseerd is op het Unierecht of het lidstatelijke recht."*

Wat precies de toegevoegde waarde is van de term eerlijkheid (in het Engels: *fairness*) in artikel 4 lid 2 sub a Richtlijn 2016/680 naast het beginsel van rechtmatigheid, wordt niet geëxpliciteerd. Hoewel eerlijkheid wordt gezien als een belangrijk uitgangspunt,[100] gaat de Nederlandse wetgever ervan uit dat het beginsel van eerlijke verwerking van gegevens geen aanvullende betekenis heeft ten opzichte van de rechtmatigheid van de verwerking.[101]

3.2.1.2 Doelbinding

Het beginsel van doelbinding is vervat in artikel 4 lid 1, sub b Richtlijn 2016/680. Dit beginsel wordt gezien als een van de 'hoekstenen van het gegevensbeschermingsrecht'.[102] Over de ratio van het doelbindingsbeginsel is veel geschreven.[103] In de kern lijkt de gedachte achter doelbinding overeen te komen met de ratio van het legaliteitsbeginsel. De ratio van het doelbindingsbeginsel is immers gelegen in het bieden van rechtszekerheid voor de betrokkene en voorzienbaarheid van de wetgeving inzake gegevensverwerking.[104] Het beginsel van doelbinding speelt ook een rol bij de beginselen van dataminimalisatie en opslagbeperking, in die zin dat het doel bepalend is voor de vraag wat niet meer als minimale gegevensverwerking kan worden gezien en voor de vraag wanneer gegevens moeten worden verwijderd. Hieronder wordt nader ingegaan op de relatie tussen doelbinding en de beginselen van dataminimalisatie en opslagbeperking.

---

100 WP29 2015, p. 6.

101 Zie ook de Memorie van Toelichting over 'fairness' bij wetsvoorstel tot wijziging Wpg: *Kamerstukken II* 2017/2018, 34 889, nr. 2, p. 61.

102 WP29 2013, p. 4.

103 Zie hierover uitgebreid Koning 2020, p. 71-78.

104 Zie Conclusie AG Pikamäe 31 maart 2022, C-77/21, ECLI:EU:C:2022:248 (*Digi Távközlési és Szolgáltató Kft./Nemzeti Adatvédelmi*), punt 41; Brouwer 2011, p. 279; Biega & Finck 2021, p. 48; Coudert 2017, p. 317.

Het doelbindingsbeginsel in de zin van de Richtlijn 2016/680 bestaat uit twee bouwstenen: doelspecificatie en verenigbaar gebruik.[105] Doelbinding houdt in de eerste plaats in dat voorafgaand aan de verwerking moet worden bepaald wat het doel van de verwerking is. In de tweede plaats houdt doelbinding in dat gegevens niet op onverenigbare wijze met dit aanvankelijk bepaalde doel mogen worden verwerkt. Op de betekenis van deze twee bouwstenen wordt hieronder nader ingegaan.

Doelspecificatie

Het eerste element van doelbinding – de doelspecificatie – bepaalt dat persoonsgegevens uitsluitend mogen worden verzameld voor welbepaalde, uitdrukkelijk omschreven en legitieme doeleinden. Die doeleinden dienen door de bevoegde autoriteit te worden vastgesteld op het ogenblik dat de persoonsgegevens worden verzameld.[106] De doeleinden dienen bij wet te worden vastgesteld.[107] In het kader van die doelspecificatie dienen ook de 'te verwerken persoonsgegevens' te worden vermeld in het lidstatelijke recht.[108] In artikel 1 lid 1 Richtlijn 2016/680 noemt de Uniewetgever de volgende verwerkingsdoeleinden:

> *"de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid"*

In de literatuur wordt aangenomen dat de doeleinden van de Richtlijn 2016/680 *afzonderlijk* onvoldoende specifiek zijn om te kunnen gelden als 'doeleinden' in de zin van artikel 4 lid 1, sub b Richtlijn 2016/680.[109] Doelen als onderzoek of voorkoming van strafbare feiten zijn niet alleen vaag, ze stellen ook niet of nauwelijks grenzen aan de wijze waarop de politie gegevens zou mogen verwerken. De onafhankelijke en gezaghebbende EU-werkgroep, de zogenoemde Artikel 29-

105 WP29 2013, p. 11 en 12. Zie ook Jasserand 2018a, p. 156; Jasserand 2018b, p. 163; De Hert & Sajfert 2021, p. 9; Hahn 2021 p. 37 en 38.
106 Overweging 26 Richtlijn 2016/680. Zie ook WP29, 2013, p. 15.
107 Overweging 26 Richtlijn 2016/680.
108 Art. 8 lid 2 Richtlijn 2016/680. Zie ook overweging 33 Richtlijn 2016/680.
109 Koning 2020, p. 181 en 182. Vergelijk ook Andelbeek 2022, p. 27.

Werkgroep (hierna: 'WP29')[110] lijkt zich op hetzelfde standpunt te stellen. In twee opinies (2013 en 2015) is de WP29 nader ingegaan op wat is vereist in het kader van doelspecificatie. In 2015 maakt de WP29 duidelijk dat 'law enforcement' onvoldoende specifiek is. Dat spreekt voor zich. *Law enforcement* omvat vrijwel elke taak van de politie. In de opinie van 2013 stelt de WP29 dat het verwerkingsdoeleinde specifiek genoeg moet zijn om te kunnen bepalen welke soort van gegevensverwerkingen binnen het doeleinde valt. Ook moet het verwerkingsdoeleinde specifiek genoeg zijn om vast te kunnen stellen of de verwerking in lijn is met de wet.[111] Hieruit kan worden afgeleid dat doelen als opsporing of voorkoming van strafbare feiten onvoldoende specifiek zijn, omdat deze doelen niet of nauwelijks de mogelijkheid bieden om te kunnen bepalen welke verwerking al dan niet is toegestaan. Tegelijkertijd sluit de WP29 de mogelijkheid van een overkoepelend of verzameldoel niet uit.[112] Omdat de opinie van de WP29 ziet op doelbinding in het algemeen en niet specifiek op doelbinding in de context van de Richtlijn 2016/680 is echter onduidelijk wat een overkoepelend of verzameldoel zou kunnen zijn in het kader van de Richtlijn 2016/680. Al met al moet worden geconcludeerd dat doelen als opsporing of de voorkoming van strafbare feiten onvoldoende specifiek zijn. Anders kan het doelbindingsbeginsel alsmede de hieraan verwante beginselen van dataminimalisatie en opslagbeperking gemakkelijk worden uitgehold. Lidstaten moeten aldus nader specificeren voor welke doelen de politie gegevens mag verwerken.

Deze doelen moeten ingevolge artikel 8 lid 2 Richtlijn 2016/680 ook in het nationale recht worden vastgelegd. Hier doet zich een complicatie voor. In abstracto – los van de concrete omstandigheden van een geval – is niet eenvoudig te specificeren wat het doel van de gegevensverwerking is. In de Wpg is daarom ervoor gekozen om enerzijds in de wet een vrij abstract doel te noemen – handhaving van de rechtsorde in een concreet geval – en anderzijds te eisen dat de politie als zij overgaat tot een concrete gegevensverwerking nader specificeert wat het doel van de verwerking is.[113]

110 De Artikel 29-Werkgroep was de onafhankelijke Europese werkgroep die tot 25 mei 2018 (de datum van inwerkingtreding van de AVG) verantwoordelijk was voor de behandeling van kwesties in verband met de bescherming van de persoonlijke levenssfeer en van persoonsgegevens. Met het van kracht worden van de AVG werd de Artikel 29-werkgroep vervangen door het European Data Protection Board (EDPB) (ex artikel 68 AVG). In het Nederlands: het Europees Comité voor gegevensbescherming.

111 WP29, 2013, p. 15.

112 WP29, 2013, p. 16. Vgl. ook Von Grafenstein 2018, p. 104.

113 Zie nader hoofdstuk 2, § 3.1.1.

Doelafwijkend gebruik en verenigbaarheid in de Richtlijn 2016/680

Uit het tweede element van doelbinding volgt dat de bevoegde autoriteit de persoonsgegevens alleen op een niet met die doeleinden onverenigbare wijze mag verwerken. Dit element is tot uitdrukking gebracht in artikel 4 lid 1, sub b Richtlijn 2016/680. Anders dan de AVG maakt de Richtlijn 2016/680 echter niet duidelijk welke factoren en gezichtspunten van belang zijn bij de vraag of twee doelen onverenigbaar zijn.[114] Ook het Hof van Justitie heeft zich nog niet uitgelaten over de invulling van de verenigbaarheidstoets in de Richtlijn 2016/680.[115] Uit de dubbele ontkenning volgt in elk geval niet dat de twee doelen verenigbaar hoeven te zijn: zij behoeven slechts niet onverenigbaar te zijn.[116] Vanwege het gebrek aan duidelijkheid in de Richtlijn 2016/680 over de onverenigbaarheidstoets is door ons nader geanalyseerd op welke wijze deze toets een rol speelt dan wel moet spelen in de Richtlijn 2016/680. In de literatuur is dit punt weliswaar aangestipt, maar niet uitgebreid geanalyseerd. Op de (mogelijke) rol van de verenigbaarheidstoets gaan wij hieronder nader in. Eerst komt artikel 4 lid 2 Richtlijn 2016/680 aan bod, nu hierin specifieke regels zijn neergelegd inzake doelafwijkend gebruik. Bovendien is een goed begrip van deze bepaling noodzakelijk voor het beantwoorden van de vraag welke rol de verenigbaarheidstoets in de Richtlijn 2016/680 toekomt.

Doelafwijkend gebruik

Artikel 4 lid 2 Richtlijn 2016/680 maakt het mogelijk om persoonsgegevens te verwerken voor een 'ander doel', mits dit voldoet aan vier cumulatieve voorwaarden:

1. Het 'andere doel' bevindt zich in het toepassingsgebied van artikel 1, eerste lid, Richtlijn 2016/680: "de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid." (art. 4, tweede lid, aanhef Richtlijn 2016/680);

114 Koning 2020, p. 135; Jasserand 2018a, p. 157.
115 Koning 2020, p. 136.
116 Vergelijk ook Moerel & Prins 2016, p. 65.

2. De verwerking voor dat andere doel is bij wet voorzien (artikel 4, tweede lid, sub a, Richtlijn 2016/680);[117]
3. De verwerking is noodzakelijk**;**
4. De verwerking staat in verhouding tot dat andere doel van de Richtlijn 2016/680 overeenkomstig het Unierecht of het lidstatelijke recht (artikel 4, tweede lid, sub b, Richtlijn 2016/680) – de proportionaliteit.

Artikel 4 lid 2 Richtlijn 2016/680 heeft het over 'een ander doel van artikel 1 lid 1 Richtlijn 2016/680'. Voor de toepassing van artikel 4 lid 2 Richtlijn 2016/680 is dus irrelevant of er sprake is van verenigbaarheid tussen het oorspronkelijke en nieuwe (andere) doeleinde. De maatstaf die hier moet worden aangelegd is 'ander doel'. De vraag is echter wanneer er sprake is van een 'ander doel'. Uit de tekst van artikel 4 lid 2 Richtlijn 2016/680 – 'een ander doel *van* artikel 1 lid 1 Richtlijn 2016/680' – volgt dat hierin afzonderlijke doelen worden benoemd.[118] De vraag is echter of de Uniewetgever dit ook daadwerkelijk zo heeft bedoeld.[119] De doelen waarnaar in artikel 4 lid 2 Richtlijn 2016/680 wordt verwezen zijn immers niet specifiek genoeg. In dit verband is het nuttig om onderscheid te maken tussen de in het Engels gebruikte termen '*objectives*' en '*purposes*'.[120] *Objectives* zijn de doelen waarop de richtlijn ziet en welke aldus tot uitdrukking komen in artikel 1 lid 1 Richtlijn 2016/680. *Purposes* zijn de doelen waarvoor in het specifieke geval gegevens worden verwerkt. *Purposes* zullen dus altijd specifieker zijn omschreven dan *objectives*.

A-G Sánchez-Bordona lijkt in een recente conclusie er vanuit te gaan dat de Uniewetgever dit wel zo heeft bedoeld. Hij zet uiteen dat de Richtlijn 2016/680 drie doelen omvat (voorkoming van strafbare feiten en gevaar, opsporing van strafbare feiten en tenuitvoerlegging van straffen) en dat pas van doelafwijking kan worden gesproken als wordt gewisseld tussen deze doelen.[121] Anders gezegd: de verwerking van gegevens verschuift naar een ander facet binnen de context van de

117 Bij de vastlegging bij wet (2) van een verwerking voor een *ander doel* hoeft het niet noodzakelijk te gaan om 'een door een parlement vastgestelde wetgevingshandeling'. Wel moet het 'lidstatelijke recht, die rechtsgrond of die wetgevingsmaatregel […] duidelijk en nauwkeurig zijn, en [moet] de toepassing daarvan […] voorspelbaar zijn voor degenen op wie deze van toepassing is.' Zie overweging 33 Richtlijn 2016/680. Zie ook Jasserand 2018a, p. 161.

118 Vergelijk Leiser & Custers 2019, p. 370.

119 Vergelijk Jasserand 2018b, p. 164.

120 Koning 2020, p. 10, 11 en 183.

121 Zie in deze zin Conclusie A-G Sánchez-Bordona 19 mei 2022, C-180/21, ECLI:EU:C:2022:406 (*Verenigde Staten/Inspektor v Inspektorata kam Visshia sadeben savet*), punt 59-63.

Richtlijn 2016/680: bijvoorbeeld van *opsporing* naar *voorkoming* van strafbare feiten. De nieuwe verwerking voor de *voorkoming* van strafbare feiten moet dan langs de weg van artikel 4 lid 2 Richtlijn 2016/680 worden beoordeeld. Daartegenover staat dan dat elke verwerking die onder de brede doelstelling of onder het facet van de *opsporing* valt en verder wordt gebruikt onder die brede doelstelling, geen 'ander doel' is in de zin van artikel 4 lid 2 Richtlijn 2016/680. In dit geval is artikel 4 lid 2 Richtlijn 2016/680 *niet* van toepassing en dient de verwerkingsverantwoordelijke te beoordelen of de nieuwe verwerking op basis van artikel 4 lid 1, sub Richtlijn 2016/680 verenigbaar is met het doeleinde waarvoor de persoonsgegevens oorspronkelijk zijn verzameld. Een dergelijke interpretatie geeft meer ruimte aan de bevoegde autoriteiten om persoonsgegevens verder te gebruiken. Er is immers ingevolge artikel 4 lid 2 Richtlijn 2016/680 geen wettelijke bepaling nodig. Onder deze interpretatie speelt de verenigbaarheidstoets mogelijk dus tóch een belangrijke rol. Deze interpretatie is echter niet aannemelijk, gelet op de eis van doelspecificatie. Het verwerkingsdoeleinde van de *voorkoming van strafbare feiten* of de *opsporing van strafbare feiten* is immers niet specifiek genoeg.

Logischer is aldus de uitleg dat een 'ander doel' betekent dat persoonsgegevens zijn verzameld in een specifieke verwerking in het kader van de *opsporing*, maar vervolgens worden gebruikt voor een *ander* specifiek verwerkingsdoel binnen het facet van de *opsporing*.[122] De nieuwe verwerking moet aldus voldoen aan de vereisten van artikel 4, tweede lid, Richtlijn 2016/680 ('bij wet voorzien', noodzakelijkheid en proportionaliteit). Deze interpretatie geeft minder manoeuvreerruimte aan de bevoegde autoriteiten voor het verder gebruiken van persoonsgegevens. Als er behoefte is bij de opsporingsautoriteit om gegevens voor een ander doel te verwerken, maar een wettelijke basis daarvoor ontbreekt, betekent dat dus dat de wetgever aan zet is.

Concluderend kan dus worden gesteld dat vrij snel aangenomen kan worden dat er sprake is van een 'ander doel'. Als de nationale wetgever dit doelafwijkende gebruik wil toestaan, moet daarvoor een wettelijke grondslag worden gecreëerd met waarborgen ter bescherming van de noodzakelijkheid en proportionaliteit van dit doelafwijkende gebruik.

Welke rol speelt verenigbaarheid in de Richtlijn 2016/680?

Gelet op de wijze waarop artikel 4 lid 2 Richtlijn 2016/680 is vormgegeven, rijst de vraag welke rol de verenigbaarheidstoets in artikel 4 lid 1 sub b Richtlijn 2016/680

122 Vergelijk De Hert & Sajfert 2021.

nog heeft in de Richtlijn 2016/680. Enerzijds is de verenigbaarheidstoets als belangrijk beginsel in de Richtlijn 2016/680 gepresenteerd en lijkt deze toets te moeten worden aangelegd voor artikel 4 lid 2 Richtlijn 2016/680 wordt toegepast. Anderzijds is niet duidelijk gemaakt hoe de verenigbaarheidstoets moet worden ingevuld en is artikel 4 lid 2 Richtlijn 2016/680 ook van toepassing als twee doelen verenigbaar met zijn elkaar, waardoor het belang van de verenigbaarheidstoets sterk kan worden gerelativeerd of zelfs overbodig wordt.[123] Voor zover de verenigbaarheidstoets een rol speelt in de Richtlijn 2016/680, is de inhoud ervan overgelaten aan de lidstaten. Als de verenigbaarheidstoets een rol speelt – en hieronder zetten wij uiteen hoe deze toets toch van belang is in de Richtlijn 2016/680 – is het dus aan de lidstaten om te bepalen welke doelen al dan niet te verenigen zijn.[124]

Mede op basis van de literatuur waarin de hier opgeworpen vraag zijdelings aan bod komt, kunnen onzes inziens twee manieren worden onderscheiden waarop de verenigbaarheidstoets wél een rol kan spelen in de Richtlijn 2016/680. In de eerste plaats kan artikel 4 lid 2 Richtlijn 2016/680 zo worden uitgelegd dat deze bepaling alleen van toepassing is als er sprake is van *onverenigbare* doelen. Steun voor deze lezing kan worden gevonden in artikel 7a van een oudere versie van de Richtlijn 2016/680. Hierin was namelijk een met artikel 4 lid 2 Richtlijn 2016/680 vergelijkbare bepaling opgenomen die specifiek zag op "further processing for incompatible purposes"[125]. Als men van deze lezing uitgaat, moet eerst worden beoordeeld of al dan niet sprake is van onverenigbaarheid van doelen. Als de doelen vervolgens onverenigbaar lijken te zijn, moet artikel 4 lid 2 Richtlijn 2016/680 worden toegepast. Uitgaande van deze lezing vormt artikel 4 lid 2 Richtlijn 2016/680 een *uitzondering* op het doelbindingsbeginsel.[126] Deze eerste interpretatievariant kan niet worden uitgesloten, maar is niet overtuigend. Artikel 7a van een oudere versie van de Richtlijn 2016/680 is uiteindelijk niet in de Richtlijn 2016/680 terechtgekomen. Hieruit kan dan ook worden afgeleid dat 'ander doel'

123 Zie in deze zin Koning 2020, p. 187.

124 In het kaderbesluit was dit expliciet in overweging 6 van de considerans opgenomen: "Het kaderbesluit laat het aan de lidstaten over om op nationaal niveau met meer nauwkeurigheid te bepalen welke andere doeleinden als onverenigbaar moeten worden aangemerkt met het doel waarvoor de persoonsgegevens aanvankelijk werden verzameld."

125 Zie art. 7a van de eerste versie van de Richtlijn 2016/680 (COM(2012)0010), te raadplegen via: https://www.europarl.europa.eu/doceo/document/A-7-2013-0403_EN.pdf.

126 In de AVG is wel uitdrukkelijk erkend dat – in geval van toestemming of een wettelijke bepaling een uitzondering kan worden gemaakt op het doelbindingsbeginsel. Zie art. 6 lid 4 AVG.

niet zo moet worden gelezen dat het om een 'onverenigbaar doel' gaat.[127] Hier komt voorts nog bij dat deze interpretatie van artikel 4 lid 2 Richtlijn 2016/680 in feite ertoe leidt dat het verwerken van gegevens voor onverenigbare doelen toelaatbaar zou zijn onder de Richtlijn 2016/680, mits aan de voorwaarden van artikel 4 lid 2 is voldaan. Dat is niet wezensvreemd aan het gegevensbeschermingsrecht. In artikel 6 lid 4 AVG zijn weliswaar ook uitzonderingen te vinden op het doelbindingsbeginsel, maar in het kader van de Richtlijn 2016/680 blijkt nergens uit dat de Uniewetgever dat ook onder de Richtlijn 2016/680 ook daadwerkelijk heeft voorgestaan.

In de tweede plaats zou de verenigbaarheidstoets ook kunnen worden ingelezen in artikel 4 lid 2 Richtlijn 2016/680.[128] Meer specifiek zou de verenigbaarheidstoets kunnen worden betrokken bij de proportionaliteitstoets die artikel 4 lid 2 Richtlijn 2016/680 voorschrijft. Steun voor deze opvatting kan allereerst worden gevonden in de voorganger van de Richtlijn 2016/680 – het Kaderbesluit 2008/977/JBZ.[129] In artikel 3 lid 2 van dit kaderbesluit was immers – voor zover hier van belang – het volgende geregeld:

> "2. Verdere verwerking voor een ander doel is toegestaan, mits
>
> a) deze verwerking niet onverenigbaar is met het doel waarvoor de gegevens zijn verzameld;
>
> b) de bevoegde autoriteiten bevoegd zijn om die gegevens te verwerken conform de toepasselijke wetsvoorschriften; en
>
> c) deze verwerking noodzakelijk is en in verhouding staat tot dat doel"

Bovendien doet deze tweede interpretatievariant – anders dan de eerste interpretatievariant – beter recht aan de ratio van doel*binding.* Zo wordt immers

127 De rapporteur, Axel Voss, heeft dan ook kritiek uitgeoefend op art. 7a. Volgens hem moeten persoonsgegevens niet voor onverenigbare doelen kunnen worden verwerkt. Het is echter onduidelijk of deze kritiek ook de reden is geweest dat art. 7a niet in de Richtlijn 2016/680 is terechtgekomen. Zie ook Jasserand 2018a, p. 158, waar zij wijst op onderlinge verdeeldheid tussen lidstaten.

128 De Hert & Sajfert 2021, p. 12 lijken deze interpretatie voor te staan. Ook A-G Sánchez-Bordona (Conclusie, 19 mei 2022), (*Verenigde Staten/Inspektor v Inspektorata kam Visshia sadeben savet*), C-180/21, ECLI:EU:C:2022:406 lijkt hiervan uit te gaan. Hij past niet eerst de verenigbaarheidstoets toe voordat hij aan toepassing van art. 4 lid 2 Richtlijn 2016/680 toekomt.

129 Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken.

voorkomen dat gegevens steeds voor een ander doel verwerkt worden, zonder dat dit voldoende voorzienbaar is voor betrokkene.

3.2.1.3 Dataminimalisatie (minimale gegevensverwerking)

Het beginsel van dataminimalisatie is opgenomen in artikel 4 eerste lid, sub c, Richtlijn 2016/680 en stelt dat persoonsgegevens toereikend, ter zake dienend en niet bovenmatig moeten zijn in verhouding tot de doeleinden waarvoor zij worden verwerkt.[130] Aan de hand van het verwerkingsdoeleinde moeten de bevoegde autoriteiten beoordelen welke persoonsgegevens mogen worden verwerkt voor het bereiken van dat doel. Dit beginsel is dan ook verwant aan het doelbindingsbeginsel.[131]

Het beginsel van minimale gegevensverwerking kan op gespannen voet staan met het analyseren van bulkgegevens die zijn verzameld in de opsporing.[132] Het aan dataminimalisatie verwante uitgangspunt van 'select-before-you-collect'[133] laat zich namelijk moeilijk rijmen met het doorzoeken van bulkgegevens die zijn vergaard op grond van het principe van 'collect-before-you-select'.[134] Daarbij is natuurlijk wel van belang hoe specifiek die verwerkingsdoeleinden in de context van de Richtlijn 2016/680 moeten worden geformuleerd. Hoe ruimer de doeleinden mogen worden geformuleerd, des te meer gegevens nodig zijn om die doeleinden te kunnen verwezenlijken, waardoor meer persoonsgegevens mogen worden verzameld.

Bovendien is dataminimalisatie in de Richtlijn 2016/680 minder streng geformuleerd dan in de AVG. Die laatste vereist dat persoonsgegevens "toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt" (zie artikel 5 eerste lid, sub c, AVG). De Richtlijn 2016/680 is een stuk soepeler: "[persoonsgegevens] moeten toereikend, ter zake dienend en niet bovenmatig [zijn] in verhouding tot de doeleinden waarvoor zij worden verwerkt" (artikel 4, eerste lid, sub c, Richtlijn 2016/680).[135] Dat gegevens

130 De verwerkingsverantwoordelijke moet ervoor zorgen dat dit beginsel ook bij het ontwerp en de standaardinstellingen in ogenschouw wordt genomen (artikel 20 Richtlijn 2016/680).

131 Zie ook WRR 2016, p. 109; Koning 2020, p. 67; De Hert & Sajfert 2021, p. 13; Coudert 2017, p. 316.

132 Zie ook Bas Seyyar & Geradts 2020, p. 5 en 7.

133 Zwenne & Schmidt 2016, p. 343.

134 WRR 2016, p. 56 en 109.

135 De Hert & Sajfert 2021, p. 13; Sajfert & Quintel 2019, p. 6; Foivi Mouzakiti 2020, p. 366; Alves Hendriques 2021. Vergelijk ook Koning 2020, p. 107; Bas Seyyar & Geradts 2020, p. 7. Zie anders Von Grafenstein 2018, p. 242; Van Hoboken 2016, p. 238.

niet bovenmatig mogen zijn, impliceert een minder zware bewijslast voor de bevoegde autoriteit.[136] Deze hoeft de verwerking van persoonsgegevens niet te beperken tot wat absoluut noodzakelijk is. Op deze manier heeft hij meer beoordelingsvrijheid ten aanzien van de persoonsgegevens die hij verwerkt.[137] Tegelijkertijd wordt door het criterium 'niet bovenmatig' voorkomen dat de bevoegde autoriteiten persoonsgegevens verzamelen voor 'het geval dat'.[138] Dit zorgt voor een evenwicht tussen het belang van de opsporing en de bescherming van persoonsgegevens. Bovendien doet een wat ruimere uitleg van dataminimalisatie ook beter recht aan het gegeven dat opsporingsautoriteiten niet altijd op voorhand precies kunnen weten welke persoonsgegevens zij al dan niet gaan verwerken. Dit is onder de AVG anders.

De beginselen doelbinding en dataminimalisatie komen ook terug in artikel 6 Richtlijn 2016/680. Daarin bepaalt de Uniewetgever dat lidstaten moeten voorschrijven dat "de verwerkingsverantwoordelijke, in voorkomend geval en voor zover mogelijk, een duidelijk onderscheid maakt tussen persoonsgegevens betreffende verschillende categorieën van betrokkenen". Een dergelijke verplichting kan bij het doorzoeken van bulkgegevens problematisch zijn. Aan de andere kant geeft de Uniewetgever wel enige ruimte aan de opsporingsautoriteiten. De Richtlijn 2016/680 geeft immers niet aan op welk moment in het gegevensverwerkingsproces het onderscheid tussen verschillende categorieën van betrokkenen moet worden gemaakt. Ook geeft de Uniewetgever aan dat dit onderscheid moet worden gemaakt, voor zover dat mogelijk is.

3.2.1.4 Juistheid

In artikel 4 eerste lid, sub d, Richtlijn 2016/680 bepaalt de Uniewetgever dat persoonsgegevens juist moeten zijn en zo nodig moeten worden geactualiseerd. Voorts moeten alle redelijke maatregelen worden genomen om persoonsgegevens die, gelet op de doeleinden waarvoor zij worden verwerkt, onjuist zijn, onverwijld te wissen of te rectificeren. Dit beginsel is verder uitgewerkt in artikel 7 Richtlijn 2016/680. Dit artikel regelt de kwaliteit (of juistheid) van persoonsgegevens. Ingevolge dit artikel moeten de lidstaten erin voorzien dat "persoonsgegevens die op feiten zijn gebaseerd, voor zover mogelijk worden onderscheiden van persoonsgegevens die op een persoonlijk oordeel zijn gebaseerd" (lid 1). In de overwegingen horende bij dit artikel zegt de Uniewetgever het volgende: "Het beginsel van

136 De Hert & Sajfert 2021, p. 13.
137 Zie ook Sajfert & Quintel 2019.
138 De Hert & Sajfert 2021, p. 14.

juistheid van gegevens moet worden toegepast met inachtneming van de aard en het doel van de verwerking in kwestie. In het bijzonder bij gerechtelijke procedures zijn verklaringen die persoonsgegevens bevatten, gebaseerd op de subjectieve perceptie van natuurlijke personen en niet altijd te controleren. Het vereiste van juistheid dient derhalve geen betrekking te hebben op de juistheid van een verklaring, maar alleen op het feit dat een specifieke verklaring is afgelegd" (overweging 30 Richtlijn 2016/680). Daarnaast moeten de opsporingsautoriteiten "ervoor zorgen dat persoonsgegevens die onjuist, onvolledig of niet langer actueel zijn, niet worden doorgezonden of beschikbaar gesteld." "Om de bescherming van natuurlijke personen en de juistheid, de volledigheid of mate waarin de persoonsgegevens actueel zijn en de betrouwbaarheid van de doorgezonden of beschikbaar gestelde persoonsgegevens te waarborgen, dienen de bevoegde autoriteiten voor zover mogelijk bij elke doorzending van persoonsgegevens de noodzakelijke informatie toe te voegen" (artikel 7 tweede lid, en overweging 32 Richtlijn 2016/680). Blijkens artikel 7, derde lid, Richtlijn 2016/680 moet de opsporingsautoriteit – indien blijkt dat onjuiste persoonsgegevens zijn doorgezonden, of dat de persoonsgegevens op onrechtmatige wijze zijn doorgezonden – de ontvanger daarvan onverwijld in kennis stellen. Dit artikel is daarmee een goed voorbeeld van een verwerkingsbeginsel dat is toegesneden op de context van de opsporing, en waarin is getracht een evenwicht te zoeken tussen de belangen van de opsporing en de bescherming van persoonsgegevens van de betrokkene.[139]

3.2.1.5 Opslagbeperking

In artikel 4, eerste lid, sub e, Richtlijn 2016/680 is het beginsel van opslagbeperking neergelegd. Het beginsel van opslagbeperking veronderstelt dat 'persoonsgegevens worden bewaard in een vorm die het mogelijk maakt de betrokkenen niet langer te identificeren dan noodzakelijk is voor de doeleinden waarvoor de persoonsgegevens worden verwerkt.' Dit komt erop neer dat persoonsgegevens niet langer worden bewaard dan nodig voor het realiseren van de doeleinden waarvoor zij zijn verwerkt. Het verwerkingsdoeleinde is daarmee bepalend voor de periode waarin persoonsgegevens herleidbaar mogen worden bewaard.[140] Doordat het verwerkingsdoeleinde het referentiepunt is voor de opslagperiode, is dit beginsel net als het beginsel van dataminimalisatie verwant aan het beginsel van

139 Zie bijvoorbeeld De Hert & Papakonstantinou 2016, p. 11.

140 Geanonimiseerde gegevens mogen op basis van artikel 4 eerste lid, sub e, en artikel 5 Richtlijn 2016/680 dus wel voor een onbepaalde periode worden opgeslagen.

doelbinding.[141] In artikel 5 Richtlijn 2016/680 wordt het beginsel van opslagbeperking nader uitgewerkt. In tegenstelling tot de AVG vereist de Richtlijn 2016/680 dat de lidstaten concrete bewaartermijnen vaststellen.[142] Dit geeft meer rechtszekerheid aan de betrokkene.

3.2.1.6 Integriteit en vertrouwelijkheid

Op grond van artikel 4, eerste lid, onder f, Richtlijn 2016/680 mogen de persoonsgegevens door de bevoegde autoriteit alleen 'met gebruikmaking van passende technische of organisatorische middelen op een dusdanige manier worden verwerkt dat de beveiliging ervan gewaarborgd is, en dat zij onder meer beschermd zijn tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.' Dit beginsel komt erop neer dat de vertrouwelijkheid, integriteit en de beschikbaarheid van de persoonsgegevens moeten worden gewaarborgd.[143] Daartoe moeten passende technische en organisatorische maatregelen worden genomen om een op het risico afgestemd beveiligingsniveau te waarborgen (artikel 29 Richtlijn 2016/680). Bij het bepalen van de passende maatregelen wordt onder meer rekening gehouden met 'de stand van de techniek, de uitvoeringskosten in verband met de risico's en de aard van de te beschermen persoonsgegevens.'[144] Ook dient 'aandacht te worden besteed aan de risico's die zich voordoen bij gegevensverwerking, zoals de vernietiging, het verlies, de wijziging of de ongeoorloofde bekendmaking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte persoonsgegevens, hetzij per ongeluk hetzij onrechtmatig, hetgeen met name tot lichamelijke, materiële of immateriële schade kan leiden.'[145]

De Richtlijn 2016/680 geeft op gedetailleerde wijze aan welke maatregelen de lidstaten aan de verwerkingsverantwoordelijke minimaal moeten voorschrijven (artikel 29 lid 2 Richtlijn 2016/680). Zo schrijft de Richtlijn 2016/680 bijvoorbeeld voor dat de verwerkingsverantwoordelijke maatregelen treft om 'te verhinderen dat onbevoegden toegang krijgen tot verwerkingsapparatuur' (sub a); 'te verhinderen dat onbevoegden de gegevensdragers lezen, kopiëren, wijzigen of verwijderen' (sub b) of 'ervoor te zorgen dat personen die bevoegd zijn om een geautomatiseerd verwerkingssysteem te gebruiken, uitsluitend toegang hebben tot de

141 Zie ook Brouwer 2011, p. 281.
142 Leiser & Custers 2019, p. 372.
143 Zie ook artikel 7 lid 2 Richtlijn 2016/680.
144 Overweging 28 Richtlijn 2016/680.
145 Overweging 60 Richtlijn 2016/680.

persoonsgegevens waarop hun toegangsbevoegdheid betrekking heeft' (sub e). Een andere specifieke maatregel is dat de lidstaten erin voorzien dat er logbestanden worden bijgehouden van de volgende verwerkingen: verzameling, wijziging, raadpleging, bekendmaking onder meer in de vorm van doorgiften, combinatie en wissing.[146]

3.2.2 Toezicht op naleving van de Richtlijn 2016/680

Toezicht op de verwerking van persoonsgegevens is een essentiële component van een doeltreffende bescherming van persoonsgegevens.[147] Dit toezicht vindt op interne wijze plaats door de functionaris voor gegevensbescherming (FG) en op externe wijze door een onafhankelijke toezichthouder. Hoewel het aanwijzen van een FG en een onafhankelijke autoriteit ingevolge de Richtlijn 2016/680 verplicht is voor de lidstaten, maakt de Richtlijn 2016/680 niet duidelijk in hoeverre deze toezichthouders een rol als poortwachter bij het verder gebruik van persoonsgegevens kunnen en moeten vervullen. Hieronder staan wij kort stil bij beide toezichtmodaliteiten.

3.2.2.1 Functionaris gegevensbescherming

De lidstaten schrijven voor dat de verwerkingsverantwoordelijke een functionaris voor gegevensbescherming aanwijst (artikel 32 Richtlijn 2016/680). De functionaris voor gegevensbescherming wordt tijdig en naar behoren betrokken bij alle aangelegenheden die met de bescherming van persoonsgegevens verband houden (artikel 33 Richtlijn 2016/680). De functionaris moet zijn taken en verplichtingen onafhankelijk in overeenstemming met het lidstatelijke recht kunnen uitvoeren.[148] Volgens artikel 34 Richtlijn 2016/680 heeft de functionaris voor gegevensbescherming de volgende taken:

a) Informeren en adviseren van de verwerkingsverantwoordelijke en de werknemers die verwerking verrichten over hun verplichtingen op grond van deze richtlijn en andere gegevensbeschermingsbepalingen van het Unierecht of het lidstatelijke recht;
b) Toezien op de naleving van deze richtlijn, van andere gegevensbeschermingsbepalingen van het Unierecht of het lidstatelijke recht en

146 Artikel 25 Richtlijn 2016/680.
147 HvJ EU 6 oktober 2015, C-362/14, ECLI:EU:C:2015:650 (*Schrems*); HvJ EU 15 juni 2021, C-645/19, ECLI:EU:C:2021:483 (*Facebook/Gegevensbeschermingsautoriteit*). Zie ook Caruana 2017, p. 257 en 259.
148 Overweging 63 Richtlijn 2016/680.

van het beleid van de verwerkingsverantwoordelijke met betrekking tot de bescherming van persoonsgegevens, met inbegrip van de toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;

c) Desgevraagd advies verstrekken met betrekking tot de gegevensbeschermingseffectbeoordeling en toezien op de uitvoering daarvan in overeenstemming met artikel 27 Richtlijn 2016/680;
d) Met de toezichthoudende autoriteit samenwerken;
e) Optreden als contactpunt voor de toezichthoudende autoriteit inzake verwerkingsaangelegenheden, met inbegrip van de in artikel 28 bedoelde voorafgaande raadpleging, en, voor zover dienstig, overleg plegen met betrekking tot enige andere aangelegenheid.

3.2.2.2 Onafhankelijke toezichthouder

De Richtlijn 2016/680 bepaalt dat elke lidstaat erin voorziet dat één of meer onafhankelijke overheidsinstanties worden belast met het toezicht op de toepassing van de Richtlijn 2016/680 (artikel 41 Richtlijn 2016/680). Voor de bescherming van natuurlijke personen acht de Uniewetgever het van wezenlijk belang dat in de lidstaten toezichthoudende autoriteiten worden ingesteld die hun taken volstrekt onafhankelijk uitvoeren.[149]

De toezichthoudende autoriteit heeft op grond van artikel 46 en 47 Richtlijn 2016/680 een aantal taken en bevoegdheden. Die bevoegdheden betreffen onderzoeksbevoegdheden, het treffen van corrigerende maatregelen en adviesbevoegdheden. De toezichthouder heeft op grond van de Richtlijn 2016/680 minder taken en bevoegdheden dan hij heeft op grond van de AVG.[150] Anders dan de AVG verplicht de Richtlijn 2016/680 de lidstaten niet om bepaalde handhavingsbevoegdheden toe te bedelen aan de toezichthouder.[151] Dit verschil tussen de Richtlijn 2016/680 en de AVG zou kunnen betekenen dat de toezichthouder meer terughoudend moet zijn bij het corrigeren van de opsporingsautoriteiten.[152] Wel merken wij op dat de Uniewetgever het in artikel 47 Richtlijn 2016/680 uiteindelijk aan de nationale wetgever laat om te bepalen welke bevoegdheden hij aan de

149 Overweging 75 Richtlijn 2016/680.

150 Zie ook Werkgroep Artikel 29, 'Advies inzake een aantal belangrijke aandachtspunten van de richtlijn gegevensbescherming bij rechtshandhaving (Richtlijn (EU) 2016/680)', WP 258, *ec.europe.eu* 7 december 2017, p. 36; Caruana 2017, p. 259; De Hert & Sajfert 2018, p. 250.

151 *Kamerstukken II* 2017/18, 34889, nr. 6, p. 24 en 25.

152 De Hert & Sajfert 2018, p. 252.

toezichthouder wil geven ten opzichte van de opsporingsautoriteiten.[153] Op grond van artikel 47 Richtlijn 2016/680 moeten die bevoegdheden 'effectief' zijn.[154] Die eis van 'effectiviteit' kan met zich meebrengen dat de nationale wetgever alsnog dezelfde bevoegdheden aan de toezichthouder ten opzichte van opsporingsautoriteiten moet geven als die zij hebben onder de AVG.[155]

Blijkens artikel 26 Richtlijn 2016/680 schrijven de lidstaten voor dat de verwerkingsverantwoordelijke en de verwerker desgevraagd met de toezichthoudende autoriteit samenwerken bij het vervullen van haar taken. Onduidelijk is wat wordt bedoeld met de term 'desgevraagd'; gaat het nu om een verzoek van de toezichthouder of om een verzoek van de verwerkingsverantwoordelijke? [156]

Ingevolge artikel 28 Richtlijn 2016/680 voorzien de lidstaten erin dat de verwerkingsverantwoordelijke of de verwerker de toezichthoudende autoriteit raadpleegt voordat de verwerking van persoonsgegevens 'in een nieuw bestand zal worden opgenomen'. De toezichthoudende autoriteit moet worden geraadpleegd indien:

a) uit een gegevensbeschermingseffectbeoordeling als bedoeld in artikel 27 blijkt dat de verwerking een hoog risico zou opleveren indien de verwerkingsverantwoordelijke geen maatregelen neemt om het risico te beperken;
b) de aard van de verwerking, in het bijzonder wanneer wordt gebruikgemaakt van nieuwe technologieën, mechanismen of procedures, een hoog risico voor de rechten en vrijheden van betrokkenen met zich meebrengt.

Uit artikel 47 derde lid Richtlijn 2016/680 volgt dat de voorafgaande raadpleging in het kader van artikel 47 Richtlijn 2016/680 een adviesbevoegdheid betreft.[157] De Richtlijn 2016/680 geeft tevens enkele gezichtspunten of er sprake is van een 'hoog risico': de aard, de reikwijdte, de context en de doeleinden van de

153 De Hert & Sajfert 2018, p. 251.
154 Vergelijk ook HvJ EU 6 oktober 2015, C-362/14, ECLI:EU:C:2015:650 (*Schrems*), punt 81.
155 Werkgroep Artikel 29, 'Advies inzake een aantal belangrijke aandachtspunten van de richtlijn gegevensbescherming bij rechtshandhaving (Richtlijn (EU) 2016/680)', WP 258, *ec.europe.eu* 7 december 2017, p. 36. Zie ook De Hert & Sajfert 2018, p. 253.
156 De Engelse tekst luidt als volgt: "Member States shall provide for the controller and the processor to cooperate, on request, with the supervisory authority in the performance of its tasks on request."
157 Zie ook Jasserand 2018b, p. 162.

gegevensverwerking moeten daarbij helpen.[158] Of de beoordeling of een verdere verwerking een hoog risico oplevert moet per geval worden bekeken.[159]

Jasserand vindt artikel 28 Richtlijn 2016/680 geen voldoende procedurele waarborg tegen eventueel misbruik van het gebruik van persoonsgegevens voor een ander doel. De bepaling vereist alleen een voorafgaande raadpleging - en niet een voorafgaande beslissing - van de onafhankelijke autoriteit of de verwerking voor een ander doel is toegestaan. [160] Bovendien is die voorafgaande raadpleging van de onafhankelijke toezichthouder afhankelijk van de invulling van het begrip 'hoog risico'. Zij merkt wel op dat het disproportioneel zou kunnen zijn als de opsporingsautoriteit telkens een verzoek zou moeten doen voor een voorafgaande toetsing door een toezichthoudende autoriteit.

3.2.3 Tussenconclusie

In de Richtlijn 2016/680 heeft de Uniewetgever een evenwicht gezocht tussen enerzijds de bescherming van persoonsgegevens en anderzijds de belangen van de opsporing. De uitwerking van de beginselen van de Richtlijn 2016/680 en de bepalingen aangaande toezicht en rechtsbescherming zijn daarom flexibeler dan hun tegenhangers in de AVG. Tegelijkertijd bestaat onduidelijkheid over sommige bepalingen. Met name het antwoord op de vraag op welke wijze moet worden getoetst of de verwerking van persoonsgegevens voor een ander doel toelaatbaar is, wordt in de Richtlijn 2016/680, de totstandkomingsgeschiedenis van de Richtlijn 2016/680 en literatuur over de Richtlijn 2016/680 niet helder uiteengezet. Het antwoord op die vraag is belangrijk, omdat dit aangeeft in hoeverre de opsporingsautoriteit persoonsgegevens verder mag gebruiken. Voorts schrijft de Richtlijn 2016/680 voor dat er toezicht moet bestaan op de gegevensverwerking door de opsporingsautoriteit. Dit toezicht dient zowel op intern als op extern niveau plaats te vinden. Tegelijkertijd is de Richtlijn 2016/680 ook op dit punt weinig concreet, anders dan dat de bevoegdheden van de toezichthouder 'effectief' moeten zijn. Het is daarom de vraag of de Richtlijn 2016/680 voldoende procedurele waarborgen biedt tegen eventueel misbruik door de opsporingsautoriteit.

158 Overweging 52 Richtlijn 2016/680.

159 Jasserand 2018b, p. 161. De AVG daarentegen geeft aanwijzingen over welke specifieke gegevensverwerkingen een 'hoog risico' opleveren (artikel 35 lid 3 AVG).

160 Jasserand 2018b, p. 162.

3.3 ARTIKEL 8 EVRM

Artikel 8 EVRM biedt bescherming aan het recht op privéleven, het familieleven, de woning en correspondentie. Deze vier rechten worden vaak onder de noemer privacy gebracht. Mede vanwege de ruime uitleg die het EHRM aan het recht op privacy geeft, bestrijkt het recht een breed scala aan onderwerpen. Een van deze onderwerpen betreft *surveillance*, waaronder wordt verstaan de vergaring en verwerking van gegevens ter bestrijding van (ernstige) criminaliteit en/of de bescherming van de nationale veiligheid. Het EHRM heeft zich inmiddels uitgelaten over verschillende *surveillance*-methoden, zoals het opbouwen van politionele gegevensbanken, inbeslagneming, het onderscheppen van communicatie en daaraan gerelateerde gegevens en locatiebepaling. Deze jurisprudentie is veelomvattend en doorgaans casuïstisch van aard. Het EHRM beoordeelt normaliter enkel of de gehanteerde methode inbreuk maakt op het recht op privacy en – indien dat het geval is – of die inbreuk kan worden gerechtvaardigd.

Een en ander neemt echter niet weg dat het EHRM via vooropstellingen in algemene overwegingen en het vergelijken van feitencomplexen invulling geeft aan de afbakening van artikel 8 EVRM alsmede de eisen en waarborgen waaraan moet zijn voldaan als inbreuk is gemaakt op het recht op privacy.[161] Bovendien heeft het EHRM in zijn rechtspraak over *surveillance* geaccepteerd dat niet alleen over de inzet van een specifieke methode in een bepaald geval, maar ook over het bestaan van wetgeving betreffende deze methode kan worden geklaagd.[162] Voor een burger kan het immers moeilijk aan te tonen zijn dat hij in de zin van het EVRM slachtoffer is van een heimelijke surveillancebevoegdheid.[163] Het EHRM heeft in dit licht een uitzondering gecreëerd op het uitgangspunt dat alleen slachtoffers mogen klagen over potentiële EVRM-schendingen.[164] Mede door deze uitzondering heeft het EHRM zich in meer algemene zin uitgelaten over de vraag wanneer

161 Zie voor een chronologische bespreking van de relevante jurisprudentie De Hert en Malgieri 2021.

162 Dat is voor het eerst gebeurd in EHRM (GK) 4 december 2015, nr. 47143/06 (*Roman Zakharov/Rusland*).

163 Artikel 34 jo. 35, derde lid, onder b EVRM.

164 Zie in dit kader o.a. Van der Sloot 2020; Van der Sloot & Kosta, par. III. De 'quality of law doctrine' stelt het Hof in staat te toetsen of landen in hun nationale wetgeving voldoende waarborgen hebben opgenomen waarin de machtsoverdracht van de wetgevende naar de uitvoerende macht aan voorwaarden en grenzen wordt gebonden inzake het verzamelen, opslaan en verwerken van gegevens, en of afdoende juridische en parlementaire controle mogelijk is op het gebruik van de bevoegdheden door de uitvoerende macht.

surveillance-methoden inbreuk maken op het recht op privacy en welke eisen daaraan moeten worden gesteld.

In het hiernavolgende wordt nader ingegaan op de relevante rechtspraak van het EHRM inzake *surveillance*. Het doel van deze bespreking is om in kaart te brengen welke richtsnoeren uit deze jurisprudentie kunnen worden afgeleid voor wat betreft de normering van onderzoek aan gegevens voor strafvorderlijke doeleinden. Daartoe zal nader worden ingegaan op de jurisprudentie inzake politionele en justitiële gegevensbanken en het onderscheppen en verder verwerken van communicatie en daaraan gerelateerde gegevens.

3.3.1 Politionele en justitiële databanken

3.3.1.1 Inbreuk

Sinds de jaren 1980 is duidelijk dat het opslaan van gegevens door de politie onder het bereik van artikel 8 EVRM kan vallen indien die gegevens het privéleven raken.[165] De vraag wanneer precies sprake is van gegevens die het privéleven raken beoordeelt het EHRM aan de hand van een aantal factoren: 1) de (juridische) aard van de gegevens; 2) hetgeen uit de gegevens kan worden afgeleid, 3) de context waarin de gegevens zijn verkregen en worden opgeslagen en 4) de wijze waarop de gegevens worden gebruikt.[166]

Op basis van bovenstaande factoren beoordeelt het EHRM telkens op casuïstische wijze of een verwerking met gegevens onder het bereik van artikel 8 EVRM valt. Toch vallen in de jurisprudentie wel enkele algemene lijnen te ontwaren. Een belangrijke notie bij de beoordeling van deze factoren is het recht op

165 EHRM 26 maart 1987, nr. 9248/81 (*Leander/Zweden*), par. 48. Zie eerder ook EHRM 6 september 1978, nr. 5029/71 (*Klass e.a./Duitsland*), par. 41. Het EHRM oordeelde in deze zaak voor het eerst dat, hoewel telefoongesprekken niet uitdrukkelijk worden genoemd in artikel 8, eerste lid, EVRM, deze gesprekken vallen onder de begrippen 'privéleven' en 'correspondentie'. Het afluisteren hiervan door de Duitse overheid, betrof dan ook een inbreuk op de privacy.

166 EHRM (GK) 4 december 2008, nr. 30562/04 (*S. en Marper/Verenigd Koninkrijk*), *NJ* 2009/410, m.nt. Alkema, *NTM/NJCM-bull.* 2009, p. 391 en m.nt. Van der Staak, par. 67. Zie ook EHRM 25 september 2001, nr. 44787/98 (*P.G. & J.H./Verenigd Koninkrijk*), *NJ* 2003/670, m.nt. Dommering, par. 24-25; EHRM 28 januari 2003, nr. 44647/98 (*Peck/Verenigd Koninkrijk*), par. 57-59; EHRM 17 juli 2003, nr. 63737/00 (*Perry/Verenigd Koninkrijk*), *NJ* 2006/40, m.nt. Dommering, par. 38 en EHRM 18 oktober 2016, nr. 61838/10 (*Vukota-Bojić /Zwitserland*), *AB* 2017/418, m.nt. Schuurmans & Uzman, par. 54-56.

informatieve zelfbeschikking.[167] Zo kunnen bepaalde gegevens op zichzelf weliswaar neutraal zijn, maar bij het collectief verzamelen en verwerken en verspreiden toch veel informatie verschaffen over het persoonlijke leven van een individu. Het vergaren en analyseren van deze neutrale gegevens raakt dan de autonomie van een persoon. Als het gaat om de verwerking van gevoelige persoonsgegevens zoals medische gegevens, gegevens waaruit iemands etniciteit blijkt of gegevens over iemands strafrechtelijk verleden, dan vallen deze zonder meer onder het bereik van artikel 8 EVRM.[168] De (juridische) aard van de gegevens is echter niet de enige factor die van belang is. Het EHRM is nooit zover gegaan dat het onder artikel 8 EVRM een recht op de bescherming van persoonsgegevens heeft erkend.[169] Het object van bescherming van artikel 8 EVRM zijn gegevens die het privéleven raken en niet persoonsgegevens. De kwalificatie persoonsgegevens betekent dus niet zonder meer dat ook het recht op privacy als bedoeld in artikel 8 EVRM van toepassing is.[170] Voor het EHRM zijn de overige factoren belangrijker.

De vraag wát uit de gegevens over iemand kan worden afgeleid, is aldus een belangrijke indicator. Daarbij tracht het EHRM te differentiëren in verschillende typen gegevens. Zo ziet het EHRM voor wat betreft de ernst van de privacyinbreuk verschil tussen verwerkingen met betrekking tot identificerende gegevens,[171] locatiegegevens[172] en communicatiegegevens. Uit identificerende

167 EHRM 30 januari 2020, nr. 50001/12 (*Breyer/Duitsland*); EHRM 27 juni 2017, nr. 931/13 (*Satakunnan Markkinapörssi Oy and Satamedia Oy/Finland*), par. 136 en137 (en verwijzingen hierin). ("It further follows from the Court's well-established case-law that where there has been a compilation of data on a particular individual, the processing or use of personal data or publication of the material concerned in a manner or degree beyond that normally foreseeable, private life considerations arise. Article 8 of the Convention thus provides for the right to a form of informational self-determination, allowing individuals to rely on their right to privacy as regards data which, albeit neutral, are collected, processed and disseminated collectively and in such form or manner that their Article 8 rights may be engaged […]").

168 EHRM (GK) 4 december 2008, nr. 30562/04 (*S. en Marper/Verenigd Koninkrijk*), *NJ* 2009/410, m.nt. Alkema, *NTM/NJCM-bull.* 2009, p. 391, m.nt. Van der Staak, par. 66 en 76; EHRM 4 mei 2000, nr. 28341/95 (*Rotaru*), par. 43-44, *EHRC* 2000/53, m.nt. Brems; EHRM 13 november 2012, nr. 24029/07, (*M.M./Verenigd Koninkrijk*), par. 188.

169 Gonzalez Fuster 2014, p. 99; De Hert en Gutwirth 2009, p. 24-26.

170 EHRM 18 oktober 2011, nr. 16188/07 (*Khelili/Zwitserland*), par. 55.

171 In EHRM 30 januari 2020, nr. 50001/12 (*Breyer/Duitsland*), par. 92-94 merkt het EHRM de opslag van identificerende gegevens door telecommunicatieaanbieders als een beperkte inbreuk op artikel 8 EVRM aan, onder meer omdat de gegevens geen hoog-persoonlijke informatie bevatten.

172 In EHRM 2 september 2010, nr. 35623/05 (*Uzun/Duitsland*), par. 53 zet het EHRM het vergaren van locatiegegevens door de politie af tegen vanuit privacy oogpunt verdergaande →

gegevens en locatiegegevens kan doorgaans een minder diepgaand beeld van iemands privéleven worden afgeleid dan uit communicatiegegevens.

Voorts is voor het EHRM ook van belang op welke wijze de gegevens kunnen worden benut. Door de opslag van gegevens wordt immers de mogelijkheid gecreëerd om later – eventueel aangevuld met andere gegevens of op basis van nieuwe technologieën – een beeld van iemands privéleven te verkrijgen. In verschillende zaken oordeelde het EHRM immers dat de opslag van gegevens reeds voldoende is voor het aannemen van een inbreuk op het recht op privacy, ook als de gegevens niet worden gebruikt.[173] Illustratief in dit verband is het arrest *Gaughran/Verenigd Koninkrijk.*[174] Hierin oordeelde het EHRM dat het nemen en het opslaan van een foto van een verdachte in een politiedatabank inbreuk maakt op het recht op privacy. Voor het vaststellen van de inbreuk was in het bijzonder van belang dat de foto werd opgeslagen in een databank omdat de foto hiermee beschikbaar blijft voor verder gebruik.[175] De foto kan in toekomstige onderzoeken of voor andere doeleinden (bijvoorbeeld gezichtsherkenningstechnologie) worden gebruikt. Deze rechtspraak laat aldus zien dat het creëren van de mogelijkheid om gegevens verder te verwerken of te gebruiken vaak een inbreuk op het recht op privacy oplevert. Hoewel het EHRM in deze rechtspraak niet over doelspecificatie of -binding rept, komt hierin wel duidelijk naar voren dat het EHRM bij de vraag of inbreuk is gemaakt rekening houdt met de vraag in hoeverre doelafwijkend gebruik mogelijk is.[176]

Kortom, op basis van bovenstaande dynamische factoren heeft het EHRM verschillende handelingen van de politie met gegevens onder het bereik van artikel 8 EVRM gebracht. De casuïstische toets van het EHRM heeft er onder meer toe geleid dat de politionele en/of justitiële verwerking van communicatiegegevens,[177]

---

inbreuken zoals het vergaren van communicatiegegevens. Vgl. ook EHRM 8 februari 2018, nr. 31446/12 (*Ben Faiza/Frankrijk*), waarin het EHRM zijn standpunt uit Uzun herhaalt, hoewel het EHRM in Ben Faiza weinig oog lijkt te hebben voor de verschillen in het feitencomplex.

173 Zie onder meer EHRM 26 maart 1987, nr. 9248/81 (*Leander/Zweden*); EHRM (GK) 16 februari 2000, nr. 27798/95 (*Amann/Zwitserland*); EHRM (GK) 4 mei 2000, nr. 28341/95 (*Rotaru/Roemenië*).

174 EHRM 13 februari 2020, nr. 45245/15 (*Gaughran/UK*), *EHRC* 2020/86, m.nt. Van der Sloot.

175 EHRM 13 februari 2020, nr. 45245/15 (*Gaughran/UK*), par. 70, *EHRC* 2020/86, m.nt. Van der Sloot.

176 In dezelfde zin Von Grafenstein 2018, p. 188-190, 194; Koning 2020, p. 145-150.

177 EHRM 6 september 1978, nr. 5029/71 (*Klass e.a./Duitsland*); EHRM 1 juli 2008, nr.58243/00 (*Liberty e.a./ Verenigd Koninkrijk*); EHRM 12 januari 2016, nr. 37138/14 (*Szabó & Vissy/Hongarije*).

locatiegegevens[178] en gegevens over iemands bewegingen in de publieke ruimte[179] onder het bereik van artikel 8 EVRM vallen. In het algemeen legt het EHRM de lat voor de beoordeling van de vraag of het recht op privéleven wordt getroffen niet hoog. Zodra de politie persoonsgegevens opslaat – ook al worden deze gegevens niet gebruikt – wordt al een inbreuk op het recht op privacy aangenomen. Door het opslaan van de gegevens wordt immers de mogelijkheid gecreëerd om later – eventueel aangevuld met andere gegevens of op basis van nieuwe technologieën – een beeld van iemands privéleven te verkrijgen.

3.3.1.2 Gerechtvaardigde inbreuk

Volgens artikel 8 lid 2 EVRM is een inbreuk gerechtvaardigd als deze bij wet is voorzien, een legitiem doel dient, en noodzakelijk is in een democratische samenleving. Deze drie stappen zijn echter niet altijd strikt van elkaar te scheiden. In *S. en Marper/Verenigd Koninkrijk* overwoog het EHRM bijvoorbeeld dat "*these questions [inzake de voorzienbaarheid van het recht, onze toevoeging] are in this case closely related to the broader issue of whether the interference was necessary in a democratic society*".[180] Wel valt op dat het EHRM voor wat betreft de vraag of de inbreuk kan worden gerechtvaardigd veel waarde toekent aan de in het nationale recht neergelegde waarborgen die misbruik moeten voorkomen. Deze eisen die het EHRM heeft afgeleid uit het noodzakelijkheids-, proportionaliteits- en subsidiariteitsbeginsel zijn nauw verwant aan de tegenwoordig geldende gegevensbeschermingsrechtelijke beginselen. Hierbij kan worden gedacht aan doelspecificatie, doelbinding, opslagbeperking, dataminimalisatie en de vertrouwelijkheid en integriteit van gegevens.[181] Als aan deze gegevensbeschermingsrechtelijke beginselen is voldaan, zal het EHRM niet snel concluderen dat sprake is van een schending van artikel 8 EVRM.[182]

178 EHRM 2 september 2010, nr. 35623/05 (*Uzun/Duitsland*); EHRM 8 februari 2018, nr. 31446/12 (*Ben Faiza/Frankrijk*).

179 EHRM 18 oktober 2016, nr. 61838/10 (*Vukota-Bojić/Zwitserland*), *AB* 2017/418 m.nt. Schuurmans & Uzman, par. 54-56. In deze zaak ging het weliswaar om observatie door een privédetective, maar principieel verschilt het observeren door een burger niet van observatie door de politie.

180 EHRM (GK) 4 december 2008, nr. 30562/04 (*S. en Marper/Verenigd Koninkrijk*), par. 99, *NJ* 2009/410, m.nt. Alkema, *NTM/NJCM-bull.* 2009/4, p. 391, m.nt. Van der Staak.

181 In dezelfde zin Koning 2020, p. 164.

182 EHRM 4 juni 2013, nrs. 7841/08 en 57900/12 (*Peruzzo en Martens/Duitsland*) is in dit verband illustratief. In deze zaak moest het Hof zich buigen over de vraag of de opslag van DNA-gegevens de toets aan artikel 8 EVRM kan doorstaan. Volgens het EHRM is dat het →

Bij de beoordeling van de vraag of een inbreuk is gerechtvaardigd speelt de ernst van de privacyinbreuk een belangrijke rol.[183] Zo maakt het EHRM bijvoorbeeld onderscheid in de eisen en waarborgen die moeten gelden voor de opslag van DNA-materiaal, foto's en vingerafdrukken.[184] Over het algemeen is het EHRM streng ten aanzien van politionele en justitiële gegevensbanken. Niet alleen in zaken waarin het draait om de opslag van hoog-persoonlijke informatie zoals DNA-materiaal,[185] ook als het gaat om databanken waarin voor het publiek toegankelijke gegevens worden opgeslagen, is het EHRM streng.[186] De reden hiervoor is dat het creëren van databanken gemakkelijk tot misbruik kan leiden en dat dient zoveel mogelijk te worden voorkomen. Dit misbruik kan zoals gezegd worden voorkomen door acht te slaan op gegevensbeschermingsrechtelijke principes als doelspecificatie, doelbinding, opslagbeperking en dataminimalisatie.

Zo is duidelijk dat het EHRM veel belang hecht aan de vraag in hoeverre het nationale recht beperkingen stelt ten aanzien van de gegevens die mogen worden verwerkt en de personen over wie de gegevens mogen worden verwerkt. Deze beoordeling zegt iets over de proportionaliteit en de subsidiariteit van een surveillancemethode, maar hier wordt ook het belang van doelspecificatie en -binding zichtbaar.[187] In *Rotaru/Roemenië* komt het EHRM tot een schending van artikel 8 EVRM, omdat het nationale recht in het geheel geen grenzen stelt aan de mogelijkheid om informatie over een individu op te slaan.[188] Het nationale Roemeense recht maakte niet duidelijk welke informatie mocht worden opgeslagen, van wie gegevens mochten worden opgeslagen, hoe lang de informatie mocht worden bewaard

geval, omdat het nationale recht het slechts toestaat om DNA voor een beperkte doelgroep te verwerken (doelspecificatie); er wordt regelmatig gecontroleerd of het nog noodzakelijk is om de gegevens op te slaan en het Duitse recht voorziet in effectieve controle; burgers kunnen een vordering indienen om de gegevens te laten verwijderen.

183 EHRM 13 november 2012, nr. 24029/07 (*M.M./Verenigd Koninkrijk*), par. 200 waarin het Hof overweegt: "[f]urther, the greater the scope of the recording system, and thus the greater the amount and sensitivity of data held and available for disclosure, the more important the content of the safeguards to be applied at the various crucial stages in the subsequent processing of the data."

184 EHRM (GK) 4 december 2008, nr. 30562/04 (*S. en Marper/Verenigd Koninkrijk*), par. 120, *NJ* 2009/410, m.nt. Alkema, *NTM/NJCM-bull.* 2009, p. 391, m.nt. Van der Staak.

185 EHRM (GK) 4 december 2008, nr. 30562/04 (*S. en Marper/Verenigd Koninkrijk*), par. 120, *NJ* 2009/410, m.nt. Alkema, *NTM/NJCM-bull.* 2009, p. 391, m.nt. Van der Staak;

186 EHRM (GK) 4 mei 2000, nr. 28341/95 (*Rotaru/Roemenië*); EHRM 6 juni 2006, nr. 62332/00 (*Segerstedt-Wiberg/Zweden*).

187 Zie hoofdstuk 3, § 1.2.1 over deze beginselen.

188 EHRM (GK) 4 mei 2000, nr. 28341/95 (*Rotaru/Roemenië*).

alsmede hoe de integriteit en de vertrouwelijkheid van de gegevens was geborgd.[189]

Voorts hecht het EHRM belang aan effectieve bewaartermijnen (opslagbeperking) en dataminimalisatie.[190] In *Brunet/Frankrijk* oordeelde het EHRM dat het opslaan en voor lange tijd bewaren van informatie (20 jaar) van individuen nadat de strafzaak is geëindigd een schending van artikel 8 EVRM oplevert.[191] Een ruime bevoegdheid tot het afnemen van vingerafdrukken in combinatie met een bewaartermijn van 25 jaar leidt ook tot een schending van artikel 8 EVRM.[192] Het nationale recht moet dus waarborgen dat gegevens relevant zijn en de omvang van de verzameling moet in verhouding staan tot het doel van de verwerking.[193] De wijze waarop de gegevens zijn beveiligd (integriteit en vertrouwelijkheid),[194] is ook een belangrijke factor in de jurisprudentie van het EHRM inzake politionele en justitiële databanken.[195] Ook hecht het EHRM belang aan toezicht.[196] Daarbij is vooral van belang dat het nationale recht ook voorziet in procedurele mogelijkheden ter voorkoming van misbruik. Waaraan dit toezicht precies moet doen, concretiseert het EHRM nauwelijks.

Zoals hierna zal blijken, valt tot slot op dat de eisen en waarborgen die het EHRM in het kader van de politionele en justitiële databanken van belang acht, overeenkomst kennen met de eisen en waarborgen die worden gesteld aan de heimelijke interceptie van communicatie. Op deze eisen gaan wij hieronder nader in.

3.3.2 Heimelijke interceptie van communicatie

3.3.2.1 Inbreuk

Voordat hieronder nader wordt ingegaan op de eisen en waarborgen die het EHRM stelt aan de vergaring en verwerking van communicatiegegevens en daaraan te relateren gegevens, dient eerst kort te worden stilgestaan bij het verschil tussen gerichte interceptie en ongerichte interceptie (bulkinterceptie).

189 Zie Koning 2020, p. 117-124 voor meer voorbeelden.
190 Zie hoofdstuk 3, § 1.5.
191 EHRM 18 september 2014, nr. 21010/10 (*Brunet/Frankrijk*).
192 EHRM 18 april 2013, nr. 19522/09 (*M.K./Frankrijk*).
193 EHRM 17 december 2009, nr. 16428/05 (*Gardel/Frankrijk*), par. 62.
194 Zie hoofdstuk 3, § 2.1.6.
195 Zie onder meer EHRM 17 december 2009, nr. 22115/06 (*M.B./Frankrijk*); EHRM 18 april 2013, nr. 19522/09 (*M.K./Frankrijk*).
196 Zie onder meer EHRM (GK) 4 mei 2000, nr. 28341/95 (*Rotaru/Roemenië*), par. 57-59; EHRM 13 november 2012, nr. 24029/07 (*M.M./Verenigd Koninkrijk*), par. 202.

Gerichte en ongerichte interceptie

Hoewel het EHRM geen definitie geeft voor gerichte interceptie, zondert het EHRM deze vorm van onderschepping onder meer in *Big Brother Watch e.a./Verenigd Koninkrijk* af van de ongerichte interceptie. Daarbij merkt het Straatburgse Hof op dat de gerichte interceptie meestal plaatsvindt met het oog op het onderzoeken van misdrijven.[197] Bij gerichte interceptie kan bijvoorbeeld worden gedacht aan het aftappen van telefoongesprekken bij specifieke verdachten. Dit kan worden gezien als een inbreuk op de privacy. Naast gerichte interceptie staat ongericht interceptie of bulkinterceptie. Ook de vraag wat precies onder bulkinterceptie moet worden verstaan, heeft het EHRM niet expliciet beantwoord. Bovendien gebruikt het EHRM niet altijd dezelfde termen voor bulkinterceptie, bijvoorbeeld '*strategic monitoring*' of '*mass surveillance*'.[198] Wel heeft het EHRM in de recente zaken *Big Brother Watch* en *Centrum för Rättvisa* nader proberen te duiden wat onder bulkinterceptie kan worden verstaan.[199] Bij bulkinterceptie gaat het volgens het EHRM vaak om 'internationale communicatie', dat is communicatie van personen buiten de territoriale jurisdictie van de staat. Vaak kan deze communicatie niet door

197 EHRM (GK) 25 mei 2021, nr. 58170/13, 62322/14 & 24960/15 (*Big Brother Watch e.a./Verenigd Koninkrijk*), *NJ* 2021/361, m.nt. Dommering, par. 344.

198 Zie onder meer EHRM 29 juni 2006, nr. 54934/00 (*Weber en Saravia/Duitsland*). Zie ook De Hert & Malgieri 2021, p. 268.

199 EHRM (GK) 25 mei 2021, nr. 58170/13, 62322/14 & 24960/15 (*Big Brother Watch e.a./Verenigd Koninkrijk*), *NJ* 2021/361, m.nt. Dommering, zie par. 322: "The present complaint concerns the bulk interception of cross-border communications by the intelligence services. While it is not the first time the Court has considered this kind of surveillance (see Weber and Saravia and Liberty and Others, both cited above), in the course of the proceedings it has become apparent that the assessment of any such regime faces specific difficulties. In the current, increasingly digital, age the vast majority of communications take digital form and are transported across global telecommunications networks using a combination of the quickest and cheapest paths without any meaningful reference to national borders. Surveillance which is not targeted directly at individuals therefore has the capacity to have a very wide reach indeed, both inside and outside the territory of the surveilling State. Safeguards are therefore pivotal and yet elusive. Unlike the targeted interception which has been the subject of much of the Court's case-law, and which is primarily used for the investigation of crime, bulk interception is also – perhaps even predominantly – used for foreign intelligence gathering and the identification of new threats from both known and unknown actors. When operating in this realm, Contracting States have a legitimate need for secrecy which means that little if any information about the operation of the scheme will be in the public domain, and such information as is available may be couched in terminology which is obscure and which may vary significantly from one State to the next."

andere surveillancemaatregelen worden verkregen.[200] De doeleinden waarvoor bulkinterceptie kan worden gebruikt lijken te verschillen van die waarvoor gerichte interceptie wordt ingezet. Gerichte interceptie vindt meestal plaats met het oog op het onderzoeken van misdrijven. Hoewel de ongerichte interceptie kán worden gebruikt om bepaalde ernstige misdrijven op te sporen, lijken lidstaten deze bevoegdheid vooral in te zetten voor het verzamelen van buitenlandse inlichtingen en het vroegtijdig opsporen en onderzoeken van cyberaanvallen, spionage en terrorisme.[201] Het EHRM geeft daarmee impliciet aan dat bulkinterceptie dus óók kan worden ingezet ten behoeve van de opsporing. Het spreekt in dit kader van 'ernstige misdrijven', maar door de verwoording met 'kan' bakent het EHRM de grenzen niet nader af. Het is dus níet zo dat het EHRM bulkinterceptie in het kader van opsporing alleen toelaatbaar acht als het zware criminaliteit betreft, althans die grens trekt het EHRM niet.

Het EHRM merkt vervolgens op dat – ook al heeft de massale onderschepping van gegevens niet noodzakelijk betrekking op bepaalde individuen – de onderschepping van gegevens wel kan worden ingezet 'to target individuals' en het wordt ook met dit oogmerk gebruikt. Als dit evenwel het geval is, worden niet de specifieke 'devices' van de beoogde personen gecontroleerd. Er wordt massaal communicatie onderschept waarbij – door de toepassing van sterke selectoren (zoals het gebruik van e-mailadressen) – gericht kan worden gezocht naar bepaalde personen. Alleen de 'pakketten' van communicatie van de individuen die door de inlichtingendiensten zijn geselecteerd aan de hand van sterke selectoren of complexe zoekopdrachten kunnen door een analist worden onderzocht.[202] Daarmee geeft het EHRM een nogal vage uitleg aan de term 'bulkinterceptie'. Het betreft in elk geval géén gerichte interceptie, maar de massale interceptie kan wel degelijk betrekking hebben op specifieke personen. Voorts lijkt het voornamelijk om de inlichtingencontext te gaan, maar het EHRM sluit niet uit dat bulkinterceptie ook in strafvorderlijk verband kan worden gebruikt. Over de inbreuk op het recht op privacy die gepaard gaat met bulkinterceptie merkt het EHRM het volgende op. Het EHRM beschouwt het in bulk vergaren en verwerken van communicatiegegevens als één gradueel proces van de initiële fase van vergaring tot aan het onderzoek en het gebruik van specifieke gegevens, waarbij de mate van de inbreuk op de privacy

200 EHRM (GK) 25 mei 2021, nr. 58170/13, 62322/14 & 24960/15 (*Big Brother Watch e.a./Verenigd Koninkrijk*), *NJ* 2021/361, m.nt. Dommering, zie par. 344.

201 EHRM (GK) 25 mei 2021, nr. 58170/13, 62322/14 & 24960/15 (*Big Brother Watch e.a./Verenigd Koninkrijk*), *NJ* 2021/361, m.nt. Dommering, zie par. 344.

202 EHRM (GK) 25 mei 2021, nr. 58170/13, 62322/14 & 24960/15 (*Big Brother Watch e.a./Verenigd Koninkrijk*), *NJ* 2021/361, m.nt. Dommering, zie par. 346.

toeneemt naarmate het proces vordert.[203] Het EHRM onderscheidt in dit kader vier fasen: 1) het verzamelen en opslaan van communicatiedata; 2) het doorzoeken van data aan de hand van selectoren; 3) het onderzoeken van geselecteerde data door een analist; 4) het gebruiken van data. Kennelijk hangt de ernst van de privacyinbreuk bij bulkinterceptie dus vooral af van de mate waarin de gegevens daadwerkelijk worden gebruikt om inzicht te verkrijgen in iemands persoonlijk leven. Als de gegevens worden onderschept, wordt weliswaar inbreuk gemaakt op het recht op privacy, maar de inbreuk is ernstiger als daadwerkelijk kennis wordt genomen van de gegevens. De zienswijze van het EHRM – waarbij de bulkinterceptie als één proces wordt beschouwd – contrasteert met de Nederlandse situatie waarin onderscheid wordt gemaakt tussen de vergaring en de verwerking van bulkgegevens.[204]

3.3.2.2. Gerechtvaardigde inbreuk

De zes Huvig criteria

Het EHRM heeft ten aanzien van de vraag of het onderscheppen van heimelijke communicatie en/of daaraan gerelateerde gegevens gerechtvaardigd is een eigen doctrine ontwikkeld. Daarbij worden de drie stappen uit artikel 8 lid 2 EVRM evenwel niet altijd doorlopen. Doorgaans beziet het EHRM de noodzakelijkheid van het vergaren van communicatie in samenhang met het legaliteitsvereiste.[205] Dit betekent dat het EHRM zich vooral concentreert op de vraag of het nationale recht voldoende waarborgen biedt tegen misbruik en willekeur.[206] De vraag is nu welke waarborgen voor het EHRM in het kader van het legaliteitsvereiste van belang zijn.

203 EHRM (GK) 25 mei 2021, nr. 58170/13, 62322/14 & 24960/15 (Big Brother Watch e.a./Verenigd Koninkrijk), *NJ* 2021/361, m.nt. Dommering, par. 325 en 350. Zie ook Hagens en Oerlemans in hun noot op *EHRC Updates* bij de zaken *BBW* en *Centrum för Rättvisa*.

204 Zie hoofdstuk 2.

205 Zie onder meer EHRM (GK) 4 december 2015, nr. 47143/06, *NJ* 2017/185, m.nt. Dommering, (*Roman Zakharov/Rusland*), par. 236; EHRM 18 mei 2010, nr. 26839/05, *NJ* 2011/333, (*Kennedy/Verenigd Koninkrijk*), par. 155. Vgl. voorts EHRM (GK) 4 december 2008, nrs. 30562/04 & 30566/04, *NJ* 2009/410, m.nt. Alkema, (*S. en Marper/Verenigd Koninkrijk*), par. 99, waar het Hof overweegt dat: '[…] the lawfulness of the interference is closely related to the question whether the "necessity" test has been complied with…'.

206 Zie bijvoorbeeld EHRM (GK) 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*), *NJ* 2021/361, m.nt. Dommering, par. 334 en 337. Het EHRM bespreekt de waarborgen rondom bulkinterceptie zowel in het licht van legaliteit als noodzakelijkheid. Het merkt daarbij op dat staten een ruime 'margin of appreciation' hebben wat betreft de keuze van een interceptiesysteem. De exploitatie van →

Het legaliteitsvereiste in zaken over gerichte interceptie van communicatie houdt in dat dat de inbreuk 1) een basis moet hebben in het nationale recht, alsook 2) voldoende toegankelijk, 3) voorzienbaar en 4) niet willekeurig moet zijn.[207] Het vereiste dat de inbreuk enige basis in het recht dient te hebben heeft in de rechtspraak van het EHRM een materieelrechtelijke inhoud gekregen.[208] Het betreft niet alleen formele wetgeving: ook jurisprudentie, beleidsregels, uitvoeringsbesluiten of zelfs ongeschreven recht kunnen als rechtsbasis dienen. Doorgaans toetst het EHRM slechts marginaal of een inbreuk op het recht op privacy een basis heeft in het recht. Wat betreft de eis van toegankelijkheid stelt het EHRM dat de burger een indicatie moet kunnen hebben van de regels die op een bepaald moment gelden. Daarvoor is in beginsel voldoende dat de burger weet waar hij de regels kan opvragen.[209] Openbare bekendmaking van de regels – publicatie in het Staatsblad of wellicht op het internet – verdient evenwel de voorkeur.[210] Aan de voorzienbaarheidseis is voldaan indien de rechtsbasis voldoende duidelijk en precies is geformuleerd, zodat de burger kan voorzien, eventueel na inwinning van juridisch advies,[211] op basis van welke toepassingsvoorwaarden en onder welke omstandigheden de overheid inbreuk kan maken op zijn privacy.[212] Dat zal het EHRM van geval tot geval beoordelen nu de voorzienbaarheid is vereist "*to a degree that is reasonable*

een dergelijk systeem valt evenwel binnen een engere marge en moet zijn voorzien van uitgebreidere waarborgen in de wet.

207 EHRM 24 april 1990, nr. 11105/84 (*Huvig/Frankrijk*), par. 26. Zie voorts Harris e.a. 2018, p. 533-534.

208 EHRM 25 maart 1983, nrs. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75 (*Silver e.a./Verenigd Koninkrijk*), par. 85 onder verwijzing naar EHRM 16 april 1979, nr. 6538/74 (*Sunday Times/Verenigd Koninkrijk*), par. 47, *NJ* 1980/146, m.nt. Alkema.

209 EHRM 28 maart 1990, nr. 10890/84 (*Groppera Radio AG e.a./Zwitserland*), par. 68.

210 Vgl. EHRM 12 mei 2000, nr. 35394/97 (*Khan/Verenigd Koninkrijk*), par. 27, *NJ* 2002/180, m.nt. Schalken. Vgl. voorts EHRM 25 maart 1983, nrs. 5947/72 & 6205/73 & 7052/75 & 7061/75 & 7107/75 & 7113/75 & 7136/75 (*Silver e.a./Verenigd Koninkrijk*), par. 87.

211 Zie bijvoorbeeld EHRM 14 maart 2013, nr. 24117/08 (*Bernh Larsen Holding AS e.a./Noorwegen*), par. 123.

212 Zie bijvoorbeeld EHRM 2 augustus 1984, nr. 8691/79 (*Malone/Verenigd Koninkrijk*), par. 66; EHRM (GK) 4 december 2008, nr. 30562/04 (*S. en Marper/Verenigd Koninkrijk*), par. 95, *NJ* 2009/410, m.nt. Alkema, *NTM/NJCM-bull.* 2009, p. 391, m.nt. Van der Staak; EHRM 12 januari 2010, nr. 4158/05 (*Gillan & Quinton/Verenigd Koninkrijk*), par. 76, *NJ* 2010/325, m.nt. Dommering; EHRM (GK) 4 december 2015, nr. 47143/06 (*Roman Zakharov/Rusland*), par. 229, *NJ* 2017/185, m.nt. Dommering.

in the circumstances".[213] Voor heimelijke opsporingsmethoden geldt dat het EHRM veel belang toekent aan het voorzienbaarheidsvereiste.[214]

Tot slot beoordeelt het EHRM of de rechtsbasis voldoende waarborgen bevat om misbruik en willekeur te voorkomen. In het kader van deze stap heeft het EHRM voor het eerst in *Huvig* zes eisen en waarborgen ontwikkeld waaraan "*secret measures of surveillance*" in nationale wetgeving moeten voldoen.[215] Deze vereisten zijn in de loop van de jaren nader ingevuld en geconcretiseerd.[216] Onder meer in de zaken *Weber en Saravia* en *Liberty* presenteert het Hof de zes *Huvig* vereisten als "*minimum* requirements".[217] Ook in het Grote Kamer arrest *Roman Zakharov/Rusland* formuleert het EHRM de zes eisen als *minimum*criteria. Het nationale recht moet voorzien in:

1) Een beschrijving van de aard van strafbare feiten die tot interceptie kan leiden;
2) Een definitie van de categorieën van personen wier communicaties onderschept kunnen worden;
3) Een beperking met betrekking tot de duur van de genomen interceptiemaatregelen;
4) De procedure voor het analyseren, gebruiken en bewaren van de verkregen data;
5) Voorzorgsmaatregelen die worden getroffen bij het delen van deze gegevens met andere partijen; en
6) De omstandigheden waaronder deze gegevens mogen of moeten worden verwijderd of vernietigd.[218]

213 EHRM 25 maart 1983, nrs. 5947/72 & 6205/73 & 7052/75 & 7061/75 & 7107/75 & 7113/75 & 7136/75 (*Silver e.a./Verenigd Koninkrijk*), par. 88.

214 Zie onder meer EHRM 25 maart 1998, nr. 23224/94 (*Kopp/Zwitserland*), par. 72; EHRM (GK) 4 mei 2000, nr. 28341/95 (*Rotaru/Roemenië*), par. 53; EHRM 29 juni 2006, nr. 54934/00 (*Weber & Saravia/Duitsland*), par. 93; EHRM 2 september 2010, nr. 35623/052010/123 (*Uzun/Duitsland*), par. 61; EHRM (GK) 4 december 2015, nr. 47143/06 (*Roman Zakharov/Rusland*), par. 229, *NJ* 2017/185, m.nt. Dommering.

215 EHRM 24 April 1990, nr. 11105/84 (*Huvig/Frankrijk*), par. 32. Zie ook Loideain 2022, p. 56.

216 Zie in dit kader ook Loideain 2022, p. 57; De Hert en Malgieri 2021, p. 255-296.

217 EHRM 29 juni 2006, nr. 54934/00 (*Weber en Saravia/Duitsland*) en EHRM 1 juli 2008, nr. 58243/00, *NJ* 2010/324, m.nt. Dommering (*Liberty e.a./Verenigd Koninkrijk*).

218 EHRM (GK) 4 december 2015, nr. 47143/06 (*Roman Zakharov/Rusland*), par. 231, *NJ* 2017/185, m.nt. Dommering.

Naast deze minimumvoorwaarden vereist het EHRM dat het nationale recht voorziet in toezicht.[219] Zo besteedt het EHRM aandacht aan de wijze waarop het toezicht op de bevoegdheden is ingericht, aan de manier waarop notificatieverplichtingen in het recht zijn opgenomen en aan de (rechts)middelen die tegen inzet van de methode open staan.[220] Doorgaans maakt het Hof onderscheid tussen toezicht vooraf, tijdens en achteraf.[221] Op alle drie de momenten moet er toezicht bestaan. Het EHRM ziet het liefst dat toetsing vooraf plaatsvindt door een rechter, maar voorafgaand toezicht door een andere autoriteit is niet uitgesloten.[222]

In bovenstaande zes minimumvoorwaarden zijn verschillende gegevensbeschermings-rechtelijke beginselen te herkennen. Zo moet allereerst worden gespecifieerd voor welk doel communicatiegegevens kunnen worden onderschept, door te omschrijven voor welke strafbare feiten en van welke personen communicatie kan worden onderschept. Ook de beginselen van data-minimalisatie en opslagbeperking zijn duidelijk te herkennen in bovenstaande criteria. Irrelevante gegevens moeten bijvoorbeeld zo snel mogelijk worden verwijderd.[223] Doelbinding in de zin van dat gegevens alleen mogen worden gebruikt voor het doel waarvoor ze zijn verkregen keert niet expliciet terug in bovenstaande criteria. Niettemin lijkt het EHRM wel belang te hechten aan doelbinding. Zo overweegt het EHRM in onder meer *Roman Zakharov/Rusland* dat gegevens die niet relevant zijn voor het doel waarvoor de gegevens zijn vergaard moeten worden vernietigd.[224] Voorts hecht het EHRM belang aan de vraag of het nationale recht voldoende waarborgen bevat ter bescherming van de rechten van derden waarop de interceptie zich aanvankelijk niet richtte. In *Amann/Zwitserland* neemt het EHRM een schending van artikel

219 Zie hierover uitgebreid Eskens, Van Daalen & Van Eijk 2016, p. 15-27; Malgieri & De Hert 2017.

220 EHRM 6 september 1978, nr. 5029/71 (*Klass e.a./Duitsland*), par. 49-50 en 59; EHRM 26 maart 1987, nr. 9248/81 (*Leander/Zweden*), par. 65-67; EHRM (GK) 4 december 2015, nr. 47143/06 (*Roman Zakharov/Rusland*), par. 233-234, *NJ* 2017/185, m.nt. Dommering.

221 EHRM (GK) 4 december 2015, nr. 47143/06 (*Roman Zakharov/Rusland*), par. 233, *NJ* 2017/185, m.nt. Dommering.

222 EHRM (GK) 4 december 2015, nr. 47143/06 (*Roman Zakharov/Rusland*), par. 249, 257-258, 275, *NJ* 2017/185, m.nt. Dommering. Vgl. voorts EHRM 12 januari 2016, nr. 37138/14 (*Szabó & Vissy/Hongarije*), par. 78; EHRM 6 september 1978, nr. 5029/71 (*Klass e.a./Duitsland*), par. 56 alsmede Malgieri & De Hert 2017, p. 509-532.

223 EHRM (GK) 4 december 2015, nr. 47143/06 (*Roman Zakharov/Rusland*), par. 255, *NJ* 2017/185, m.nt. Dommering. Zie ook EHRM 6 september 1978, nr. 5029/71 (*Klass e.a./Duitsland*), par. 52; EHRM 18 mei 2010, nr. 1, *NJ* 2011/333 (*Kennedy/Verenigd Koninkrijk*), par. 188.

224 EHRM (GK) 4 december 2015, nr. 47143/06 (*Roman Zakharov/Rusland*), par. 255, *NJ* 2017/185, m.nt. Dommering.

8 EVRM aan, onder meer omdat het nationale recht niet duidelijk maakte welke eisen golden voor het gebruik van informatie over derden.[225]

Hoewel het EHRM in zijn rechtspraak over interceptie van communicatie en daaraan gerelateerde gegevens veel waarde toekent aan de zes 'minimum' vereisten, rijzen tegelijkertijd vragen.[226] Allereerst is de vraag of deze eisen nu ten aanzien van *alle* 'surveillance'-methoden gelden, dus ook ten aanzien van methoden waarmee geen communicatie of daaraan gerelateerde gegevens worden vergaard. Ten tweede is de vraag relevant hoe de criteria zich laten toepassen op interceptie van communicatie door inlichtingendiensten, waarbij vaak ongericht gegevens worden vergaard. Kán bij dergelijke interceptie wel tegemoet worden gekomen aan de eerste twee *Huvig* criteria, te weten een beschrijving van de aard van strafbare feiten die tot interceptie kan leiden en een definitie van de categorieën van personen wier communicaties onderschept kunnen worden. Immers, bij het onderscheppen van grote hoeveelheden gegevens is het mogelijk lastig de groep precies te definiëren.

Op bovenstaande vragen geeft de jurisprudentie van het EHRM gedeeltelijk antwoord. Wat betreft de eerste vraag lijkt het EHRM in *Uzun/Duitsland* duidelijk te maken dat het de zes minimum voorwaarden niet altijd even streng invult.[227] Het ging in deze zaak om het vergaren van locatiegegevens door middel van gps-trackers. Het EHRM geeft aan dat het systematisch verzamelen van gpsgegevens een inbreuk op de privacy behelst, maar dat die inbreuk minder ingrijpend is dan bijvoorbeeld het afluisteren van telefoongesprekken.[228] Deze constatering lijkt gevolgen te hebben voor de omvang van het wettelijke kader. Het EHRM stelt in *Uzun/Duitsland* meer globaal vast dat uit de wet moet blijken wat de gronden zijn om de bevoegdheid in te zetten, wat de omvang en de duur van de bevoegdheid is en welke autoriteit bevoegd is om de bevoegdheid toe te staan, uit te voeren, te controleren, en of er een rechtsmiddel openstaat tegen de bevoegdheid.[229] Het EHRM vermeldt in dit geval niet specifiek dat in de wet moet worden opgenomen bij welke categorieën van personen de bevoegdheid kan worden ingezet, bij welke strafbare feiten, welke procedure moet worden gevolgd, of de rechter de bevoegdheid dient te beoordelen en wanneer de gegevens moeten worden

225 EHRM (GK) 16 februari 2000, nr. 27798/95 (*Amann/Zwitserland*), par. 61.

226 Zie in dit kader ook De Hert en Malgieri 2021, p. 264.

227 EHRM 2 september 2010, nr. 35623/05 (*Uzun/Duitsland*), par. 63-74.

228 EHRM 2 september 2010, nr. 35623/05 (*Uzun/Duitsland*), par. 46 en 52. Zie ook De Hert & Malgieri 2021, p. 265-266.

229 EHRM 2 september 2010, nr. 35623/05 (*Uzun/Duitsland*), par. 63. In EHRM 10 maart 2009, nr. 4378/02 (*Bykov/Rusland*), par. 78 en in EHRM 27 oktober 2015, nr. 62498/11 (*R.E./ Verenigd Koninkrijk*), par. 128, herhaalt het EHRM dit uitgangspunt.

vernietigd. Anders dan in *Huvig/Frankrijk* benoemt het EHRM in deze zaak dan wel weer de mogelijkheid van een rechtsmiddel tegen de ingezette bevoegdheid. In de zaken *Bykov/Rusland* en *R.E/Verenigd Koninkrijk* herhaalt het EHRM dit uitgangspunt.[230] In *Uzun/Duitsland* erkent het EHRM weliswaar dat bovenstaande minimumvereisten als inspiratie kunnen dienen in zaken over heimelijke opsporingsmethoden die minder vergaande privacyinmengingen impliceren, maar dat deze daarop niet één op één zijn toe te passen. Het EHRM overweegt: "*What is required by way of safeguard will depend, to some extent at least, on the nature and extent of the interference in question.*"[231]

Voor wat betreft de tweede vraag – in hoeverre kunnen de zes minimumvoorwaarden ook worden toegepast op het intercepteren van communicatie en daaraan gerelateerde gegevens door inlichtingendiensten – heeft het EHRM lang vastgehouden aan de zes minimum voorwaarden. In onder meer *Weber en Saravia/Duitsland*,[232] *Liberty/Verenigd Koninkrijk*[233] en *Kennedy/Verenigd Koninkrijk*[234] ging het om het in bulk onderscheppen van communicatie.[235] In *Liberty/Verenigd Koninkrijk* gaat het EHRM specifiek in op het verschil tussen meer op het individu gerichte vormen van het onderscheppen van communicatiegegevens en het in bulk onderscheppen van communicatiegegevens. Het Hof ziet dan echter niet in dat een onderscheid dient te worden gemaakt in regels voor de diverse vormen van interceptie; zowel voor de meer individuele vormen van interceptie als de collectieve interceptie zijn de zes minimum vereisten van toepassing.[236] Dit uitgangspunt

230 EHRM 10 maart 2009, nr. 4378/02 (*Bykov/Rusland*), par. 78 en EHRM 27 oktober 2015, nr. 62498/11 (*R.E./ Verenigd Koninkrijk*), par. 128. Hoewel het in deze zaken dan weer gaat om gevoeligere informatie, te weten een privégesprek en het afluisteren van rechtsconsultatie op een politiebureau.

231 EHRM 2 september 2010, nr. 35623/05 (*Uzun/Duitsland*), par. 63-74. Vgl. voorts EHRM 25 september 2001, nr. 44787/98, *NJ* 2003/670, m.nt. Dommering (*P.G. & J.H./Verenigd Koninkrijk*), par. 46; EHRM 27 oktober 2015, nr. 62498/11 (*R.E./Verenigd Koninkrijk*), par. 127 en 130.

232 EHRM 29 juni 2006, nr. 54934/00 (*Weber en Saravia/Duitsland*).

233 EHRM 1 juli 2008, nr. 58243/00, *NJ* 2010/324, m.nt. E.J. Dommering (*Liberty e.a./Verenigd Koninkrijk*).

234 EHRM 18 mei 2010, nr. 26839/05, *NJ* 2011/333 (*Kennedy/Verenigd Koninkrijk*).

235 In deze uitspraken spreekt het EHRM niet van 'bulk interception', maar van 'strategic monitoring' of 'mass surveillance'. Zie nader De Hert en Malgieri 2021, p. 268.

236 EHRM 1 juli 2008, nr. 58243/00 (*Liberty e.a./Verenigd Koninkrijk*), *NJ* 2010/324, m.nt. Dommering, par. 63.

verandert evenwel in de Grote Kamer zaken *Big Brother Watch e.a./Verenigd Koninkrijk* en *Centrum för Rättvisa/Zweden*.[237]

De acht waarborgen bij Big Brother Watch

Mede gelet op de kritiek op *Weber en Saravia, Kennedy* en *Liberty* gaat de Grote Kamer in *Big Brother Watch* en *Centrum för Rättvisa* nader in op de vraag of voor het bulk intercepteren van communicatiegegevens dezelfde eisen moeten gelden als voor op het individu gerichte vormen van het onderscheppen van communicatiegegevens. Het EHRM erkent dan voor het eerst dat bulkinterceptie, waarbij de vergaring (en deels ook de verwerking) ongericht is, een groot potentieel bereik heeft en dat daarbij aangepaste waarborgen nodig zijn.[238] Net zoals het EHRM in eerdere jurisprudentie de toepassing van nieuwe technologische inlichtingen- en opsporingsmethoden met betrekking tot gerichte gegevensverzameling begrijpelijk acht, geldt dat ook voor bulkinterceptie. De veranderde digitale samenleving, de technische, maatschappelijke en politieke situatie zorgen ervoor dat de ongerichte gegevensvergaring een waardevolle aanvulling is om bedreigingen van de nationale veiligheid in kaart te brengen. Lidstaten genieten een ruime beoordelingsmarge bij het vaststellen hoe ze die nationale veiligheid beschermen.[239] Ze mogen zelf de vorm van interceptie kiezen, gericht of ongericht. Indien voor een ongerichte vorm van interceptie wordt gekozen, geldt echter een aantal aangepaste eisen om misbruik te voorkomen.[240] Dit is een belangrijk punt. Het EHRM eist dus níet van lidstaten dat zij verantwoorden waarom zij niet kunnen volstaan met enkel een systeem van gerichte gegevensvergaring. De uitspraak leidt op dit punt tot kritiek vanuit het oogpunt van privacybescherming. Het EHRM beschouwt massasurveillanceregimes in Europa als de nieuwe realiteit en acht het legitiem in het kader van

237 EHRM (GK) 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*), *NJ* 2021/361, m.nt. Dommering; EHRM (GK) 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD003525208 (*Centrum för Rättvisa/Zweden*), *JBP 2021/62*, m.nt. Moyakine; *EHRC Updates*, m.nt. Hagens en Oerlemans.

238 EHRM (GK) 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*), *NJ* 2021/361, m.nt. Dommering; EHRM (GK) 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD003525208 (*Centrum för Rättvisa/Zweden*), *JBP* 2021/62, m.nt. Moyakine; *EHRC Updates*, m.nt. Hagens en Oerlemans.

239 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*), *NJ* 2021/361, m.nt. Dommering, par. 338.

240 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*), *NJ* 2021/361, m.nt. Dommering, par. 347.

het beschermen van de nationale veiligheid, zonder dat op dit punt een subsidiariteitstoets hoeft te worden aangelegd.[241]

Áls wordt gekozen voor bulkinterceptie, dan geldt een aangepast kader om misbruik te voorkomen.[242] Het EHRM verschuift het accent van de toetsing van de eerste drie van de '*Huvig* criteria' naar de laatste drie, terwijl het EHRM die laatste drie preciseert en uitbreidt.[243] Het EHRM stelt acht criteria voor waaraan het wettelijk kader moet voldoen met betrekking tot bulkinterceptie. In de wet moet duidelijk zijn weergegeven:

1) De gronden waarop bulkinterceptie is toegestaan;
2) De omstandigheden waaronder communicatie mag worden onderschept;
3) De procedure voor het verlenen van autorisatie/machtiging;
4) De procedures voor het selecteren, analyseren en gebruiken van het ond schepte materiaal;
5) De te nemen voorzorgsmaatregelen voor het verstrekken van dat materiaal aan andere partijen;
6) De beperkingen van de duur van interceptie, de opslag van het onderschepte materiaal en de omstandigheden waaronder dit materiaal moet worden verwijderd en vernietigd;
7) De procedures en modaliteiten voor het toezicht op naleving van de bovengenoemde waarborgen door een onafhankelijke instantie en haar bevoegdheden om niet-naleving aan te pakken;

241 Zie de *partly concurring* en *partly dissenting opinion* van rechter Pinto de Albuquerque. Zie ook Moyakine in zijn noot bij onderhavig arrest en voorts de blogs van Marko Milanovic, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för Rättvisa', 26 May 2021(); Nora Ni Loideain, 'Not So Grand: The Big Brother Watch ECtHR Grand Chamber judgment', Information Law and Policy Centre, 28 mei 2021 (Not So Grand: The Big Brother Watch ECtHR Grand Chamber judgment - Information Law & Policy Centre (sas.ac.uk)), Eliza Watt, 'Much Ado About Mass Surveillance – the ECtHR Grand Chamber 'Opens the Gates of an Electronic "Big Brother" in Europe' in Big Brother Watch v UK', Strasbourg Observers 28 juni 2021 (Much Ado About Mass Surveillance - the ECtHR Grand Chamber 'Opens the Gates of an Electronic "Big Brother" in Europe' in Big Brother Watch v UK - Strasbourg Observers); Mark Klamberg, 'Big Brother's little, more dangerous brother', 1 juni 2021 (Big Brother's Little, More Dangerous Brother – Verfassungsblog).

242 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*), *NJ* 2021/361, m.nt. Dommering, par. 347.

243 Zie ook Dommering in zijn annotatie bij onderhavig arrest onder punt 12 (*NJ* 2021/361).

8) De procedures voor een onafhankelijke ex post facto evaluatie van een dergelijke naleving en de bevoegdheden van een daartoe competente instantie om mogelijke gevallen van niet-naleving aan te pakken.[244]

Het is lastig de zes eerder geformuleerde '*Huvig* criteria' één op één te vergelijken met *Big Brother Watch*, omdat de eerdere criteria meer zijn toegespitst op opsporingsonderzoek en *Big Brother Watch* betrekking heeft op de inlichtingenfase. Tegelijkertijd stelt het EHRM expliciet in *Liberty* dat de legality-eis bij '*strategic monitoring*' voor gerichte interceptie (in het kader van opsporing zoals bij *Huvig*) en ongerichte interceptie (in het kader van inlichtingen zoals in *Liberty*) dezelfde is.[245] In *Big Brother Watch* is het EHRM zich ervan bewust dat bulkinterceptie kan worden ingezet ten behoeve van de opsporing. Het Hof stelt niet expliciet dat dan dezelfde criteria van toepassing zijn als in de inlichtingenfase, maar het presenteert in dit licht ook geen apart juridisch kader.[246] Als we ervan uitgaan dat de *Big Brother Watch*-criteria ook van toepassing zijn bij strafvorderlijke doeleinden, valt op dat in de zes minimumcriteria van Huvig een 'beschrijving van de aard van strafbare feiten' wordt verlangd, daar waar in *Big Brother Watch* enkel nodig is dat de 'gronden voor interceptie' zijn omschreven. Ook later in het proces, waar de vergaring overgaat in het analyseren van gegevens, dwingt het EHRM niet tot een nadere strafrechtelijke afbakening. Dat wil zeggen: het EHRM vereist níet van staten dat zij alleen bij een bepaalde dreiging van de nationale veiligheid interceptie inzetten of bij het voorkomen van bepaalde (zware) strafbare feiten. Voorts beperkt het EHRM de lidstaten niet ten aanzien van de groep personen bij wie gegevens mogen worden onderschept. Mogelijk dat een nadere begrenzing lastig is in een eerste fase van de vergaring van bulkdata, maar het EHRM verlangt dit ook niet in de volgende fase bij het analyseren van gegevens. Er hoeft geen sprake te zijn van personen ten aanzien van wie 'een redelijke verdenking' bestaat. Wel dient duidelijk te zijn wat de selectoren zijn op basis waarvan gegevens worden geanalyseerd. Daarmee kan natuurlijk de kring van personen worden afgebakend. Het EHRM geeft echter geen nadere begrenzing aan die vast te stellen selectoren.

244 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*), *NJ* 2021/361, m.nt. Dommering, par. 361.

245 EHRM 1 juli 2008, nr. 58243/00 (*Liberty e.a./Verenigd Koninkrijk*), *NJ* 2010/324, m.nt. Dommering, par. 63.

246 EHRM (GK) 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*), *NJ* 2021/361, m.nt. Dommering, par. 344. Daarin geeft het EHRM aan dat bulkinterceptie ook kan worden ingezet voor de opsporing van misdrijven.

Ten aanzien van het onderzoeken en het doorzoeken van data merkt het EHRM voorts op dat niet alle selectie- en zoekcriteria uitgebreid vooraf kunnen worden verantwoord. Zowel de regering van Nederland als van het Verenigd Koninkrijk had aangegeven dat toestemming/autorisatie ten aanzien van het gebruiken van de diverse zoekcriteria onnodig beperkend zou werken bij het werken met bulkdata.[247] Het EHRM toont zich daar gevoelig voor; het is volgens het rechterlijk college niet werkbaar en realistisch alle selectiecriteria uiteen te zetten, maar meer in het algemeen moeten typen of categorieën criteria kunnen worden geïdentificeerd. Er dient controle mogelijk te zijn ten aanzien van de subsidiariteit en proportionaliteit van gemaakte keuzes. In hun *joint partly concurring opinion* uiten Lemmens, Vehabović en Bošnjak hier kritiek op, de rechters zien niet in dat het niet mogelijk is de selectiecriteria nauwkeurig uiteen te zetten.[248] Hoe dan ook geeft het EHRM de lidstaten hiermee ruimte. Het zet 'enkel' vereisten voor een wat meer globale beoordeling uiteen. Er dient te worden voorzien in onafhankelijk toezicht bij de procedure voor het verlenen van autorisatie/machtiging; bij de procedure voor het selecteren, analyseren en gebruiken van het onderschepte materiaal en bij de procedure omtrent het vernietigen van het materiaal; dat is dus voorafgaand aan het interceptieproces, tijdens het proces én aan het einde van het proces. Daarnaast moet worden voorzien in een 'onafhankelijke ex post facto evaluatie'. De burger die vermoedt dat zijn of haar communicatie ten onrechte is afgetapt moet beschikken over een effectief rechtsmiddel.[249] Het EHRM gaat niet zo ver dat het een notificatieplicht stelt voor lidstaten.[250] Maar áls burgers menen slachtoffer te zijn van bulkinterceptie, dan moeten zij bij een onafhankelijke instantie terecht kunnen. Daarbij moet deze instantie zo veel mogelijk een contradictoir proces garanderen waarbij de procedure leidt tot gemotiveerde en juridisch bindende besluiten.[251]

247 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*), m.nt. Dommering, par. 353.

248 Joint partly concurring opinion van rechters Lemmens, Vehabović en Bošnjak onder par. III.

249 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD005817013 (*Big Brother Watch e.a./Verenigd Koninkrijk*), m.nt. Dommering, par. 413.

250 Zie ook EHRM (GK) 4 december 2015, nr. 47143/06 (*Roman Zakharov/Rusland*), par. 286-287, *NJ* 2017/185, m.nt. Dommering. Kritisch hierover De Hert en Malgieri 2021, p. 279-284.

251 EHRM 25 mei 2021, ECLI:CE:ECHR:2021:0525JUD003525208 (*Centrum för Rättvisa v. Sweden*), *JBP* 2021/62, m.nt. Moyakine, *EHRC Updates*, m.nt. Hagens en Oerlemans, par. 362.

Concluderend zet het EHRM in *Big Brother Watch* in eerste instantie een beoordelingskader voor bulkinterceptie door inlichtingendiensten uiteen.[252] Zoals hiervoor reeds vermeld, lijkt het kader echter eveneens van toepassing te zijn op bulkinterceptie in de strafvorderlijke context. In *Huvig* neigde het Straatburgse Hof meer naar een 'rule-based' benadering, in die zin dat het zes *minimum* eisen stelde aan surveillance-opsporingsbevoegdheden. In de wet moest onder andere zijn opgenomen ten aanzien van welke strafbare feiten en bij welke personen interceptie mogelijk was. Door die benadering werd de fase van gegevensvergaring meer aan banden gelegd. In *Big Brother Watch* kiest het EHRM voor een nog sterkere 'principle based' benadering.[253] Het EHRM ziet bulkinterceptie als één proces waarbij voldoende 'end-to-end' waarborgen aanwezig moeten zijn om adequate en effectieve garanties te bieden tegen willekeur en het risico van misbruik. De introductie van dit nieuwe kader heeft als gevolg dat het EHRM meer ruimte biedt voor grootschalige gegevensvergaring in de initiële fase.[254] Tegelijkertijd moet met betrekking tot de verwerkingsfase worden voorzien in voldoende bescherming en controlemogelijkheden voorafgaand aan het proces, tijdens én achteraf. Daarbij geldt dat, hoe verder de fase van verwerking gaat, des te groter de inbreuk op de privacy is, waardoor steeds meer waarborgen in de procedure moeten worden ingebouwd.[255] Omdat het EHRM niet meer spreekt van 'minimum' criteria, maar 'voldoende' eind-tot-eind-waarborgen, kan met minder stelligheid worden betoogd dat het niet voldoen aan één van de voorwaarden direct tot een schending van artikel 8 EVRM zou leiden. Juist vanwege de meer principiële benadering, lijkt het mogelijk dat bijvoorbeeld het niet afdoende voorzien in toezicht voorafgaand aan de interceptie kan worden gecompenseerd met sterk toezicht tijdens of achteraf. Het gaat er uiteindelijk om dat het gehele interceptieproces voldoende garanties biedt tegen misbruik en willekeur.

252 In de zaak *Ekimdzhiev e.a.* herhaalt het EHRM het kader zoals uiteengezet in *Big Brother Watch* en past het toe op enerzijds het Bulgaarse wettelijk regime voor geheim toezicht en anderzijds het wettelijk regime rondom dataretentie en toegang tot communicatiedata. Het EHRM had in 2007 reeds geoordeeld dat het Bulgaarse wettelijk kader inzake 'secret surveillance' in strijd was met artikel 8 EVRM. Inmiddels is de wetgeving gewijzigd, maar de nieuwe regelgeving is volgens het EHRM nog steeds niet toereikend. Zie EHRM 11 januari 2022, nr. 70078/12 (*Ekimdzhiev e.a./Bulgarije*), par. 291, 394, 356 en 419.

253 Zie over de verschuiving van een meer 'rule-based' benadering naar een 'principle based' benadering ook Van der Sloot 2012, par. V.

254 Zie over meer ruimte voor gegevensvergaring ook Galič 2022, par. 3.2.

255 Zie in dit kader ook Galič 2022, par. 4.

3.3.3 Tussenconclusie

In deze paragraaf is in kaart gebracht welke richtsnoeren uit de rechtspraak van het EHRM inzake *surveillance* kunnen worden afgeleid voor wat betreft de normering van onderzoek aan gegevens voor strafvorderlijke doeleinden. Daartoe is enerzijds ingegaan op de jurisprudentie inzake politionele en justitiële gegevensbanken en anderzijds relevante jurisprudentie inzake het onderscheppen en verwerken van communicatiegegevens besproken.

Allereerst wordt op grond van de Straatsburgse rechtspraak duidelijk dat de opslag van gegevens voor strafvorderlijke doeleinden snel een inbreuk op het recht op privacy behelst. Door de opslag wordt immers de mogelijkheid gecreëerd om – in een later stadium – een beeld van iemands leven te verkrijgen. Uiteraard speelt hierbij wel mee in hoeverre de gegevens daadwerkelijk iets over het privéleven kunnen zeggen. Inbreuken kunnen evenwel zijn gerechtvaardigd mits (in elk geval) is voorzien in adequate wetgeving. Het EHRM spreekt daarbij niet expliciet van gegevensbeschermingsbeginselen, maar om misbruik en willekeur te voorkomen dienen wel degelijk gegevensbeschermingsrechtelijke beginselen in acht te worden genomen, zoals doelspecificatie, opslagbeperking en data-minimalisatie.

De jurisprudentie inzake het – gericht – onderscheppen en verwerken van communicatie-gegevens laat voorts zien dat het EHRM óók belang hecht aan voldoende waarborgen in de verwerkingsfase. Onder meer in de zaak *Zakharov/Rusland* wordt duidelijk dat niet alleen de vergaring zelf met voldoende waarborgen moet zijn omgeven, maar tevens het gebruik van gegevens. Het EHRM spreekt in dit kader wederom niet expliciet van gegevensbeschermingsbeginselen. De voorwaarden die het EHRM stelt om de inbreuk op het recht op privacy te kunnen rechtvaardigen, kunnen evenwel opnieuw gekoppeld worden aan gegevensbeschermingsrechtelijke uitgangspunten zoals opslagbeperking en data-minimalisatie.

In *Big Brother Watch* en *Centrum för Rättvisa* introduceert het EHRM het begrip 'bulkinterceptie'. Het EHRM voorziet daarbij niet in een duidelijke definitie, maar het is helder dat deze vorm van interceptie *ongericht* is. Het EHRM concludeert in deze uitspraken dat de waarborgen voor de vergaring en verwerking voor meer klassieke, op het individu gerichte opsporingsmethoden niet zonder meer van toepassing zijn op de vergaring en verwerking van bulkgegevens. Het stelt dat voor bulkinterceptie door inlichtingen- en veiligheidsdiensten aangepaste waarborgen nodig zijn. Het EHRM hanteert daarbij geen afzonderlijke kaders voor de vergaring en de verwerking van bulkgegevens. Het beschouwt de vergaring en verwerking van bulkgegevens veeleer als één proces. Dit komt niet overeen met de

Nederlandse situatie waarin onderscheid wordt gemaakt tussen de vergaring en de verwerking van bulkgegevens. Het EHRM acht bulkinterceptie legitiem in het kader van het beschermen van de nationale veiligheid, zonder dat op dit punt een subsidiariteitstoets hoeft te worden aangelegd. Hoewel het beoordelingskader van het EHRM in eerste instantie ziet op de inlichtingencontext, sluit het EHRM niet uit dat bulkinterceptie eveneens wordt ingezet ten behoeve van de opsporing en lijkt het kader daarmee ook van toepassing in strafvorderlijk verband.

Het EHRM presenteert vervolgens nog sterker dan voorheen een 'principle based'-kader. Misbruik van de bevoegdheid dient te worden voorkomen door voldoende 'end-to-end' waarborgen in de wet te incorporeren. Daarbij geldt dat, hoe verder de fase van verwerking gaat, des te groter de inbreuk op de privacy is, waardoor steeds meer waarborgen in de procedure moeten worden ingebouwd. In de fase van het vergaren van gegevens laat het EHRM lidstaten ruimte, in die zin dat bulkinterceptie niet slechts mogelijk is bij een bepaalde mate van dreiging van de nationale veiligheid of bij het voorkomen van bepaalde strafbare feiten. Ook stelt het EHRM geen minimumeis wat betreft de groep personen ten aanzien van wie communicatie wordt onderschept (zoals personen ten aanzien van wie een redelijke verdenking bestaat). Waar het EHRM bij gerichte interceptie verlangt dat staten voorzien in een kader waarbij de interceptie enkel plaatsvindt ten aanzien van vooraf omschreven strafbare feiten en/of groepen personen, eist het EHRM dat dus niet bij ongerichte interceptie. Ook dwingt het EHRM lidstaten niet tot een notificatieplicht. Wel moet de wetgeving – zowel in het kader van de 'legality'-eis als de 'necessity'-eis –voldoen aan meer algemene uitgangspunten; de proportionaliteit en subsidiariteit van de suveillancemaatregel moet worden geborgd door de procedure van interceptie in de wet op te nemen. Voorts moet toezicht worden gehouden op het proces *ex tunc*, *ex nunc* en *ex post* en dient een rechtsmiddel open te staan voor de burger. In de wet moet worden opgenomen: op basis van welke gronden bulkinterceptie is toegestaan, onder welke omstandigheden communicatie mag worden onderschept, wie bevoegd is tot het verlenen van autorisatie, hoe de procedures voor het selecteren, analyseren en gebruiken van het onderschepte materiaal zijn geregeld, welke voorzorgsmaatregelen in acht worden genomen bij het verstrekken van materiaal aan andere partijen, wat de beperkingen van de duur van interceptie zijn, hoe de opslag van het onderschepte materiaal en de omstandigheden waaronder dit materiaal moet worden verwijderd en vernietigd is geregeld, welke procedures gelden voor het toezicht door een onafhankelijke instantie voorafgaand, tijdens en na het interceptieproces. De voorwaarden die het EHRM stelt kunnen gekoppeld worden aan uitgangspunten van het gegevensbeschermingsrecht (doelbinding, doelspecificatie en data-minimalisatie).

Het EHRM laat zich in *Big Brother Watch* niet uit over verschillende soorten bulkinterceptiemethoden. Het is onduidelijk of het EHRM nog een verschil maakt tussen meer of minder privacygevoelige informatie. Het is mogelijk dat het EHRM de legaliteit en noodzakelijkheid bij het interceptieregime dat gevoeliger gegevens onderschept strenger beoordeelt, zoals het EHRM in *Big Brother Watch* ook binnen de fase van analyse stelt dat de privacyinbreuk toeneemt naarmate het onderzoek aan de gegevens vordert en dat dan de behoefte aan waarborgen toeneemt.

3.4 Artikel 7 en 8 Handvest Grondrechten EU

Anders dan het EHRM heeft het Hof van Justitie EU (HvJ EU) zich vooralsnog nauwelijks uitgelaten over het vergaren en verwerken van gegevens met als doel de opsporing van strafbare feiten. Op een specifiek terrein heeft het HvJ EU echter wel richtinggevende jurisprudentie gewezen: het bewaren en vorderen van metagegevens in het belang van de opsporing en/of de nationale veiligheid in het kader van prejudiciële procedures inzake Richtlijn 2002/58.[256] In het bijzonder heeft het HvJ EU zich uitgelaten over de vraag onder welke omstandigheden en met inachtneming van welke waarborgen het bewaren van metagegevens en het verlenen van toegang hiertoe verenigbaar is met de in het Handvest van de Grondrechten van de Europese Unie (HGEU) neergelegde rechten inzake privacy (art. 7), gegevensbescherming (art. 8) en de vrijheid van meningsuiting (art. 11). De jurisprudentie van het HvJ EU concentreert zich hier met name op de reikwijdte van de uitzondering die de Richtlijn 2002/58 aan staten verschaft om af te wijken van enkele in de richtlijn vastgestelde verplichtingen en rechten. Hoewel deze jurisprudentie betrekking heeft op een zeer specifiek onderwerp en louter op *metagegevens,* kan aan deze jurisprudentie niet voorbij worden gegaan.[257] Het HvJ EU toetst – anders dan het EHRM – niet alleen aan het recht op privacy, maar ook aan het recht op persoonsgegevensbescherming. In het navolgende wordt in kaart gebracht welke voorwaarden uit de jurisprudentie van het HvJ EU kunnen worden afgeleid voor wat betreft onderzoek van gegevens voor strafvorderlijke doeleinden. Daartoe komt aan bod op welke wijze het HvJ EU het recht op privacy en persoonsgegevensbescherming afbakent alsmede welke eisen en waarborgen het HvJ EU

256 Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) van 31 juli 2002, p. 37-47.

257 De jurisprudentie van het EHRM ziet ook op andersoortige gegevens, zoals de inhoud van communicatie alsmede publiek toegankelijke gegevens.

verlangt als inbreuk wordt gemaakt op deze rechten. Vervolgens wordt kort stilgestaan bij enkele onduidelijkheden en volgt een tussenconclusie.

3.4.1 Inbreuk

Voor een goed begrip van de Unierechtelijke jurisprudentie inzake dataretentie zijn twee onderscheidingen van belang. In de eerste plaats maakt het HvJ EU onderscheid tussen het bewaren en vorderen van gegevens. Bij het bewaren van gegevens gaat het om de vraag in hoeverre telecommunicatieaanbieders gegevens mogen opslaan in het belang van de opsporing of de nationale veiligheid. Het vorderen van gegevens heeft betrekking op de vraag in hoeverre nationale (opsporings)autoriteiten toegang mogen verkrijgen tot de gegevens.[258] In de tweede plaats maakt het HvJ EU onderscheid tussen enerzijds verkeers- en locatiegegevens en anderzijds identificerende gegevens en IP-adressen. Zoals hieronder zal blijken, leidt de verwerking van verkeers- en locatiegegevens doorgaans tot een ernstigere inbreuk op met name het recht op privacy dan de verwerking van identificerende gegevens en IP-adressen.

3.4.1.1. Verkeers- en locatiegegevens

Volgens het HvJ EU maakt het *bewaren* van verkeers- en locatiegegevens door telecommunicatieaanbieders inbreuk op de artikelen 7, 8 en 11 van het HGEU.[259] Niet alleen het recht op privacy (artikel 7 HGEU) en persoonsgegevensbescherming (artikel 8 HGEU) is dus in het geding, ook het recht op vrijheid van meningsuiting (artikel 11 HGEU). De reden hiervoor is voornamelijk dat het bewaren van verkeers- en locatiegegevens een *chilling effect* kan hebben op de gebruikers doordat deze zich steeds in de gaten gehouden kunnen voelen.[260] De inbreuk die op artikel 11 HGEU wordt gemaakt, blijft in het vervolg buiten beschouwing.

Over de wijze waarop en de mate waarin het bewaren van verkeers- en locatiegegevens inbreuk maakt op het recht op privacy en het recht op gegevensbescherming heeft het HvJ EU zich nader uitgelaten. Daarbij moet worden

258 In Nederland spreken we van het vorderen van gegevens. Dat is geregeld in 126nc-126ni, 126uc-126ui, 126zk-126zp Sv.

259 HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:2014:238 (*Digital Rights Ireland*), par. 25 en 70; HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB*), *EHRC* 2017/79, par. 91-92; HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), par. 113 en 118.

260 HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB*), *EHRC* 2017/79, par. 100-101; HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), par. 113, 114 en 118.

vooropgesteld dat het HvJ EU in zijn jurisprudentie ter zake dataretentie duidelijk maakt dat het recht op privacy en het recht op persoonsgegevensbescherming weliswaar overlappen, maar tegelijkertijd van elkaar verschillende rechten zijn.[261] Het recht op persoonsgegevensbescherming is in het geding zodra persoonsgegevens worden verwerkt. Daarvan is kort gezegd sprake als gegevens over een geïdentificeerd of te identificeren individu worden verwerkt.[262] Voor toepassing van het recht op gegevensbescherming is dus niet van belang om hoeveel gegevens het gaat en/of de gegevens gevoelig van aard zijn.[263] Het HvJ EU differentieert dan ook niet of nauwelijks in de mate en de wijze waarop inbreuk wordt gemaakt op het recht op persoonsgegevensbescherming.

Voor het recht op privacy ligt een en ander wat anders. Of het recht op privacy van toepassing is, wordt eerst en vooral bepaald door de vraag in hoeverre uit de gegevens conclusies kúnnen worden afgeleid over het privéleven van een of meerdere personen. Inzake verkeers- en locatiegegevens heeft het HvJ EU geoordeeld dat deze gegevens informatie prijsgeven "*over een groot aantal aspecten van het privéleven van de betrokken personen, waaronder ook gevoelige informatie, zoals seksuele geaardheid, politieke opvattingen, religieuze, filosofische, maatschappelijke of andersoortige overtuigingen en gezondheid*".[264] Verkeers- en locatiegegevens maken het mogelijk om onder meer de bron en de bestemming van communicatie, de datum, het tijdstip, de duur, de frequentie, en de aard van communicatie en het adres en telefoonnummer van gebruikers te achterhalen.[265] Uit verkeers- en locatiegegevens kunnen aldus het HvJ EU 'precieze, ja zelfs zeer nauwkeurige conclusies' worden afgeleid over iemand persoonlijk leven. Tussen de inhoud van communicatie en verkeers-

261 Zie in het bijzonder HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland Ireland*), par. 29, 33-37. Overigens maakt het HvJ EU niet altijd goed onderscheid tussen deze rechten. Zie daarover nader Brkan 2017, p. 10-31.

262 Zie in het bijzonder HvJ EU, C-293/12 en C-594/12, ECLI:EU:2014:238 (*Digital Rights Ireland*).

263 Over de waarde van het recht op persoonsgegevensbescherming bestaat dan ook veel discussie. Zie onder meer Gonzalez Fuster 2014; Van der Sloot 2017.

264 HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland Ireland*), par. 27; HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB.*), *EHRC* 2017/79, par. 99; HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net.*), par. 117; HvJ EU 5 april 2022, C-140/20, ECLI:EU:C:2022:258 (*G.D./Commissioner An Garda Síochána*), par. 45.

265 HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland*), par. 27; HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB.*), *EHRC* 2017/79, par. 98-99; HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net.*), par. 117.

en locatiegegevens kan volgens het HvJ EU dan ook geen principieel onderscheid meer worden gemaakt.[266]

Dat het bewaren van verkeers- en locatiegegevens (nog) niet ertoe leidt dat daadwerkelijk inzicht wordt verkregen in iemands privéleven, doet aan het voorgaande niet af. De bewaring vormt als zodanig een inbreuk op het recht op privacy, ongeacht het eventuele latere gebruik van deze gegevens, of het eventuele nadeel dat betrokkenen ondervinden.[267] Bij de beoordeling van de ernst van de inmenging in het privéleven die de bewaring van en toegang tot gegevens door opsporingsautoriteiten met zich meebrengt, stelt het HvJ EU aldus voorop wat uit de gegevens kán worden afgeleid.[268] Dit komt overeen met de benadering van het EHRM, zoals hiervoor is uiteengezet.

Over de vraag of de toegang van overheidsinstanties tot de bewaarde verkeers- en locatiegegevens inbreuk maakt op grondrechten heeft het HvJ EU zich eveneens expliciet uitgelaten. Het HvJ EU beschouwt de toegang tot de bewaarde verkeers- en locatiegegevens als een op zichzelf staande inbreuk op grondrechten die losstaat van de bewaring van de gegevens.[269] Het toegang verschaffen tot verkeers- en locatiegegevens beschouwt het HvJ EU – evenals de bewaring – zonder meer als een inbreuk op het door artikel 8 HGEU gewaarborgde recht op bescherming van persoonsgegevens.[270] Daarnaast maakt de toegangsverschaffing volgens het HvJ EU inbreuk op het recht op privacy, waarbij het HvJ EU bovendien overweegt dat deze inbreuk hoe dan ook ernstig van aard is, ongeacht de aard en de hoeveelheid van de gegevens alsmede de duur waarvoor toegang wordt gevraagd. Volgens het HvJ EU kan zelfs een beperkte hoeveelheid verkeers- en locatiegegevens over een korte periode nauwkeurige informatie over het privéleven verschaffen. In het verlengde hiervan heeft het HvJ EU geoordeeld dat het in *real time* toegang verkrijgen tot verkeers- en locatiegegevens alsmede het geautomatiseerd

266 HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland*), par. 26-27; HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB*), *EHRC* 2017/79, par. 98-99.

267 HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), par. 116.

268 In dit opzicht wijkt het HvJ EU niet af van het EHRM, dat vaak ook vooropstelt wat uit de gegevens kan worden afgeleid. Zie daarover nader hoofdstuk 3, § 3.1.1.

269 HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB*), *EHRC* 2017/79, par. 113.

270 HvJ EU 2 oktober 2018, C-207/16, ECLI:EU:C:2018:788 (*Ministerio Fiscal*), par. 51.

analyseren van verkeers- en locatiegegevens – aan de hand van filtertechnieken – zonder meer ernstig inbreuk maakt op het recht op privacy.[271]

3.4.1.2 IP-adressen en identificerende gegevens

Naast verkeers- en locatiegegevens heeft het HvJ EU zich ook uitgelaten over identificerende gegevens en IP-adressen. Deze categorie gegevens kan doorgaans minder over het privéleven vrijgeven dan verkeers- en locatiegegevens.[272] De bewaring[273] van en de toegangsverschaffing[274] tot deze gegevens betreft derhalve geen 'ernstige' inbreuk op de rechten in artikelen 7 en 8 HGEU. Desalniettemin sluit het HvJ EU niet uit dat de verwerking van IP-adressen tot een ernstige inbreuk op de artikelen 7 en 8 HGEU kán leiden. Dit is het geval als de adressen in een later stadium "*worden gebruikt om de volledige zoekgeschiedenis van een internetgebruiker te traceren en dus om een volledig beeld te krijgen van diens online activiteit*", waarmee vervolgens een gedetailleerd profiel van de betrokkene kan worden opgesteld.[275] Ook hier weegt voor het vaststellen van de inbreuk op het recht op privacy dus mee op welke wijze de gegevens kunnen worden gebruikt.

3.4.2 Gerechtvaardigde inbreuk

3.4.2.1 Verkeers- en locatiegegevens

Ter zake van de vraag of het bewaren van verkeers- en locatiegegevens ter bestrijding van (ernstige) criminaliteit is toegestaan, is het HvJ EU duidelijk. Lidstaten mogen alleen voorzien in de verplichting tot *gerichte* bewaring van verkeers- en locatiegegevens ten behoeve van *zware criminaliteit*. Een algemene en ongedifferentieerde bewaarplicht van verkeers- en locatiegegevens is dus niet toegestaan ter

271 HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net.*), par. 174.
272 HvJ EU 2 oktober 2018, C-207/16, ECLI:EU:C:2018:788 (*Ministerio Fiscal*), par. 59-60; HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net.*), par. 152.
273 HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net.*), par. 152 en 153.
274 HvJ EU 2 oktober 2018, C-207/16, ECLI:EU:C:2018:788 (*Ministerio Fiscal*), par. 60 en 61.
275 HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), par. 153.

bestrijding van ernstige criminaliteit.[276] Onder bepaalde omstandigheden kan een ongedifferentieerde en algemene bewaarplicht in het belang van de nationale veiligheid wel gerechtvaardigd zijn.[277] Voorts heeft het HvJ EU enkele piketpaaltjes geslagen aan de hand waarvan een gerichte bewaarplicht kan worden afgebakend. Het HvJ EU benoemt twee factoren:

1. De kring van bepaalde personen die op een of andere wijze betrokken kunnen zijn bij zware criminaliteit of personen waarvan de bewaring van gegevens om andere redenen zou kunnen helpen bij het bestrijden van zware criminaliteit; en/of
2. Een bepaalde tijdperiode en/of geografische zone.[278]

Ondanks recente jurisprudentie over de invulling van deze factoren,[279] blijft veel onduidelijkheid bestaan over de wijze waarop nationale lidstaten de geformuleerde factoren moeten omzetten in een gerichte bewaarplicht.[280]

Met betrekking tot het verlenen van toegang van overheidsinstanties in het kader van strafvordering tot de bewaarde verkeers- en locatiegegevens (niet slechts identificerende gegevens) formuleert het HvJ EU vijf eisen:

276 Een algemene en ongedifferentieerde bewaring van verkeers- en locatiegegevens ten behoeve van de bestrijding van zware criminaliteit, gaat volgens het HvJ EU verder dan strikt noodzakelijk en is niet gerechtvaardigd in een democratische samenleving. Zie HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), par. 141.

277 HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB*), *EHRC* 2017/79, par. 134. Dergelijke bewaring kan onder omstandigheden wel gerechtvaardigd zijn in het belang van de nationale veiligheid. HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), par. 134-139.

278 HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:C:2014:238 (*Digital Rights Ireland*), par. 59; HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB*), *EHRC* 2017/79, par. 106; HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net.*), par. 144. In HvJ EU 5 april 2022, C-140/20, ECLI:EU:C:2022:258 (*G.D./Commissioner An Garda Síochána*), par. 75 heeft het HvJ EU verduidelijkt dat een voorwaarde dat een concrete verdachte of plaatsen waar een ernstig strafbaar feit kan worden gepleegd op voorhand bekend zijn, niet wordt gesteld.

279 Zie o.a. HvJ EU 5 april 2022, C-140/20, ECLI:EU:C:2022:258 (*G.D./ Commissioner An Garda Síochána*).

280 Zie nader hierover: M. Koning, annotatie bij HvJ EU 21 december 2016, C-203/15 en C698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB*), *EHRC* 2017/79, onder 6; A-G Campos Sanches-Bordona 15 januari 2020, C-520/18, ECLI:EU:C:2020:7 (*Ordre des barreaux francophones et germanophone e.a.*), par. 88; Te Molder 2021.

1. De toegang tot gegevens is beperkt tot de doelstelling van de bestrijding van zware of ernstige criminaliteit;[281]
2. De toegang mag alleen worden verleend indien het gaat om personen die ervan worden verdacht een ernstig strafbaar feit te plannen, te plegen of te hebben gepleegd of op een andere wijze betrokken zijn bij een dergelijk misdrijf;[282]
3. De toegang dient voorafgaand te worden getoetst door een rechter of een bestuurlijke onafhankelijke entiteit;[283]
4. Er geldt een notificatieplicht;[284] en
5. Lidstaten dienen te voorzien in regels over de beveiliging en bescherming van gegevens.

Waar het HvJ EU de toegang tot gegevens beperkt tot 'ernstige criminaliteit', kent het EHRM niet een dergelijke beperking. Voorts begrenst het HvJ EU de toegang tot gegevens tot een beperkte kring van personen (namelijk verdachten), terwijl het EHRM ook dat niet doet.

In tegenstelling tot het EHRM formuleert het HvJ EU bovendien een notificatieplicht bij het verkrijgen van toegang tot bewaarde gegevens door communicatiediensten. Deze verschillen in benadering kunnen worden verklaard door de specificiteit van het kader waarin het HvJ EU de genoemde rechtspraak heeft gewezen. Het gaat om het bewaren en het verkrijgen van toegang tot gegevens die in het kader van commerciële activiteiten van een aanbieder van elektronische-communicatiediensten zijn verwerkt en bewaard, en *vervolgens* door de bevoegde overheidsdiensten zijn opgevraagd en gebruikt. De bescherming van de gegevens wordt hier beheerst door Richtlijn 2002/58/EG (de Richtlijn betreffende privacy en elektronische communicatie). Deze situatie dient onderscheiden te worden van

281 Wat precies als ernstige of zware criminaliteit kan worden gekwalificeerd, is niet duidelijk. Zie daarover onder meer Sholeh 2022 alsmede HR 5 april 2022, ECLI:NL:HR:2022:475.

282 De Hoge Raad werpt in HR 5 april 2022, ECLI:NL:HR:2022:475, r.o. 6.10.2-6.10.4 de vraag op of ook toegang mag worden verkregen tot gegevens die (nog) niet te herleiden zijn tot een persoon. De Hoge Raad oordeelt van wel.

283 In HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152 (*H.K., in tegenwoordigheid van Prokuratuur*) heeft het HvJ EU geoordeeld dat een openbaar aanklager doorgaans niet voldoende onafhankelijk is. Zie over de consequenties van dit onderdeel van Prokuratuur HR 5 april 2022, ECLI:NL:HR:2022:475.

284 Daarmee worden betrokken personen in staat gesteld om gebruik te maken van het recht op beroep, zoals expliciet door artikel 15 lid 2 Richtlijn 2002/58 voorzien HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 (*Tele2 Sverige AB*), *EHRC* 2017/79, par. 121.

gegevens die *rechtstreeks* door activiteiten van de overheid op strafrechtelijk gebied worden vergaard en verwerkt. In dit geval wordt de bescherming van de gegevens van personen niet beheerst door Richtlijn 2002/58/EG, maar door nationaal recht en de vereisten van het EVRM.[285] In dit geval geldt dus niet de limitatie van 'ernstige criminaliteit', 'kring van verdachte personen' en geldt geen notificatieplicht.

3.4.2.2 IP-adressen en identificerende gegevens

Zoals hierboven uiteengezet, vormen identificerende gegevens en IP-adressen een bijzondere categorie verkeersgegevens, nu hieruit doorgaans minder vergaande conclusies over het privéleven zijn af te leiden dan de zojuist besproken verkeers- en locatiegegevens. Wettelijke maatregelen die strekken tot verwerking van identificerende gegevens (bewaring van en toegang tot), zonder dat deze gegevens in verband kunnen worden gebracht met informatie over de tot stand gebrachte communicatie, kunnen dan ook worden gerechtvaardigd door de in artikel 15 lid 1 Richtlijn 2002/58 genoemde doelstelling van het voorkomen van strafbare feiten in het algemeen (en dus niet alleen de zware criminaliteit). Deze doestelling maakt het dus mogelijk voor lidstaten om te voorzien in een verplichting tot algemene, ongedifferentieerde en ongelimiteerde bewaring van identificerende gegevens van gebruikers van telecommunicatiediensten, zoals naam, voornaam en adres.[286]

Voor de bewaring van IP-adressen ligt een en ander wat genuanceerder. Hoewel IP-gegevens een ernstige inmenging in de door artikelen 7 en 8 HGEU gewaarborgde rechten kunnen vormen, toont het HvJ EU begrip voor de argumenten van staten dat IP-adressen in geval van cybercriminaliteit soms het enige onderzoeksmiddel kunnen vormen voor de identificatie van personen die betrokken zijn bij zeer ernstige strafbare feiten online, zoals kinderporno. Om deze reden acht het HvJ EU een algemene en ongedifferentieerde bewaring van de IP-adressen die zijn toegewezen aan de bron van een verbinding (en dus niet aan die van de ontvanger) gerechtvaardigd ter bestrijding van *zware criminaliteit*, ondanks het gegeven dat de bewaarplicht zich uitstrekt tot personen die niet eens een indirecte band met het doel van criminaliteitsbestrijding hebben.[287] De bewaartermijn mag ook hier niet langer dan strikt noodzakelijk zijn. Tot slot moet de nationale maatregel ook in

285 Zie ook HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*), par. 103.

286 HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net.*), par. 157-158.

287 HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net.*), par. 155-156.

strikte voorwaarden en waarborgen bieden voor het *gebruik van die gegevens*, in het bijzonder voor wat betreft het in kaart brengen van de online-communicatie en de online-activiteiten van de personen.[288]

3.4.3 Openstaande vragen en kritiek

De jurisprudentie van het HvJ EU is onderwerp van discussie, zowel in de rechtspraktijk als in de wetenschappelijke literatuur.[289] In het kader van het onderhavige onderzoek is het niet noodzakelijk deze discussie hier uitgebreid weer te geven. Wel willen wij nader de aandacht richten op de wijze waarop het HvJ EU het recht op privacy afbakent, nu dit recht een van de belangrijkste normerende kaders vormt voor de ontwikkeling van wetgeving op het gebied van onderzoek aan gegevens voor strafvorderlijke doeleinden.

Uit het voorgaande volgt dat het HvJ EU kiest voor een benadering waarbij de inbreuk op het recht op privacy wordt bepaald door de vraag in hoeverre het verwerken van (een combinatie van) gegevens iets kan prijsgeven over het privéleven van een of meer individuen. Belangrijk hierbij is dus dat het HvJ EU niet alleen kijkt naar wat uit een gegeven als zodanig kan worden afgeleid, maar ook naar wat uit de gegevens in combinatie kan worden afgeleid.[290] Zo zegt een verkeersgegeven of een IP-adres als zodanig weinig over iemands privéleven, maar als deze gegevens gecombineerd worden verwerkt kan hieruit worden afgeleid waar iemand zich heeft bevonden of welke handelingen iemand heeft verricht op het internet. Deze benadering past goed bij de gedigitaliseerde samenleving, waarin het steeds gemakkelijker wordt om gegevens gekoppeld te verwerken.[291] Het probleem is echter dat het HvJ EU bij de vraag onder welke omstandigheden en met inachtneming van welke waarborgen de inbreuk kan worden gerechtvaardigd uit het oog lijkt te verliezen dat niet elke verwerking van bepaalde type gegevens tot een ernstige inbreuk op het recht op privacy *hoeft* te leiden. Zo behoeft het vorderen van locatiegegevens – ook als dat gebeurt aan de hand van

288 HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*.), par. 156.

289 Zie onder meer HR 5 april 2022, ECLI:NL:HR:2022:475 alsmede Oerlemans e.a. 2021; Te Molder 2021; Sholeh 2022; De Keersmaecker & Van de Heyning 2022; Eskens 2022.

290 In deze benadering is dus duidelijk de in de literatuur over privacy bekendstaande mozaïektheorie te herkennen. Zie daarover nader Koops 2021, p. 541 en 542 en in relatie tot locatiebepaling als opsporingsmethode.

291 Zie in dit verband onder meer de conclusie van A-G Piruzella, par. 81. Vgl. voorts A-G Keulen 21 december 2021, ECLI:NL:PHR:2021:1184, pnt. 108.

filteringssoftware[292] – van een concreet individu over een relatief beperkte periode niet tot een ernstige inbreuk op het recht op privacy te leiden, omdat hiermee hooguit inzicht kan worden verkregen in waar iemand zich in een bepaalde periode bevond. Het HvJ EU heeft echter geoordeeld dat de toegang van overheidsinstanties tot locatiegegevens zonder meer een ernstige inbreuk op het recht op privacy oplevert en dus alleen is toegestaan als het gaat om 'ernstige criminaliteit'.[293] De benadering van het HvJ EU bergt dus het risico van *overnormering* in zich, in die zin dat voor relatief beperkte inbreuken op het recht op privacy wel erg strenge eisen en waarborgen worden geformuleerd.[294] In recente jurisprudentie heeft de Hoge Raad het HvJ EU door middel van het stellen van een prejudiciële vraag aangespoord zich nader uit te laten over de vraag in hoeverre het verwerken van verkeers- en locatiegegevens steeds tot een dusdanig ernstige inbreuk op het recht op privacy leidt dat zulks alleen onder bepaalde voorwaarden met inachtneming van strenge waarborgen is toegestaan.[295]

3.4.4 Tussenconclusie

De vraag is nu welke lessen kunnen worden getrokken uit de jurisprudentie van het HvJ EU voor de normering van opsporingsonderzoek aan reeds verkregen gegevens. Allereerst is een voorbehoud op zijn plaats. De jurisprudentie van het HvJ EU omtrent de conformiteit van bewaring van en toegang tot verkeers- en locatiegegevens van telecommunicatieaanbieders is in ontwikkeling. Het gaat om gezaghebbende arresten, vaak door de Grote Kamer gewezen, die vooralsnog vele vragen doen rijzen. De consequentie hiervan is dat uit deze jurisprudentie weinig harde conclusies zijn af te leiden met betrekking tot onderzoek van gegevens voor strafvorderlijke gegevens. Niettemin vallen een tweetal punten op.

---

292 Het HvJ EU heeft zich ook uitgelaten over filteringssoftware en geoordeeld dat deze software alleen mag worden toegepast in het kader van terrorisme. Vanwege de prejudiciële vraag heeft het HvJ EU zich niet uitgelaten over de vraag of deze software ook kan worden gebruikt voor andere strafbare feiten dan terrorisme.

293 Bovendien laat A-G Keulen (21 december 2021, ECLI:NL:PHR:2021:1184, pnt. 71) zien dat het ook niet altijd logisch is om een koppeling te maken tussen de ernst van de privacyinbreuk en de ernst van een strafbaar feit. Een ingrijpende inmenging is het privéleven van personen, door bijvoorbeeld een doorzoeking van een woning, is niet beperkt tot bestrijding van ernstige criminaliteit. De forse inmenging in het privéleven rechtvaardigt wel dat het aan de rechter-commissaris en niet aan de Officier van Justitie of een gewone opsporingsambtenaar is om de doorzoekingsbeslissing te nemen.

294 Zie in deze zin ook A-G Keulen, 21 december 2021, ECLI:NL:PHR:2021:1184, pnt. 97-113.

295 HR 5 april 2022, ECLI:NL:HR:2022:475, r.o. 8.4.

In de eerste plaats is opmerkelijk dat het HvJ EU weliswaar steeds vaststelt dat inbreuk is gemaakt op het recht op gegevensbescherming, maar dat het hieraan niet of nauwelijks consequenties lijkt te verbinden. Bij de vraag of de inbreuk van een verwerkingshandeling kan worden gerechtvaardigd, besteedt het HvJ EU bijvoorbeeld geen aandacht aan de in artikel 8 HGEU neergelegde beginselen van doelbinding. Hierdoor ontstaat onduidelijkheid over de relatie tussen artikel 7 en 8 HGEU. Privacy en gegevensbescherming zijn verschillende rechten, maar de eisen en waarborgen die uit deze rechten voortvloeien lijken te overlappen.

In de tweede plaats valt op dat het HvJ EU uitgaat van een privacybegrip, waarbij voor de vraag of het verwerken van gegevens inbreuk maakt op het recht op privacy niet alleen wordt gekeken naar wat uit de gegevens als zodanig kan worden afgeleid, maar ook naar wat de gegevens in combinatie over het privéleven kunnen prijsgeven. Deze benadering komt op dit punt overeen met de Straatburgse interpretatie. De benadering heeft als voordeel dat niet te gemakkelijk wordt voorbijgegaan aan het feit dat gegevens vaak in samenhang veel over het privéleven kunnen zeggen. De consequentie die het HvJ EU hieraan vervolgens verbindt bij de vraag onder welke omstandigheden en met welke waarborgen de inbreuk kan worden gerechtvaardigd is evenwel niet altijd goed te volgen. In zijn jurisprudentie lijkt het HvJ EU te hebben gekozen voor een benadering waarbij de verwerking van bepaalde type gegevens – bijvoorbeeld verkeers- en locatiegegevens – zonder meer tot een ernstige privacyinbreuk leidt en daarom slechts onder bepaalde omstandigheden (alleen ter bestrijding van ernstige criminaliteit) is toegestaan en met strenge waarborgen moet worden omgeven. Deze benadering, waarbij de mate van rechtsbescherming wordt gekoppeld aan een type gegeven, kan leiden tot overnormering. Niet elke verwerking van verkeers- en locatiegegevens hoeft immers tot een ernstige inbreuk op het recht op privacy te leiden. Het koppelen van het verwerken van een bepaald type gegeven aan strengere waarborgen wijkt voorts weer af van het EHRM-kader.

3.5 Conclusie

In dit hoofdstuk is in kaart gebracht welke eisen en waarborgen relevante Europese rechtsbronnen stellen aan de normering van onderzoek van reeds in de opsporing verkregen gegevens. Daarbij is allereerst ingegaan op de verplichtingen die volgen uit de Richtlijn 2016/680. De Richtlijn 2016/680 gaat uit van het recht op gegevensbescherming, maar heeft tegelijkertijd oog voor de belangen van autoriteiten bij de opsporing van strafbare feiten. EU-lidstaten die gegevens verzamelen en

verwerken voor strafvorderlijke doeleinden dienen het rechtmatigheidsbeginsel, het eerlijkheidsbeginsel, het doelbindingsbeginsel, het data-minimalisatiebeginsel en het juistheidsbeginsel in acht te nemen. Van belang is dat het doelbindingsbeginsel geen absolute werking kent. Doelafwijkend gebruik is toegestaan, mits dit is voorzien bij wet en alleen als het noodzakelijk en proportioneel is. De Richtlijn 2016/680 maakt niet precies duidelijk hoe breed of eng afzonderlijke doeleinden in de nationale wetgeving moeten worden geformuleerd en wanneer aldus sprake is van verenigbaar doelgebruik dan wel doelafwijkend gebruik. Het lijkt erop dat aan lidstaten een bepaalde marge voor de invulling van het doelbindingsbeginsel is voorbehouden. Voorts schrijft de Richtlijn 2016/680 voor dat lidstaten dienen te voorzien in intern en onafhankelijk extern toezicht. De bevoegdheden van toezichthouders bestaan uit het doen van onderzoek, het nemen van corrigerende maatregelen en het geven van advies. Het is de vraag of de Richtlijn 2016/680 lidstaten verplicht tot het opnemen van enkele concrete bevoegdheden zoals deze in de Richtlijn 2016/680 tot uitdrukking komen. Belangrijk hierbij is de verplichting voor lidstaten om de effectiviteit van het toezicht te waarborgen.

Vervolgens is ingegaan op de verplichtingen die voortvloeien uit het recht op privacy in artikel 8 EVRM. Het wordt op grond van de jurisprudentie van het EHRM duidelijk dat zowel de vergaring, de opslag als de verdere verwerking van gegevens voor strafvorderlijke doeleinden een inbreuk op de privacy met zich meebrengen en met voldoende waarborgen dienen te zijn omkleed. Het EHRM beoordeelt de waarborgen uiteraard in het licht van het recht op privacy en niet in het licht van het recht op gegevensbescherming. Tegelijkertijd valt op dat de condities waar het EHRM waarde aan hecht gekoppeld kunnen worden aan gegevensbeschermingsrechtelijke uitgangspunten zoals doelbinding, opslagbeperking en data-minimalisatie. Met betrekking tot bulkinterceptie presenteert het EHRM een afzonderlijk 'principle based' kader van acht waarborgen die van het begin tot het einde van het interceptietraject in aanmerking moeten worden genomen. Het beschouwt daarbij het proces van dataverzameling en verwerking als één geheel. Hoe verder de fase van verwerking gaat, des te groter de inbreuk op de privacy is, waardoor steeds meer waarborgen in de procedure moeten worden ingebouwd. Staten dienen de proportionaliteit en subsidiariteit van gegevensvergaring en verwerking te borgen door te voorzien in duidelijke en voldoende afgebakende regelgeving omtrent de gronden, omstandigheden en procedure van gegevensverwerking en inzake de opslag van gegevens. Voorts moet worden voorzien in toezicht vooraf, ten tijde van en na het interceptieproces en dient een rechtsmiddel open te staan voor de burger.

Het Hof van Justitie heeft zich bij de beantwoording van prejudiciële vragen met betrekking tot Richtlijn 2002/58/EG zowel uitgelaten over het recht op privacy als bedoeld in artikel 7 HGEU als het recht op bescherming van persoonsgegevens in artikel 8 HGEU. Wat opvalt is dat het HvJ EU tot strengere eisen komt dan het EHRM als het gaat om het opvragen van gegevens door de overheid bij communicatieaanbieders en het gebruik van deze gegevens voor strafvorderlijke doelen. Meer principieel lijkt het HvJ EU een privacybegrip te hanteren waarbij een inbreuk niet alleen wordt beoordeeld aan de hand van gegevens als zodanig, maar ook naar wat gegevens in combinatie over het privéleven kunnen prijsgeven. Dit komt overeen met de Straatsburgse benadering. Tegelijkertijd lijkt het HvJ EU alle verkeers- en locatiegegevens te waarderen als privacygevoelig, waardoor direct een strenger regime van waarborgen wordt vereist. Dit komt niet overeen met de benadering van het EHRM.

4 Verzameling en verwerking van gegevens onder de Wiv 2017

4.1 Inleiding

In dit hoofdstuk wordt ingegaan op de normering van de gegevensverwerking en verdere verwerking van gegevens door de inlichtingen- en veiligheidsdiensten zoals deze tot uitdrukking komt in de Wet op de inlichtingen- en veiligheidsdiensten 2017 (afgekort tot: Wiv 2017). Het gaat daarbij om onderzoek dat wordt uitgevoerd door de Algemene Inlichtingen- en Veiligheidsdienst (hierna: AIVD) en door de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). De taken van de AIVD en MIVD komen tot uitdrukking in artikel 8 lid 2 respectievelijk artikel 10 lid 2 Wiv 2017. Beide diensten werken op vergelijkbare wijze waarbij de AIVD zich vooral richt op bedreigingen en ernstige risico's voor de Nederlandse samenleving[296], terwijl de MIVD onderzoek doet naar onderwerpen die defensie raken. In de Wiv 2017 zijn de bevoegdheden van de diensten nader geregeld, zowel voor wat betreft het verzamelen als voor het verder verwerken van gegevens. Daarnaast is er een aantal andere onderwerpen geregeld, waaronder het toezicht op de diensten.

De inlichtingentaak van de diensten moet worden onderscheiden van de opsporingstaak van de politie. Het gaat hier om duidelijk gescheiden sferen. Inlichtingendiensten verzamelen inlichtingen om langs die weg hun informatiepositie te versterken en zicht te krijgen op de bedreigingen en ernstige risico's voor de Nederlandse samenleving of krijgsmacht.[297] Analyses van de inlichtingendiensten hebben vooral een voorspellend karakter, terwijl het bij de opsporing van oudsher gaat om het vergaren van bewijs over reeds gepleegde strafbare feiten.[298] Dat het gescheiden sferen betreft, komt onder andere tot uitdrukking in artikel 13 Wiv 2017 waarin is opgenomen dat de ambtenaren van de diensten geen bevoegdheid hebben tot het opsporen van strafbare feiten. De door de diensten verzamelde

296 Meer specifiek worden in art. 8 lid 2 onder a Wiv 2017 verwezen naar gevaren 'voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat'.

297 Onder inlichtingen worden verstaan producten die door speciale eenheden van de politie of inlichtingen- en veiligheidsdiensten worden geleverd aan afnemers, zodat zij betere beslissingen kunnen nemen. Zie Oerlemans 2020, p. 6. Vis definieert inlichtingen als 'informatie-items die heimelijk en proactief, dat wil zeggen op eigen initiatief, zijn verzameld' (Vis 2012, p. 5).

298 Van Wifferen 2003, p. 618. Zie voor het klassieke onderscheid tussen het werk van de veiligheidsdiensten en de politie: Vis 2012, p. 58-60. Zie voorts *Kamerstukken II* 2016/17, 34 588, nr. 3 (MvT Wiv 2017), p. 13.

gegevens mogen ook niet zomaar voor strafvorderlijke doeleinden worden gebruikt.[299] De diensten beschikken immers over ruimere bevoegdheden. Het onbeperkt en ongeclausuleerd gebruiken van gegevens verzameld door inlichtingendiensten zou het risico meebrengen dat strafvorderlijke waarborgen buiten toepassing blijven. Voorts is het probleem dat de gegevens die de diensten vergaren niet door opsporingsdiensten zelf op hun betrouwbaarheid kunnen worden getoetst in verband met de bronbescherming.[300] Indien de diensten stuiten op relevante informatie omtrent (nog te plegen) strafbare feiten, dan kan die informatie wel worden verstrekt aan de politie, maar uitsluitend langs de daarvoor bestemde procedure, te weten in de vorm van een ambtsbericht aan de landelijke Officier van Justitie (art. 62 Wiv 2017). De AIVD en MIVD mogen – anders dan in sommige andere landen – geen mensen aanhouden, hun activiteiten zijn primair op informatievergaring gericht.[301] 'Inlichtingenwerk is immers in essentie gegevensverwerking', aldus de Memorie van Toelichting bij de Wiv 2017.[302]

Hoewel de opsporing en de diensten in gescheiden sferen, in aparte organisaties en met eigen wettelijke bevoegdheden opereren, zijn hun activiteiten steeds meer naar elkaar toegegroeid doordat ook de politie steeds meer proactief en informatie-gestuurd is gaan werken. Er vallen duidelijk parallellen te trekken tussen het vergaren van informatie ten behoeve van de opsporing en het verzamelen van informatie ten behoeve van de inlichtingentaak. De diensten hebben echter aanmerkelijk meer ervaring met het verwerken van grote hoeveelheden informatie, waarbij ook informatie over willekeurige derden (non-targets) wordt verwerkt. Het is dan ook nuttig te kijken hoe de verwerking van informatie in dit domein wordt genormeerd, temeer daar de Wiv als gevolg van de voortschrijdende techniek al meermalen is herzien en ook recent is geëvalueerd.[303] Hoewel daaruit blijkt dat ook de Wiv 2017 nog niet geheel naar ieders voldoening functioneert, is wel duidelijk dat de discussie over de relatie tussen het verzamelen van informatie en verder verwerken van die informatie en de waarborgen die daarvoor moeten gelden al op een hoger niveau wordt gevoerd. Bovendien is het nuttig met een 'inlichtingenbril' te kijken naar de praktijk binnen de opsporing/strafvordering, omdat dan andere zaken eruit springen dan wanneer uitsluitend vanuit strafvorderlijk

299 Zie het verschil tussen inlichtingen en opsporing Brinkhoff 2014 en Van Wifferen 2003, p. 617-621.

300 Zie hierover in meer detail Brinkhoff 2014, p. 184 e.v.

301 Zij kunnen echter onder bepaalde omstandigheden wel acteren op de vergaarde informatie door bepaalde activiteiten te verstoren en targets kenbaar te maken dat de diensten hen op het oog heeft.

302 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 27.

303 Zie het *Rapport Commissie Jones-Bos* 2020 en daaraan voorafgaand het *Rapport Commissie Dessens* 2013. Onlangs is ook een advies van de Commissie Bovend'Eert verschenen dat vooral is gericht op het toezicht op de diensten. *Rapport Commissie Bovend'Eert* 2022.

perspectief wordt gekeken. Echter, de wijze waarop normering in de Wiv 2017 is vormgegeven kan niet leidend zijn in de zin van identieke eisen die moeten worden gesteld aan de strafvorderlijke gegevensverwerking, nu vanuit internationaal mensenrechtelijk perspectief andere eisen worden gesteld aan het optreden van veiligheids- en inlichtingendiensten dan aan opsporingsdiensten, ook daar waar zij identieke bevoegdheden hebben. Ten behoeve van de bescherming van de nationale veiligheid is meer toegestaan dan ten behoeve van een concreet strafbaar feit, zoals ook tot uitdrukking komt in de meer verstrekkende bevoegdheden van de diensten.[304]

In dit hoofdstuk zal antwoord worden gegeven op de vraag welke relevante gezichtspunten aan de Wiv 2017 kunnen worden ontleend voor wat betreft de normering van gegevensverwerking voor (strafvorderlijke) onderzoeksdoeleinden. Daartoe wordt in kaart gebracht welke keuzes en uitgangspunten ten grondslag liggen aan de normering van de verwerking van gegevens in de Wiv 2017 en welke lessen daaruit mogelijk voor de wetgever te trekken zijn met het oog op de normering van de verwerking van persoonsgegevens voor de opsporing. Bij de bespreking ligt het zwaartepunt bij de systematiek en uitgangspunten. De wet zal dan ook op hoofdlijnen worden besproken, waarbij vooral de samenhang tussen de fase van het verzamelen en het verder verwerken en de daaraan gekoppelde normering centraal staat. Tevens zal – daar waar relevant – worden gerefereerd aan de plannen van de wetgever zoals die tot uitdrukking komen in het conceptwetsvoorstel 'Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma' dat op 1 april 2022 in consultatie is gegaan en ten tijde van het afronden van het rapport aanhangig was bij de Raad van State.[305] Met die tijdelijke wet is beoogd dat de AIVD en de MIVD, deels in aanvulling op en deels in afwijking van de Wiv 2017, effectiever en sneller invulling kunnen geven aan de bestaande bevoegdheden tot bulkinterceptie en hacken om zodoende beter zicht te houden op de dreiging van landen met een offensief cyberprogramma. De bedoeling is dat deze tijdelijke voorziening wordt vervangen door een definitieve regeling neergelegd in een breder wetsvoorstel dat thans wordt voorbereid.[306] De

304 Dat komt nadrukkelijk naar voren in de rechtspraak van het HvJ EU inzake dataretentie. Uit HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (*La Quadrature du Net*) volgt bijvoorbeeld dat onder omstandigheden, in het belang van de nationale veiligheid, een algemene dataretentieplicht is toegestaan, terwijl zo een algemene retentieplicht ter bestrijding van (ernstige) criminaliteit is uitgesloten.

305 Consultatieversie d.d. 1 april 2022 te raadplegen op https://www.internetconsultatie.nl/tijdelijkewetcyber/b1.

306 Zie de MvT bij het eerdergenoemde conceptwetsvoorstel, p. 5 en de brief van de minister van BZK aan de Tweede Kamer van 24 februari 2022, *Kamerstukken II*, 2021/22, 34588, nr. 91, p. 2.

gedachte is daarbij dat ervaringen die worden opgedaan met de maatregelen in de Tijdelijke wet, in die brede wetswijziging kunnen worden meegenomen.[307]

Het hoofdstuk is als volgt opgebouwd. Allereerst wordt in paragraaf 2 stilgestaan bij het object en de plaats van de normering van gegevens binnen Wiv 2017, waarna in paragraaf 3 kort aandacht wordt besteed aan algemene uitgangspunten en beginselen in de wet. Vervolgens komen achtereenvolgens in paragraaf 4 en 5 de methoden van gegevensverzameling en de wettelijk genormeerde methoden van gegevensverwerking aan bod. De nadruk ligt daarbij op de bevoegdheden en hun onderlinge verhouding en in mindere mate bij de concrete toepassingsvoorwaarden om de reden die hiervoor is genoemd. Paragraaf 6 is gewijd aan het stelsel van toezicht op de Wiv 2017. Het is relevant ook aan dit thema aandacht te besteden, nu normering en toezicht nauw met elkaar zijn verbonden. Het in het leven roepen van (extra) waarborgen en nadere eisen is alleen zinvol als op de naleving daarvan ook toezicht wordt gehouden.[308] Bovendien volgt duidelijk uit de eisen van het EHRM zoals besproken in hoofdstuk 3 dat staten dienen te voorzien in adequaat toezicht op de vergaring en verwerking van gegevens.

4.2 Object en plaats van normering

De Wiv 2017 biedt de grondslag voor het optreden van de AIVD en MIVD. De thans geldende Wiv 2017[309] is de vervanger van de Wiv 2002[310] die op haar beurt de oude Wiv daterend uit 1987 verving.[311] Zoals uit de naamgeving reeds naar voren komt, betreft het in beide gevallen (grotendeels) nieuwe regelingen, die zijn ingevoerd telkens met een beroep op de voortschrijdende techniek. Met de Wiv 2017 is onder meer de mogelijkheid geïntroduceerd tot interceptie van telecommunicatie via kabelgebonden netwerken.[312] Aan de inwerkingtreding van de Wiv 2017 op 1 mei 2018 ging een raadgevend referendum vooraf, waarbij vooral aandacht

307 Concept MvT bij de Tijdelijke wet, p. 11.

308 Zie voor een nadere analyse ten aanzien van de verhouding tussen normering en toezicht (gerelateerd aan de opsporing): Samadi 2020.

309 *Kamerstukken II* 2016/17, 34588, nr. 3 (MvT Wiv 2017).

310 *Kamerstukken II* 1997/98, 25877, nr. 3 (MvT Wiv 2002).

311 De oude Wiv dateert van 3 december 1987 (*Stb*. 1987/635) en is op 1 februari 1988 in werking getreden (*Stb.* 1988/11).

312 Onder de Wiv 2002 kon alleen communicatie via de ether in bulk worden geïntercepteerd. Echter, sinds de invoering van de Wiv in 2002 heeft een wezenlijke verschuiving plaatsgevonden van communicatie van de lucht naar kabelnetwerken die volgens de wetgever 'de ruggengraat zijn gaan vormen van het digitale domein'. De bevoegdheid tot bulkinterceptie is onder Wiv 2017 meer techniekonafhankelijk geformuleerd en wordt daarin aangeduid als onderzoeksopdrachtgerichte interceptie. *Kamerstukken II* 2016-2017, 34 588, nr. 3. p. 8.

was voor bulkinterceptie in het licht van de risico's voor de privacy die daarmee gepaard gaan.[313] Niet alleen zijn met de introductie van de Wiv 2017 de onderzoeksmogelijkheden uitgebreid, er zijn ook nieuwe waarborgen voor burgers gecreëerd vanuit de idee dat de nieuwe bevoegdheden ook verscherpte controle vergen. Met dat doel is onder meer een toets geïntroduceerd voorafgaand aan de daadwerkelijke uitoefening van de meeste bijzondere bevoegdheden door een nieuwe onafhankelijke toetsingscommissie, te weten de Toetsingscommissie Inzet Bevoegdheden (hierna: TIB).[314]

In de Wiv 2017 zijn de taak, de doelstellingen en de bevoegdheden van de diensten en voorts ook het toezicht op de diensten geregeld. De Wiv 2017 is ingedeeld in verschillende hoofdstukken, waarbij een apart hoofdstuk is gewijd aan de verwerking van gegevens. Wat onder de verwerking van gegevens of gegevensverwerking moet worden verstaan, valt terug te lezen in artikel 1 onder f Wiv 2017, namelijk 'elke handeling of elk geheel van handelingen met betrekking tot gegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens'. Ook in de Wiv 2017 heeft de wetgever voor de definitie van 'verwerken' aansluiting gezocht bij de wijze waarop dit begrip in het gegevensbeschermingsrecht is gedefinieerd.[315] Onder het begrip verwerking is dus ook het verzamelen van gegevens geschaard. Niettemin maken wij in dit hoofdstuk – conform de in het eerste hoofdstuk gepresenteerde definities – verschil tussen het verzamelen en verwerken van informatie waarbij met verwerking wordt gedoeld op alle de verzameling opvolgende handelingen met de desbetreffende gegevens (aanknopend bij de terminologie van de AVG en Wiv gaat het dan in feite om de 'verdere' verwerking).[316]

Wanneer we de systematiek van de Wiv 2017 in ogenschouw nemen, dan zien we dat zowel de bevoegdheden tot het verzamelen, als de bevoegdheden tot de (verdere) verwerking tezamen in het derde hoofdstuk zijn opgenomen. Dat derde hoofdstuk begint met een paragraaf met algemene bepalingen waarin is

313 Zie Oerlemans & Hagens 2019, p. 560 en de brief van de ministers van BZK en Defensie naar aanleiding van de uitslag van het raadgevend referendum (*Kamerstukken II* 2017/18, 34588, 70).

314 Zie voor een meer uitvoerige uiteenzetting over de totstandkoming van de Wiv 2017 en de daarin neergelegde wijzigingen: Voermans & Muller 2017. Aan de nieuwe wet ging een uitgebreide evaluatie van de Wiv 2002 vooraf: *Rapport Commissie-Dessens* 2013.

315 In de Wpg is dat ook gebeurd, zie daarover hoofdstuk 2.

316 Zie ook het *Rapport Commissie Jones-Bos* 2020, p. 28 waarin dit onderscheid ook zo wordt gehanteerd, omdat dit naar het oordeel van de commissie ook van belang is voor de omgang met bulkdata en de scheidslijn tussen toezicht ex ante en ex post.

neergelegd dat de diensten bevoegd zijn tot het verwerken van gegevens, maar daarbij de wettelijke waarborgen uit de Wiv en de Wet veiligheidsonderzoeken in acht moeten nemen (art. 17 Wiv 2017).[317] Vervolgens is de tweede paragraaf gewijd aan het verzamelen van gegevens. Daarin valt te lezen welke bevoegdheden de diensten hebben en welke rol toekomt aan de TIB. Voorts is daarin iets geregeld over het uitbrengen van verslag naar aanleiding van het uitoefenen van bijzondere bevoegdheden. De derde paragraaf van hoofdstuk drie is gewijd aan de bevoegdheid tot het toepassen van een geautomatiseerde data-analyse. Hoewel het op het eerste gezicht lijkt alsof de bevoegdheden tot verzameling en verdere verwerking duidelijk in aparte subparagrafen zijn geregeld, blijken ook in de paragraaf met de titel 'de verzameling van gegevens' bevoegdheden te zijn opgenomen die op de verdere verwerking betrekking hebben.[318] Een strikte scheiding is er derhalve niet. Wel wordt de verdere verwerking waarbij datasets op geautomatiseerde wijze worden doorzocht en gegevens met elkaar worden vergeleken zoals dat tot uitdrukking komt in artikel 50 en artikel 60 Wiv 2017, uitdrukkelijk als bevoegdheid van de diensten gepositioneerd, met daaraan gekoppelde normering. In de vierde paragraaf zijn bevoegdheden opgenomen die betrekking hebben op de uitwisseling van gegevens tussen inlichtingen- en veiligheidsdiensten onderling en met andere personen of instanties. Bij de uitwisseling van gegevens wordt in dit hoofdstuk verder niet uitgebreid stilgestaan.[319]

4.3 Richtinggevende beginselen en uitgangspunten

De verwerking van gegevens en de daaraan gekoppelde inzet van bevoegdheden moet allereerst passen binnen de wettelijke taakomschrijving van de diensten.[320] Bepaalde informatiebronnen, namelijk die zijn aangeboord met behulp van de inzet van bijzondere bevoegdheden, kunnen alleen voor specifieke taakonderdelen van de diensten worden gebruikt. Daaraan worden ook nadere, op het gebruik toegesneden eisen gesteld. Is van een dergelijke, nadere clausulering geen sprake, dan

317 Die waarborgen zullen in de volgende paragraaf worden besproken.

318 Deze bevoegdheden zullen in de volgende paragraaf aan de orde komen.

319 Voorts zijn er ook nog (bijzondere) bevoegdheden opgenomen in het vierde hoofdstuk. Deze bevoegdheden hebben niet zozeer te maken met het verwerken van (persoons)gegevens, maar betreffen het oprichten en inzetten van rechtspersonen ter voorbereiding op en ondersteuning van operationele activiteiten (art. 72 Wiv 2017) en het treffen van maatregelen ter bescherming van de door de dienst te behartigen belangen (art. 73 Wiv 2017).

320 En binnen de Geïntegreerde Aanwijzing op de Inlichtingen- en Veiligheidsdiensten waarin eens per vier jaar de onderzoeksgebieden worden bepaald en die door de Minister-President, Minister van Algemene Zaken, de Minister van BZK en de Minister van Defensie gezamenlijk wordt vastgesteld.

kunnen de informatiebronnen voor alle taakonderdelen worden ingezet. Ten aanzien van alle taken kunnen informanten en openbare bronnen worden geraadpleegd, waarbij de memorie van toelichting ook de openbaar toegankelijke delen van het internet, zoals Facebook, Twitter en LinkedIn noemt.[321]

Naast de eis van taakgebondenheid wordt de verwerking voorts genormeerd door een aantal andere richtinggevende beginselen en uitgangspunten. Veel van deze beginselen zijn ook te herkennen in de Wpg. Zo is bepaald dat de verwerking van gegevens slechts plaatsvindt 'voor een bepaald doel en slechts voor zover dat noodzakelijk is voor een goede uitvoering' van de Wiv of de Wet veiligheidsonderzoeken (art. 18 lid 1 Wiv 2017). Hierin zien we naast het noodzakelijkheidsbeginsel ook het doelbindingsvereiste terugkomen. Deze twee beginselen gelden niet alleen voor de verzameling, maar strekken zich uit tot alle vormen van gegevensverwerking.[322] Wel heeft de wetgever benadrukt dat 'de eis dat informatie voor een bepaald doel wordt vergaard, niet wil zeggen dat deze informatie louter en alleen voor dat doel (verder) mag worden gebruikt.' Indien verder gebruik noodzakelijk is voor een goede taakuitvoering van diensten, is dat wel degelijk toegestaan.[323] Daarbij wordt voor wat betreft de inzet van bijzondere bevoegdheden onderscheid gemaakt tussen de ruwe opbrengst van de inzet en de geëvalueerde gegevens.[324] De ruwe opbrengst van de inzet van bijzondere bevoegdheden mag alleen worden aangewend in het kader van het onderzoek waarbinnen de gegevens zijn verworven of ten behoeve van een ander lopend onderzoek dat onder de inlichtingen- of veiligheidstaken van de diensten valt. Zijn de gegevens eenmaal geëvalueerd, dan mogen ze volgens de wetgever 'in het kader van alle taken van de diensten (dus ook andere dan de inlichtingen- en veiligheidstaken) worden aangewend'.[325] De Wiv 2017 biedt derhalve ruimte voor zogenaamd doelafwijkend gebruik van reeds verzamelde gegevens, maar stelt daaraan wel enige beperkingen voor zover deze gegevens afkomstig zijn van de inzet van bijzondere bevoegdheden.

De verwerking van gegevens moet voorts plaatsvinden 'in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze' (art. 18 lid 2 Wiv 2017). In Artikel 26 Wiv 2017 worden voor het verzamelen van gegevens nog een aantal vereisten daaraan toegevoegd. Zo moet de dienst kiezen voor de bevoegdheid die het minste nadeel voor de betrokkene oplevert (het subsidiariteitsvereiste; art. 26 lid 1 Wiv 2017) en de uitoefening van de bevoegdheid dient evenredig te zijn met

321 *Kamerstukken II* 2016/17, 34588, nr. 3 (MvT Wiv 2017), p. 39.
322 *Kamerstukken II* 2016/17, 34588, nr. 3 (MvT Wiv 2017), p. 241.
323 *Kamerstukken II* 2016/17, 34588, nr. 3 (MvT Wiv 2017), p. 31.
324 Zie hierover ook: reactie op de wetsevaluatie in de brief van de CTIVD van 11 augustus 2020 met kenmerk 2020/0096, p. 18.
325 *Kamerstukken II* 2016/17, 34588, nr. 3 (MvT Wiv 2017), p. 31.

het beoogde doel en mag geen onevenredig nadeel voor betrokkenen veroorzaken (het proportionaliteitsbeginsel, art. 26 lid 2 en 3 Wiv 2017). Voorts dient de uitoefening van een bevoegdheid 'zo gericht mogelijk' te zijn en onmiddellijk te worden gestaakt indien het doel is bereikt, dan wel met de uitoefening van een minder ingrijpende bevoegdheid kan worden volstaan (art. 26 lid 4 en 5 Wiv 2017).

Het vereiste dat de uitoefening van een bevoegdheid 'zo gericht mogelijk' dient te zijn, zoals neergelegd in artikel 26 lid 5 Wiv 2017 is ingevoerd naar aanleiding van de motie-Recourt, vanwege de zorgen die bestonden over de privacy van burgers als gevolg van de introductie van een bevoegdheid tot kabelinterceptie.[326] Daarbij wordt volgens de memorie van toelichting bij de Wijzigingswet waarmee dit criterium is ingevoerd, gekeken 'in hoeverre bij de verwerving sprake is van het tot een minimum beperken van niet strikt voor het onderzoek noodzakelijke gegevens, gelet op de technische en operationele omstandigheden van de casus'. Van de diensten wordt in dit verband verlangd dat zij hieraan – zo goed als redelijkerwijs mogelijk is – in hun verzoeken invulling geven 'door de te vergaren gegevens af te bakenen: geografisch, naar tijdstip, naar soort data/type verkeer, naar object/target, naar gedraging of anderszins. Daarbij moet onder meer rekening worden gehouden met de inlichtingencontext waarin juist naar de tot dan toe ongekende dreiging moet worden gezocht, met de fase waarin het onderzoek zich bevindt, met de noodzaak tot falsificatie, met het tijdselement en de reële technische mogelijkheden'.[327] Het gerichtsheids-criterium geldt zowel voor algemene als voor de bijzondere bevoegdheden tot gegevens*verzameling* (en dus ook voor het stelselmatig verzamelen van gegevens uit open bronnen en voor het raadplegen van informanten). Het is echter volgens de Memorie van Toelichting niet de bedoeling om het op alle vormen van gegevensverwerking van toepassing te laten zijn.[328]

Voor wat betreft de verwerking van *persoons*gegevens stelt de wet nog aanvullende eisen. Zo mag de AIVD in beginsel alleen gegevens verwerken ten aanzien van personen die aanleiding geven tot het ernstige vermoeden 'dat zij een gevaar vormen voor de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat' (art. 19 lid 1 sub a Wiv 2017) of 'dat zij een gevaar vormen voor de veiligheid of de paraatheid van de krijgsmacht' (art. 19 lid 2 sub a Wiv 2017).[329] Met andere woorden, de diensten mogen niet zomaar persoonsgegevens verwerken. Echter, artikel 19 lid 5 Wiv 2017 creëert wel een

326 *Kamerstukken II* 2016/17, 34588, 66. Zie hierover ook Oerlemans & Hagens 2019, p. 66.

327 *Kamerstukken II* 2018/19, 34242, nr. 3 (MvT Wijzingswet Wiv 2017), p. 5 e.v. Zie ook art. 5 van het Besluit van de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie van 25 april 2018, nr. 2018-0000251025, houdende vaststelling van beleidsregels met betrekking tot de uitvoering van de Wiv 2017.

328 *Kamerstukken II* 2018/19, 34242, nr. 3 (MvT Wijzingswet Wiv 2017), p. 4.

329 Er worden in art. 19 Wiv 2017 ook andere categorieën personen genoemd die onder meer samenhangen met andere taakstellingen van de AIVD, zoals het verrichten van veiligheidsonderzoeken, het maken van dreigingsanalyses en de uitwisseling met gegevens van andere inlichtingen- of veiligheidsdiensten.

uitzondering voor gegevens van andere personen die 'een logisch en onlosmakelijk onderdeel vormen van de door de diensten te verwerven of verworven gegevensbestanden'.

Naast voornoemde beginselen valt uit de algemene bepalingen ook een aantal uitgangspunten te destilleren. Zo geldt als uitgangspunt dat 'gegevens die, gelet op het doel waarvoor zij worden verwerkt, geen betekenis hebben of hun betekenis hebben verloren, worden verwijderd' (art. 20 Wiv 2017). Voor gegevens die zijn verkregen door de uitoefening van bijzondere bevoegdheden (waarover hierna meer), geldt voorts dat zij – binnen de daarvoor gestelde termijnen – onderzocht worden op hun relevantie voor het onderzoek waarvoor zij zijn verworven.[330] De beoordeling van de relevantie en daarmee het schonen van irrelevante data moet worden gezien als een vorm van datareductie (een streven dat ook aan de orde kwam in hoofdstuk 3).[331] Gegevens die niet relevant zijn voor het onderzoek of ander lopend onderzoek, moeten worden vernietigd. Deze eis hangt samen met het eerdergenoemde doelbindingsvereiste. Alleen geëvalueerde gegevens kunnen verder worden verwerkt voor andere doeleinden. Niet relevante ruwe opbrengst moet derhalve worden vernietigd. Dat wil zeggen dat de gegevens onomkeerbaar verwijderd worden/ontoegankelijk gemaakt worden.[332]

De hoofden van de diensten dragen voorts verantwoordelijkheid voor de geheimhouding van de verzamelde gegevens, de bronnen waaruit de gegevens afkomstig zijn en de veiligheid van personen die aan de gegevensverzameling hebben bijgedragen (art. 23 Wiv 2017). Zij moeten tevens maatregelen nemen ter bevordering van de kwaliteit van de gegevensverwerking, waaronder ook de gehanteerde algoritmen en modellen en maatregelen ter beveiliging tegen verlies of aantasting van gegevens en onbevoegde gegevensverwerking (art. 24 Wiv 2017). Dit is in artikel 24 geformuleerd als een zorgplicht. Om privacy-risico's te minimaliseren worden naast de eerdergenoemde waarborgen en de geldende autorisatieprocedures waaraan hierna nog zal worden gerefereerd ook andere maatregelen

330 Dit geldt dus niet voor gegevens die zijn verkregen uit openbare bronnen. Zie meer hierover *Kamerstukken II* 2016/17, 34588, nr. 3 (MvT Wiv 2017), p. 40 e.v.

331 *Kamerstukken II* 2016/17, 34588, nr. 3 (MvT Wiv 2017), p. 36 e.v. Dat is in praktijk zeer problematisch met name waar het bulkdatasets betreft.

332 *Kamerstukken II* 2016/17, 34588, nr. 3 (MvT Wiv 2017), p. 40. De Wiv 2017 maakt onderscheid tussen verwijdering en vernietiging. Door verwijdering zijn gegevens niet langer toegankelijk zijn voor het reguliere bedrijfsproces (dat wil zeggen ten behoeve van de taakuitvoering van de diensten). Zij blijven echter wel beschikbaar voor archiefdoeleinden en klachtbehandeling, totdat het moment is aangebroken om deze te vernietigen. Zolang de gegevens echter niet zijn vernietigd kunnen zij 'onder omstandigheden toch weer opnieuw gebruikt worden, indien het doel waarvoor ze aanvankelijk waren verworven weer actueel is geworden of voor een eventueel ander doel, mits uiteraard wordt voldaan aan de eisen die in algemene zin aan gegevensverwerking worden gesteld' (MvT, p. 35).

getroffen. Een belangrijk aspect in dit verband is de maatregel van functiescheiding, waarbij systeemgebruikers alleen toegang hebben tot die informatie die voor hun taakuitvoering noodzakelijk is.[333] Dit komt niet alleen tot uitdrukking in artikel 24 lid 2 sub c Wiv 2017 waarbij het gaat om 'de aanwijzing van personen die bij uitsluiting van anderen bevoegd zijn tot de bij de aanwijzing vermelde werkzaamheden in het kader van de verwerking van gegevens', maar ook op andere plekken in de wet waar het bijzondere bevoegdheden tot interceptie betreft (art. 47 lid 5, 48 lid 4 en 49 lid 5 Wiv 2017).

4.4 Methoden van gegevensverzameling

In artikel 25 Wiv 2017 staat opgesomd uit welke bronnen de diensten in ieder geval kunnen putten voor wat betreft het verzamelen van gegevens.[334] De wet maakt vervolgens onderscheid tussen de 'gewone' bevoegdheden van de diensten, te weten het stelselmatig verzamelen van gegevens omtrent personen uit openbare bronnen (art. 38 Wiv 2017) en het raadplegen van zogenaamde informanten (art. 39 Wiv 2017), en de bijzondere bevoegdheden van de diensten. Voor het verzamelen van gegevens uit voor een ieder toegankelijke informatiebronnen is geen toestemming vereist (tenzij dit een stelselmatig karakter draagt). Voor de inzet van andere bevoegdheden moet de betrokken minister toestemming geven. Voor de zogenaamde bijzondere bevoegdheden gelden voorts nog extra eisen. Zo mogen deze ingevolge artikel 28 Wiv 2017 slechts worden uitgeoefend in relatie tot specifieke taken van de diensten. Voor de AIVD betreft dat onderzoek naar personen en organisaties die een bedreiging vormen voor het voortbestaan van de democratische rechtsorde, de veiligheid of andere gewichtige belangen van de staat (art. 8 lid 2 onder a Wiv 2017) en het verrichten van onderzoek betreffende andere landen (art. 8 lid 2 onder d Wiv 2017). Voor de andere taken mag de AIVD geen bijzondere bevoegdheden inzetten.[335] Onder de bijzondere bevoegdheden vallen onder meer: het observeren en volgen van natuurlijke personen of gegevens (art. 40 Wiv 2017); het inzetten van agenten al dan niet onder dekmantel (art. 41 Wiv 2017); onderzoek van besloten plaatsen, gesloten voorwerpen en aan voorwerpen (art. 42 Wiv 2017); DNA-onderzoek ter vaststelling of verificatie van de identiteit van een persoon (art. 43 Wiv 2017); het openen van brieven en andere geadresseerde zendingen (art. 44 Wiv 2017); het verkennen van en binnendringen in geautomatiseerde werken

333 *Kamerstukken II* 2016/17, 34588, nr. 3 (MvT Wiv 2017), p. 37. Zie over de problemen met datareductie en de wijze waarop daaraan adequaat invulling kan worden gegeven de rapporten van de CTIVD 2019/66 en 2020/69.

334 Het betreft geen limitatieve opsomming zoals tot uitdrukking wordt gebracht in de wet met het woord 'in ieder geval'. Zie hierover: *Kamerstukken II* 2016-2017, 34588, nr. 3, p. 38

335 Zie nog wel de uitzondering neergelegd in art. 28 lid 2 Wiv 2017.

(de zogenaamde hackbevoegdheid, art. 45 Wiv 2017) en het verkrijgen van toegang tot plaatsen om de uitoefening van andere bevoegdheden mogelijk te maken (art. 57 Wiv 2017). Deze bevoegdheden vertonen grote gelijkenis met de bevoegdheden die ook de politie tot haar beschikking heeft ten behoeve van het opsporen van strafbare feiten, met dien verstande dat de toepassingsvoorwaarden verschillen en dat het doel van de inzet verschilt.

In paragraaf 3.2.5.6 van de Wiv 2017 zijn de bevoegdheden neergelegd met betrekking tot het onderzoek aan communicatie.[336] Daarbij ziet artikel 47 Wiv 2017 op het met een technisch hulpmiddel aftappen, ontvangen, opnemen en afluisteren van gesprekken, telecommunicatie of gegevensoverdracht. In de artikelen daarna is de zogeheten onderzoeksopdrachtgerichte (hierna OOG) interceptie oftewel de bulkinterceptie geregeld. Hierbij gaat het dus niet om het afluisteren van specifieke personen of organisaties, maar om het – op grote schaal – onderscheppen en analyseren van telecommunicatie zonder dat er aanwijzingen tegen een specifiek persoon zijn.[337] In de aanloop naar de inwerkingtreding van de nieuwe Wiv werd de wet omwille van deze bevoegdheid ook wel de 'sleepwet' genoemd.[338] Ten tijde van de Wiv 2002 werd dit nog aangeduid als 'ongerichte interceptie' waarvoor artikel 27 Wiv 2002 toen de wettelijke grondslag bood. Thans spreekt men van OOG-interceptie waarmee de wetgever tot uitdrukking heeft willen brengen dat het intercepteren van bulkgegevens niet geheel ongericht plaatsvindt, maar aan de hand van onderzoeksopdrachten.[339] Het gaat om het in grote hoeveelheden via de ether of kabel onderscheppen van gegevens (zowel met betrekking tot de inhoud van de communicatie als met betrekking tot metagegevens).[340] De bulkgegevens kunnen zowel worden gebruikt bij onderzoek naar dreigingen en targets die reeds in beeld zijn, als bij onderzoek gericht op nieuwe of verborgen targets.[341] Het onderscheppen zelf is geregeld in artikel 48 Wiv 2017. Het zogenaamde optimaliseren oftewel voorbewerken van de bulkgegevens is in artikel 49 Wiv 2017 geregeld. In dat proces wordt onder meer gezocht naar relevante selectiecriteria.[342] In de praktijk wordt gebruik gemaakt van de activiteit van het snapshotten, waarbij het gaat om het 'doen van korte integrale opnames van de beschikbare gegevensstromen om de veronderstelde inlichtingenwaarde te

336 Zie over bulkinterceptie: Oerlemans en Hagens 2019, p. 560-568 en Oerlemans 2020, p. 260-267.

337 Voermans & Muller 2017, p. 103.

338 Zie over deze kwalificatie Oerlemans & Hagens 2019, p. 560 e.v.

339 *Rapport Commissie Jones-Bos* 2020, p. 79.

340 In dit verband wordt ook wel gesproken van s*ignals intelligence* (afgekort: *sigint*) omdat de analyse geschiedt op basis van informatie uit communicatie die via signalen wordt overgebracht (Oerlemans & Hagens 2017, p. 563).

341 *Rapport Commissie Jones-Bos* 2020, p. 42.

342 Zie hierover in meer detail: *Kamerstukken II* 2016/17, 34588, nr. 3, p. 104.

kunnen vaststellen'.[343] Deze gegevens mogen nog niet worden gebruikt voor inhoudelijk onderzoek, maar zijn bedoeld om de interceptie te optimaliseren en vooraf de gerichtheid van de inzet te kunnen motiveren.[344] De nadere analyse van de gegevens oftewel de verdere verwerking is in artikel 50 Wiv 2017 neergelegd.[345] Artikel 50 lid 1 onder a Wiv 2017 voorziet in een selectiebevoegdheid die het mogelijk maakt om van de *inhoud* van de gegevens kennis te nemen.[346] De inhoud van het geïntercepteerde materiaal wordt dan ook pas na de selectie zichtbaar.[347] Om deze selectie mogelijk te maken moeten criteria worden geformuleerd. Deze selectiecriteria zien bijvoorbeeld op de identiteit van personen, telefoonnummers en/of aan een nader omschreven onderwerp gerelateerde trefwoorden.[348] Het is de minister of het hoofd van de dienst die toestemming moet geven voor de vaststelling van selectiecriteria bij een persoon, activiteit of een onderwerp, maar het hoofd van de dienst kan dit weer ondermandateren (art. 50 lid 3 Wiv 2017).[349]

Echter, er zijn ook andere bevoegdheden die het mogelijk maken om bulkgegevens te verkrijgen. Zo kunnen bulkgegevens worden verkregen via het gebruik van de hiervoor genoemde hackbevoegdheid (art. 45 Wiv 2017) of via informanten (art. 39 Wiv 2017). Bulkgegevens kunnen tevens worden verkregen van medeoverheidsinstanties zoals de politie, Koninklijke Marechaussee en Belastingdienst.[350] Daar zit volgens de Evaluatiecommissie Wiv 2017 een probleem, nu voor het verwerven en verwerken van deze gegevens een ander, lichter regime geldt. Voor de toepassing van bulkinterceptie op grond van artikel 48 Wiv 2017 gelden zeer strikte eisen, waarbij de betrokken minister toestemming moet geven en de TIB de rechtmatigheid toetst zowel voor wat betreft de verwerving als de (verdere)

343 Zie de Beleidsreactie op het rapport van de CTIVD 2022/75 over inzet van kabelinterceptie door de AIVD en de MIVD: de snapshotfase.

344 Rapport CTIVD 2022/75, p. 6. De CTIVD komt met oog op de voorzienbaarheid en rechtszekerheid met de aanbeveling om het snapshotten te voorzien van expliciet wettelijke basis, nu deze thans ontbreekt.

345 De terminologie in de Wiv wijkt af van het dagelijks taalgebruik. Onder selectie wordt verstaan 'de bijzondere bevoegdheid waarmee de AIVD en de MIVD kennis kunnen nemen van de inhoud van gegevens die met behulp van onderzoeksopdrachtgerichte interceptie zijn verworven', aldus de CTIVD in het rapport dat aan de selectiebevoegdheid is gewijd (2019/64).

346 Rapport CTIVD 2019/64, p. 4.

347 Bij de bijzondere regeling voor geautomatiseerde gegevensanalyse met metadata verkregen uit onderzoeksopdrachtgerichte interceptie gericht op het identificeren van personen en organisaties neergelegd in art. 50 lid 1 onder b jo. lid 4 staan wij hierna in par. 4.5 nader stil.

348 *Kamerstukken II* 2016/17, 34588, nr. 3, p. 108.

349 Rapport CTIVD 2019/64, p. 4.

350 De commissie constateert dat een eenduidige en voorzienbare grondslag hiervoor ontbreekt. De uitwisseling geschiedt nu zowel op grond van art. 39 als art. 94 Wiv 2017. *Rapport Commissie Jones-Bos* 2020, p. 48-49.

verwerking. De Evaluatiecommissie vindt het opvallend 'dat in de systematiek van de Wiv 2017 de waarborgen dus niet volgen uit de aard en omvang van de gegevens, maar afhangen van de bevoegdheid waarmee die gegevens worden verworven. Dit leidt tot inconsistentie omdat vergelijkbare gegevens via verschillende bevoegdheden kunnen worden verworven. De Evaluatiecommissie ziet hierin een ernstig gebrek aan voorzienbaarheid en uniformiteit.'[351] Zij stelt voor om een uniform kader te creëren voor de verwerking van bulkdata, waarbij kan worden aangehaakt bij het kader dat nu reeds geldt voor bulkdata verkregen uit onderzoeksopdrachtgerichte interceptie, te weten:

1. 'Waarborg op **handeling**: wat mag met de bulkdata worden gedaan?
2. Waarborg op **toegang**: wie mag er bij de bulkdata?
3. Waarborg op **tijd**: hoe lang mag de bulkdata worden bewaard?'[352]

Daarbij is het volgens de commissie van belang om de waarborgen niet te koppelen aan de wijze/het middel van vergaren, maar aan de aard van gegevens.[353]Al voor dat de commissie haar rapport uitbracht, is een tijdelijke bulkregeling opgesteld waarin regels zijn opgenomen over de verwerking van alle bulkdata ongeacht de wijze van verkrijgen, waarbij het toegangsregime wordt bepaald door de zwaarte van inbreuk op de privacy.[354] Dit vormt ook een belangrijke les met het oog op strafvorderlijk onderzoek. Er moet voor de normering niet alleen worden gekeken naar de wijze van verzameling, maar vooral naar de zwaarte van de privacy-inbreuk die met de verwerking wordt gemaakt.

Een ander probleem bij het verwerven van gegevens is gelegen in het eerdergenoemde gerichtheidsvereiste. Niet duidelijk is hoe dit vereiste dient te worden ingevuld in relatie tot bulkinterceptie. Weliswaar wordt niet langer gesproken van ongerichte interceptie, de doelbinding[355] is bij dit type bevoegdheid volgens de Evaluatiecommissie 'minder eenduidig, omdat soms bij de verwerking pas specifieke gebruiksdoelen kunnen worden vastgesteld'.[356] Bulkinterceptie kenmerkt zich erin dat ook gegevens worden binnengehaald met betrekking tot personen en

351 *Rapport Commissie Jones-Bos* 2020, p. 42. Oerlemans gaat in zijn oratie dieper in op de informantenbevoegdheid en stelt dat deze onvoldoende voorzienbaar is (Oerlemans 2020, p. 19-20).

352 *Rapport Commissie Jones-Bos* 2020, p. 53.

353 *Rapport Commissie Jones-Bos* 2020, p. 53. Ook de CTIVD deelt dit oordeel. Zie hieromtrent in meer detail de reactie op de wetsevaluatie in de brief van de CTIVD van 11 augustus 2020 met kenmerk 2020/0096.

354 Regeling van 5 november 2020, *Stcrt.* 2020, 56482.

355 Eigenlijk wordt hier bedoeld de doelspecificatie, maar deze term zijn we in de context van de Wiv 2017 niet tegengekomen.

356 *Rapport Commissie Jones-Bos* 2020, p. 49.

organisaties die geen target zijn en dat ook niet zullen worden. Het is volgens de evaluatiecommissie juist 'gericht op het verkrijgen van een informatiepositie bij een dreiging waarvan de targets nog niet of maar deels bekend zijn.'[357] Wanneer van tevoren een te scherpe afbakening wordt vereist, hindert dat het werk van de diensten, aldus de Evaluatiecommissie. Ook de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) constateert in een toezichtrapport uit 2022 dat de uitleg die aanvankelijk aan kabelinterceptie is gegeven 'wringt met de aard van de bevoegdheid, het middel en met de uitvoering in de (technische) praktijk'.[358] In de concept Memorie van Toelichting bij de eerdergenoemde Tijdelijke wet valt te lezen dat de bevoegdheid tot onderzoeksopdrachtgerichte interceptie tot dusver slechts beperkt is ingezet ten behoeve van het inlichtingenproces. Als reden hiervoor wordt genoemd 'de onduidelijkheid met betrekking tot de wijze waarop het gerichtheidsvereiste bij de inzet van deze bevoegdheid moet worden geïnterpreteerd en de verschillende zienswijzen ter zake van de ministers en de Toetsingscommissie over de inzet van bevoegdheden'.[359] Er wordt thans voorgesteld om bij onderzoeken in het cyberdomein het gerichtheidsvereiste bij de bevoegdheid tot verkennen van de data buiten beschouwing te laten. 'De bevoegdheid tot verkennen is immers per definitie ongericht', aldus de MvT.[360] Het voorgaande maakt duidelijk dat bij het introduceren van wettelijke waarborgen goed moet worden gekeken naar de aard van de bevoegdheid en de technische realiteit.

4.5 Wettelijk genormeerde methoden van gegevensverwerking

Op grond van artikel 17 Wiv 2017 zijn de diensten bevoegd tot het verwerken van gegevens voor zover dit valt binnen hun wettelijke taak en met in achtneming van de wettelijke eisen. Gegevensverwerking werd en wordt gezien als een van de kernactiviteiten van de diensten.[361] Daartoe staan de diensten verschillende informatiebronnen ter beschikking. De Wiv 2017 stelt echter ook eisen aan de nadere analyse van die gegevens. Zo werd uit de voorgaande paragraaf duidelijk dat voor het verwerken van data uit bulkinterceptie verkregen via artikel 48 Wiv 2017 een bijzonder regime geldt en na het verwerven van de informatie ook specifieke eisen worden gesteld aan de (verdere) verwerking in artikel 49 en artikel 50 Wiv 2017. In

357 *Rapport Commissie Jones-Bos* 2020, p. 49. Zie over het proces van selectie ook Jacobs 2016, p. 256-261.

358 Rapport CTIVD 2022/75, p. 6 en 55.

359 Concept MvT bij de Tijdelijke wet, p. 4.

360 Concept MvT bij de Tijdelijke wet, p. 23. Zie over het vereiste van gerichtheid in relatie tot bulkinterceptie meer uitvoerig het rapport van de CTIVD 2022/75.

361 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 131 (MvT Wiv 2017). Zie ook concept MvT bij de Tijdelijke wet, p. 25.

de Wiv 2017 is daarnaast nog in artikel 60 een specifieke bepaling opgenomen die betrekking heeft op het toepassen van geautomatiseerde data-analyse (ook wel aangeduid als GDA) in de verschillende gegevensbestanden die de diensten ter beschikking staan. Over deze GDA-bevoegdheid is de nodige discussie ontstaan, waaraan in deze paragraaf nader aandacht zal worden besteed. Het geautomatiseerd vergelijken en verrijken van informatie uit een of meerdere informatiebronnen is immers ook in strafvorderlijke context een belangrijk punt.

Artikel 60 Wiv 2017 vormde in de kern een codificatie van een bestaande werkmethode van de diensten.[362] De wetgever achtte het wenselijk om '....gelet op de toegenomen betekenis van verwerkingen met een big data-karakter [..] geautomatiseerde data-analyse als werkmethode van de diensten van een expliciete wettelijke grondslag te voorzien'.[363] Zonder toepassing van data-analysetechnieken is het echter vrijwel onmogelijk om grote gegevensbestanden te ontsluiten.[364] In het eerste lid van artikel 60 Wiv 2017 wordt opgesomd welke bestanden dat zijn, namelijk gegevens uit eigen geautomatiseerde gegevensbestanden; gegevens uit voor een ieder toegankelijke informatiebronnen, gegevens uit geautomatiseerde gegevensbestanden waartoe de diensten rechtstreeks toegang hebben en gegevens uit door derden verstrekte geautomatiseerde gegevensbestanden. In het tweede lid wordt uiteengezet welke handelingen in dit verband 'in ieder geval' kunnen worden uitgevoerd, te weten a) het geautomatiseerd vergelijken van gegevens met elkaar; b) het doorzoeken van de bestanden aan de hand van profielen en c) het vergelijken met het oog op het ontdekken van bepaalde verbanden.

Van belang is op te merken dat aan deze vorm van gegevensverwerking geen specifieke toestemmingsvereisten zijn verbonden, met uitzondering wanneer zij worden toegepast op OOG-data (waarvoor in art. 50 lid 1 onder b jo lid 4 Wiv 20017 een bijzondere regeling is getroffen). Wel zijn de algemene bepalingen van kracht. Zo volgt uit artikel 18 Wiv 2017 immers dat verwerking van gegevens alleen plaatsvindt voor zover dat noodzakelijk is voor een goede taakuitvoering. Ook moet de analyse op behoorlijke en zorgvuldige wijze plaatsvinden waarbij de diensthoofden maatregelen moeten treffen ter bevordering van de kwaliteit en de gehanteerde algoritmen en modellen (art. 24 lid 2 sub a Wiv 2017). [365] Tevens is in

362 Ook onder de Wiv 2002 gebruikte de diensten immers al geavanceerde vormen van gegevensverwerking. *Kamerstukken II* 2016/17, 34588, nr. 3 (MvT bij Wiv 2017), p. 129 en 131 en *Rapport Commissie Jones-Bos* 2020, p. 69.

363 *Kamerstukken II* 2016/17, 34588, nr. 3 (MvT bij Wiv 2017), p. 131.

364 Concept MvT bij de Tijdelijke wet, p. 25.

365 Uit de in art. 24 neergelegde zorgplicht volgt ook dat de diensten bij het ontwerpen, aankopen en in gebruik nemen van technische systemen rekening moeten houden met de beginselen van gegevensbescherming. In dit verband worden in de Nota naar aanleiding van het verslag genoemd gegevensbescherming *by design* en *by default*. →

het derde lid van artikel 60 Wiv 2017 bepaald dat het niet is toegestaan om maatregelen te treffen of te bevorderen jegens een persoon uitsluitend op basis van de resultaten van deze geautomatiseerde gegevensverwerking. Met andere woorden, de uitkomsten moeten alvorens de dienst actie onderneemt jegens een concreet individu, altijd eerst door een mens worden geverifieerd.[366]

In art. 50 lid 1 onder b Wiv 2017 is – zoals hiervoor aangegeven – een bijzondere regeling getroffen voor de mogelijkheid tot het verrichten van GDA aan de hand van metadata verkregen uit onderzoeksopdrachtgerichte interceptie, waarbij ook verwezen wordt naar artikel 60 Wiv 2017. In artikel 50 lid 4 komt tot uitdrukking dat als GDA wordt toegepast op metadata verkregen uit de bulkinterceptie en deze gericht is op het identificeren van personen en organisaties daarvoor aanvullende waarborgen gelden, te weten toestemming van de betrokken minister met een rechtmatigheidstoetsing door de TIB. In het verzoek tot toestemming moet voorts worden aangegeven welke vorm van GDA wordt toepast en voor zover mogelijk welke gegevensbestanden in de analyse worden betrokken.

Er doen zich in dit verband echter meerdere problemen voor. Allereerst is een probleem dat alleen voor geautomatiseerde data-analyse op OOG-data gericht op het identificeren van personen en organisaties nadere waarborgen gelden en niet voor (bulk)gegevens die via andere bevoegdheden zijn vergaard. Het verschil in waarborgen kwam ook in de vorige paragraaf aan de orde. Voor wat betreft de bevoegdheid tot het verrichten van GDA biedt de regeling in feite slechts gedeeltelijke rechtsbescherming voor burgers, nu de verscherpte eisen van artikel 50 Wiv 2017 op een groot aantal informatiebronnen niet van toepassing is, terwijl het voor de privacy-inbreuk die met de GDA-bevoegdheid wordt gemaakt niet uitmaakt langs welke weg de gegevens zijn vergaard. De CTIVD stelt dat de regeling in dit opzicht niet in balans is.[367]

Voorts is in de praktijk discussie ontstaan wat onder GDA moet worden begrepen en voor welke handelingen met OOG-data een dergelijke toestemming nu precies is vereist. Uit het Evaluatierapport Wiv 2017 blijkt dat de diensten en de toezichthouders in dezen lijnrecht tegenover elkaar staan. De Evaluatiecommissie schrijft dat waar de toezichthouders van mening zijn dat zowel eenvoudige als complexere vormen van gegevensverwerking als GDA moeten worden

'Gegevensbescherming by design houdt in dat de diensten bij de ontwikkeling van systemen het belang van privacy en gegevensbescherming inbouwen. Gegevensbescherming by default ziet erop dat systemen zo ontworpen en ingericht worden dat zo min mogelijk persoonsgegevens worden verwerkt'. *Kamerstukken II* 2016/17, 34588, nr. 18, p. 28.

366 Zie hierover ook het rapport van CTIVD 2019/62 en het *Rapport Commissie Jones-Bos* 2020, p. 70.

367 Zie de reactie op de wetsevaluatie in de brief van de CTIVD van 11 augustus 2020 met kenmerk 2020/0096, p. 5.

aangemerkt, de diensten zich op het standpunt stellen dat het belangrijk is om te kijken naar de mate van inbreuk op de persoonlijke levenssfeer, waarbij alleen de zwaardere inbreuken op de persoonlijke levenssfeer als GDA worden aangemerkt.[368] Een eenvoudige naslag in de gegevensbestanden geldt dan niet als GDA en daarvoor hoeft in de optiek van de diensten dan ook niet (afzonderlijk) toestemming te worden verkregen.[369] Deze discussie speelt thans vooral in relatie tot OOG-data, omdat in die context verscherpte waarborgen gelden in de vorm van toestemming van de betrokken minister en een rechtmatigheidstoetsing van de TIB. De vraag is echter ook breder op te vatten, namelijk voor welke vormen van geautomatiseerde data-analyse er nadere eisen zouden moeten gelden en welke dat dan zouden moeten zijn.

Hier wreekt zich dat de Europese jurisprudentie op dit punt niet helder is. Zowel het EHRM als het HvJ EU lijken vrij snel aan te nemen dat data-analyses inbreuk maken op het recht op privacy; zo wordt algemeen aangenomen dat een data-analyse van aan communicatie gerelateerde gegevens een ernstige inbreuk oplevert. Onduidelijk is echter wat de beide hoven precies onder data-analyse verstaan, alsmede aan welke eisen een dergelijke analyse moet voldoen; is regulering op basis van de algemene beginselen inzake gegevensverwerking voldoende of moet hiervoor een 'bijzondere' bevoegdheid worden gecreëerd, waarbij ook toestemming wordt verkregen van bijvoorbeeld de TIB, de minister of een andere onafhankelijke autoriteit? Bovendien is de vraag wat precies uit jurisprudentie kan worden afgeleid. Die jurisprudentie van het HvJ EU ziet steeds op het analyseren van verkeers- en locatiegegevens, maar de vraag is in hoeverre zij ook geldt voor een eenvoudige naslag.

De Evaluatiecommissie Wiv 2017 signaleert in ieder geval 'dat de discussie over de interpretatie van GDA vermengd is geraakt met de discussie voor de benodigde waarborgen voor verwerking van OOG-data'.[370] De waarborgen omtrent de toegang en waarborgen omtrent de handelingen (welke vormen van gegevensverwerking mogen worden verricht) zijn door elkaar gaan lopen en de commissie beveelt dan ook aan om deze waarborgen te scheiden, waarbij ze elkaar overigens wel kunnen aanvullen. De Evaluatiecommissie heeft geprobeerd – redenerend vanuit het recht op privacy – onderscheid te maken in verschillende vormen van gegevensverwerking, vanuit de gedachte dat bepaalde vormen van gegevensverwerking op zichzelf gevoelig zijn en extra waarborgen vergen. De commissie stelt zich op het standpunt dat vooral naar het resultaat van de

368 Dit valt ook terug te lezen in de rechtseenheidbrief van het TIB en de CTIVD aan de Tweede Kamer over hun interpretatie van de Wiv 2017 van 23 november 2018. *Kamerstukken II* 2018/19, 29 924, nr. 173, p. 3.

369 Zie in meer detail: *Rapport Commissie Jones-Bos* 2020, p. 71 en72.

370 *Rapport Commissie Jones-Bos* 2020, p. 72.

gegevensverwerking moet worden gekeken. Kort weergegeven: is het resultaat in essentie een deelverzameling van de betrokken gegevens, dan zijn geen additionele waarborgen vereist; voegt het resultaat daarentegen iets toe aan de betrokken gegevens, dan zijn wel extra waarborgen vereist.[371] Met andere woorden, aan een eenvoudige zoekslag in de beschikbare databronnen waarbij gericht wordt gezocht naar specifieke informatie over een target kunnen lichtere eisen worden gesteld dan aan meer complexe data-analyses waarbij gegevens uit verschillende bronnen met elkaar worden gecombineerd om tot nieuwe inzichten te komen. Ook de CTIVD meent dat GDA beter gereguleerd moet worden. De CTIVD benadrukt echter dat de privacy-impact niet wordt bepaald door de vraag of een 'simpel' of 'eenvoudig instrument' wordt ingezet.[372] Zij lijken meer de nadruk te leggen op de privacy-inbreuk dan op de vorm die GDA aanneemt. De vraag is evenwel of een eenvoudige naslag, waarover zoveel discussie bestaat tussen de diensten en de toezichthouders, ook een ernstige privacy-inbreuk oplevert.

Een ander probleem betreft het toezicht op de uitoefening van de inzet van GDA bij OOG-data gericht op het identificeren van personen en organisaties. Hiervoor is voorafgaande toestemming van de minister vereist en voert de TIB een rechtmatigheidscontrole uit. De CTIVD merkt echter op dat een 'onafhankelijke voorafgaande toets voor de inzet van data-analyse [..] niet altijd goed mogelijk [is], omdat niet altijd goed van te voren het proces van data-analyse kan worden ingeschat. Voorafgaand en gedurende het gebruik is het wel mogelijk om juist de ontwikkeling van applicaties (op basis van o.a. *machine learning* en AI) goed te documenteren en hier verantwoording over af te leggen.' De waarborgen dienen volgens de CTIVD daarnaast veel meer in de manier van omgaan met de gegevens (de 'behoorlijke en zorgvuldige gegevensverwerking') dan in een vooraf-toets op noodzaak, proportionaliteit en gerichtheid te worden vormgegeven. Bij het toezicht zal in de volgende paragraaf nader worden stilgestaan. De wetgever is in ieder geval voornemens de *ex ante*-toetsing voor GDA bij OOG-data te laten vervallen in het kader van de Tijdelijke wet.[373]

Tot slot maken we nog een opmerking over de bewaartermijnen. Immers, GDA kan alleen worden toegepast op gegevens die ook daadwerkelijk in de systemen aanwezig zijn (dus nog niet zijn verwijderd of vernietigd). Ook over de bewaartermijnen is discussie ontstaan in relatie tot de relevantiebeoordeling van bulkdatasets, die binnen één jaar moet plaatsvinden (met een mogelijke verlenging van een half jaar, zie art. 27 lid 1 Wiv 2017). Daarbij gaat het dan over bulkdatasets die niet via de OOG zijn verzameld, maar via andere bevoegdheden zoals de

371 Zie meer uitvoerig: *Rapport Commissie Jones-Bos* 2020, p. 76.

372 De reactie op de wetsevaluatie in de brief van de CTIVD van 11 augustus 2020 met kenmerk 2020/0096, p. 15.

373 Concept MvT Tijdelijke wet, p. 25.

hackbevoegdheid (voor OOG-data geldt namelijk een ruimere bewaartermijn van drie jaar, zie art. 48 lid 5 Wiv 2017). Gegevens die niet binnen de gestelde termijn zijn onderzocht, moeten terstond worden vernietigd. In de praktijk is deze termijn problematisch gebleken, omdat bulkdatasets veel langer van waarde kunnen en blijken te zijn.[374] De kunstgreep die vervolgens in de praktijk werd toegepast – namelijk om bij het verlopen van de bewaartermijn de dataset grotendeels of geheel relevant te verklaren en gegevens uit de dataset verder te verwerken – is door de CTIVD als onrechtmatig beoordeeld.[375] Een relevantiebeoordeling is volgens de CTIVD in feite ook niet goed mogelijk gelet op de aard en omvang van bulkdatasets.[376] De wetgever koerst er in het conceptwetsvoorstel voor de tijdelijke wet op om de beoordelingstermijnen voor bulkdatasets verkregen door inzet van hackbevoegdheden te verlengen met telkens een jaar en de relevantiebeoordeling van artikel 27 lid 1 Wiv 2017 buiten toepassing te verklaren.[377] Het gaat dan wel uitsluitend om bulkdatasets 'die gegevens bevatten die verworven zijn in onderzoeken naar landen met een offensief cyberprogramma tegen Nederland of Nederlandse belangen', want alleen die onderzoeken vallen onder het bereik van de tijdelijke regeling. Mogelijk zal de wetgever de uiteindelijke regeling echter ook op dit punt aanpassen, nu hier de juridische eisen niet goed lijken te stroken met de praktische realiteit.

4.6 Toezicht op de naleving van de Wiv 2017

In het voorgaande is reeds aangegeven dat normering en toezicht nauw met elkaar samenhangen. Zonder toezicht zijn er immers weinig (externe) prikkels om de gestelde normen/regels ook daadwerkelijk na te leven. Toezicht heeft ook een belangrijke rol in het preciseren van de gestelde normen[378], wat ook te constateren valt in de rapporten van de CTIVD waarin veelvuldig wordt ingegaan op vragen over hoe de norm nu precies luidt dan wel moet worden ingevuld en wat het toepassingsbereik is van bepaalde in regels vervatte normen. De Evaluatiecommissie Wiv 2017 legt bovendien ook een duidelijk verband tussen de inhoud van de norm en de effectiviteit van het toezicht.[379] Effectief toezicht is voorts belangrijk voor de legitimiteit van het optreden van de diensten en voorts een voorwaarde voor de toepassing van bepaalde verstrekkende bevoegdheden. Alle aanleiding derhalve om in

374 Concept MvT Tijdelijke wet, p. 20.
375 De reactie op de wetsevaluatie in de brief van de CTIVD van 11 augustus 2020 met kenmerk 2020/0096, p. 8.
376 Brief van de CTIVD, p. 8.
377 Concept MvT Tijdelijke wet, p. 25.
378 Samadi 2020, p. 125 en 359.
379 *Rapport Commissie Jones-Bos* 2020, p. 115.

deze paragraaf nader stil te staan bij de wijze waarop het toezicht op de Wiv 2017 in grote lijnen is vormgegeven en om mogelijke aandachtspunten voor het strafvorderlijk toezicht te identificeren. De analyse is beperkt tot het niet-parlementaire toezicht. De controle die de vaste Kamercommissies van BZK en Defensie en Commissie voor de Inlichtingen- en Veiligheidsdiensten (CIVD) uitoefenen op de taakuitoefening van de diensten blijft dan ook verder buiten beschouwing nu dat voor toezicht in een strafvorderlijke context niet rechtstreeks relevant is.

4.6.1 Huidige inrichting toezichtstelsel

Het niet-parlementaire toezicht op de taakuitoefening van de diensten is thans neergelegd bij twee instanties, de CTIVD en de TIB die onafhankelijk van elkaar opereren maar wel rechtseenheidoverleg voeren. Er bestaan derhalve verschillende vormen van 'toezicht' op uiteenlopende momenten, voorafgaand aan de inzet *(ex ante),* tijdens de inzet *(ex durante/ex nunc)* en na afloop van de inzet *(ex post)* van een bevoegdheid.[380]

De CTIVD is in het leven geroepen bij de vorige wijziging van de Wiv in 2002 en oefent sindsdien toezicht uit zowel tijdens de inzet van bevoegdheden door de diensten als achteraf.[381] De CTIVD doet onderzoek naar de uitvoering van de wet en brengt verslag uit in openbare rapporten en kan de betrokken ministers gevraagd en ongevraagd adviseren over haar conclusies (art. 112 en 113 Wiv 2017). De CTIVD bestaat sinds de inwerkingtreding van de Wiv 2017 uit twee afdelingen, te weten een afdeling toezicht en een afdeling klachtbehandeling (art. 97 lid 2 Wiv 2017). In het kader van het toezicht geeft de CTIVD een oordeel over de rechtmatigheid van het optreden van de diensten in een specifiek geval of dossier. De afdeling klachtbehandeling behandelt klachten over het handelen van de diensten en meldingen over mogelijke misstanden bij de diensten (art. 97 lid 4 Wiv 2017). Anders dan de oordelen over de rechtmatigheid in het kader van haar toezichtstaak, zijn de oordelen over klachten bindend.[382] In het navolgende richten wij ons

380 Er wordt in de praktijk een strikt onderscheid gemaakt tussen de toetsing en toezicht, waarbij de TIB wordt aangemerkt als toetsingscommissie en CTIVD de toezichthouder is, zo komt naar voren uit de interviews. Echter, de rechtmatigheidstoetsing van de TIB kan ook worden gezien als een vorm van toezicht, zo wordt ook tot uitdrukking gebracht in het schema van het toezichtstelsel in de MvT bij de Wiv 2017 (*Kamerstukken II* 2016/17, 34588, nr. 3 (MvT Wiv 2017), p. 69).

381 *Rapport Commissie Jones-Bos* 2020, p. 116.

382 Er is wel voor gepleit om de CTIVD bindende rechtmatigheidsoordelen te laten uitspreken, maar daar heeft de wetgever destijds bewust van afgezien, zie *Kamerstukken II* 2013/14, 33 820, nr. 2, p. 6. Over het algemeen worden de aanbevelingen van de CTIVD wel opgevolgd. Zie *Rapport Commissie Jones-Bos* 2020, p. 123. De Evaluatiecommissie 2017 acht een bindende toetsing niet passend, daar dan de commissie het laatste woord zou →

op de toezichtstaak van de CTIVD.[383] Ten aanzien van haar toezichtstaak beschikt de CTIVD over vergaande bevoegdheden, die zijn neergelegd in artikel 107 e.v. Wiv 2017. Zo heeft zij rechtstreekse toegang tot alle relevante informatie en systemen van de AIVD en MIVD, maar kan ook medewerkers van de diensten horen (al dan niet onder ede) die verplicht zijn hun medewerking te verlenen en antwoord te geven. Ook heeft de commissie de bevoegdheid deskundigen in te schakelen ten behoeve van de uitoefening van haar taken en kan zij bepaalde plaatsen betreden. Van belang is dat de commissie zelf bepaalt welke thema's zij onderzoekt en op welke wijze.[384] De CTIVD heeft zich volgens de evaluatiecommissie in de afgelopen jaren meer toegelegd op het houden van dynamisch toezicht (*ex durante*) waarbij het zoveel mogelijk real-time meekijkt met bepaalde handelingen.[385]

De TIB is ingevoerd met de inwerkingtreding van de Wiv 2017 op 1 mei 2018. Deze commissie is eveneens belast met een rechtmatigheidstoets, maar dat betreft een *ex ante*-toetsing in de autorisatiefase waarbij de rechtmatigheid van de toestemming van de minister voor de inzet van een bepaalde bijzondere bevoegdheid wordt getoetst voorafgaand aan de daadwerkelijke inzet van die bevoegdheid (die in art. 36 lid 1 Wiv 2017). Dat leidt tot een bindend oordeel. Indien de toetsingscommissie oordeelt dat de toestemming niet rechtmatig is verleend, dan vervalt de toestemming van rechtswege, zo valt te lezen in artikel 36 lid 3 Wiv 2017. De *ex ante*-toets wordt door de evaluatiecommissie gezien als een grote meerwaarde voor het toezichtstelsel.[386] Die meerwaarde is volgens de evaluatiecommissie onder meer gelegen in het feit dat de diensten door de toetsing de vorm en inhoud van de aanvragen voor het inzetten van bijzondere bevoegdheden naar een

hebben over de uitleg van wetsbepalingen en dit ook dialoog met de diensten zou kunnen schaden. *Rapport Commissie Jones-Bos* 2020, p. 124. De wetgever zit op dit punt echter op een ander spoor, zoals hierna nog duidelijk zal worden.

383 Notabene, binnen de Wiv wordt de toezichtstaak onderscheiden van de taak tot klachtbehandeling. Daar zijn ook andere afdelingen binnen de CTIVD mee belast. Dit is om te voorkomen dat 'commissieleden die in het kader van het rechtmatigheidstoezicht over een bepaalde kwestie hebben geoordeeld, over diezelfde kwestie tevens oordelen ingeval een klacht ter zake is ingediend' *Kamerstukken II* 2016/17, 34588, nr. 3 (MvT Wiv 2017), p. 179. Klachtbehandeling kan echter ook worden gezien als een toezichtsinstrument. Burgers kunnen tenslotte langs die weg een bindende uitspraak krijgen van de CTIVD en de minister is ook verplicht die op te volgen (MvT, p. 15). Zie in dit verband ook Toe Laer 2019, p. 734-738.

384 De onafhankelijkheid van de CTIVD blijkt onder meer uit de benoemingsprocedure en de financiering. Het budget is deel van de Rijksbegroting. De CTIVD valt ook niet onder het ministerie van BZK of Defensie maar onder het ministerie van Algemene Zaken.

385 *Rapport Commissie Jones-Bos* 2020, p. 118.

386 *Rapport Commissie Jones-Bos* 2020, p. 119.

hoger plan brengen.[387] Tevens speelt de TIB 'een belangrijke rol in het scherp houden van diensten in hun overwegingen om bijzondere bevoegdheden in te zetten'. De wetgever heeft er uitdrukkelijk voor gekozen deze toetsing bij een andere instantie dan de CTIVD te beleggen, omdat anders de autorisatie vooraf, het toezicht tijdens en achteraf en de klachtbehandeling in één hand zou zijn, hetgeen afbreuk zou doen aan de onafhankelijkheid van de toetsing.[388]

4.6.2 Controverse over het toezicht en de plannen van de wetgever

Mede naar aanleiding van de bevindingen en aanbevelingen van de Evaluatiecommissie Wiv 2017 is de nodige discussie ontstaan over de wijze waarop het toezicht op de diensten thans is ingericht. Volgens de Evaluatiecommissie 2017 heeft de wetgever de relatie tussen het ex-ante en ex-post toezicht niet goed doordacht, hetgeen heeft geleid tot spanningen in het stelsel. De commissie acht het niet gelukkig dat de TIB niet alleen een rol is toebedeeld bij de verwerving van gegevens hetgeen passend is bij de aard van een ex-ante toetsing (waarbij een *go/no-go*-beslissing zal moeten worden genomen), maar ook bij bepaalde bevoegdheden in de verwerkingsfase.[389] De commissie vindt de statische aard van de *ex ante*-toets niet goed passen bij de dynamische verwerkingsfase. Zij ziet derhalve uitsluitend een rol voor de TIB weggelegd in de autorisatiefase (voor de verzameling), maar niet in hetgeen daarop volgt.[390] Hoewel de commissie in algemene zin tevreden is over de structuur van het bestaande stelsel van toezicht, beveelt zij aan de regeling op dit punt aan te passen door de TIB alleen een rol toe te bedelen bij de verwervende bevoegdheden.[391] Daarbij past het volgens de commissie ook niet om voorwaarden aan een rechtmatigheidsoordeel te verbinden zoals dat thans in de praktijk wel gebeurt.[392]

Op de voorstellen van de Evaluatiecommissie Wiv 2017 zijn kritische reacties gevolgd. Die kritische reacties zijn onder meer afkomstig van de toezichthouders. Zo kan de TIB zich niet vinden in de aanbeveling om de toetsing van de TIB te beperken tot een statische *ex ante*-toets ten aanzien van het verwerven van

387 In die aanvragen moeten de diensten ingevolge het bepaalde in art. 26 Wiv 2017 aangeven waarom de inzet van de bijzondere bevoegdheid volgens de diensten voldoet aan de vereisten van proportionaliteit, subsidiariteit, noodzakelijkheid en gerichtheid.

388 *Kamerstukken II* 2016/17, 34 588, nr. 3, p. 234 (MvT) en *Kamerstukken II* 2016/17, 34 588, nr. 18, p. 47 (Nota naar aanleiding van het Verslag Wiv 2017). Zie ook *Rapport Commissie Jones-Bos* 2020, p. 116.

389 *Rapport Commissie Jones-Bos* 2020, p. 145.

390 *Rapport Commissie Jones-Bos* 2020, p. 129. De TIB denkt daar zelf anders over, zoals in de conclusie nog aan de orde zal komen.

391 Zie aanbeveling 44 van het *Rapport Commissie Jones-Bos* 2020.

392 *Rapport Commissie Jones-Bos* 2020, p. 145.

gegevens. De TIB vreest dat het verwordt tot stempelmachine,[393] terwijl de CTIVD graag ziet dat zij bindende oordelen kan geven en instrumenten krijgt toebedeeld om te handhaven bij onrechtmatige gegevensverwerkingen.[394] Tevens heeft de Algemene Rekenkamer zijn zorgen geuit over de administratieve lasten die de toetsingen meebrengen en wat voor effect die hebben op de taakuitoefening en slagkracht van de diensten.[395] Vanwege de uiteenlopende opvattingen over hoe het toezicht moet worden ingericht heeft de minister van BZK een commissie ingesteld om nader advies uit te brengen over een duurzaam stelsel van toezicht en toetsing op de inlichtingen- en veiligheidsdiensten, (mede) in het licht van de recente jurisprudentie van het EHRM.[396] Die commissie onder voorzitterschap van Bovend'Eert adviseert om de TIB om te vormen tot een rechterlijke instantie, waarbij het nieuwe RTIB (Rechtscollege Toetsing inzet Bevoegdheden) zich niet hoeft te beperken tot de verwerving van gegevens, maar ook de wijze van verwerking van gegevens in zijn toetsing kan betrekken.[397]

In het conceptvoorstel voor de Tijdelijke wet vaart de wetgever een deels andere koers. Indien de plannen in hun huidige vorm doorgang vinden, dan komt bindende toetsing die de TIB uitvoert ten aanzien van een aantal bevoegdheden waaronder het verkennen van OOG-data te vervallen voor die onderzoeken waarop de tijdelijke regeling van toepassing is.[398] Het toezicht van de CTIVD tijdens en na de inzet van een bevoegdheid zou vervolgens in de ontstane leemte moeten voorzien. De CTIVD krijgt in die gevallen de bevoegdheid om een bindend oordeel te geven.[399] Het idee is dat het *ex durante*-toezicht tijdens het uitoefenen van bepaalde bevoegdheden wordt geïntensiveerd. Tevens wordt er een mogelijkheid gecreëerd om beroep aan te tekenen bij de afdeling Bestuursrechtspraak van

393 S. Derxi & R. Wassens, *NRC Handelsblad* 7 maart 2021.

394 Zie de brief van de CTIVD aan de Evaluatiecommissie Wiv 2017 van 11 augustus 2020 waarin de CTIVD een reactie geeft op de wetsevaluatie, p. 8.

395 De toegenomen lastendruk ligt niet alleen aan de Wiv 2017 en de gebrekkige voorbereiding, maar ook aan de inrichting van de interne werkprocessen bij de diensten. Zie het rapport van de Algemene Rekenkamer, *Slagkracht AIVD en MIVD. De wet dwingt, de tijd dringt, de praktijk wringt,* Den Haag 2021. Zie over de controverses in het toezicht meer uitgebreid: Jansen 2021, p. 419-443.

396 Kamerbrief van 9 december 2021, kenmerk 2021-0000588756.

397 *Rapport Commissie-Bovend'Eert* 2022, p. 5. De evaluatiecommissie Wiv 2017 had ook nog geadviseerd om een mogelijkheid te creëren om in beroep te baan tegen beslissingen van de TIB bij de Afdeling bestuursrechtspraak van de Raad van State, maar dit voorstel wordt door de commissie Bovend'Eert als niet effectief en overbodig terzijde geschoven. Zij ziet meer heil in het creëren van een aanvullende voorziening tot het stellen van prejudiciële vragen over de uitleg van wettelijke regels.

398 Art. 9 Tijdelijke wet, dat een uitzondering creëert op het bepaalde in art. 36 lid 1 Wiv 2017.

399 Zie concept MvT Tijdelijke wet, p. 14 en 30.

de Raad van State tegen bepaalde beslissingen van de TIB en de nieuwe bindende bevoegdheid van de CTIVD.[400] Dit moet het probleem oplossen dat toezichthouders 'niet alleen in het laatste woord in een concrete casus hebben, maar ook wat betreft de uitleg van begrippen en criteria, en de wijze waarop zij hieraan toetsen', wat in de afgelopen jaren verschillende malen tot knelpunten heeft geleid. Hierbij krijgt de rechter alsnog een rol in het toezicht op diensten.

4.6.3 Reflectie

Het voorgaande maakt duidelijk dat er de nodige discussie is over de inrichting van het toezichtstelsel en de rollen van verschillende actoren daarbinnen. Die discussie over het toezicht kan niet worden losgezien van de normering zelf. Niet alleen is toezicht van belang om de gestelde normen te handhaven (vanuit de aanname dat van toezicht een belangrijke prikkel tot naleving van de regels zal uitgaan), maar het kan ook andersom werken. Het creëren van een goed toezichtsysteem inclusief klachtafhandeling biedt wellicht ook de mogelijkheid om de materie zelf iets 'losser' te regelen, meer vanuit de beginselen dan vanuit strikte regels en scherpe juridische onderscheidingen. Toezicht en normering kunnen in die zin ook worden gezien als complementair aan elkaar. De normering vooraf moet vanzelfsprekend voldoende helder zijn, zodat de betrokkenen weten onder welke omstandigheden bevoegdheden mogen worden ingezet, maar te veel regels en discussie over toepassingsvoorwaarden kunnen adequaat optreden belemmeren. Dat zal niet alleen voor inlichtingendiensten gelden, maar ook voor de politie. Waarborgen voor de burger kunnen echter mede worden gevonden in de wijze waarop toezicht wordt gehouden vanuit de gedachte dat langs die weg de zorgvuldigheid van de inzet gemonitord kan worden. Waar dan vervolgens de juiste balans ligt tussen enerzijds normering en toetsing vooraf en anderzijds toezicht tijdens en achteraf is niet in zijn algemeenheid op voorhand te bepalen. Het hangt in ieder geval mede af van het type bevoegdheid dat wordt ingezet en het soort informatie dat daarmee wordt verwerkt. De ervaringen met de Wiv 2017 maken in ieder geval duidelijk dat bij het dynamische proces van gegevensverwerking een statische *ex ante*-toetsing niet optimaal is. Dat is ook de reden dat de TIB soms ook voorwaarden stelt aan de gegevensverwerking bij de vraag of een bevoegdheid die primair strekt tot vergaring mag worden ingezet. Onder de nieuwe voorgestelde regeling koerst de wetgever duidelijk op het versterken van het *ex durante* en *ex post* toezicht door de CTIVD. Er wordt daarbij ook nagedacht over de vraag hoe een systeem van *ex durante*-toezicht dan precies moet worden ingericht. Een dergelijk systeem zou mogelijk ook van nut kunnen zijn in de strafvorderlijke context waarbij de politie gegevens die voor andere doeleinden zijn vergaard verder gaat verwerken.

400 Art. 14 Tijdelijke wet en MvT Tijdelijke wet, p. 32.

4.7 Conclusie

Hoewel inlichtingendiensten en opsporingsdiensten onder verschillende regimes opereren, vallen er duidelijk parallellen te trekken tussen het vergaren van informatie ten behoeve van de opsporing en het verzamelen van informatie ten behoeve van de inlichtingentaak. De inlichtingendiensten hebben evenwel aanmerkelijk meer ervaring met het verwerken van grote hoeveelheden gegevens. Dit kan worden gezien als een van hun kernactiviteiten. De normering in de Wiv is in de loop der jaren diverse malen aangepast aan de voortschrijdende techniek en jurisprudentie, maar nog niet naar ieders tevredenheid. Juist de problemen waartegen men in de praktijk aanloopt, werpen nader licht op zaken waarmee de wetgever bij de nadere normering in het kader van strafvorderlijke gegevensverwerking rekening kan houden.

Wat betreft de *systematiek van normering* kan worden geconstateerd dat hoewel alle verwerkingsbevoegdheden in één wet zijn neergelegd, er niettemin vragen kunnen rijzen over de verhouding tussen bevoegdheden. Het brede verwerkingsbegrip waaronder ook de verzameling wordt geschaard speelt daarbij parten. De Wiv 2017 maakt wel onderscheid tussen verzameling en verwerking in de systematiek, maar dat is niet strikt doorgevoerd. Dat komt ook doordat de wijze van verzameling tot op grote hoogte leidend is voor de eisen die worden gesteld aan de verdere verwerking van gegevens. Anders dan in het WvSv kent de verwerking van gegevens (los van de verzameling) een expliciete grondslag in de wet en is dit als zelfstandige bevoegdheid geformuleerd. Wat daarbij wel opvalt, is dat de verzameling op andere en striktere wijze is genormeerd dan de (verdere) verwerking. De verzameling is meer *rule based,* hetgeen vooral tot uitdrukking komt in het systeem van vereiste autorisaties, terwijl de verdere verwerking meer *principle based* is, waarbij voor de verdere verwerking het noodzakelijkheidsbeginsel en het doelbindingsbeginsel een belangrijk richtsnoer vormen.

Wanneer de *inhoud van de normering* nader in ogenschouw wordt genomen, dan blijkt allereerst vooral de koppeling van de normering aan de vergaring problematisch te zijn. De eisen aan de verwerking zijn grotendeels afhankelijk van de wijze waarop de informatie is vergaard en niet van het type informatie of het doel waarvoor die informatie wordt verwerkt. Dit wordt door een van de respondenten aangemerkt als een systeemfout in de Wiv 2017.[401] Het probleem doet zich vooral voor bij de verzameling van bulkgegevens. Anders dan politiediensten beschikken de diensten over een specifieke bulkinterceptiebevoegdheid; zij kunnen gegevens via de ether of via de kabel in bulk binnenhalen. Echter, ook gegevens die niet via deze specifieke interceptiebevoegdheid zijn verkregen vallen als

401 Respondent AIVD.

bulkgegevens te kwalificeren. Denk aan datasets die zijn vergaard met behulp van een grote hackoperatie en waarin zich ook allerlei gegevens van 'onschuldige' burgers bevinden. Voor de verdere verwerking van deze gegevens gelden echter andere eisen dan voor gegevens die zijn verkregen via de bulkinterceptiebevoegdheid, hetgeen naar de inhoud niet goed valt te rechtvaardigen nu het zwaartepunt van de privacy-inbreuk ligt bij de verdere verwerking. Daar ligt een duidelijk leerpunt voor de wetgever, namelijk om deze zaken tot op zekere hoogte los van elkaar te zien. Voorts valt er iets te leren van de Wiv 2017 voor wat betreft de toegang tot die gegevens. Binnen de Wiv is duidelijk sprake van een functiescheiding; niet iedereen heeft toegang tot die grote verzameling van gegevens. Daaromheen is een systeem van autorisaties gebouwd.

Voorts maken de ervaringen met de Wiv 2017 opnieuw duidelijk dat bij de normering en het introduceren van juridische begrippen en onderscheidingen goed moet worden gekeken naar de praktijk. De tekst van de wet maakt diverse juridische onderscheidingen, die niet (meer) goed aansluiten bij de technische werkelijkheid. Er wordt in dit verband wel gesproken van een *mismatch* tussen de juridische begrippen en de technische realiteit. Dat de juridische begrippen niet goed aansluiten is problematisch, nu daardoor allerlei discussies kunnen ontstaan over de inzet van bevoegdheden die enerzijds slagvaardig optreden in de weg kunnen staan en anderzijds de regeling minder voorzienbaar maken. Een voorbeeld van een dergelijke discussie is het vereiste van gerichtheid dat in de wet is geïntroduceerd naar aanleiding van de uitbreiding van de mogelijkheden tot bulkinterceptie. Het vereiste van gerichtheid sluit slecht aan bij de aard van de bevoegdheid, waar gegevens in bulk (en ongericht) worden binnengehaald. De wetgever wil voor het verkennen van de gegevens dat vereiste van gerichtheid – in ieder geval bij onderzoeken in het cyberdomein – dan ook loslaten.

Een ander voorbeeld is de geautomatiseerde data-analyse. Er bestaat verschil van inzicht over wanneer daarvan precies sprake is, terwijl dat juridisch wel van belang is omdat voor geautomatiseerde gegevensverwerking meer waarborgen in het leven zijn geroepen dan voor 'gewone' gegevensverwerking en voor de bevoegdheid van GDA bij gegevens uit onderzoeksopdrachtgerichte interceptie ter identificatie van personen of organisaties nog extra eisen gelden. Eén van de respondenten stelt dat pogingen om bepaalde zaken te definiëren met als doel een onderscheid te maken tussen wat wél als GDA moet worden gezien wat niet tot op zekere hoogte vruchteloos zijn gebleken.[402] Het verschil van inzicht gaat echter verder dan alleen de vraag hoe een wettelijke term moet worden uitgelegd. Opvattingen lopen ook uiteen over welke waarborgen nu eigenlijk moeten gelden en welke gezichtspunten daarin voor de normering leidend moeten zijn. De discussie over

402 Respondent AIVD.

de verschillende vormen van geautomatiseerde gegevensanalyse en wat in dit verband nu precies uit de jurisprudentie van het EHRM kan worden afgeleid is ook in de strafvorderlijke context hoogst relevant. De ervaringen met Wiv 2017 leren dat als dit niet helder is genormeerd, daarover in de praktijk veel discussie kan ontstaan.

Een ander leerpunt betreft *het toezicht*. Weliswaar zijn er de nodige verschillen van inzicht over de inrichting van het toezicht binnen de Wiv en is daar ook het laatste woord nog niet over gezegd, het is wel duidelijk dat de aard van het toezicht niet los kan worden gezien van het soort bevoegdheid dat wordt ingezet. Het dynamische proces van gegevensverwerking voor onderzoeksdoeleinden (of het versterken van de informatiepositie), laat zich in ieder geval minder goed vangen in harde regels en een statische *ex ante*-toets. Dat is ook een aspect waarmee men in het kader van strafvordering rekening dient te houden. Wellicht valt er ook voor de politie iets te leren van een nieuw te ontwerpen systeem van *ex durante*-toezicht. Op te merken valt dat het toezicht zoals dat thans is vormgegeven voor wat betreft gegevensverwerking in strafvorderlijke context wel mager afsteekt tegen het uitgebreide stelsel van toezicht in de Wiv 2017. Daar vallen verschillende verklaringen voor aan te wijzen. Zo wordt het meer uitgebreide stelsel van toezicht deels gerechtvaardigd door de meer ingrijpende bevoegdheden (zoals de interceptiebevoegdheid) van de diensten en het ontbreken van rechterlijke toetsing achteraf. Tegelijkertijd vraagt het verschuiven van een meer reactieve naar een meer proactieve wijze van inzet van bevoegdheden bij de politie wellicht ook om een andersoortig systeem van toezicht, zodat de rechten van burgers die - tegen hun wil en zonder dat zij betrokken zijn bij strafbare feiten - in dat proactieve onderzoek worden betrokken voldoende zijn gewaarborgd.

5 Een blik over de grens: gegevensverwerking voor strafvorderlijke doeleinden in België, Duitsland en Noorwegen

5.1 Inleiding

In dit hoofdstuk staat de volgende deelvraag centraal: *op welke manier is de verwerking van persoonsgegevens voor de opsporing geregeld in Duitsland, België en Noorwegen, in hoeverre wijkt deze regeling af van de huidige regeling in Nederland en welke lessen kan de wetgever trekken die relevant zijn voor de normering van de verwerking van persoonsgegevens voor de opsporing?* Gezien de reikwijdte van het onderzoek gaat het hier niet om een klassieke juridische rechtsvergelijking in de zin van een diepgravende studie van de rechtstelsels van de geselecteerde landen. De blik over de grens betreft een verkenning van de regelingen in het buitenland, met als doel het verkrijgen van inspiratie voor de wettelijke normering van onderzoek aan gegevens voor strafvorderlijke doeleinden.

Voor elk van de geselecteerde landen is gekeken naar een drietal ankerpunten dat tevens ter structurering van de onderstaande paragrafen is gebruikt. Ten eerste is gekeken naar het wettelijke systeem inzake de verwerking van gegevens voor opsporing. Welke wetten reguleren de verzameling en de verwerking van gegevens? Wordt op het niveau van wetgeving expliciet onderscheid gemaakt tussen vergaren en verwerken van gegevens en welke verklaringen zijn er voor de gemaakte wetssystematische keuzes te geven?

Ten tweede is aandacht besteed aan de inhoud van de normering van de vergaring en verwerking van gegevens voor de opsporing. Hoe wordt het beginsel van doelbinding uitgelegd? Zijn er voor de verwerking van bulkgegevens andere criteria ontwikkeld dan de gebruikelijke beginselen die hoe dan ook gelden voor het verwerken van gegevens? Hoe wordt doelafwijkend gebruik van gegevens uitgelegd en genormeerd? Welke grondslagen kent de wet voor het combineren van gegevens (als een vorm van doelafwijkend gebruik) voor het opsporen van strafbare feiten? Welke discussie vindt er thans plaats aangaande de verwerking van bulkgegevens in de opsporing? Welke problemen kunnen worden geïdentificeerd voor wat betreft de toepassing van het huidige normerende kader in de praktijk?

Ten derde is ook het toezichthoudend kader in kaart gebracht. Welke procedures en modaliteiten kent de wet- en regelgeving met betrekking tot het toezicht op verwerking van bulkgegevens? Welke bevoegdheden heeft de bevoegde autoriteit om bij niet-naleving op te treden? Welke procedures bestaan voor een onafhankelijke *ex post facto*-toetsing van de naleving van de regels inzake verwerking van bulkgegevens en welke bevoegdheden heeft de bevoegde autoriteit om gevallen van niet-naleving aan te pakken?

Bij de verslaglegging in dit hoofdstuk is ervoor gekozen steeds in te gaan op de voor Nederland relevante aspecten in de geselecteerde landen. Het navolgende bevat dus geen uitputtende beschrijving van het geldende recht ter zake de hierboven genoemde ankerpunten. Tevens worden de regelingen van de geselecteerde landen niet diepgaand met elkaar noch met de relevante in hoofdstuk 3 besproken EU-regelgeving vergeleken.

De opbouw van dit hoofdstuk is als volgt. In paragraaf 5.2 wordt eerst de keuze voor landen en de gehanteerde methodologie nader toegelicht. Vervolgens worden de resultaten aan de hand van de bovengenoemde driedelige structuur voor elk van de geselecteerde landen gepresenteerd (par. 5.3. België, par. 5.4. Duitsland en 5.5. Noorwegen). In paragraaf 5.6 volgt de conclusie.

5.2 Landenkeuze en methodologie

Voorafgaand aan de landenkeuze is een oriënterend onderzoek uitgevoerd. Door middel van openbare bronnen en relevante wet- en regelgeving is in kaart gebracht welke landen mogelijk interessant zouden kunnen zijn voor dit onderzoek. Bij dit oriënterende onderzoek is met name gekeken naar landen die de Richtlijn 2016/680 hebben geïmplementeerd. Ook in niet EU-landen bestaat aandacht voor gegevensverwerking in het kader van de opsporing, maar de Richtlijn 2016/680 kan worden beschouwd als het meest ontwikkelde instrument op dit terrein. Om deze reden zijn niet EU-landen niet in het oriënterende onderzoek betrokken.

Uit het oriënterende onderzoek kwam naar voren dat de meeste recente ontwikkelingen op het gebied van normering van verwerking van (bulk)gegevens in het kader van de opsporing het gevolg zijn van het (recent) implementeren van de Richtlijn 2016/680.[403] Met name op het terrein van digitalisering en

403 De deadline voor de implementatie van de Richtlijn 2016/680 was 6 mei 2018 (artikel 59 Richtlijn 2016/680). De Europese Commissie heeft Griekenland, Spanje en Duitsland op de vingers getikt vanwege het niet of onvolledig implementeren van de Richtlijn 2016/680.

technologisering ervaren andere landen met Nederland vergelijkbare knelpunten.[404] Over het algemeen hebben EU-landen de Richtlijn 2016/680 in (hoofdstukken van) specifieke nationale wetgeving geïmplementeerd.[405] Veel landen hebben de AVG en de Richtlijn 2016/680 in een gezamenlijke wet geïncorporeerd, waarbij de nationale wetteksten vaak vrij nauw bij de tekst van de Richtlijn 2016/680 aansluiten.[406]

De uiteindelijke selectie van landen is gemaakt op basis van de wens te kiezen voor landen die enerzijds goed zijn te vergelijken met Nederland, bijvoorbeeld doordat de opsporing goeddeels op dezelfde wijze is genormeerd, en anderzijds enige verschillen met betrekking tot de normering van gegevensverwerking voor opsporing ten opzichte van Nederland vertonen. In het bijzonder is gezocht naar verschillen in de wettelijke systematiek voor de normering van dataverwerking in de opsporing en het toezichthoudende kader. De voorselectie heeft geleid tot vijf landen die op één of meerdere onderdelen afwijken: België, Duitsland, Noorwegen, Verenigd Koninkrijk en Zwitserland. In deze landen is relevante wet- en regelgeving, literatuur en jurisprudentie nader onderzocht, waarna een definitieve landenselectie is gemaakt, bestaande uit België, Duitsland en Noorwegen.

Voor de eerste selectie van landen is gekozen omdat deze landen enerzijds veel overeenkomsten hebben met Nederland. De landen (op het Verenigd Koninkrijk na) zijn geworteld in een *civil law* traditie en kennen aldus een WvSv waarin op basis van het legaliteitsbeginsel de regeling inzake de opsporing is ontwikkeld. Anderzijds verschillen deze landen ook van Nederland. Zo is in België toezicht op de verwerking van gegevens niet neergelegd bij een algemene gegevensbeschermingsautoriteit, maar bij een orgaan dat specifiek is belast met toezicht op gegevensverwerking door de politie. Duitsland besteedt – anders dan Nederland – ook in het WvSv veel aandacht aan de bescherming van persoonsgegevens. Bovendien is in Duitsland een eigen doctrine ontwikkeld op het gebied van doelbinding. In Noorwegen is de verwerking van gegevens vrijwel geheel buiten het WvSv in een vrij nieuwe politionele gegevensbeschermingswet geregeld.

404 In dit kader onderstreept de European Data Protection Board (EDPB) de noodzaak om staten vanuit de EU nadere sturing te geven. Zie de bijdrage van de EDPB aan de evaluatie van de Richtlijn 2016/680. Beschikbaar via: https://edpb.europa.eu/system/files/2021-12/edpb_contribution_Richtlijn 2016/680_review_en.pdf.

405 Hudobnik 2020, p. 485-500. Op de website van de Europese Commissie kan een voorbeeld voor de implementatiewet van de Richtlijn 2016/680 worden geraadpleegd: https://ec.europa.eu/home-affairs/system/files/2019-12/bremen_model_law_20191023_en.pdf).

406 Dat is bijvoorbeeld in Frankrijk, Ierland, Letland, Oostenrijk, Verenigd Koninkrijk het geval.

In de definitieve selectie van landen zijn het Verenigd Koninkrijk en Zwitserland niet meegenomen. Uit nadere bestudering bleek dat het systeem van het Verenigd Koninkrijk zodanig afwijkend is van het Nederlandse, onder meer omdat de wet- en regelgeving op het gebied van de opsporing en gegevensverwerking zeer versnipperd is,[407] dat het heel moeilijk zou worden om voor Nederland bruikbare gezichtspunten te distilleren.[408] Voor wat betreft Zwitserland geldt dat hier geen opvallende relevante ontwikkelingen lijken plaatsvinden. Daar komt verder nog bij dat Zwitserland in veel opzichten overeenkomsten met Duitsland vertoont en daarom ook niet meteen een wezenlijk nieuw perspectief biedt op de wettelijke systematiek, de normering of het toezicht op het gebied van gegevensverwerking en de opsporing.

Ten behoeve van de rechtsvergelijkende blik over de grens is een juridische analyse uitgevoerd van de relevante wet- en regelgeving, is een (beperkte) literatuurstudie verricht en zijn met experts in de drie verschillende landen interviews gehouden. Voor de juridische analyse is met name gekeken naar de wettelijke kaders voor de normering van opsporingsbevoegdheden waarmee gegevens kunnen worden verzameld en het kader voor de normering van de verwerking van deze gegevens. Waar mogelijk zijn ook de jurisprudentie en de wetshistorische stukken geraadpleegd. Voor een beter begrip en een nadere duiding van de bevindingen uit de juridische analyse zijn ook relevante rechtswetenschappelijke literatuur en (beleids)rapportages geraadpleegd. De focus lag steeds op het verzamelen van de meest recente inzichten in de manier waarop in het desbetreffende land is omgegaan met de implementatie van de Richtlijn 2016/680, welke discussie dit heeft gegenereerd, en welke actuele vragen en debatten in de

407 Relevant zijn bijvoorbeeld de *Criminal Justice and Police Act 2001* (die toelaat dat politie materiaal dat niet van ander materiaal kan worden gescheiden, zoals digitale data, in beslag kan nemen); de *Criminal Procedure and Investigations Act 1996* (regelt hoe politie relevant materiaal moet vastleggen, bewaren en aan de aanklager ter beschikking stellen, maar heeft weinig aanpassingen die relevant zijn voor de verwerking van bulkdata ondergaan sinds 1996); de *Investigatory Powers Act 2016* bevat bepalingen over interceptie van communicatie); en bevat de Britse *Data Protection Act 2018* in deel 3 de implementatie van de Richtlijn 2016/680, maar verschaft geen zelfstandige grondslag op basis waarvan gegevens mogen worden verwerkt. Zie nader ook Information Commissioner's Office, *Guide to Law Enforcement Processing*.

408 Zo zijn alleen voor de inbeslagneming van en analyse van gegevens in een smartphone verschillende wetten van belang. Zie hierover uitgebreid het kritische rapport van het Information Commissioner's Office over de wijze waarop de Britse politie omgaat met het in beslag nemen van mobiele telefoons, *Mobile phone data extraction by police forces in Engeland and Wales*, 2020, p. 21-30, te raadplegen via: https://ico.org.uk/about-the-ico/what-we-do/mobile-phone-data-extraction-by-police-forces-in-england-and-wales/.

rechtswetenschappelijke literatuur recent naar voren worden gebracht. Deze focus lag ook ten grondslag aan de aanvullende interviews die in de laatste fase met landenexperts zijn afgenomen. Voor de selectie van de te interviewen personen was met name van belang dat deze blijk hebben gegeven (in het recente wetenschappelijke discours) van kennis van zowel het nationale strafprocesrecht en met name de verzameling van bulkgegevens, en ook thuis zijn in de gegevensbeschermingsrecht. Omdat vragen die ten grondslag liggen aan dit onderzoek van relatief recente datum zijn, blijkt het aantal academici dat zich op beide terreinen nadrukkelijk profileert relatief beperkt. Per land is dan ook getracht in elk geval te spreken met (1) een respondent uit de academische wereld die recent onderzoek heeft gedaan naar strafvorderlijke bevoegdheden voor gegevensverzameling; (2) een respondent uit de academische wereld die zich met name met (politiële) dataverwerking bezighoudt; en (3) een respondent die goed zicht heeft op de praktijk van gegevensverwerking door de politie. In de bijlage is een overzicht van de geïnterviewde personen opgenomen.

Voorafgaand aan de interviews hebben respondenten nadere informatie en een topiclist met de te bespreken onderwerpen ontvangen. De interviews met buitenlandse respondenten vonden plaats via videoverbinding. Aan de respondenten is voorafgaand aan het interview toestemming gevraagd voor het maken van een audio-opname van het gesprek met het oog op de uitwerking van een verslag ten behoeve van het datamanagementplan. Voorts is afgesproken dat het gespreksverslag na uitwerking aan de respondenten ter inzage zal worden verstrekt en dat voor het gebruik van citaten steeds expliciet toestemming zal worden gevraagd. De respondenten zijn verder ingelicht dat de informatie die zij verschaffen alsmede hun naam in een publiekelijk toegankelijk rapport zal worden opgenomen. In een aantal gevallen hebben respondenten ook (aanvullende) schriftelijke informatie met betrekking tot de relevante topics gegeven.

De interviews zijn semigestructureerd afgenomen, waarbij de vragen binnen de verschillende topics steeds enigszins aan de specifieke respondent zijn aangepast (gelet op de open vragen uit de juridische analyse en de literatuurstudie voor dat land; en op de kennis en positie van de respondent). Hierdoor was het aldus mogelijk om respondenten op hun specifieke kennis te bevragen met het oog op het verkrijgen van een zo volledig mogelijk overzicht. Globaal bevatte de topiclist per land een viertal onderwerpen waarover steeds specifieke nadere vragen werden gesteld: (1) wetssystematische keuzes en verklaringen (vergaring van bulkgegevens in de opsporing en de verwerking ervan, implementatie van de Richtlijn 2016/680); (2) de nadere normering van de verwerking van gegevens (grondslagen voor verwerking, de uitlegging en toepassing van het

doelbindingsbeginsel, doelafwijkend gebruik van gegevens); (3) de vormgeving van het toeziend kader voor de vergaring en verwerking van gegevens; en (4) de relevante recente ontwikkelingen op het niveau van wet- en regelgeving, in de rechtswetenschappelijke literatuur, knelpunten in de rechtspraktijk. Aan respondenten is voorts gevraagd om relevante (niet anders toegankelijke) publicaties te delen, wat velen ook hebben gedaan.

5.3 België

5.3.1 Systematiek wettelijk kader

België kent net als Nederland een WvSv met daarin allerlei bevoegden ter vergaring van gegevens. Hierbij moet worden gedacht aan het doorzoeken van informaticasystemen en databeslag,[409] (online) infiltratie,[410] inkijkoperatie in informaticasystemen[411] en hackbevoegdheden.[412] De regeling inzake de opsporingsbevoegdheden is vanwege allerlei digitale ontwikkelingen in 2016 herzien met de Wet Digitale Recherche.[413] Deze herziening heeft geleid tot een aantal nieuwe opsporingsbevoegdheden, zoals de online infiltratie en de openlijke en heimelijke

409 Artikel 39bis Belgisch WvSv heeft betrekking op het doorzoeken van een informaticasysteem, ook op afstand. Dit is vergelijkbaar met de Nederlandse smartphone-bevoegdheid en de netwerkzoeking.

410 Zie artikel 46sexies Belgisch WvSv.

411 Zie artikel 89ter Belgisch WvSv. Deze bevoegdheid is bedoeld om een private plaats te treden en daar zoekend rond te kijken. Deze bevoegdheid is dus niet bedoeld ter inbeslagneming. Dat geldt ook voor de digitale equivalent van de bevoegdheid. Tegelijkertijd laat deze bevoegdheid ook wel toe om gegevensdragers in beslag te nemen.

412 Artikel 90ter Belgisch WvSv heeft betrekking op het met een heimelijk oogmerk onderscheppen, kennis nemen van, doorzoeken en opnemen van niet voor het publiek toegankelijke communicatie of gegevens van een informaticasysteem of een deel ervan, of uitbreiden van het doorzoeken van een informatiesysteem of een deel daarvan, met technische hulpmiddelen. De hackbevoegdheden kunnen alleen worden ingezet in uitzonderlijke gevallen, als het onderzoek dit vereist, bij een ernstige aanwijzing van het bestaan van tevens een ernstig strafbaar feit. Voorts kan de maatregel alleen worden bevolen ten aanzien van communicatiemiddelen of informaticasystemen van personen op wie een verdenking rust of ten aanzien van de plaatsen waar de verdachte persoon vermoed wordt te vertoeven, dan wel ten aanzien van personen van wie op grond van precieze feiten vermoed wordt dat zij geregeld in verbinding staan met de verdachte.

413 Wet 25 december 2016 houdende diverse wijzigingen van het Wetboek van Strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken, BS 17 januari 2017, 2738.

informaticazoekingen.[414] Over onder meer deze bevoegdheden heeft het Grondwettelijk Hof zich in 2018 uitgelaten.[415] De belangrijkste conclusie is dat de herziening grotendeels grondwettig is. Anders dan in Nederland kent het Belgische WvSv in het geheel geen regels over het gebruik van in de opsporing verkregen gegevens.[416]

Voor de analyse van in de opsporing verkregen gegevens vormt de Wet Verwerking Persoonsgegevens en de Wet op het Politieambt het belangrijkste juridische kader. Deze wetten bevatten – evenals de Nederlandse Wpg – algemene normen over de wijze waarop met persoonsgegevens moet worden omgegaan, onder meer in het kader van de opsporing.

De Wet Verwerking Persoonsgegevens is een algemene gegevensverwerkingswet waarin zowel de AVG als de Richtlijn 2016/680 zijn geïmplementeerd. In het kader van dit onderzoek is vooral de tweede titel van de Wet Verwerking Persoonsgegevens van belang. Deze titel komt overeen met de Nederlandse Wpg. Zo bevat deze titel een aantal definities, de algemene beginselen op basis waarvan de verwerking moet geschieden en de rechten van betrokkenen (verdachte, dader, getuige) en de maatregelen die moeten worden getroffen om de gegevens te beveiligen. Ook beschrijft deze titel de instelling van een nieuw Controleorgaan op de politionele informatie. Op dit controleorgaan gaan wij in § 5.3.4 nader in.

De Wet op het Politieambt (Wpa) is de Belgische politiewet, vergelijkbaar met de Nederlandse politiewet. Deze wet regelt dan ook de taken en bevoegdheden van de Belgische politie. Voor wat betreft de politietaak wordt in België onderscheid gemaakt tussen enerzijds de bestuurlijke politie en anderzijds de gerechtelijke politie. De bestuurlijke politie houdt zich bezig met wat in Nederland de handhaving van de openbare orde wordt genoemd, terwijl de gerechtelijke politie zich vooral bezighoudt met de strafrechtelijke handhaving van de rechtsorde: het voorkomen en opsporen van strafbare feiten.[417] In de Wet op het Politieambt is ook aandacht besteed aan gegevensverwerking door de politie. Artikel 44/1 Wpa bevat een regeling inzake de verwerking van door zowel de gerechtelijke als de bestuurlijke politie verkregen gegevens. Hierin staat onder meer dat de Belgische politie ten behoeve van haar taken gegevens mag verwerken, dat zij bepaalde databanken

414 Zie hierover Yperman, Royer & Verbruggen 2019, p. 389-416 en het proefschrift van Conings (Conings 2017).

415 GwH 6 december 2018, nr. 174/2018, ECLI:BE:GHCC:2018:ARR.174.

416 Vgl. Royer 2020, p. 400. Een uitzondering vormt hier het DNA-onderzoek waarover het Belgische WvSv wel regels kent. Zie voorts Koops, Conings & Verbruggen 2016, p. 120-122.

417 Uit interviews met respondenten bleek dat het onderscheid in de praktijk steeds meer onder druk komt te staan. Zie ook Schuermans 2017, p. 717.

mag oprichten en dat zij de nodige beveiligingsmaatregelen moet treffen. De inhoud van deze bepalingen komt overeen met de Wpg.

België kent drie verschillende databanken: de Algemene Nationale Gegevensbank (ANG); de basisgegevensbanken (BGB's) en de bijzondere gegevensbanken (GBO). De ANG bevat zowel bestuurlijke als gerechtelijke informatie en is vooral bedoeld om personen te identificeren en om te voorkomen dat twee politiediensten aan hetzelfde onderzoek werken zonder elkaars medeweten.[418] In de BGB's worden gegevens opgeslagen voor de uitoefening van de aan de politie toebedeelde opdrachten en het gebruik van de daarin vervatte persoonsgegevens indien dat noodzakelijk is voor deze opdrachten. De gegevens in BGB's zijn dus in beginsel alleen raadpleegbaar voor de politiediensten die ze erin hebben gezet. In uitzonderlijke omstandigheden en voor bijzondere behoeften kan tot slot een GBO worden opgericht.[419] De wet maakt niet duidelijk wat een dergelijke GBO precies is.

5.3.2 Inhoud normering

5.3.2.1 Doelbinding

Voor wat betreft de regels inzake het gebruik van persoonsgegevens die in de opsporing zijn verkregen kent België weinig specifieke regels. De regels die in de Wet Verwerking Persoonsgegevens en de Wet op het Politieambt zijn te vinden, zijn sterk ingegeven door de Richtlijn 2016/680.[420] In het Belgische recht is dan ook geen uitgebreide doctrine ontwikkeld op het gebied van doelbinding.[421] Sterker nog, België kent maar één algemene bepaling op basis waarvan zowel de bestuurlijke als de gerechtelijke politie gegevens mag verwerken: artikel 44/1 Wpa. Deze bepaling luidt als volgt:

> *"§ 1. In het kader van de uitoefening van hun opdrachten, bedoeld in hoofdstuk III,, afdeling 1, en overeenkomstig de doeleinden omschreven in artikel 27 van de wet gegevensbescherming kunnen de politiediensten informatie en persoonsgegevens verwerken voor zover deze laatste toereikend, terzake dienend en niet overmatig van aard zijn in het licht van de doeleinden van bestuurlijke en van*

418 Schuermans 2017, p. 722.
419 Artikel 44/11/3 Wpa.
420 Winter e.a. 2020, p. 35.
421 Dit beeld wordt bevestigd door interviews die wij hebben gehouden met respondenten uit België.

> *gerechtelijke politie waarvoor ze verkregen worden en waarvoor ze later verwerkt worden."*

Op wettelijk niveau heeft de Belgische wetgever dus niet in aparte verwerkingsgrondslagen voorzien voor de verschillende doelen waarvoor de politiegegevens mag verwerken. De opdrachten van de Belgische politie zijn – kort gezegd – de handhaving van de openbare orde alsmede het verlenen van bijstand en de strafrechtelijke handhaving van de rechtsorde.[422] De handhaving van de openbare orde alsmede het verlenen van bijstand wordt uitgeoefend door de bestuurlijke politie en de handhaving van de rechtsorde wordt uitgeoefend door de gerechtelijke politie. De gerechtelijke politie verwerkt dus persoonsgegevens met als doel de opsporing van misdrijven, bewijsverzameling, het vatten van daders en terbeschikkingstelling aan de rechter. Omdat deze opdrachten vrij ruim zijn geformuleerd, lijkt artikel 44/1 Wpa dan ook nauwelijks grenzen te stellen aan welke gegevens de Belgische politie al dan niet mag verwerken. Op een andere plaats in de Wpa heeft de wetgever de mogelijkheden tot verwerking van persoonsgegevens echter wel verder ingeperkt. Artikel 44/5 Wpa somt immers voor zowel de bestuurlijke als de gerechtelijke politie nader op welke categorieën van gegevens kunnen worden verwerkt in de algemene gegevensbank of de basisgegevensbank. Opvallend aan deze bepaling is dat doelspecificatie hierin vooral heeft plaatsgevonden aan de hand van de personen over wie gegevens mogen worden verwerkt en niet zozeer – zoals in de Wpg gebruikelijk is –aan de hand van specifieke doelen binnen de taken van de politie.[423] Zo maakt artikel 44/5 Wpa bijvoorbeeld duidelijk dat de gerechtelijke politie gegevens mag verwerken over onder meer verdachten, veroordeelden, getuigen en slachtoffers.

5.3.2.2 Onderzoek van bulkgegevens in België

Het debat over de vergaring en verwerking van bulkgegevens is in België nog niet of nauwelijks op gang gekomen. De focus ligt op de normering van de vergaring in de wet, maar niet op het gebruik naderhand.[424] De eerste zaak waarin bulkhacking heeft plaatsgevonden is inmiddels wel voor de Belgische strafrechter

422 Zie nader artikel 14 en 15 Wet op het Politieambt. Artikel 14 ziet op de bestuurlijke politie en artikel 15 op de gerechtelijke politie.

423 In artikel 9 Wpg vindt doelspecificatie bijvoorbeeld vooral plaats aan de hand van het concrete doel van een opsporingsonderzoek.

424 Zo bevestigen ook de drie verschillende respondenten uit België in de interviews.

verschenen en heeft tot een veroordeling geleid.[425] Wel is er in België discussie gaande over de toelaatbaarheid van dataretentie (er ligt thans een nieuw wetsvoorstel) en in een recente uitspraak heeft het Hof van Cassatie nog geoordeeld dat telefoongegevens die door middel van dataretentie zijn verkregen niet uit het bewijs hoeven te worden geweerd.[426]

5.3.3 Toezicht

Anders dan in veel andere landen kent België een onafhankelijke toezichthouder op het gebied van gegevensverwerking die zich specifiek met de politie bezighoudt: het Controleorgaan op politionele informatie (COC).[427] Dit controleorgaan is in 2018 opgericht en is belast met toezicht op de politionele informatiehuishouding.[428] Voor 2018 bestond dit controleorgaan al wel, maar naar aanleiding van de Richtlijn 2016/680 zijn in 2018 de bevoegdheden van dit orgaan uitgebreid en is de titel van het orgaan aangepast.[429]

Dit controleorgaan heeft verschillende taken.[430] In het kader van het onderhavige onderzoek is in het bijzonder relevant dat de COC zowel reactief (naar aanleiding van een klacht) als proactief controle uitoefent op de verwerking van informatie en persoonsgegevens in de politionele gegevensbanken.[431] Bij de uitoefening van deze taak houdt het controleorgaan niet alleen rekening met het recht op privacy en persoonsgegevensbescherming, maar ook met de belangen van effectiviteit en efficiëntie. Het COC heeft dus een algemene toezichtsbevoegdheid op

425 https://www.vrt.be/vrtnws/nl/2022/03/25/eerste-veroordeling-in-sky-ecc-drugsdossier-ziekenhuismedewerks/#:~:text=Een%20voormalige%20ziekenhuismedewerkster%20uit%20Borgerhout,doorgespeeld%20aan%20het%20criminele%20milieu.&text=De%20vrouw%20werkte%20als%20administratief,van%20Ziekenhuisnetwerk%20Antwerpen%20(ZNA.

426 Zie in dit kader Hof van Cassatie van België, 29 maart 2022, P.22.0078.N/1, https://justitie.belgium.be/sites/default/files/P.22.0078.N-29032022-dataretentie.pdf.

427 Zie voor informatie https://www.controleorgaan.be/#. Zie hierover tevens kort het opiniestuk van Schuermans 2020, *Tijdschrift Privacy & Persoonsgegevens* 2020/3. In dit onderzoek is alleen dit specifieke toezichtsorgaan betrokken en is niet nader ingegaan op andere politionele toezichthouders zoals het Vast Comité van Toezicht op de politiediensten (beter bekend als: Comité P).

428 Artikel 71 WVP.

429 Voor 2018 werd de toezichthouder 'Controleorgaan op de politionele informatie' genoemd.

430 Zie nader over deze taken Berkmoes, *Controle op de politiediensten* 2022, C47/55. Het COC houdt bijvoorbeeld ook toezicht op toepassing van de AVG door de politie.

431 Zie nader § 5.3.1.

alle operationele en niet operationele (persoons)gegevensverwerkingen door de politie.[432]

Ter uitoefening van haar taken heeft het COC ruime bevoegdheden. Zo heeft het controleorgaan een onbeperkt recht op toegang tot alle informatie en gegevens van de politiediensten die het controleert, kan het ter plaatse onderzoek uitvoeren en heeft het toegang tot alle plaatsen waar persoonsgegevens worden verwerkt.[433] Overigens heeft de politie zelf ook een plicht om uit eigen beweging alle nuttige inlichtingen, instructies en andere interne documenten inzake het verwerken van gegevens aan het controleorgaan ter beschikking te stellen. Ook kan het orgaan mensen horen indien zij dat noodzakelijk acht.[434] Voorts heeft het COC een aantal vergaande sanctionerende bevoegdheden, die de AP in Nederland niet ter beschikking staan. Het controleorgaan kan onder meer politiediensten gelasten een verwerking in overeenstemming te brengen met de wet; een tijdelijke of definitieve verwerkingsbeperking opleggen of eisen dat politiediensten gegevens rectificeren.[435]

Over het functioneren van het COC is weinig bekend. Wel heeft Van Brakel zich recent kritisch uitgelaten over dit orgaan. Zij meent dat het COC mede vanwege een gebrek aan geld en capaciteit onvoldoende in staat is toezicht te houden op het politionele gebruik van nieuwe technologieën zoals *predictive policing*.[436]

5.4 DUITSLAND

5.4.1 Systematiek wettelijk kader

5.4.1.1 Overzicht relevante wetgeving

In Duitsland bestaat er uitgebreide wetgeving op het gebied van het gebruik van in de opsporing verkregen gegevens. Voor een goed begrip van deze wetgeving is

432 Zie voor een voorbeeld waarin het COC het gebruik van drones door de politie beoordeelt: DIO20009-1_RapportAdvies_COC_Drones_15.03.2022_N.pdf (controleorgaan. be) https://www.controleorgaan.be/files/DIO20009-1_RapportAdvies_COC_Drones_15.03.2022_N.pdf. En een ander voorbeeld waarin de COC het gebruik van de *Clearview* gezichtsherkenningstechnologie in België controleert: Rapport (controleorgaan.be) https://www.controleorgaan.be/files/DIO21006_Toezichtrapport_Clearview_N_00050443.pdf https://www.controleorgaan.be/files/DIO21006_Toezichtrapport_Clearview_N_00050443.pdf.

433 Artikel 244 Wvp.

434 Artikel 245 Wvp.

435 Artikel 247 Wvp.

436 Van Brakel 2020.

het belangrijk onderscheid te maken tussen de preventieve politietaak (*Gefahrabwehr*) en de repressieve (*Strafverfolgung*).[437] De preventieve politietaak bestaat onder meer uit het preventief bestrijden van strafbare feiten en wordt genormeerd in de politiewetten van de zestien afzonderlijke Bundesländer (deelstaten).[438] De repressieve politietaak ziet op de opsporing en vervolging van strafbare feiten nadat een strafbaar feit is gepleegd en is voornamelijk geregeld in het Duitse WvSv: *Strafprozessordnung* (StPO). De StPO geldt op bondsniveau. Het onderscheid tussen *Gefahrabwehr* en *Strafverfolgung* bepaalt aldus welk juridisch kader van toepassing is. Voorts dient te worden gewezen op de *Bundeskriminalamtgesetze* (BKAG), waarin de taken en bevoegdheden van de federale politie nader zijn geregeld. De federale politie beschikt – evenals de politie in de afzonderlijke Länder – over preventieve bevoegdheden, maar is alleen actief op federaal niveau. Het *Bundeskriminalamt* houdt zich vooral bezig met deelstaatoverstijgende criminaliteit, zoals terrorisme en mensenhandel.[439]

Naast deze bijzondere wetten die specifiek zien op de verschillende politionele autoriteiten kent Duitsland ook nog algemene gegevensverwerkingswetten, zowel op bonds- als op deelstaatniveau. Op bondsniveau geldt de *Bundesdatenschutzgesetz* (BDSG), waarin zowel de AVG als de Richtlijn 2016/680 zijn geïmplementeerd. Deze wet is vooral van belang voor de repressieve politietaak, zo volgt ook uit § 500 lid 1 StPO. De BDSG staat in een generalis verhouding tot de StPO: de BDSG is alleen van toepassing indien in de StPO geen bijzondere regeling is getroffen.[440] Voor wat betreft de preventieve politietaak geldt dat op deelstaatniveau vaak algemene gegevensverwerkingswetten zijn ontwikkeld, waarop kan worden teruggevallen als de politiewetten niets regelen.[441]

In het vervolg van dit hoofdstuk richten wij ons specifiek op de StPO, de BDSG en de BKAG. De wetgeving op het gebied van de Länder blijft aldus buiten beschouwing. Niet alleen verschilt deze wetgeving per deelstaat, ook verschilt deze wetgeving op het niveau van uitgangspunten niet fundamenteel van de BKAG.

437 Zie over dit onderscheid nader: Bleichrodt, Mevis & Volker 2011 p. 77-82.

438 Zie ter illustratie § 1 lid 1 van de *Polizeigesetze Nordrhein-Westfalen* waarin nader is gedefinieerd wat onder *Gefahrabwehr* moet worden verstaan.

439 Zie nader § 2 *Bundeskriminalamtgesetz*.

440 Singelnstein, *Münchener Kommentar zur StPO*, Auflage 2019, § 474, Rn. 6; BeckOK StPO/von Häfen 37, Auflage 2020, § 500, Rn. 5.

441 Singelnstein 2020, p. 639.

5.4.1.2 Keuzes inzake de verkrijging en verwerking van gegevens in het strafrecht

De wettelijke systematiek op het gebied van opsporingsonderzoek aan reeds verkregen gegevens is complex. Dat is in belangrijke mate het gevolg van de federale structuur en het onderscheid tussen *Gefahrabwehr* en *Strafverfolgung*. Niettemin laat de systematiek in Duitsland zien dat het niet zonder meer vanzelfsprekend is om de verwerking van gegevens buiten het WvSv te regelen.

De StPO bevat – in tegenstelling tot het Nederlandse WvSv - een algemene regeling over het verwerken van in de opsporing verkregen gegevens.[442] Boek 8 van de StPO geeft algemene regels over gegevensverwerking door - kort gezegd - de rechterlijke macht en het openbaar ministerie. De regeling in dit boek valt te vergelijken met de Nederlandse Wjsg. Dit boek regelt verschillende onderwerpen, zoals de doelen waarvoor gegevens mogen worden verwerkt, doelafwijkend gebruik, bewaartermijnen, het delen van gegevens met derden, beveiliging van opgeslagen gegevens en rechtsbescherming. De belangrijkste reden om dit onderwerp in StPO te regelen, is het in Duitsland ontwikkelde recht op informationele zelfbestemming.[443] Voor zover hier relevant houdt dit recht in – algemeen en kort gezegd – dat burgers de controle hebben over hun eigen persoonsgegevens. Dit recht is ontwikkeld als reactie op de risico's die gepaard gaan met het verwerken van persoonsgegevens. In wezen vormt het recht op informationele zelfbestemming een van de grondslagen van het huidige gegevensbeschermingsrecht. Veel normen op het gebied van persoonsgegevensbescherming in de StPO vloeien rechtstreeks voort uit het recht op informationele zelfbestemming.[444]

Naast deze algemene bepalingen kent de StPO ook een aantal bijzondere bepalingen die specifiek in het kader van een of meer bijzondere opsporingsbevoegdheden zijn ontwikkeld. Zo kent de StPO enkele bepalingen over het geautomatiseerd vergelijken van in de opsporing verkregen gegevens. Het gaat om *Rasterfahndung* (§ 98a-98b StPO) en het machinaal vergelijken van reeds vergaarde gegevens (§ 98c StPO).[445] "Rasterfahndung" is een methode waarbij de politie op basis van vooraf opgestelde profielen reeds vergaarde gegevens onderzoekt, met als

442 Boek 8 van de StPO.

443 De grondslag van het recht op informationele zelfbeschikking gelegen in artikel 2 lid 1 van het Duitse Grundgesetz ("*Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.*"). Dit recht is voor het eerst erkend in Bundesverfassungsgericht (BVerfG) 15 februari 1983, BvR 209/83.

444 Singelnstein, *Münchener Kommentar zur StPO*, Auflage 2019, § 474, Rn. 9.

445 Over *Rasterfahndung* heeft het *Bundesverfassungsgericht* ook een belangwekkende uitspraak gedaan. Zie BVerfG 4 april 2006 - 1 BvR 518/02.

doel om verdachten op het spoor te komen.[446] "Rasterfahndung" is een methode die als zodanig niet is genormeerd in het Nederlandse recht. In geval van § 98c StPO gaat het om het vergelijken of doorzoeken van gegevens die reeds bij de politie aanwezig zijn. In dit kader is van belang op te merken dat deze bepaling enkel kan worden gebruikt voor lichte inbreuken op grondrechten; de toepassing van gezichtsherkenning waarbij ook gegevens moeten worden vergeleken, is bijvoorbeeld niet toelaatbaar op grond van deze bepaling.[447] In Nederland is het vergelijken of doorzoeken van gegevens in de Wpg geregeld.

Hiernaast bevat het StPO nog een aantal bepalingen waarin specifiek eisen worden gesteld aan de wijze waarop in de opsporing verkregen gegevens (verder) kunnen worden gebruikt. Op de inhoud van deze bepalingen wordt hieronder nader ingegaan. Deze bepalingen kennen enige overeenkomsten met artikel 126dd in het Nederlandse WvSv, waarin voor een aantal opsporingsbevoegdheden is geregeld hoe gegevens in een andere strafzaak of jegens andere personen kunnen worden gebruikt.

Voor alles dat niet in StPO is geregeld, geldt de BDSG.[448] In § 45 e.v. BDSG zijn regels te vinden over verwerking van in de opsporing verkregen gegevens. Evenals de Nederlandse Wpg maakt deze wet eerst duidelijk wanneer de wet van toepassing is en worden enkele belangrijke definities gegeven.[449] De kern van deze regeling is neergelegd in 47 BDSG. Deze bepaling behelst de algemene beginselen inzake persoonsgegevensverwerking. Deze bepaling bevat geen bijzonderheden. Voor wat betreft de formulering van deze beginselen is goeddeels herhaald wat in de Richtlijn 2016/680 is opgenomen.[450]

Tot slot verdient hier de BKAG vermelding. Deze wet regelt onder meer de bevoegdheden van het *Bundeskriminalamt.* Ook bevat deze wet in § 12 en verder regels over de wijze waarop het *Bundeskriminalamt* gegevens mag verwerken. Op de inhoud van deze regels wordt hieronder nader ingegaan.

5.4.2 Inhoud normering

5.4.2.1 Doelbindingsbeginsel

In Duitsland is een uitgebreide doctrine ontwikkeld omtrent het doelbindingsbeginsel en de mogelijkheden tot doelafwijkend gebruik. Voor wat betreft de

446 MüKoStPO/Günther, 1, Auflage 2014, StPO § 98a Rn. 1.
447 BeckOK StPO/Gerhold, 43, Auflage 2022, StPO § 98c, Rn. 1.
448 Dit uitgangspunt is ook gecodificeerd in § 500 StPO.
449 § 45 en 46 BDSG.
450 Veel van deze beginselen vloeien in Duitsland ook al voort uit andere grondrechten, zoals het recht op informationele zelfbestemming. Zie Singelnstein 2020, p. 640.

verwerking van gegevens die in de opsporing (*Strafverfolgung*) zijn verkregen, zijn de StPO en de BDSG van belang.

In de BDSG is gecodificeerd wat het doelbindingbeginsel inhoudt, alsmede in welke gevallen en met inachtneming van welke eisen doelafwijkend gebruik van gegevens is toegestaan. § 47 lid 2 BDSG codificeert het doelbindingsbeginsel. Voor wat betreft de formulering van deze bepaling is aansluiting gezocht bij de Richtlijn 2016/680. Deze bepaling kent dan ook geen bijzonderheden. In § 49 BDSG is bepaald dat doelafwijkend gebruik van eerder verkregen gegevens mogelijk is, indien aan bepaalde voorwaarden is voldaan. Zo moet de doelafwijking worden voorzien van een wettelijke grondslag, moet dat andere doel genoemd zijn in § 45 BDSG en moet de doelafwijking proportioneel zijn. Ook § 49 BDSG kent geen bijzonderheden, nu deze bepaling vrijwel letterlijk herhaalt wat reeds in artikel 4 lid 2 Richtlijn 2016/680 staat. Wel bestaat er in de Duitse literatuur discussie over de uitleg die aan § 49 BDSG moet worden gegeven. Omdat voor de formulering van § 49 BDSG aansluiting is gezocht bij de Richtlijn 2016/680, is niet duidelijk of de in § 45 BDSG geformuleerde doelen reeds als doelspecificatie hebben te gelden of dat de politie binnen deze doelen een en ander nog verder moet specificeren.[451]

De BDSG is te beschouwen als een kaderwet. De wet schetst aldus waaraan moet zijn voldaan, maar bevat zelf geen grondslagen op basis waarvan gegevens kunnen worden verwerkt.[452] Deze specifieke grondslagen zijn voor wat betreft de opsporing in de StPO te vinden.

Conform het doelbindingsbeginsel in § 47 BDSG is in de StPO het uitgangspunt dat in de opsporing vergaarde gegevens alleen mogen worden gebruikt in de strafzaak waarvoor ze zijn vergaard.[453] Als de vergaarde gegevens voor andere doelen worden gebruikt, bijvoorbeeld in een andere strafzaak of in het kader van een andere taak zoals *Gefahrabwehr*, dan betekent dit dat opnieuw inbreuk wordt gemaakt op het grondrecht van informationele zelfbestemming. Deze inbreuk moet zelfstandig worden gerechtvaardigd, onder meer door een (specifieke) wettelijke grondslag.

Omdat in het Duitse recht al snel sprake is van doelafwijkend gebruik, zijn in de StPO verschillende grondslagen te vinden op basis waarvan in de opsporing verkregen gegevens voor andere doeleinden mogen worden gebruikt.[454] Voor

451 Heckmann/Scheurer, 13. Aufl. 2019, BDSG § 49 Rn. 5-8.

452 Vgl. ook met betrekking § 49 Gola/Heckmann/*Heckmann/Scheurer* BDSG, 13. Aufl. 2019, § 49 Rn. 12.

453 Singelnstein, *NStZ* 2020, p. 641.

454 Singelnstein, *NStZ* 2020, p. 641.

een goed begrip van deze bepalingen moet onderscheid worden gemaakt tussen enerzijds het vergaren van gegevens met bijzondere opsporingsbevoegdheden die in de regel (diep) ingrijpen in een of meer grondrechten en anderzijds het vergaren van gegevens met 'lichte' bevoegdheden die niet of nauwelijks ingrijpen in grondrechten. Bijzondere opsporingsbevoegdheden zijn in het Duitse strafprocesrecht bevoegdheden die alleen zijn toegestaan ter opsporing van bepaalde strafbare feiten die in de catalogus zijn opgenomen (*Katalogstraftaten*/ *Katalogtaten*).

Voor wat betreft de 'lichte' bevoegdheden geldt dat de verkregen gegevens weliswaar voor een specifiek doel worden verwerkt, maar dat doelafwijkend gebruik ruimschoots is toegestaan. De paragrafen 474 en 477 StPO zien bijvoorbeeld op het gebruik van gegevens in andere strafzaken dan waarin ze zijn verzameld en § 161 lid 1 alsmede 163 lid 1 StPO regelen het gebruik van gegevens in het strafproces die voor andere doelen, bijvoorbeeld de *Gefahrabwehr*, zijn verzameld. Deze bepalingen zijn algemeen en stellen dan ook niet of nauwelijks eisen aan de doelafwijking. Zo staat in § 474 en § 477 StPO - kort gezegd - geregeld dat de rechterlijke macht en het openbaar ministerie kennis mogen nemen van in de opsporing verkregen gegevens indien dat noodzakelijk is voor hun taakoefening.

Voor bijzondere opsporingsbevoegdheden ligt een en ander genuanceerder. Het uitgangspunt is hier dat gegevens die met deze bevoegdheden zijn verkregen in beginsel alleen mogen worden gebruikt voor het doel waarvoor de bevoegdheid is ingezet. Doelbinding wordt dus, met andere woorden, strikter uitgelegd als het gaat om bijzondere opsporingsbevoegdheden. De consequentie hiervan is dat doelafwijkend gebruik slechts in bepaalde gevallen is toegestaan. Op verschillende plekken in de StPO keert deze toets dan ook terug in het kader van verschillende bijzondere opsporingsbevoegdheden.[455] Ter illustratie wordt hier gewezen op § 479 lid 2, eerste volzin, StPO, waarin is bepaald dat gegevens die met bijzondere opsporingsbevoegdheden zijn verkregen alleen dan in andere strafzaken als bewijs mogen worden gebruikt als de ingezette opsporingsbevoegdheid ook in die andere strafzaak had mogen worden ingezet.[456] De hier beschreven toets, waarbij moet worden nagegaan of de bevoegdheid ook in de strafzaak waarin men gebruik wil maken van de gegevens mocht worden ingezet, staat beter bekend als *hypothetische Datenneuerhebung.* Deze toets is door het *Bundesverfassungsgericht*

455 Zie onder meer § 161 lid 3 StPO; § 100e lid 6 StPO alsmede § 479 lid 2, tweede volzin StPO.

456 Het antwoord op de vraag of de verkregen gegevens als startinformatie mogen worden gebruikt, wordt niet bepaald door § 479 lid 2, eerste volzin, StPO maar door de algemenere bepalingen in § 474 en 477 StPO. Zie daarover Singelnstein 2020, *NStZ* 2020, p. 642.

ontwikkeld en speelt in het kader van diep in het privéleven ingrijpende opsporingsbevoegdheden een belangrijke rol.[457]

Naast het StPO en de BDSG zijn ter *Gefahrabwehr* de politiewetten van de verschillende *Länder* en de BKAG van belang voor de normering van door de politie verkregen gegevens. In het vervolg van deze paragraaf wordt kort ingegaan op de wijze waarop invulling is gegeven aan het beginsel van doelbinding in de BKAG. In § 12 BKAG is geregeld op welke wijze het *Bundeskriminalamt* gegevens (verder) mag verwerken.

Het uitgangspunt is dat door het *Bundeskriminalamt* verzamelde gegevens mogen worden gebruikt voor de doelen waarvoor ze zijn verkregen, ter bescherming van dezelfde rechtsbelangen als waarvoor ze zijn verkregen of voor de vervolging en preventie van dezelfde strafbare feiten als waarvoor ze zijn verkregen.[458] Doelbinding wordt in dit geval dus niet zo streng uitgelegd dat gegevens alleen mogen worden gebruikt voor het doel waarvoor ze zijn verzameld. De gegevens mogen ook voor vergelijkbare doelen of ter preventie van vergelijkbare strafbare feiten worden gebruikt. Een en ander ligt anders voor de verdere verwerking van gegevens die met het afluisteren in een woning en hacken zijn vergaard. Hiervoor geldt dat verdere verwerking van met deze bevoegdheden verkregen gegevens alleen is toegestaan als dat noodzakelijk en in overeenstemming is met de voorwaarden voor het verkrijgen van gegevens.[459] Verdere verwerking van gegevens die met de hackbevoegdheid zijn verworven is bijvoorbeeld alleen toegestaan als er sprake is van gevaar voor het lichaam, leven of vrijheid van een persoon. In dit geval wordt doelbinding dus zeer streng uitgelegd. Als dit gevaar niet meer bestaat, mogen de gegevens niet meer verder worden verwerkt.

Voorts regelt § 12 lid 2 BKAG doelafwijkend gebruik. In deze bepaling keert de toets inzake *hypothetische Datenneuerhebung* terug. Bovendien gelden met betrekking tot het gebruik van gegevens die met afluisteren in een woning alsmede het hacken van een computer zijn verkregen weer verzwaarde eisen.

5.4.2.2 Verwerking van bulkdata in Duitsland

In Duitsland is net als in Nederland veel rechtspraak over het verder verwerken van de op een in Frankrijk gesitueerde EncroChat server verkregen gegevens. In

457 In § 100e lid 6 StPO waarin een regeling is getroffen voor het gebruik van gegevens die zijn verkregen met bijvoorbeeld hacken wordt deze toets ook aangelegd.

458 § 12 lid 1 BKAG.

459 Zie in dit verband ook de door het Bundesverfassungsgericht geformuleerde eisen: BVerfG 20 april 2016, ECLI:DE:BVerfG:2016:rs20160420.1bvr096609.

Duitsland heeft de hoogste rechter op het gebied van het strafrecht (*Bundesgerichtshof*) zich ook reeds uitgelaten over de rechtmatigheid van het gebruik van EncroChat-data voor bewijs.[460] Kort gezegd oordeelde het BGH dat de in Frankrijk verkregen gegevens in het Duitse strafprocesrecht mogen worden gebruikt, omdat de rechtmatigheid van het onderzoek in Frankrijk in beginsel moet worden erkend. Voorts is ook niet gebleken dat er sprake is van bewijsverkrijging in strijd met fundamentele rechten. De zaak kan nog wel aan het *Bundesverfassungsgericht* worden voorgelegd.

De argumentatie van het BGH, die ook in eerdere uitspraken van lagere rechters is te vinden, is niet zonder kritiek gebleven.[461] Singelnstein en Derin betogen bijvoorbeeld dat de vraag of de gegevens kunnen worden gebruikt in het Duitse strafprocesrecht moet worden beoordeeld aan de hand van de *hypothetische Datenneuerhebung* die onder meer in art. 100e lid 6 StPO is neergelegd. Op basis van deze toets moet de vraag worden gesteld of de methode die in Frankrijk is ingezet ook in de Duitse strafzaak waarin men het bewijs wil gebruiken ingezet had mogen worden. Singelnstein en Derin menen van niet, omdat het StPO grootschalige hackoperaties, waarbij veel personen subject van onderzoek worden, niet toestaat.

5.4.3 Toezicht

Op het gebied van toezicht kent Duitsland veel overeenkomsten met Nederland. Naast strafvorderlijke actoren (strafrechter, onderzoeksrechter) kent Duitsland verschillende gegevensbeschermingsautoriteiten die toezicht houden op de gegevensverwerking door politie en justitie.[462] Op de verwerking van gegevens door het *Bundeskriminalamt* houdt de algemene, federale gegevensbeschermingsautoriteit toezicht.[463] Als deze autoriteit overtredingen van de BKAG vaststelt, kan het passende maatregelen treffen zonder dat nader is geconcretiseerd wat hieronder moet worden verstaan. Voorts verplicht de BKAG – conform de Richtlijn 2016/680 – ertoe om een functionaris gegevensbescherming aan te stellen.[464]

460 BGH 25 maart 2022, ECLI:DE:BGH:2022:020322B5STR45.
461 Derin & Singelnstein 2021.
462 Op het niveau van de Länder bestaat ook een gegevensbeschermingsautoriteit.
463 § 69 BKAG.
464 § 70 BKAG.

5.5 NOORWEGEN

Noorwegen is weliswaar geen EU-lidstaat, maar heeft als 'Schengenland' de Richtlijn 2016/680 geïmplementeerd in de politiedatabankenwet (*Politiregisterloven*).[465]

5.5.1 Systematiek wettelijk kader

In Noorwegen is voor wat betreft de politie onderscheid gemaakt tussen de politie (*Politi- og lensmannsetaten*) die zich bezig houdt met het opsporen van strafbare feiten en de politieveiligheidsdienst (*Politiets sikkerhetstjeneste*) die zich specifiek richt op het voorkomen en onderzoeken van bepaalde specifieke strafbare feiten die de onafhankelijkheid van Noorwegen kunnen bedreigen, onrechtmatige afluisterpraktijken, proliferatie van wapens, politiek gemotiveerd geweld en terrorisme.[466] De politieveiligheidsdienst is dus veeleer te beschouwen als een inlichtingendienst, vergelijkbaar met de Nederlandse AIVD.[467] Belangrijk verschil is evenwel dat de politieveiligheidsdienst ook handhavende bevoegdheden heeft, terwijl de AIVD niet over dergelijke bevoegdheden beschikt. De tweedeling tussen de repressieve en preventieve politie keert ook terug in de Noorse wet. Voor de repressieve politietaken vormt het Noorse WvSv (*Straffeprosessloven*)[468] het belangrijkste kader en de preventieve politietaak is voornamelijk in de Noorse politiewet geregeld (*Politiloven*).[469] Zowel het Noorse WvSv als de Noorse Politiewet bevatten op een enkele uitzondering na enkel bevoegdheden ter vergaring van gegevens.[470] Artikel 216g *Straffeprosessloven* is bijvoorbeeld een uitzondering, nu hierin is bepaald dat opnamen en aantekeningen die tijdens het opnemen van communicatie

465 Lov om behandling av opplysninger i politiet og påtalemyndigheten (politiregisterloven), van 28 mei 2010, nr. 16, (voor het laatst aangepast op 21 juni 2019, nr. 50). Deze wet is beschikbaar in een Engelse versie, Act relating to the processing of data by the police and the prosecuting authority (the Police Databases Act). Beschikbaar via: https://lovdata.no/dokument/NLE/lov/2010-05-28-16.

466 Art. 17b *Politiloven*.

467 Zie hierover uitgebreid het proefschrift van Bruce 2021.

468 Lov om rettergangsmåten straffesaker (*Straffeprosessloven*), LOV-1981-05-22-25. Beschikbaar via: https://lovdata.no/dokument/NL/lov/1981-05-22-25?q=Straffeprosessloven.

469 Zie Regulation of the Criminal Investigational Responsibilities and Prosecutorial Competence of the Police Security Service (2007) and Guidelines by the Norwegian Director of Public Prosecutions on Criminal Investigations (1999).

470 Zie bijvoorbeeld ook de wetshistorische informatie over *Politiregisterloven*, Ot. Prp. Nr. 108 (2008-2009), hoofdstuk 9 (https://www.regjeringen.no/no/dokumenter/otprp-nr-108-2008-2009-/id572473/?ch=9#kap9-6), par. 9.6.4.1 waarin de minister stelt dat het Noorse WvSv niet is ontworpen met het oog op het normeren van de verwerking van gegevens zoals deze in latere privacywetgeving is geregeld.

('communication control') zijn gemaakt zo snel mogelijk moeten worden vernietigd in zoverre dat deze opnamen of aantekeningen niet van belang zijn voor de preventie op opsporing van strafbare feiten.

Voor de verwerking van gegevens vormt de politiedatabankenwet (*Politiregisterloven*) het belangrijkste juridische kader.[471] In deze wet is geregeld of, en zo ja, op welke wijze de Noorse politie gegevens mag verwerken. Deze wet bevat dus regels voor de reguliere politie alsmede de politieveiligheidsdienst.[472] Deze wet kent enige gelijkenis met de Nederlandse Wpg. Verschil is evenwel dat de wet niet van toepassing is op de verwerking van gegevens in verband met bestuurlijke activiteiten van de reguliere politie of civiele taken van de politiediensten (art. 3 *Politiregisterloven*).[473]

5.5.2 Inhoud normering

5.5.2.1 Politiedatabankenwet

De *Politiregisterloven* was oorspronkelijk gebaseerd op het Kaderbesluit 2008/977/JIS van de Raad van 27 november 2008 betreffende de bescherming van persoonsgegevens in verband met politiële samenwerking en justitiële samenwerking in strafzaken. Om de regels in overeenstemming te brengen met Richtlijn 2016/680, is de wet in 2017 licht gewijzigd.[474] Nadere regels betreffende de informatieverwerking bij de politie en justitie worden in het Reglement politieregister (*Politiregisterforskriften*) voorzien.[475]

De *Politiregisterloven* heeft het doel om enerzijds bij te dragen aan een effectieve taakuitoefening door politie en justitie en anderzijds de privacy en voorspelbaarheid van de verwerking van gegevens voor het individu te waarborgen

471 Police Register Act ("Politiregisterloven") van 28 mei 2010, nr. 16, (voor het laatst aangepast op 21 juni 2019, nr. 50).

472 Hoofdstuk 11 *Politiregisterloven*.

473 Bestuurlijke taken betreffen bijvoorbeeld paspoort-, wapen-, rijbewijs- en immigratiebeheerstaken en controle op beveiligingsactiviteiten en onder civiele taken worden taken begrepen die niet politietaken of bestuurlijke taken betreffen, zoals interne administratie en aanschaf van apparatuur en deurwaardersactiviteiten (zie bv. art. 9-5 Reglement politieregister). Op deze activiteiten van de politie zijn de Wet persoonsgegevens (Wet van 15 juni 2018 nr. 38) en de AVG (EU 2016/679) van toepassing. Zie ook het (vooralsnog beperkte) commentaar op de wet Karnov 2022.

474 Zie ook het commentaar op de wet Karnov 2022.

475 Forskrift om behandling av opplysninger i politiet og påtalemyndigheten (*Politiregisterforskriften*), FOR-2013-09-20-1097 (https://lovdata.no/dokument/SF/forskrift/2013-09-20-1097/*).

(art. 1 *Politiregisterloven*). Artikel 4 *Politiregisterloven* stipuleert dat gegevens mogen worden verwerkt voor de doelen waarvoor ze zijn vergaard alsmede andere politiedoeleinden, tenzij bij of krachtens de wet is bepaald dat het recht om gegevens te verwerken beperkt is of dat de gegevens mogen worden verwerkt voor andere doelen dan politiedoelen.[476] Onder politiedoeleinden verstaat de wet activiteiten van de politie ter bestrijding van criminaliteit, met inbegrip van opsporing en preventiemaatregelen, en de dienst en de hulpverleningsfuncties van de politie en het bijhouden van politielogboeken.[477] Bij de totstandkoming van de wet is gediscussieerd over de vraag hoe specifiek het doel van de verwerking van gegevens in de wet moet worden opgenomen. In het bijzonder was de vraag of de taak van de politie als één verwerkingsdoel is te bestempelen, of dat de afzonderlijke taken van de politie ook afzonderlijke verwerkingsdoelen vormen, zodat de politietaak uit meerdere verwerkingsdoelen bestaat. Het laatste uitgangspunt wordt gehanteerd, wat inhoudt dat de opsporing, preventie, rechtsordehandhaving, de dienstfunctie, de hulpfunctie en het bijhouden van dienstadministratie als afzonderlijke verwerkingsdoelen worden aangemerkt. Het gevolg van deze benadering is dat sprake is van doelafwijkend ('secundair') gebruik van gegevens wanneer gegevens voor een ander doel binnen deze opsomming worden gebruikt.[478]

Volgens het commentaar op artikel 4 *Politiregisterloven* biedt deze bepaling veel ruimte voor het vrij gebruiken van gegevens binnen de verschillende politiedoeleinden (*free flow of information*). Zo kunnen gegevens verkregen in het kader van misdaadbestrijding worden gebruikt voor administratieve politietaken.[479] Artikel 4 *Politiregisterloven* bevat zelf twee uitzonderingen op de hoofdregel: (1) indien de wet de verwerking van gegevens beperkt, of (2) indien de wet een doelafwijkend (in de zin dat gegevens voor niet-politiedoeleinden worden verwerkt) gebruik van gegevens juist toestaat. Artikel 4 dient in samenhang met artikel 5

476 Beperkingen zijn bijvoorbeeld te vinden in art. 5 lid 2 *Politiregisterloven* of art. 216i WvSv. Wat betreft de ruimte om gegevens voor andere doelen dan politiedoelen te verwerken verwijst de wet in art. 29, 30 en 31 zelf naar de mogelijkheid om gegevens die voor politiedoeleinden zijn verkregen te gebruiken voor administraties van politie, openbare lichamen of particulieren in hun belang. Tevens mogen gegevens met toestemming voor andere doeleinden worden gebruikt. Zie Peters, commentaar op artikel 4 *Politiregisterloven*.

477 Art. 2 onder 13 ("Police purposes: (a) the police's activities against crime, including investigation, preventive efforts and the activities of the uniformed service, and (b) the police's service and assistance functions and keeping of police logs.")

478 Zie de wetshistorische informatie over *Politiregisterloven*, Ot. Prp. Nr. 108 (2008-2009), (https://www.regjeringen.no/no/dokumenter/otprp-nr-108-2008-2009-/id572473/?ch=9#kap9-6), par. 9.2 (doelbinding).

479 Zie Peters, commentaar op artikel 4 PRA (http://www.rettsdata.no).

Politiregisterloven te worden gelezen. In artikel 5 *Politiregisterloven* is het noodzakelijkheidsbeginsel neergelegd.

Artikel 5 *Politiregisterloven* stelt voorop dat gegevensverwerking alleen mag plaatsvinden indien dit noodzakelijk is met het oog op de in artikel 4 *Politiregisterloven* neergelegde doeleinden. Hoewel het noodzakelijkheidsvereiste in de wet alleen aan het doel gekoppeld is, geldt de eis ingevolge artikel 4 *Politiregisterforskriften* voor alle onderdelen van een gegevensverwerking, inclusief de beoordeling welke informatie moet worden geregistreerd, welke personen toegang hebben tot de informatie en hoe lang de informatie moet worden opgeslagen. Wat noodzakelijk is, hangt af van een specifieke beoordeling in het concrete geval. Het noodzakelijkheidsbeginsel bevat een proportionaliteitstoetsing waarbij het doel van de gegevensverwerking, de aard van de gegevens, of de verwerking ernstige of minder ernstige criminaliteit betreft en het aantal personen dat toegang heeft tot gegevens relevant zijn.[480] Artikel 4 lid 3 van de *Politiregisterforskriften* bepaalt voorts dat wanneer *Politiregisterloven* of *Politiregisterforskriften* voorschrijven dat gegevensverwerking strikt noodzakelijk moet zijn, de verwerking alleen mag plaatsvinden wanneer deze de enige mogelijkheid is om het doel van de verwerking te bereiken of als er toestemming voor de verwerking voorhanden is. De eis van strikte noodzakelijkheid geldt bijvoorbeeld voor allerlei 'gevoelige' gegevens (art. 7 *Politiregisterloven*).

Voorts staat in artikel 5 *Politiregisterloven* hoe het noodzakelijkheidsbeginsel moet worden uitgelegd in het kader van opsporing. Artikel 5 lid 1 *Politiregisterloven* stelt dat de vraag naar noodzakelijkheid primair wordt bepaald door het Noorse WvSv. Het Noorse WvSv regelt aldus in welke gevallen, voor welke doelen en op welke wijze gegevens mogen worden verwerkt in het kader van de opsporing.[481] Daartoe voorziet het Noorse WvSv in verschillende opsporingsbevoegdheden. Verder bevat het Noorse WvSv een aantal bepalingen over het hergebruik of doelafwijkend gebruik van met opsporingsbevoegdheden verkregen gegevens. Zo is in artikel 216i *Straffeprosessloven* bepaald dat gegevens die door tappen zijn verkregen mogen worden gebruikt in een andere strafzaak dan de zaak waarin de bevoegdheid is ingezet. Ook indien de strafvorderlijke bevoegdheid niet zou kunnen worden toegepast in deze andere strafzaak is dit het geval, mits het gebruik niet disproportioneel is en het gebruik van de gegevens een substantiële bijdrage

480 Art. 4 lid 2 Politiregisterforskriften.

481 Zie nader ook de wetshistorische informatie over *Politiregisterloven*, Ot. Prp. Nr. 108 (2008-2009), (https://www.regjeringen.no/no/dokumenter/otprp-nr-108-2008-2009-/id572473/?ch=9#kap9-6), par. 9.3 (de eis van noodzakelijkheid).

levert aan de oplossing van de tweede zaak.[482] Naast deze specifieke bepalingen die zijn toegespitst op een of enkele bevoegdheden inzake doelafwijkend gebruik, bevat artikel 5 lid 2 *Politiregisterloven* een meer algemene regeling voor doelafwijkend gebruik. In deze bepaling is neergelegd dat gegevens die met bijzondere opsporingsbevoegdheden zijn verkregen ook mogen worden verwerkt buiten het kader van het onderzoek waarvoor de bevoegdheid is ingezet. Wel stelt de wet hieraan de voorwaarde dat alleen van bepaalde categorieën personen gegevens mogen worden verwerkt, te weten: (1) personen die in georganiseerd verband strafbare feiten begaan of van wie het vermoeden bestaat, op basis van objectieve redenen, dat zij strafbare feiten zullen begaan; (2) personen die een bijzondere band hebben met onder (1) genoemde personen, zoals familie, vrienden, collega's indien kan worden aangenomen dat de band van betekenis is voor het vermogen van de politie om toezicht te houden op de onder (1) genoemde activiteiten;[483] (3) personen die slachtoffer zijn van strafbare feiten of waarvan het aannemelijk is dat zij dat kunnen worden; of (4) informanten.[484] Hoewel deze lijst uitputtend is, is daarmee niet gezegd dat verwerking van gegevens van personen buiten deze vier categorieën niet is toegestaan op grond van toestemming.[485] Niettemin achtte de Noorse minister het aangewezen om met het oog op de voorzienbaarheid van de wettelijke

482 Zie ook Peters, commentaar bij 4 PRA (http://www.rettsdata.no).

483 Art. 47-4 *Politiregisterforskriften.*

484 Data may only be processed when this is necessary for such purposes as are mentioned in section 4. Moreover, the following limitations apply:
1) In an individual criminal case, data may be processed in accordance with the provisions of the Criminal Procedure Act.
2) The processing of personal data shall be permitted for the purpose of combating crime beyond the scope of the individual criminal case if the person in question
a) is associated with a group whose activities largely consist of committing criminal offences, or who may be assumed, on the basis of other objective grounds, to commit such offences. This applies even if the person is below the age of criminal responsibility or the personal conditions for criminal liability are otherwise not satisfied
b) has a special connection with such persons as are mentioned in (a),
c) has been, or is likely to be, the victim of a criminal offence, or
d) is an informant
d) also applies in criminal cases.
3) For such police purposes as are mentioned in section 2, sub-section 13(b), processing of data, including data relating to persons who present a special security risk, may extend beyond the purpose of the activity in order to ensure the safety of an individual.

485 Zie nader ook de wetshistorische informatie over *Politiregisterloven*, Ot. Prp. Nr. 108 (2008-2009), (https://www.regjeringen.no/no/dokumenter/otprp-nr-108-2008-2009-/id572473/?ch=9#kap9-6), par. 9.3.5.

regeling in de wet vast te leggen van welke personen gegevens kunnen worden verwerkt buiten het kader van een concreet opsporingsonderzoek.[486]
Artikel 6 *Politiregisterloven* bepaalt verder dat gegevens die worden verwerkt (1) adequaat en relevant voor het doel van verwerking moeten zijn; (2) accuraat en up-to-date moeten zijn en (3) niet langer dan noodzakelijk voor het doel mogen worden bewaard.

Interessant is voorts artikel 8 *Politiregisterloven*, dat een tijdsgebonden uitzondering bevat op het doelbindingsbeginsel, de eis van noodzakelijkheid en de eis van relevantie.[487] Gegevens die de politie ontvangt buiten de kaders van een concreet strafrechtelijk onderzoek kunnen ingevolge artikel 8 *Politiregisterloven* voor vier maanden worden verwerkt teneinde te bepalen of aan de eisen van doelbinding, noodzakelijkheid en relevantie wordt voldaan. Deze bepaling vormt een uitzondering op de kwaliteitseisen die de wet aan gegevens stelt.[488] De gegevens moeten zo snel mogelijk worden verwerkt om deze te verwijderen of om te verwerken op een wettelijke grondslag anders dan artikel 8 *Politiregisterloven.* De tijdlimiet van vier maanden is absoluut,[489] maar niet van toepassing op gegevensverwerking in individuele strafzaken.[490]

Artikel 8 is volgens de Noorse wetgever bedoeld om gegevens te verwerken, ondanks dat niet voldaan is aan de algemene voorwaarden voor de verwerking onder *Politiregisterloven*. Omdat een dergelijke verwerking van gegevens, met name buiten een individuele strafzaak, vanuit het oogpunt van privacybescherming "twijfelachtig" is, stelt de wet duidelijke grenzen aan deze verwerking.[491] Hoewel de politie op grond van deze bepaling in principe alle gegevens kan registreren, biedt artikel 8 volgens de wetgever geen 'open volmacht' om alle informatie te registreren die de politie mogelijk ontvangt. Wanneer duidelijk is dat gegevens niet van belang zijn voor het werk van de politie, mogen deze gegevens ook

486 Zie nader ook de wetshistorische informatie over *Politiregisterloven*, Ot. Prp. Nr. 108 (2008-2009), (https://www.regjeringen.no/no/dokumenter/otprp-nr-108-2008-2009-/id572473/?ch=9#kap9-6), par. 9.3.5.

487 Zie nader de wetshistorische informatie over *Politiregisterloven*, Ot. Prp. Nr. 108 (2008-2009), par. 9.6.2. Beschikbaar via: https://www.regjeringen.no/no/dokumenter/otprp-nr-108-2008-2009-/id572473/?ch=9#kap9-6.

488 Zie nader de wetshistorische informatie over *Politiregisterloven*, hoofdstuk 9.

489 Bij het bepalen van een geschikte tijdslimiet verwijst de Noorse wetgever naar de Nederlandse regeling. Zie nader de wetshistorische informatie over *Politiregisterloven*, par. 9.6.4.4.

490 Ingevolge art. 50 *Politiregisterloven* zullen gegevens niet langer dan noodzakelijk voor verwerking worden bewaard.

491 Zie de wetshistorische informatie over *Politiregisterloven*, par. 9.6.2.

491 Zie nader de wetshistorische informatie over *Politiregisterloven*, par. 9.6.4.2.

niet worden vastgelegd.[492] De bepaling is geschreven met het oog op door de politie 'ontvangen' gegevens, wat betekent dat de politie niet zelf actief dergelijke informatie kan vergaren, zoals het downloaden van grote hoeveelheden data via internet.[493] Met het oog op een technologie-neutrale formulering van de wettelijke bepaling heeft de wetgever niets geregeld over de wijze waarop de artikel 8 gegevens moeten worden opgeslagen. Gelet op de specificiteit van dergelijke gegevens, ging de wetgever ervanuit dat deze gegevens dan wel in aparte systemen, dan wel op een speciaal gemarkeerde wijze zullen worden opgeslagen.[494]

Hoofdstuk 3 van de *Politiregisterloven* bevat voorts de aanduiding van verschillende politiedatabanken. Zo ziet artikel 9 op de strafdatabank, artikel 10 op het politielogboek, artikel 11 op een intelligencedatabank, artikel 12 op een DNA-databank en artikel 13 op een databank voor vingerafdrukken en afbeeldingen. Andere databanken dan de in dit hoofdstuk specifiek genoemde databanken kunnen op basis van het ruime artikel 4 *Politiregisterloven* worden ontwikkeld.[495] Voordat een databank mag worden aangelegd, moet in lijn met artikel 14 *Politiregisterforskriften* een Koninklijke regeling worden getroffen.[496] Hoofdstuk 11 van de *Politiregisterforskriften* bevat de noodzakelijke nadere voorschriften met betrekking tot het doel, de rechtsgrond en verwerkingsverantwoordelijkheid en ook regels met betrekking tot de vraag welke informatie mag worden verwerkt, over toegang en openbaarmaking, informatieplicht en inzage, correctie, blokkering en verwijdering, informatiebeveiliging en interne controle. Artikel 14 lid 2 vermeldt dat de eis van nadere regels niet van toepassing is op "*the alignment of data from databases that are subject to the Police Databases Regulations if the processing follows the rules that apply to the source database.*" Deze bepaling maakt het mogelijk om gegevens uit verschillende databanken bij elkaar te voegen. Hieraan zijn geen nadere eisen gesteld, mits de databanken waaruit de te compileren gegevens afkomstig zijn aan de gestelde wettelijke voorschriften voldoen. Grenzen aan de omvang of de duur van de compilaties worden niet gesteld. Dit betekent dat vooral bepalingen over het doel, de eisen met betrekking tot verwijdering, openbaarmaking en toegangsbeperking van de bronregisters grenzen zullen stellen aan de verwerking van data in compilaties. Volgens het commentaar op artikel 14 *Politiregisterloven* laat deze bepaling ruimte voor de verwerking van data uit andere databanken dan op grond van

492 Zie nader de wetshistorische informatie over *Politiregisterloven*, par. 9.6.4.3.
493 Zie Peters, commentaar op artikel 8 *Politiregisterloven.*
494 Zie nader de wetshistorische informatie over *Politiregisterloven*, par. 9.6.4.5.
495 Sinds februari 2022 zijn er 19 centrale registers in de Wet politieregisters geautoriseerd. Zie Karnov 2022, opmerkingen bij hoofdstuk 3 *Politiregisterloven.*
496 Artikel 14 *Politiregisterloven.*

Politiregisterloven waartoe politie toegang heeft, zoals bestuursregisters. De eis geldt immers dat de verwerking de voorschriften van het bronregister moet volgen, niet voor data uit andere registers die niet in het reglement van de politieregisters zijn geregeld. De verwerking van dergelijke informatie wordt slechts beperkt door de doelbinding in artikel 4 *Politiregisterloven* (verwerking voor een politiedoel).[497]

5.5.2.2 Verwerking van (bulk)data in Noorwegen

Noorwegen is nog niet ingespeeld op het vergaren en verwerken van bulkdata. Zowel in het *Straffeprosessloven* als de *Politiregisterloven* is geen regelgeving te vinden waarin specifiek rekening is gehouden met het vergaren en verwerken van grote hoeveelheden gegevens.

Sinds de inwerkingtreding van het *Straffeprosessloven* in 1986 zijn er weinig fundamentele wijzigingen doorgevoerd.[498] Wel hebben vanwege technologische ontwikkelingen enkele veranderingen plaatsgevonden met betrekking tot bijzondere opsporingsbevoegdheden, maar vooralsnog zijn structurele wijzigingen om het wetboek te moderniseren en technologie-onafhankelijk te maken, blijven liggen.[499] Pogingen om tot modernisering van het WvSv te komen, zijn vooralsnog gestrand.[500] Respondenten stellen dat het huidige wetboek verouderd en gefragmenteerd is, en typeren het als een 'lappendeken'.

Voor de normering van de vergaring van (bulk)gegevens wordt aansluiting gezocht bij de bevoegdheden inzake inbeslagneming,[501] die nadien nader zijn aangevuld door de Noorse Hoge Raad. Meer recent ingevoerde artikelen hebben betrekking op doorzoeking van computersystemen (art. 199a) en de in 2017 ingevoerde bepalingen ten aanzien van onderzoek aan gegevens (*dataavlesing*) teneinde

497 Zie Peters, commentaar op artikel 14 *Politiregisterloven*.

498 Het *Straffeprosessloven* uit 1981 steunt sterk op de voorganger uit 1887.

499 Een speciaal opgestelde commissie onder voorzitterschap van Torgersen heeft een voorstel voor een nieuw *Straffeprosess loven* gedaan. Zie hierover een Engelstalige publicatie Torgensen 2016 en het rapport van de commissie zelf. Beschikbaar via: (https://www.regjeringen.no/no/dokumenter/nou-2016-24/id2517932/). De aandacht voor de technologische vernieuwingen met betrekking tot opsporingsbevoegdheden was echter zeer beperkt.

500 De voorstellen van de commissie Torgersen zijn vooralsnog blijven liggen.

501 Art. 192 en 200a *Straffeprosessloven* met betrekking tot doorzoeking ("opslagplaats" heeft tevens betrekking op systemen of toestellen waarop elektronische gegevens zijn opgeslagen) en art. 203 en 208a *Straffeprosessloven* betreffende inbeslagneming (waarbij onder het "object" van inbeslagneming tevens gegevens worden verstaan).

de problemen met encryptie van data het hoofd te bieden.[502] Ingevolge artikel 216o kan de rechter toestemming geven voor het uitlezen van niet-openbaar beschikbare informatie in computersystemen. Artikel 216p *Straffeprosessloven* specificeert de bevoegdheid voor het verrichten van het onderzoek, de wijze waarop de politie zich toegang tot gegevens kan verschaffen (inclusief een hackbevoegheid) en de waarborgen ten aanzien van bescherming van doorzochte systemen. Deze bepalingen beperken het onderzoek aan gegevens tot systemen die door verdachten worden of kunnen worden gebruikt. De Noorse wet voorziet vooralsnog niet in een met EncroChat-zaak vergelijkbare vergaring van bulkdata. Overigens is recent een onderzoek verricht waarin de huidige bevoegdheden voor doorzoeking- en inbeslagneming zijn geëvalueerd en er is een voorstel gedaan tot noodzakelijke wijzigingen met betrekking tot de vergaring van digitaal bewijs.[503]

Van gegevens die de politie in bulk tot haar beschikking krijgt, zoals via doorzoeking van computersystemen of smartphones, mogen alleen gegevens die relevant zijn voor verdenking waarop het doorzoekingsbevel betrekking heeft worden opgeslagen teneinde later ook aan de verdediging ter beschikking te worden gesteld met het oog op een contradictoir proces. In de praktijk houdt dit in dat in de fase van doorzoeking en inbeslagneming van de gegevensdrager alle gegevens worden gekopieerd en opgeslagen zonder een beoordeling van de relevantie van de data (oftewel, het relevantiecriterium wordt zeer breed uitgelegd).[504] In de daaropvolgende fase wordt de originele dataset geanalyseerd op de voor de zaak relevante gegevens. Daarbij heeft de Noorse Hoge Raad bepaald dat er pas sprake is van inbeslagneming van gegevens op het moment dat de relevante gegevens in het strafdossier worden opgeslagen. De Hoge Raad vergelijkt de doorzoeking van de originele dataset met een huiszoeking: in een huis kijkt de politie rond en ziet dan ook veel meer dan dat er uiteindelijk in beslag wordt genomen. Gegevens die geen bewijswaarde hebben mogen in beginsel niet worden verwerkt via de intelligence database van de politie. Gegevens met bewijswaarde die ook als intelligence relevant zijn, kunnen ook in de intelligence databank worden opgeslagen, onder voorwaarden van *Politiregisterloven*.[505] De originele dataset waarin vele voor een strafzaak niet relevante gegevens zich bevinden, wordt thans in een ander systeem opgeslagen (National Network for Digital Seizure) en er is thans geen

502 Art. 216o en 216p *Straffeprosessloven.*
503 Zie Sunde 2021. De auteur van dit rapport is in het kader van dit onderzoek geïnterviewd.
504 Sunde 2021.
505 Zie EU Project FORMOBILE questionnaire voor Noorwegen, 2021, p. 26. Beschikbaar op: https://www.timelex.eu/sites/default/files/2021-01/FORMOBILE%20Expert%20Questionnaire%20%2B%20Norway.pdf

interconnectiviteit met de intelligence database van de politie (Indicia). In een recent rapport stelt Inger Marie Sunde een nieuw wettelijk kader voor met betrekking tot doorzoeking, beveiliging en inbeslagname van digitale gegevens. In het bijzonder ontwikkelt zij een normerend kader voor de fase waarin de verzamelde gegevens worden geanalyseerd met het oog op het bepalen van de relevantie van deze gegevens.[506]

Hoewel aandacht voor de vergaring en verwerking van (bulk)gegevens lijkt toe te nemen, is vooralsnog onduidelijk of en wanneer de recente onderzoeksresultaten, zoals het rapport van Sunde, aandacht op wetgevend niveau zullen genereren.[507] In toenemende mate is er discussie over de verwerking van bulkgegevens en de wens om te komen tot nadere regulering. Recent heeft een voorstel voor de uitbreiding van de bevoegdheden van de Politieveiligheidsdienst met betrekking tot vergaring van bulkdata van publiek toegankelijke bronnen (zoals het internet) veel discussie gegenereerd. Het voorstel gaat niet zover dat vergelijkbare bevoegdheden aan de 'gewone' politie worden toegekend. Het voorstel ligt na een zeer kritische consultatieronde bij het Ministerie van Justitie en wordt thans herzien.[508]

5.5.3 Toezicht

Op het verwerken van gegevens door de politie houdt een gegevensbeschermingsautoriteit toezicht.[509] Deze autoriteit is vergelijkbaar met de Nederlandse AP. De gegevensbeschermingsautoriteit kan controle uitvoeren op de rechtmatigheid van gegevensbescherming op verzoek van een individu (art. 59 *Politiregisterloven*) en kan ingevolge artikel 60 *Politiregisterloven* verschillende handhavende bevoegdheden uitoefenen. De Noorse autoriteit mag in enkele nader omschreven gevallen gegevensverwerkingen stopzetten of bepaalde voorwaarden stellen bij de niet naleving waarbij de gegevensautoriteit een bestuurlijke boete kan opleggen. Tevens kan de autoriteit niet-bindende waarschuwingen afgeven.

Voorts houdt een speciaal door de Koning ingestelde controlecommissie toezicht op de manier waarop de politie en de vervolgende instantie omgaan met bevoegdheden uit hoofdstuk 16a van het Noorse WvSv dat interceptie van

506 Sunde 2021, p. 136-140.

507 Dit wordt ook bevestigd in de interviews.

508 Beschikbaar via: https://www.regjeringen.no/no/dokumenter/horing-endringer-i-politiloven-og-politiregisterloven-mv.-psts-etterretningsoppdrag-og-behandling-av-apent-tilgjengelig-informasjon.pdf/id2874615/.

509 Art. 58 *Politiregisterloven*. De politieveiligheidsdienst is onderworpen aan een ander regime van toezicht.

audiocommunicatie en andere controlebevoegdheden van communicatiesystemen reguleert (communicatiecontrole in art. 216a – 216k *Straffeprosessloven*). Artikel 216h *Straffeprosessloven* bepaalt dat de controlecommissie toezicht houdt op de behandeling van zaken op grond van het genoemde hoofdstuk / de genoemde hoofdstukken? en op grond van artikel 50 lid 3 van *Politiregisterloven*. De commissie heeft tevens toegang tot alle gegevens, documenten, geluidsopnamen over communicatiecontrole die de commissie in het kader van haar controlefunctie nodig acht en kan tevens betrokkenen horen waarbij een meewerkverplichting geldt ongeacht een geheimhoudingsplicht.[510]

5.6 Conclusie

Deze blik over de grens heeft diverse inzichten opgeleverd die helpen bij het nadenken over een geschikt kader inzake de verwerking van gegevens door de politie. Het eerste inzicht is dat in zowel België, Duitsland als Noorwegen onderscheid wordt gemaakt tussen de normering van opsporingsactiviteiten enerzijds en de omgang met persoonsgegevens anderzijds. In België en Noorwegen is de opsporing in een WvSv geregeld en is de omgang met persoonsgegevens in een met de Wpg vergelijkbare wet neergelegd. In Duitsland is weliswaar ervoor gekozen om in het Duitse StPO ook aandacht te besteden aan gegevensverwerking door het openbaar ministerie en de rechterlijke macht, maar ook hier zien we dat de normering van opsporingsactiviteiten in een andere titel van het StPO is neergelegd. De blik over de grens maakt dus duidelijk dat het niet per se voor de hand ligt om de omgang van persoonsgegevens ook in het WvSv te regelen. Voorts zien we in Duitsland en Noorwegen dat de wettelijke normering van opsporingsactiviteiten niet enkel de vergaring van gegevens regelt, maar waar noodzakelijk ook de verwerking van gegevens.

510 Art. 50 lid 3 *Politiregisterloven*: "Data obtained through interception of communications which has not been used in the case shall be restricted when the case has been decided by final and enforceable judgment or final decision not to prosecute. Restricted data may be used in the event of a petition for reopening of a court case, the resumption of a criminal investigation, or to protect the legitimate interests of a person charged. Data which is not lawful to retain pursuant to the Criminal Procedure Act 216 g shall be erased as soon as possible. The provision applies correspondingly to data obtained pursuant to the Criminal Procedure Act sections 216 m and 216 o, and to data obtained pursuant to the Criminal Procedure Act sections 202 a and 202 c insofar as appropriate. The King will make regulations containing more detailed provisions on the erasure and use of restricted data from interception of communications."

Het tweede inzicht is dat op verschillende manieren invulling kan worden gegeven aan het doelbindingsbeginsel en daarmee de mogelijkheden tot doelafwijkend gebruik. In Duitsland – waar op het gebied van doelbinding een uitgebreide doctrine bestaat – dient elke verdere verwerking van gegevens (waaronder ook doelafwijkend gebruik) op een wettelijke grondslag te berusten. Het nadeel hiervan is dat het Duitse recht tamelijk complex is. Wel valt hieruit te leren dat doelbinding niet steeds op dezelfde wijze hoeft te worden uitgelegd. In Duitsland is ervoor gekozen om doelbinding bij de toepassing van opsporingsmethoden waarmee diep kan worden ingegrepen in het persoonlijke leven, strikter uit te leggen dan in het geval dat met andere, minder ingrijpende bevoegdheden gegevens worden vergaard. In de praktijk betekent dit dat gegevens die via in de persoonlijke levenssfeer ingrijpende bevoegdheden zijn verkregen niet zomaar verder mogen worden verwerkt of voor andere doeleinden mogen worden gebruikt. In het algemeen geldt dat deze gegevens alleen verder mogen worden verwerkt of voor andere doelen mogen worden verwerkt, indien het gaat om vergelijkbare doelen.

Noorwegen laat deels een vergelijkbare benadering zien. In relatie tot opsporingsbevoegdheden wordt doelbinding streng uitgelegd. In de wet is nader bepaald in welke gevallen gegevens die met bijzondere opsporingsbevoegdheden zijn verkregen verder mogen worden verwerkt. Voor gegevens die niet met bijzondere opsporingsbevoegdheden zijn verkregen is ervoor gekozen om doelafwijking in beginsel toe te staan, tenzij de wet dat expliciet verbiedt. In deze gevallen krijgt doelbinding dus een minder strikte uitleg. Op deze wijze wordt het ook mogelijk gemaakt doelbinding niet steeds op dezelfde manier uit te leggen. Dit is een vereenvoudiging ten opzichte van de Nederlandse situatie, waarin voor elke vorm van doelafwijking een wettelijke grondslag is gecreëerd.

Een derde inzicht is tot slot dat toezicht niet vanzelfsprekend hoeft te worden neergelegd bij een gegevensbeschermingsautoriteit die ook toezicht houdt op naleving van de AVG. In België bestond reeds een toezichthouder die zich specifiek bezighield met toezicht op gegevensverwerking door de politie, maar naar aanleiding van de Richtlijn 2016/680 zijn de taken en bevoegdheden van dit orgaan herzien. Toezicht op het verwerken van reeds in de opsporing verkregen gegevens door een andere autoriteit dan de algemene gegevensbeschermingsautoriteit zou interessant kunnen zijn voor Nederland, omdat dan rekening kan worden gehouden met de specifiek strafvorderlijke context waarbinnen gegevens worden verzameld. Voorts kent Noorwegen een interessant figuur in de vorm van een toezichtscommissie die naleving van de uitoefening van enkele bijzondere opsporingsbevoegdheden controleert. Het voordeel van zo'n commissie is dat op structurele

basis toezicht wordt gehouden op de toepassing van bijzondere opsporingsbevoegdheden. De rechter krijgt slechts een specifieke zaak ter beoordeling voorgelegd.

6 Conclusie

6.1 Inleiding

Het vergaren van gegevens om strafbare feiten op te helderen vormt van oudsher een belangrijk onderdeel van het takenpakket van de politie. Voor de vergaring van gegevens kan de politie uiteenlopende opsporingsmethoden inzetten. De digitalisering van de maatschappij heeft de mogelijkheden tot het vergaren van gegevens aanzienlijk doen toenemen. In het kader van de lopende wetgevingsoperatie voor een nieuw WvSv is in wetenschappelijke en beleidskringen gediscussieerd over de vraag hoe de bevoegdheden tot het vergaren van gegevens wettelijk moeten worden genormeerd. De vergaring van deze gegevens maakt immers gemakkelijk inbreuk op het recht op privacy en als dat het geval is, moet hiervoor een wettelijke basis bestaan met voldoende waarborgen tegen misbruik.

Het thans voorliggende conceptvoorstel voor een nieuw WvSv bevat een aantal nieuwe bevoegdheden ter *vergaring* van gegevens. Een onderwerp dat binnen de strafvorderlijke context vooralsnog echter minder aandacht heeft gekregen, betreft de *verwerking* van gegevens. In de praktijk vergaren de opsporingsautoriteiten niet alleen gegevens, zij nemen deze gegevens ook regelmatig over in de politiesystemen om deze later al dan niet met behulp van geavanceerde *data science*-technieken te doorzoeken, te ordenen, te analyseren of in verband te brengen met andere gegevens. Handelingen met betrekking tot gegevens nadat ze zijn vergaard, worden binnen strafvordering niet meer gerekend tot de 'vergaring', maar aangeduid als de 'verwerking' van gegevens.

De behoefte aan het verwerken of analyseren van gegevens is de laatste jaren sterk toegenomen. Dat wordt op twee manieren zichtbaar. In de eerste plaats komen gegevens steeds vaker in bulk terecht bij de opsporingsautoriteiten, met als gevolg dat deze gegevens eerst moeten worden geanalyseerd en op relevantie moeten worden beoordeeld. Illustratief zijn recente zaken waarin de politie toegang heeft gekregen tot miljoenen versleutelde berichten van verschillende servers, zoals Ennetcom, EncroChat, Sky Global. Deze bulkdatasets worden pas relevant wanneer de politie deze gegevens nader analyseert, en in verband brengt met andere gegevens. Daarmee komt het zwaartepunt van de door de overheid gemaakte inbreuk op de privacy van burgers naast vergaring, ook nadrukkelijk bij de verdere

verwerking van die gegevens te liggen. Dit roept allerlei (nieuwe) vragen op over de nadere normering van onderzoek van (bulk)gegevens voor strafvorderlijke doeleinden. In de tweede plaats bestaat er bij de opsporingsautoriteiten steeds meer behoefte om gegevens die reeds in de politiesystemen zijn overgenomen nader te onderzoeken, met als doel om hieraan nieuwe informatie te ontlenen. Door gegevens met elkaar in verband te brengen en te verrijken, kan immers informatie worden gegenereerd die daarvoor als zodanig nog niet bekend was. Een voorbeeld is de voorziening 'Raffinaderij'.[511] Deze voorziening maakt het mogelijk om grote hoeveelheden politiegegevens, zoals informatie uit inbeslaggenomen telefoons of computers, in samenhang te analyseren met tapverslagen, data van peilbakens en gegevens die uit het openbare bronnen afkomstig zijn om zo tot nieuwe inzichten te komen.

Hoewel de verwerking van gegevens door de recente ontwikkelingen nadrukkelijker dan voorheen onderdeel is geworden van het politieke en wetenschappelijke debat, is de bestaande wettelijke regeling nog niet aangepast aan deze nieuwe realiteit, waarbij (1) informatie steeds vaker in bulk bij de politie terecht komt door inbeslagname of het hacken van geautomatiseerde werken of grote digitale-gegevensdragers en (2) in toenemende mate gegevens met elkaar worden gecombineerd gebruikmakende van geavanceerde technologie.[512] In de huidige regeling wordt de verwerking van gegevens voornamelijk in de Wpg genormeerd, terwijl de vergaring vooral in het WvSv is geregeld. De vraag is of beide activiteiten zich wel op deze wijze laten scheiden en wat de mogelijke implicaties zijn van een dergelijke separate normering. De Wpg is immers primair bedoeld om een zorgvuldige omgang met gegevens te waarborgen en niet om de opsporing te normeren. Van belang is verder de vraag welke waarborgen en eisen Europeesrechtelijke rechtsbronnen stellen aan het verwerken van gegevens voor strafvorderlijke doeleinden. De vragen op het gebied van de normering van gegevensverwerking zijn niet uniek voor de Nederlandse strafvorderlijke context. Daarom is ter inspiratie voor een nieuwe regeling ook gekeken naar de Wiv 2017 en relevante wet- en regelgeving in België, Duitsland en Noorwegen.

511 Zie voor een beschrijving van Raffinaderij: De Vries, 2017, p. 254-259. Deze voorziening is gestart als pilot maar wordt inmiddels landelijk toegepast door de politie, zo blijkt uit het jaarrapport van de politie over 2020. Beschikbaar via: https://www.politie.nl/binaries/content/assets/politie/onderwerpen/jaarverantwoording/2020/jaarverantwoording-politie-2020-inclusief-accountantsverklaring.

512 Zie onder meer *Rapport Commissie-Koops* 2018, p. 25-48; Schermer 2017, p. 207-216; Stevens e.a. 2021, p. 234-245; Dubelaar, Fedorova & Te Molder 2021, p. 53-81.

Naar aanleiding van het bovenstaande hebben in dit onderzoek drie vragen centraal gestaan:

1. Waar liggen de juridische knelpunten in het huidige wettelijke kader ter zake het doen van onderzoek aan vergaarde gegevens voor strafvorderlijke doeleinden?
2. Welke eisen en waarborgen stellen relevante Europeesrechtelijke juridische rechtsbronnen aan de normering van het verwerken van gegevens voor strafvorderlijke doeleinden?
3. Welke voor deze normering relevante gezichtspunten kunnen worden ontleend aan de Wiv 2017 en het recht in België, Duitsland en Noorwegen?

In de voorgaande hoofdstukken is het bestaande wettelijk kader inzake strafvorderlijke gegevensverwerking in kaart gebracht en daarbij zijn enkele knelpunten geïdentificeerd. Tevens zijn Europeesrechtelijke relevante rechtsnormen op het gebied van onderzoek aan gegevens in het kader van de opsporing geanalyseerd, en is onderzocht hoe de vergaring en verwerking van gegevens in de WIV 2017 is geregeld alsmede hoe België, Duitsland en Noorwegen de verwerking van gegevens die in de opsporing zijn verkregen hebben genormeerd. In dit slothoofdstuk wordt nader gereflecteerd op de betekenis van deze inzichten voor de inrichting van een nieuwe regeling ten aanzien van strafvorderlijke gegevensbescherming.

Dit hoofdstuk is als volgt opgebouwd. Allereerst worden bevindingen ten aanzien van het Europeesrechtelijke kader op het gebied van de verwerking van gegevens voor strafvorderlijke doeleinden uiteengezet (paragraaf 6.2). Bij de ontwikkeling van nieuwe regelgeving of aanpassing van de bestaande regeling op het gebied van de verwerking van gegevens voor strafvorderlijke doeleinden vormen de Europeesrechtelijke standaarden immers een normatief kader waaraan in elk geval moet zijn voldaan. Vervolgens volgt een nadere reflectie op de keuzes die nu voorliggen voor wat betreft de (her)inrichting van de wettelijke regeling (paragraaf 6.3). Deze reflectie vindt plaats aan de hand van de vier in hoofdstuk 2 geïdentificeerde aandachtpunten in het huidige juridische kader op het gebied van de verwerking van gegevens voor strafvorderlijke doeleinden. Dat betreft zowel de systematiek als de inhoud van de normering. In deze nadere reflectie worden ook inzichten betrokken die zijn opgedaan naar aanleiding van de bestudering van de Wiv 2017 en regelgeving in België, Duitsland en Noorwegen.

6.2 EUROPEESRECHTELIJK KADER VOOR NORMERING VAN ONDERZOEK AAN GEGEVENS VOOR STRAFVORDERLIJKE DOELEINDEN

Voor de normering van onderzoek aan in opsporing verkregen gegevens zijn drie Europese rechtsbronnen van belang: (1) de EU-Richtlijn 2016/680 betreffende de verwerking van persoonsgegevens voor opsporing en vervolging; (2) het recht op privacy zoals neergelegd in artikel 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) en de uitleg die het Europees Hof voor de Rechten van de Mens (EHRM) daaraan in zijn jurisprudentie heeft gegeven; en (3) artikelen 7 en 8 van het Handvest van de Grondrechten van de Europese Unie (HGEU) inzake het recht op privacy respectievelijk gegevensbescherming en de uitleg daarvan door het Hof van Justitie EU (HvJ EU). Uit het Europese recht kan een aantal belangrijke lessen worden getrokken over het recht op gegevensbescherming en het recht op privacy.

6.2.1 EU Richtlijn 2016/680

In de EU Richtlijn 2016/680 heeft de EU-wetgever een evenwicht gezocht tussen enerzijds de bescherming van gegevens en anderzijds de belangen van de opsporing en vervolging van strafbare feiten. De uitwerkingen van verschillende bepalingen aangaande toezicht en rechtsbescherming zijn daarom flexibeler dan van hun tegenhangers in de Europese Algemene Verordening Gegevensbescherming (AVG). De Richtlijn 2016/680 regelt uitsluitend de verwerking van gegevens in het kader van de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten, tenuitvoerlegging van straffen en bescherming tegen en voorkoming van gevaren voor de openbare veiligheid en is gericht op minimumharmonisatie van de regelgeving in verschillende EU-lidstaten. Daarmee biedt de Richtlijn 2016/680 lidstaten behoorlijk wat ruimte voor de nadere invulling in nationale wetgeving van belangrijke gegevensbeschermingsrechtelijke beginselen en uitgangspunten. In het derde hoofdstuk van het voorliggende rapport is nader stil gestaan bij de kernpunten uit de Richtlijn inzake de verwerking van gegevens voor strafvorderlijke doeleinden.

De voor dit onderzoek belangrijke vraag betreft de invulling van het doelbindingsbeginsel en de mogelijkheden tot doelafwijkend gebruik van gegevens. Immers, het nader analyseren van eerder in de opsporing verkregen gegevens kan ook voor andere doelen geschieden dan waarvoor de gegevens zijn verkregen. Ingevolgde artikel 4 lid 1 sub b Richtlijn 2016/680 mogen gegevens voor welbepaalde, uitdrukkelijk omschreven en legitieme doeleinden worden verzameld en op een

niet met die doeleinden onverenigbare wijze worden verwerkt. Hierin worden de twee componenten van het doelbindingsbeginsel tot uitdrukking gebracht, namelijk doelspecificatie en verenigbaar gebruik. Voor beide componenten geldt dat de Richtlijn 2016/680 maar in beperkte mate duidelijkheid verschaft over de precieze invulling daarvan. Met betrekking tot de doelspecificatie is verdedigbaar dat de in artikel 1 lid 1 Richtlijn 2016/680 ruim geformuleerde doelen (voorkoming, onderzoek, opsporing en vervolging van strafbare feiten, tenuitvoerlegging van straffen en bescherming van openbare veiligheid) afzonderlijk onvoldoende specifiek zijn om als verwerkingsdoeleinden te kunnen dienen. Als staten steeds gegevens zouden mogen verwerken voor algemene doeleinden, bijvoorbeeld de opsporing of vervolging van strafbare feiten, dan kan nauwelijks meer worden gesproken van een zinvolle invulling van het doelbindingsbeginsel. Ook worden dan hieraan verwante beginselen als dataminimalisatie en opslagbeperking uitgehold.

Met betrekking tot het aspect van verenigbaar gebruik is voorts van belang dat de Richtlijn 2016/680 de verenigbaarheidstoets sterk lijkt te relativeren door de in artikel 4 lid 2 Richtlijn gekozen formulering. Deze bepaling laat de verwerking van gegevens voor een 'ander doel' dan waarvoor de gegevens zijn vergaard toe, mits dit doelafwijkende gebruik bij wet is voorzien, noodzakelijk en proportioneel is in relatie tot het oorspronkelijke doel. De gekozen formulering leidt er evenwel toe dat vrij snel kan worden aangenomen dat sprake is van een 'ander' doel. Aangezien deze bepaling rept van 'ander doel' en niet van 'onverenigbaar doel', is de bepaling ook op verenigbare doelen van toepassing met als gevolg dat de verenigbaarheidstoets niet of nauwelijks meer een rol in de Richtlijn 2016/680 lijkt te spelen. In het licht van de ratio van het doelbindingsbeginsel – namelijk het bieden van voldoende rechtszekerheid voor betrokkenen en voorzienbaarheid van de wetgeving inzake gegevensverwerking – is verdedigbaar dat de verenigbaarheidstoets in artikel 4 lid 2 Richtlijn 2016/680 moet worden ingelezen en zodoende een rol speelt bij de door de bepaling vereiste proportionaliteitstoets.

Tot slot verplicht de richtlijn lidstaten tot het tot stand brengen van een toezichthoudend kader voor de gegevensverwerking door autoriteiten in de strafvorderlijke context. Ook hier laat de Richtlijn 2016/680 staten behoorlijk wat marge in de precieze inrichting van dit kader. De randvoorwaarden die de Richtlijn stelt zijn: (1) het toezicht dient zowel op intern als extern niveau plaats te vinden; (2) het toezicht moet 'onafhankelijk' zijn; en (3) de toezichthouders moeten voldoende bevoegdheden hebben om te kunnen spreken van 'effectief' toezicht.

6.2.2 *Het recht op privacy en gegevensbescherming*

Voor de invulling van het recht op privacy en gegevensbescherming zijn artikelen 8 EVRM en artikel 7 en artikel 8 HGEU en de invulling die daaraan wordt gegeven in de jurisprudentie van het EHRM respectievelijk het HvJ EU belangrijke Europese rechtsbronnen. Hoewel de twee kaders (EVRM en HGEU) afzonderlijk van elkaar tot ontwikkeling zijn gekomen en een eigen specificiteit kennen, zien wij dat het EHRM en het HvJ EU bij de uitleg van het recht op privacy en het recht op gegevensbescherming elkaar volgen en beïnvloeden. In het navolgende zal eerst kort het EHRM-kader worden geschetst, waarna het kader van het HvJ EU aan de orde zal komen.

Artikel 8 EVRM

De jurisprudentie van het EHRM aangaande artikel 8 EVRM leert ons dat zowel de vergaring, de opslag als de verdere verwerking van gegevens voor strafvorderlijke doeleinden afzonderlijk een inbreuk op de privacy met zich kan brengen en dat dergelijke handelingen zelfstandig met voldoende waarborgen dienen te zijn omkleed. Belangrijke waarborgen in dit verband zien op het specificeren van een doel en doelbinding, opslagbeperkingen en dataminimalisatie (irrelevante gegevens moeten zo snel mogelijk worden verwijderd) en effectief (rechterlijk) toezicht. Voorts kan ook het verwerken van gegevens voor doelen die afwijken van de doelen waarvoor gegevens in eerste instantie zijn vergaard, een inbreuk op het recht op privacy opleveren.

Voor de normering van de vergaring en verwerking van bulkgegevens heeft het EHRM een afzonderlijk kader ontwikkeld en in recente jurisprudentie verder verfijnd. Van belang is dat het EHRM verschillende fasen van gegevensverwerking onderscheidt, maar het gehele proces van gegevensverzameling en -verwerking in samenhang als één (doorlopend) proces beschouwt. Hoe verder de fase van verwerking gaat, des te groter de inbreuk op de privacy is, waardoor steeds meer waarborgen in het proces moeten worden ingebouwd. Deze benadering laat een bepaalde mate van flexibiliteit voor staten om het normerende kader zo vorm te geven dat rekening kan worden gehouden met de aard van de interceptie*tool*. Voor bulkinterceptie die ongericht van aard is, laat het EHRM lidstaten ruimte, in de zin dat bulkinterceptie niet hoeft te worden beperkt tot gevallen waarbij sprake is van een bepaalde mate van dreiging van de nationale veiligheid of bij het voorkomen van bepaalde strafbare feiten. Het EHRM stelt verder geen minimumeis wat betreft de groep personen ten aanzien van wie communicatie wordt

onderschept (zoals personen ten aanzien van wie een redelijke verdenking bestaat). Dit is anders dan bij de gerichte interceptie, waarbij interceptie moet plaatsvinden ten aanzien van vooraf omschreven strafbare feiten en/of groepen personen.

Bij de inrichting van hun wetgeving dienen staten de proportionaliteit en subsidiariteit van gegevensvergaring en -verwerking te borgen door te voorzien in duidelijke en voldoende afgebakende regelgeving omtrent de gronden, omstandigheden en procedure van gegevensverwerking en inzake de opslag van gegevens. In de wet moet worden opgenomen: (1) op basis van welke gronden bulkinterceptie is toegestaan; (2) onder welke omstandigheden communicatie mag worden onderschept; (3) wie bevoegd is tot het verlenen van autorisatie; (4) hoe de procedures voor het selecteren, analyseren en gebruiken van het onderschepte materiaal is geregeld; (5) welke voorzorgsmaatregelen in acht worden genomen bij het verstrekken van materiaal aan andere partijen; (6) wat de beperkingen van de duur van interceptie zijn; (7) hoe de opslag van het onderschepte materiaal en de omstandigheden waaronder dit materiaal moet worden verwijderd en vernietigd is geregeld; (8) welke procedures gelden voor het toezicht door een onafhankelijke instantie voorafgaand, tijdens en na het interceptieproces. Omdat het EHRM deze voorwaarden niet als minimumvoorwaarden formuleert, biedt dit kader staten ruimte om de normering afhankelijk te stellen van het type bevoegdheid en voor een afweging in specifieke omstandigheden van het geval. Met betrekking tot toezicht maakt het EHRM nadrukkelijk onderscheid tussen toezicht vooraf (autorisatie door een onafhankelijke autoriteit), toezicht tijdens de uitoefening van de bevoegdheid en toezicht achteraf (toegang tot de rechter of andere rechtsmiddelen). Het is aan staten om hier meer concrete vormen aan te geven. Hoewel het EHRM lidstaten niet dwingt tot een notificatieplicht in het kader van de inzet van surveillancebevoegdheden, moeten zij wel voorzien in een effectief rechtsmiddel wanneer burgers menen dat gegevens ten onrechte door autoriteiten zijn verwerkt.

Artikelen 7 en 8 HGEU

Het HvJ EU benadert het privacybegrip op een vergelijkbare manier als het EHRM en beoordeelt een inbreuk op de privacy niet alleen aan de hand van de aard van de gegevens, maar ook naar wat gegevens in combinatie met elkaar over het privéleven kunnen prijsgeven. Tevens neemt het HvJ EU tot uitgangspunt dat de opslag van gegevens op zichzelf reeds een inmenging vormt op het recht op privacy en gegevensbescherming, onafhankelijk van het verdere gebruik van die gegevens. Voor identificerende gegevens (zoals naam, voornaam en adres) geldt dat deze

minder privacygevoelig zijn dan IP-adressen of andere verkeers- en locatiegegevens. Voor deze laatste categorie geldt dat de bewaring van dergelijke gegevens op zichzelf en dus onafhankelijk van het eventuele latere gebruik van de gegevens, reeds een zware inmenging op het recht op privacy vormt.

In de specifieke context van dataretentie van verkeers- en locatiegegevens door telecommunicatieaanbieders en de toegang tot en het gebruik van deze gegevens door autoriteiten verplicht het HvJ EU de lidstaten om de twee onderscheiden fasen van verwerking - (1) opslag van en (2) toegang tot telecommunicatiegegevens - afzonderlijk te normeren. Omdat het HvJ EU het bewaren van en de toegang tot alle verkeers- en locatiegegevens (niet zijnde identificerende gegevens) als zeer privacygevoelig waardeert, vereist het HvJ EU direct een streng regime van waarborgen voor de toegang door autoriteiten tot de opgeslagen gegevens. Daarmee laat het HvJ EU geen ruimte om de normering van de opslagfase afhankelijk te stellen van de normering van de toegang tot (en het latere gebruik van) gegevens – en vice versa. Minder strenge normering van één fase kan dus niet worden gecompenseerd door strengere normering van de andere fase.

Met betrekking tot het verlenen van toegang van overheidsinstanties tot de bij de telecommunicatiediensten bewaarde verkeers- en locatiegegevens (niet zijnde slechts identificerende gegevens) stelt het HvJ EU een vijftal eisen: (1) de toegang tot gegevens is beperkt tot de doelstelling van de bestrijding van zware of ernstige criminaliteit waarbij geldt dat het HvJ EU ook steeds strikt hiërarchisch onderscheid maakt naar het doel waarvoor gegevens zijn bewaard (bijvoorbeeld nationale veiligheid of bestrijding zware of 'gewone' criminaliteit) en het doelafwijkende (secundaire) gebruik van gegevens is gekoppeld aan de hiërarchie in deze doelen, waarbij gegevens steeds kunnen worden verwerkt voor een hoger geplaatst doel, maar niet andersom; (2) de toegang mag alleen worden verleend indien het gaat om personen die ervan worden verdacht een ernstig strafbaar feit te plannen, te plegen of te hebben gepleegd of op een andere wijze betrokken zijn bij een dergelijk misdrijf; (3) de toegang dient voorafgaand te worden getoetst door een rechterlijke of bestuurlijke onafhankelijke autoriteit (een Officier van Justitie) is geen onafhankelijke autoriteit); (4) in beginsel geldt een notificatieverplichting; en (5) er moeten wettelijke regels met betrekking tot de beveiliging en bescherming van gegevens in het leven worden geroepen.

6.3 Reflectie op de systematiek en de inhoud van de normering

Uit onze analyse van het huidige wettelijke stelsel in het tweede hoofdstuk, kwam een viertal – met elkaar samenhangende – aandachtspunten naar voren waarmee rekening moet worden gehouden bij de normering van het onderzoeken van gegevens voor strafvorderlijke doeleinden. De navolgende reflectie richt zich op de keuzes inzake de inrichting van een nieuwe wettelijke regeling zoals die thans voorliggen, waarbij tevens relevante inzichten uit de vergelijking met de Wiv 2017 alsmede de blik over de grens worden betrokken. De reflectie wordt aan hand van de vier geïdentificeerde aandachtspunten vormgegeven, waarbij eerst zal worden stilgestaan bij de systematiek van normering (aandachtspunt 1) en vervolgens bij de inhoud van normering (aandachtspunten 2-4). Daarbij zij gezegd dat de systematiek en de inhoud met elkaar samenhangen.

6.3.1 Aandachtspunt 1: de systematiek van de normering

Het eerste aandachtspunt betreft de verhouding tussen het vergaren en verwerken van gegevens en de implicaties hiervan voor de wettelijke systematiek. De vergaring van gegevens is als gezegd voornamelijk in het WvSv geregeld en de verdere verwerking in de Wpg.[513] In bepaalde gevallen wordt echter wel in het WvSv aandacht besteed aan de verdere verwerking van gegevens. Zo bevat WvSv een aantal normen voor wat betreft de verdere verwerking (opslagbeperkingen en doelafwijkend gebruik) van gegevens die met bijzondere opsporingsbevoegdheden zijn verkregen. Dit onderzoek laat enerzijds zien dat de verzameling en verdere verwerking van gegevens zich niet altijd eenvoudig van elkaar laten scheiden; noch qua terminologie (aangezien verzamelen in de Wpg en AVG ook onder verwerken wordt begrepen), noch naar handeling (omdat verzameling en verdere verwerking in elkaar kunnen overlopen). Anderzijds maakt het onderzoek duidelijk dat een onderscheid tussen de verzameling en verdere verwerking van gegevens wel nuttig is met het oog op de normering. Het is echter onverstandig de normering van de verdere verwerking van gegevens geheel of grotendeels te koppelen aan de wijze van de vergaring van die gegevens, zo leren ook de bevindingen ten aanzien van het functioneren van de Wiv 2017.

Dat de vergaring en (verdere) verwerking van gegevens niet goed vallen te scheiden, kan worden geïllustreerd aan de hand van enkele voorbeelden. Als de bevoegdheid tot binnendringen in een geautomatiseerd werk wordt ingezet om

513 Dit onderscheid ligt ook besloten in de wettelijke kaders in België, Duitsland en Noorwegen.

gegevens over te nemen, zullen vervolgens vaak allerlei verwerkingshandelingen moeten worden verricht om deze ook daadwerkelijk ten behoeve de opsporing te kunnen gebruiken. De gegevens moeten in elk geval nader worden ontsloten en op relevantie worden beoordeeld. Hetzelfde geldt voor het overnemen van gegevens uit publiek toegankelijke bronnen of voor het overnemen van gegevens uit computers of smartphones. Doorgaans zal de politie nadat deze gegevens zijn overgenomen, allerlei vervolghandelingen moeten verrichten die strikt genomen tot de (verdere) verwerking van gegevens worden gerekend. De hier beschreven verwerkingshandelingen vinden weliswaar ná de vergaring van gegevens plaats, maar staan wel in nauw verband met de vergaring van de gegevens. De verwerkingshandelingen zijn immers gericht op het ontsluiten van relevante informatie. Voorts moet worden bedacht dat deze verwerkingshandelingen niet noodzakelijkerwijs ná de vergaring plaats hoeven te vinden. Ook vóórdat gegevens worden overgenomen, is het soms mogelijk om alvast een selectie te maken op relevantie van deze gegevens.

In de plannen inzake de modernisering van het WvSv wordt strikt onderscheid gemaakt tussen enerzijds de normering van de vergaring van gegevens langs de weg van het uitoefenen van strafvorderlijke bevoegdheden en anderzijds de (verdere) verwerking van gegevens. De aanvankelijke bedoeling van de wetgever was om alle bepalingen die in het huidige WvSv betrekking hebben op de verdere verwerking van gegevens, over te hevelen naar een nieuw te vormen gegevensverwerkingswet. Op deze gedachte is de wetgever – zoals in het eerste hoofdstuk aangegeven – teruggekomen in de zin dat er op korte termijn geen geheel nieuwe gegevensverwerkingswet tot stand zal komen. De vraag naar wat de aangewezen plek is om de verwerking van gegevens nader te normeren en in hoeverre een strikte scheiding tussen de vergaring en (verdere) verwerking voor de hand ligt, blijft echter onverminderd actueel.

De keuze in het gemoderniseerde WvSv om het onderscheid vergarenverwerken strikt door te voeren, valt in ieder geval niet goed te verdedigen. Zo regelen de huidige artikelen 125n lid 1 en 126cc lid 6 Sv die in het gemoderniseerde Wetboek zijn geschrapt, dat gegevens die tijdens de uitoefening van respectievelijk de doorzoeking ter vastlegging van gegevens en de hackbevoegd zijn verkregen, moeten worden vernietigd als zij niet relevant blijken te zijn voor het opsporingsonderzoek.[514] Deze vernietigingsverplichtingen beogen aldus te voorkomen dat

514 Zie over het schrappen van de bepalingen nader de Memorie van Toelichting (ambtelijke versie 2020), p. 228-229 waar enkel wordt toegelicht dat de bepalingen worden geschrapt en worden ondergebracht in een nieuw te vormen gegevensbeschermingswet.

gegevens die tijdens de uitoefening van opsporingsbevoegdheden worden vergaard, te gemakkelijk in de politiesystemen terechtkomen zonder dat hiervoor een goede reden bestaat. Strikt genomen zien deze bepalingen op de verwerking van gegevens, maar zonder nadere motivering is niet duidelijk waarom deze bepalingen niet in het WvSv thuishoren. De opsporing in het digitale domein zorgt er bovendien voor dat de processen van vergaring en verwerking steeds meer door elkaar lopen en daardoor geen logisch aanknopingspunt (meer) voor nadere normering opleveren.

Het voorgaande leert ons dat hoewel de begrippen vergaren en verwerken nuttig kunnen zijn om nader te duiden welke handelingen met gegevens worden verricht, dit onderscheid in theorie en praktijk niet steeds scherp kan worden gemaakt. Wij komen tot de conclusie dat het niet logisch is om de verhouding tussen het WvSv en de Wpg vorm te geven aan de hand van welke verwerkingshandeling – vergaring of verwerking – met gegevens wordt verricht. Het ligt veel meer voor de hand om te kijken in welke context en met welk doel verwerkingshandelingen worden verricht en aan de hand daarvan te bepalen in welke wet welk onderwerp thuishoort. Wij stellen dan ook voor om verwerkingshandelingen die zijn gericht op kennisvermeerdering én een strafvorderlijk doel dienen, in het WvSv onder te brengen en aldaar nader te normeren. De overige verwerkingshandelingen kunnen in de Wpg worden genormeerd. Zo wordt recht gedaan aan het uitgangspunt dat het WvSv de inzet en uitoefening van opsporingsmethoden normeert, zoals dat ook voortvloeit uit het strafvorderlijk legaliteitsbeginsel.[515] Tegelijkertijd wordt het WvSv niet belast met allerlei normen die niet of nauwelijks van belang zijn voor het strafproces en de daarin beschermde belangen.

Het voorgaande zou betekenen dat het conceptvoorstel voor het gemoderniseerde WvSv moet worden aangepast. Dat geldt in het bijzonder voor de normering van digitale opsporingsbevoegdheden, waarbij allerlei verwerkingshandelingen worden verricht.[516] In het conceptvoorstel voor het gemoderniseerde WvSv is thans vooral de vergaring en daarmee de voorwaarden voor de *inzet* van

515 Niet alle normering is ook daadwerkelijk in het WvSv neergelegd. Zo normeren de beginselen van behoorlijke procesorde ook de opsporing, maar deze beginselen zijn niet in WvSv gecodificeerd. In het gemoderniseerde WvSv gaat dat voor wat betreft de opsporing veranderen. Daarnaast worden ook niet alle opsporingshandelingen in het WvSv genormeerd. Als de betreffende opsporingshandelingen niet meer dan een beperkte inbreuk op mensenrechten maken of een risico vormen voor de integriteit van de opsporing kan art. 3 Polw. 2012 als grondslag worden gebruikt. Ook dit laatste gaat in het gemoderniseerde WvSv veranderen.

516 Onder digitale opsporingsbevoegdheden verstaan wij alle bevoegdheden die het mogelijk maken om onderzoekshandelingen te verrichten ten aanzien van computergegevens.

bevoegdheden genormeerd. Het conceptvoorstel regelt in het bijzonder in welke gevallen, voor welke doelen en met toestemming van welke autoriteit gegevens mogen worden vergaard.[517] Het gevolg hiervan is dat de vraag naar de normering van de *uitoefening* van opsporingsbevoegdheden en de verwerkingshandelingen die daarmee gepaard gaan, onderbelicht is gebleven. Gevolg is tevens dat veel normen die voor de uitoefening van digitale opsporingsbevoegdheden van belang zijn – zoals doelspecificatie, verenigbaar gebruik, verwijderings- en transparantieverplichtingen – (vooralsnog) niet in het gemoderniseerde WvSv terecht zijn gekomen, terwijl ze wel van belang zijn voor de opsporing. Weliswaar kent een aantal van de gegevensbeschermingsrechtelijke normen overlap met de algemene beginselen van proportionaliteit en subsidiariteit, maar deze algemene beginselen bieden weinig houvast bij het normeren van de uitoefening van digitale opsporingsbevoegdheden.[518] Voor onderzoek aan gegevens geldt immers dat deze activiteit nauwelijks wordt beperkt door feitelijke belemmeringen zoals mankracht.[519]

Gelet op het voorgaande stellen wij voor om in een algemene titel (vergelijkbaar met de huidige titel Vd) een algemeen normeringskader te ontwikkelen, waarin de belangrijkste normen met betrekking tot het doen van onderzoek aan gegevens in het kader van de opsporing worden neergelegd. Zo zou de wetgever onder meer het volgende tot uitdrukking kunnen brengen: (a) voorafgaand aan het uitvoeren van gegevensonderzoek moet het doel van dat onderzoek worden bepaald; (b) gegevens die redelijkerwijs niet relevant zijn voor dit doel moeten worden verwijderd c.q. ontoegankelijk worden gemaakt;[520] (c) in welke gevallen en met inachtneming van welke waarborgen gegevens voor een ander doel dan het doel van vergaring kunnen worden gebruikt (doelafwijkend gebruik); en (d) alsmede dat alle handelingen die in het kader van dit onderzoek worden verricht moeten worden gelogd.

Voorts is van belang dat naast het creëren van algemene richtinggevende beginselen voor onderzoek aan gegevens, er ook een expliciete grondslag wordt gecreëerd voor vormen van geautomatiseerde gegevensanalyse die een meer dan

517 Noemenswaardige uitzondering betreft het voorgestelde art. 2.7.39 nieuw Sv waarin onderzoek van gegevens in of overgenomen uit geautomatiseerde werken en digitale-gegevensdragers nader is genormeerd.

518 In het gemoderniseerde WvSv worden deze beginselen gecodificeerd. Zie art. 2.1.3 van het conceptvoorstel voor het gemoderniseerde WvSv.

519 Zie in gelijke zin *Rapport-Commissie Koops* 2018, p. 15.

520 Bij het vormgeven van deze relevantietoets en de daarmee samenhangende plicht om gegevens te verwijderen, moet de wetgever wel de belangen van de verdediging voldoende borgen.

beperkte inbreuk maken op de persoonlijke levenssfeer van betrokkenen.[521] Nu biedt artikel 11 Wpg daartoe een grondslag, maar het strafvorderlijk systeem zou aan consistentie winnen indien het WvSv hierin zelf zou voorzien, opnieuw vanuit de gedachte dat het niet logisch is om een principieel onderscheid te maken tussen het type verwerkingshandelingen, maar veeleer moet worden gekeken in welke context en met welk doel verwerkingshandelingen worden verricht. Wij bevelen dan ook aan dat in het nieuw te creëren algemene kader voor onderzoek aan gegevens er een expliciete grondslag met bijbehorende waarborgen wordt gecreëerd voor de meer dan beperkt inbreukmakende vormen van geautomatiseerde gegevensverwerking.

6.3.2 Aandachtspunt 2: normering van onderzoek aan bulkgegevens

Het tweede aandachtspunt betreft het onderzoek aan bulkgegevens die met (heimelijke) opsporingsbevoegdheden zijn verkregen. In zowel het huidige WvSv als het conceptvoorstel voor een nieuw WvSv is het onderzoek van de in bulk verkregen gegevens niet expliciet genormeerd. De bevoegdheid tot vergaring impliceert dan ook dat gegevens verder mogen worden verwerkt, onder meer door te onderzoeken op wie de gegevens betrekking hebben en wat de gegevens inhouden. Het uitgangspunt inhoudende dat de bevoegdheid tot vergaring ook kennisneming van de gegevens betekent, lijkt in de context van bulkgegevens niet goed verdedigbaar. Bulkgegevens zijn immers te beschouwen als een gegevensverzameling waarvan het merendeel betrekking heeft op personen die geen onderwerp van onderzoek zijn en dat ook nooit zullen worden.[522] Het verkrijgen van bulkgegevens is dus vanuit het oogpunt van het recht op privacy gevoeliger dan het verkrijgen van gegevens die wel te relateren zijn aan een of meer personen die reeds onderwerp van onderzoek zijn. Met het verkrijgen van bulkgegevens komen namelijk gegevens over veel personen in de systemen van de politie te staan zonder dat daartoe voor elk van deze personen een legitieme reden bestaat.

Vanwege de gebrekkige normering in het huidige WvSv wordt in de rechtspraktijk tamelijk *ad-hoc* naar oplossingen gezocht om toch enige grenzen te stellen aan het onderzoek van bulkgegevens. Zo is in recente jurisprudentie waarin

521 Wij beperken ons tot inbreuken die meer dan een beperkte (dat wil zeggen: stelselmatige) inbreuk maken op de persoonlijke levenssfeer nu voor beperkte inbreuken op de persoonlijke levenssfeer geen expliciet wettelijke grondslag is vereist, dat thans nog zijn basis vindt in art. 3 Politiewet. De algemene strafvorderlijke beginselen van proportionaliteit en subsidiariteit zijn daar wel op van toepassing.

522 Zie hoofdstuk 2, § 4.2.

de politie bulkgegevens heeft verkregen "ten overvloede" (zonder dat dit wettelijk is verplicht) een rechter-commissaris ingeschakeld die vervolgens eisen heeft gesteld aan de wijze waarop de gegevens onderzocht mogen worden.[523] Vanwege het toenemende belang van bulkgegevens is het belangrijk dat de wetgever het onderzoek van bulkgegevens in het WvSv nader normeert. De vraag is nu hoe de wetgever dat zou kunnen doen.

De eerste manier waarop de wetgever dat zou kunnen doen, sluit nauw aan bij de wijze waarop de strafrechtspraktijk tot een oplossing is gekomen. De wetgever zou immers ervoor kunnen kiezen om de waarborgen te versterken in de bestaande opsporingsbevoegdheden waarmee bulkgegevens kunnen worden vergaard.[524] Denkbaar is bijvoorbeeld dat in de hackbevoegdheid wordt opgenomen dat het OM bij de rechter-commissaris een vordering moet indienen tot het doen van onderzoek nadat bulkgegevens zijn vergaard. Vervolgens kan de rechter-commissaris eisen stellen die in acht moeten worden genomen bij het onderzoeken van bulkgegevens. In de onderzoeken die hebben geleid tot bulkgegevens, zoals Ennetcom en EncroChat, is dit ook de werkwijze geweest. De wijze waarop de rechter-commissaris is ingeschakeld, verschilt echter. Soms was dat op basis van artikel 181 WvSv, en soms op basis van artikel 126uba Sv. De belangrijkste eisen die in dit verband door de rechter-commissaris zijn gesteld zijn: (a) dat alleen mag worden gezocht op zoekwoorden die te relateren zijn aan het doel van het onderzoek; (b) dat de met de zoekwoorden gevonden informatie eerst aan de rechter-commissaris moet worden voorgelegd en daarna pas kan worden verstrekt aan de politie en het OM; en (c) dat de rechter-commissaris het onderzoek tussentijds kan beëindigen indien de tussentijdse toets hiertoe aanleiding zou geven. Met deze eisen is beoogd de proportionaliteit van het onderzoek te waarborgen en te voorkomen dat het onderzoek een *fishing expedition* zou worden.

De vraag is echter of de hierboven beschreven werkwijze voldoende werkbaar is in de praktijk en de proportionaliteit van het onderzoek voldoende kan borgen. Het probleem is immers dat bij onderzoek aan bulkgegevens niet zeker is waarnaar precies moet worden gezocht. Dit onderzoek is veelal een dynamisch proces, waardoor moeilijk vooraf kan worden bepaald wat al dan niet relevant is. Het gevolg hiervan kan zijn dat de zoektermen die worden gebruikt nogal ruim en vaag zijn en de rechter-commissaris die gevraagd wordt zich hierover te buigen, weinig concrete handvatten heeft om een beoordeling te maken van de

523 Zie hoofdstuk 2, § 4.2.

524 Bestaande (heimelijke) opsporingsbevoegdheden waarmee bulkgegevens kunnen worden vergaard zijn in elk geval de inbeslagneming van geautomatiseerde werken en gegevensdragers en de hackbevoegdheid.

proportionaliteit. Bovendien betekent het versterken van de waarborgen van enkele opsporingsbevoegdheden dat deze waarborgen slechts voor deze bepaalde opsporingsbevoegdheden gelden. Het is dan ook niet aan te bevelen het WvSv zo aan te passen dat alleen voor specifieke opsporingsbevoegdheden waarmee bulkgegevens kunnen worden verkregen, verzwaarde waarborgen worden opgenomen.

Inspiratie voor hoe het onderzoek aan bulkgegevens nader kan worden genormeerd, bieden de ervaringen met de Wiv 2017. Niet alle waarborgen die in het kader van bulkinterceptie in de Wiv 2017 zijn ontwikkeld, kunnen worden overgenomen omdat de diensten voor hun opdracht grotere bulksets mogen vergaren en verwerken. Niettemin biedt het Wiv 2017 kader enkele aanknopingspunten voor waarborgen die voor het onderzoek aan bulkgegevens van belang kunnen zijn en de wijze waarop dit wettelijk geregeld zou kunnen worden.

Een belangrijke waarborg in de Wiv 2017 is een functiescheiding in combinatie met een bewaartermijn. Functiescheiding houdt in dat de personen die het onderzoek aan gegevens verrichten niet dezelfde personen zijn als de personen die het inlichtingenwerk verrichten. In de wettelijke normering van onderzoek van bulkgegevens voor strafvorderlijke doeleinden zou een vergelijkbare functiescheiding tot uitdrukking kunnen worden gebracht. Dat impliceert dat de gegevens eerst worden doorzocht door analisten en dat enkel de voor het opsporingsonderzoek relevante informatie aan de tactische onderdelen van de politie en het OM ter beschikking wordt gesteld. Dat brengt ons bij de bewaartermijn. Voor bulkgegevens geldt doorgaans dat niet eenvoudig kan worden vastgesteld welke gegevens niet relevant zijn en daarmee voor verwijdering in aanmerking komen. Het probleem is immers dat bulkgegevens zodanig veel gegevens bevatten dat het binnen de voor opsporing beschikbare capaciteit en tijd niet mogelijk is om snel een beeld te vormen van de inhoud van alle gegevens. Tegelijkertijd kan het onderzoek aan bulkgegevens gelet op het recht op privacy niet eindeloos duren, met als risico dat de gegevens ook voor andere doelen dan waarvoor de gegevens zijn vergaard worden geanalyseerd. In de Wiv 2017 is er daarom voor gekozen om het onderzoek aan bulkgegevens te koppelen aan een bewaartermijn. Dit betekent dat de gegevens een bepaalde periode – bijvoorbeeld een jaar – mogen worden onderzocht. Na deze termijn dient de gehele set met bulkgegevens te worden vernietigd. In WvSv kennen we een dergelijke functiescheiding in combinatie met bewaartermijnen niet, maar dit zou dus wel nuttig kunnen zijn. Over de vraag hoe lang die bewaartermijn moet zijn, kan natuurlijk gemakkelijk discussie ontstaan. Het is daarom belangrijk dat de wetgever hierin keuzes maakt, waarbij zowel recht wordt gedaan aan het recht op privacy als het opsporingsbelang.

Een tweede manier waarop onderzoek aan bulkgegevens kan worden geregeld, is dan ook door een algemeen normeringskader te creëren specifiek voor het doen van onderzoek aan bulkgegevens, ongeacht de vraag hoe deze gegevens zijn verkregen. In dit normeringskader zou functiescheiding en de bewaartermijn tot uitdrukking kunnen worden gebracht. Ook zou in dit normerende kader een motiveringsverplichting kunnen worden opgenomen ter waarborging van de noodzakelijkheid (subsidiariteit) van inzet van de opsporingsbevoegdheid. Dit betekent dat de opsporingsautoriteiten – voordat zij overgaan tot inzet van een opsporingsbevoegdheid die naar verwachting redelijkerwijs kan resulteren in bulkgegevens – voldoende gemotiveerd moeten kunnen onderbouwen waarom inzet van de bevoegdheid op deze wijze noodzakelijk is. Bij het vormgeven van een grondslag waarin onderzoek aan bulkgegevens die met bijzondere of heimelijke opsporingsbevoegdheden wordt geregeld, is tot slot van belang om de eisen niet te verbinden aan één bevoegdheid, omdat meerdere digitale opsporingsbevoegdheden (hacken, inbeslagneming, vorderen gegevens, overnemen van gegevens uit publiek toegankelijke bronnen) tot het vergaren van bulkgegevens kunnen leiden.

6.3.3 Aandachtspunt 3: doelbinding en doelafwijkend gebruik

Het derde aandachtspunt is de invulling van het doelbindingsbeginsel en daarmee samenhangend de mogelijkheden tot doelafwijkend gebruik. Het doelbindingsbeginsel houdt in dat gegevens alleen mogen worden verwerkt ten behoeve van het doel waarvoor de gegevens zijn verkregen en op een wijze die niet onverenigbaar is met dat doel. Dat doel moet voorts voorafgaand aan de vergaring door de opsporingsautoriteiten worden gespecificeerd.[525] Een zeer strikte invulling van het doelbindingsbeginsel beperkt de mogelijkheden tot het verder of ander gebruik van gegevens. Op deze manier kan doelbinding het werk van de opsporingsautoriteiten frustreren, omdat bij de opsporingsautoriteiten ook behoefte bestaat om gegevens die voor uiteenlopende doelen zijn vergaard en verwerkt te combineren en zo te verrijken. Tegelijkertijd kent het doelbindingsbeginsel een belangrijke waarborgfunctie. Door vooraf te expliciteren wat het doel van de verwerking is en vervolgens alleen handelingen toe te staan die niet onverenigbaar zijn met dat doel, wordt immers de mogelijkheid tot misbruik beperkt.[526]

525 Dit laatste wordt ook wel aangeduid als doelspecificatie.

526 In het kader van strafvordering wordt dit doel vaak door de wetgever geëxpliciteerd, maar in sommige gevallen moet de verwerkingsverantwoordelijke zelf ook aan nadere doelspecificatie voldoen. Zie bijvoorbeeld art. 9 lid 2 Wpg.

Uit het voorgaande in paragraaf 6.2 is duidelijk geworden dat doelbinding in de EU Richtlijn 2016/680 inhoudt dat de met heimelijke opsporingsbevoegdheden verkregen gegevens in beginsel alleen mogen worden gebruikt voor het concrete doel waarvoor de bevoegdheid is ingezet.[527] Tegelijkertijd wordt in de EU Richtlijn 2016/680 wel erkend dat gegevens ook voor andere doelen dan het doel van vergaring mogen worden verwerkt, mits dat doelafwijkende gebruik bij wet is voorzien, noodzakelijk en proportioneel is. Over het antwoord op de vraag hoe stringent deze proportionaliteitstoets invulling moet krijgen, is de EU Richtlijn 2016/680 niet duidelijk. Met name is onduidelijk in welke mate een ander, secundair verwerkingsdoeleinde nog verband moet houden met het primaire verwerkingsdoeleinde.[528]

Op dit punt loopt de normering in het buitenland ook uiteen. In Duitsland wordt aan het doelafwijkende gebruik van gegevens die zijn verkregen met opsporingsbevoegdheden die ernstig inbreuk maken op grond- en mensenrechten strenge eisen gesteld.[529] Hier wordt immers de zogeheten *hypothetischen Datenneuerhebung*-toets toegepast. Deze toets houdt voor wat betreft bijzondere opsporingsbevoegdheden in dat de met deze bevoegdheden verkregen gegevens in beginsel alleen in andere opsporingsonderzoeken mogen worden gebruikt indien het in die andere onderzoeken ook gaat om strafbare feiten van dezelfde ernst of ernstiger.

In Noorwegen lijkt de lat voor doelafwijkend gebruik van gegevens minder hoog te zijn gelegd. Als algemeen uitgangspunt wordt hier gehanteerd dat de doelen waarvoor de politie gegevens verwerkt in beginsel verenigbaar zijn met elkaar. Dit betekent dan ook dat gegevens die voor een specifiek doel worden verwerkt, ook voor een ander doel mogen worden verwerkt. Tegelijkertijd beperkt het Noorse recht op diverse plaatsen de mogelijkheden tot doelafwijkend gebruik. Voor wat betreft de met opsporingsbevoegdheden verkregen gegevens geldt bijvoorbeeld dat deze gegevens alleen voor '*intelligence*'-doelen mogen worden verwerkt als de gegevens betrekking hebben op – kort gezegd – personen waarvan wordt vermoed dat zij in georganiseerd verband strafbare feiten zullen begaan en personen (familie, vrienden, collega's) die hiermee een nauwe band hebben. Gegevens die met bijzondere opsporingsbevoegdheden zijn verkregen, kunnen – in afwijking van het algemene uitganspunt – dus niet zomaar voor andere politiedoelen worden verwerkt. In België is de gedachtenvorming inzake doelafwijkend gebruik van in de opsporing verkregen gegevens niet of nauwelijks ontwikkeld. Weliswaar

527 In Noorwegen en Duitsland wordt doelbinding ook op deze wijze uitgelegd.
528 Zie Hoofdstuk 3.
529 Hierbij moet bijvoorbeeld worden gedacht aan de hackbevoegdheid.

sluit het Belgische recht de mogelijkheid van doelafwijkend gebruik niet uit, maar in het WvSv is niet nader uitgewerkt in welke gevallen en onder welke omstandigheden doelafwijkend gebruik van in de opsporing verkregen gegevens toelaatbaar is.

Voor de inrichting van nieuwe wetgeving op het gebied van doelafwijkend gebruik van gegevens voor strafvorderlijke doeleinden dient de wetgever aldus na te denken over de vraag in welke gevallen behoefte bestaat aan doelafwijkend gebruik van in de opsporing verkregen gegevens, alsmede welke eisen daaraan moeten worden gesteld zodat dit doelafwijkende gebruik bij wet is voorzien en de noodzakelijkheid en de proportionaliteit van dit gebruik is geborgd. In abstracto kan moeilijk worden bepaald wanneer doelafwijkend gebruik noodzakelijk en proportioneel is. Niettemin is het wel nuttig om bij de ontwikkeling van nieuwe regels op dit terrein onderscheid te maken tussen twee vormen van doelafwijkend gebruik: *repurposing* en *recontextualization*.[530] Dit onderscheid is vooral nuttig bij het nadenken over de vraag welke waarborgen in de wet moeten worden opgenomen.

Aan de ene kant staat *repurposing*, waarbij geëvalueerde gegevens die eerst voor een bepaald doel zijn verwerkt later voor een ander doel worden gebruikt. Met geëvalueerde gegevens wordt hier bedoeld dat de gegevens op relevantie voor een bepaald opsporingsonderzoek zijn beoordeeld en dat de aard en inhoud van de gegevens bekend is. Een voorbeeld van *repurposing* is het gebruik van gegevens in een ander opsporingsonderzoek dan het onderzoek waarin de gegevens zijn verkregen. *Repurposing* is onder meer te herkennen in artikel 126dd Sv en artikel 9 lid 3 Wpg. Deze bepalingen bevatten als belangrijkste waarborg dat voorafgaand aan het doelafwijkende gebruik, wordt getoetst door een officier van justitie of een andere functionaris of de gegevens ook voor dat andere doel kunnen worden verwerkt. Onduidelijk is echter aan welke maatstaven dit doelafwijkende gebruik moet worden getoetst, terwijl de Richtlijn 2016/680 voorschrijft dat dit doelafwijkende gebruik noodzakelijk en proportioneel moet zijn. Het verdient dus aanbeveling dat de wetgever in onder meer artikel 126dd Sv en artikel 9 lid 3 Wpg eisen van noodzakelijkheid en proportionaliteit in de wet opneemt. Ook zou het goed zijn dat de wetgever in de bijbehorende toelichtende stukken uiteenzet hoe deze begrippen moeten worden getoetst.

Aan de andere kant staat *recontextualization.* Hierbij worden de gegevens ook voor een ander doel gebruikt dan waarvoor ze zijn vergaard, maar het verschil met *repurposing* is dat de gegevens opnieuw worden geëvalueerd. Hierbij kan bijvoorbeeld gedacht worden aan verwerkingen waarbij gegevens die voor

530 Dit onderscheid is ontleend aan Custers & Ursic 2016.

verschillende doelen zijn verwerkt bij elkaar worden gebracht met als doel om daar informatie uit af te leiden die als zodanig nog niet bekend was. Artikel 11 lid 4 Wpg maakt *recontextualization* mogelijk. Zo kunnen de opsporingsautoriteiten gegevens die eerder met bijzondere opsporingsbevoegdheden zijn vergaard opnieuw analyseren met als doel om hieruit informatie af te leiden die tot nieuwe inzichten leidt. Hierdoor kunnen personen die een bepaalde hoedanigheid hebben (verdachte, getuige, slachtoffer of anderszins) mogelijk een andere hoedanigheid krijgen. Aan *recontextualization* zitten in het algemeen dan ook meer risico's dan aan *repurposing*. In de normering moet hiermee rekening worden gehouden. In artikel 11 Wpg is dat onvoldoende gebeurd. Met name is onduidelijk in welke gevallen en voor welke doelen artikel 11 lid 4 Wpg zou kunnen worden toegepast. Deze onduidelijkheid wordt verder versterkt doordat niet geheel duidelijk is welke onderzoekshandelingen op basis van deze bepaling mogen worden verricht. Het toetsen van proportionaliteit van een onderzoekshandeling wordt hierdoor verder bemoeilijkt. Aanbevolen wordt aldus om artikel 11 Wpg te herzien. Niet alleen moet de wetgever duidelijker maken in welke gevallen en voor welke doelen de bepaling kan worden toegepast, ook moet de wetgever helder uiteenzetten welke onderzoekshandelingen de bepaling beoogt te normeren. Dit laatste neemt echter niet weg dat in de wettekst zelf met een containerbegrip zal moeten worden gewerkt, waaronder verschillende onderzoekshandelingen vallen. Het proces waarbij gegevens uit verschillende bronnen worden gecombineerd, geordend, gevisualiseerd en verrijkt om zo informatie te genereren die als zodanig nog niet bekend was, is immers zeer dynamisch van aard. Dit proces laat zich dan ook niet eenvoudig vangen in scherp definieerbare begrippen.

6.3.4 Aandachtspunt 4: toezicht

Een vierde aandachtspunt betreft – tot slot – het toezicht op de gegevensverwerking. Zoals uit eerdere hoofdstukken naar voren komt, is het thema van normering onlosmakelijk verbonden met toezicht. Verondersteld wordt immers dat van (effectief) toezicht een belangrijke prikkel tot naleving uitgaat. De Richtlijn 2016/680 verplicht eveneens tot effectief toezicht. Ook het EHRM en het HvJ EU leggen de nadruk hierop. Met het oog daarop dient de toezichthouder over voldoende corrigerende, toezichthoudende en raadgevende bevoegdheden te beschikken. Toezicht heeft ook een belangrijke rol bij de normering zelf; door het houden van toezicht wordt niet alleen de norm bevestigd (en eventueel afgedwongen), maar kan de norm – daar waar nodig – nader worden uitgelegd. Normprecisering vormt derhalve een belangrijk onderdeel van toezicht, hetgeen met name in een snel

veranderende omgeving van gegevensverwerking voor strafvorderlijke doeleinden van grote meerwaarde kan zijn. Daarbij geldt ook dat een goed functionerend stelsel van toezicht mogelijke problemen of onduidelijkheden in de normering kan ondervangen. Zoals in het vierde hoofdstuk reeds geopperd,[531] biedt het creëren van een goed toezichtsysteem wellicht ook de mogelijkheid om de normering minder strikt in te richten. Dat wil zeggen meer vanuit de beginselen dan vanuit harde regels en scherpe juridische onderscheidingen.

In dit onderzoek is geen uitgebreid empirisch onderzoek gedaan naar het functioneren van het stelsel van toezicht. Niettemin leggen de literatuurstudie en interviews de nodige knelpunten bloot die nopen tot nadere reflectie met het oog op de toekomst. In de kern is het probleem dat weliswaar verschillende onafhankelijke en niet-onafhankelijke toezichtsorganen toezicht kunnen houden op de verwerking van gegevens voor strafvorderlijke doeleinden, maar dat vanwege de taakopvatting en verschillende capaciteitsoverwegingen niet daadwerkelijk van effectief toezicht kan worden gesproken. Bij het nadenken over een nieuwe systematiek of andere inhoudelijke normering, kan een nadere reflectie op het toezicht dus niet achterwege blijven. Er zijn in dit verband twee vragen die nadere aandacht behoeven. De eerste is de vraag bij welke autoriteit(en) het toezicht moet worden belegd en de tweede vraag betreft het type toezicht en in hoeverre het toezicht op onderzoek aan gegevens met een strafvorderlijk doel aanvulling behoeft.

Naar een gespecialiseerde toezichthouder?

De eerste vraag betreft de verhouding tussen toezichthouders en wie het best geequipeerd is om toezicht te houden op strafvorderlijke gegevensverwerking. Wanneer we kijken naar de huidige verdeling is deze op het eerste gezicht helder: de strafrechter beoordeelt individuele zaken (vooral aan de hand van artikel 359a Sv)[532] en de Autoriteit Persoonsgegevens (AP) is er voor het grotere geheel. In de praktijk valt echter te betwijfelen of daadwerkelijk sprake is van voldoende effectieve rechtsbescherming.[533] Voor de strafrechter geldt dat deze uiteindelijk maar een zeer beperkt aantal zaken voor zich krijgt en bovendien de nodige terughoudendheid betracht met het verbinden van rechtsgevolgen aan privacy-schendingen.[534] In de praktijk heeft dit tot gevolg dat doorgaans niet uitvoerig wordt

531 Zie hoofdstuk 4, § 6 en 7.

532 De bescheiden rol van de OvJ laten we hier verder buiten beschouwing, nu deze niet is geformaliseerd en de OvJ hierin ook geen grote rol lijkt te spelen.

533 Zie hoofdstuk 2, § 4.4.

534 Ook in het interview met een strafrechtadvocaat kwam dit knelpunt naar voren.

gecontroleerd of de Wpg en de daarin vervatte gegevensbeschermingsrechtelijke beginselen zijn nageleefd, nu dergelijke schendingen toch vaak niet tot een rechtsgevolg hoeven te leiden.[535] Voorts wordt ook aangenomen dat het niet tot de taak van de strafrechter behoort om de opsporing te controleren.[536] De AP lijkt deze rol ook niet voor haar rekening te kunnen nemen, nu deze autoriteit vooral systeemtoezicht houdt en niet op concrete strafzaken.[537] Bovendien houdt de AP vooral toezicht op naleving van het gegevensbeschermingsrecht, maar het gegevensbeschermingsrecht is niet het enige gezichtspunt dat relevant is bij de normering van de verwerking van gegevens voor strafvorderlijke doeleinden.

Het verdient aanbeveling een toezichthouder in het leven te roepen die specifiek toezicht kan houden op de verwerking van gegevens voor strafvorderlijke doeleinden. Hiermee wordt tegemoetgekomen aan de leemte in het huidige toezichthoudende kader. Voorts kan een gespecialiseerde toezichthouder aan normprecisering doen. Daaraan lijkt zeker op het gebied van gegevensverwerking voor strafvorderlijke doeleinden behoefte te bestaan. De wet dienaangaande kent immers vaak abstracte en vage begrippen. Tot slot kan een gespecialiseerde toezichthouder ook voor een breder publiek inzichtelijk maken waar de vragen en dilemma's liggen zodat daarover een bredere maatschappelijke of politieke discussie kan plaatsvinden. Een nadeel van een nieuwe gespecialiseerde toezichthouder is verdere fragmentatie nu op het terrein van gegevensverwerking voor strafvorderlijke doeleinden reeds verschillende toezichthouders actief zijn. Toch lijkt dit geen zwaarwegend bezwaar te zijn, nu op dit terrein altijd meerdere toezichthouders opereren; de strafrechter zal in een individuele strafzaak toch moeten beoordelen hoe een eventuele onrechtmatigheid in de gegevensverwerking doorwerkt op de bewijsvraag dan wel de straftoemeting. Het blijft dus een kwestie van goed afstemmen welke autoriteit, welk onderdeel afdekt.

Voor wat betreft de vormgeving van een gespecialiseerde toezichthouder zijn verschillende opties denkbaar. In de eerste plaats zou men – zoals dat in België is gebeurd – naast een algemene gegevensbeschermingsautoriteit een

535 Zie ter illustratie verschillende rechtbankzaken, waarin gevoerde verweren op basis van de Wpg steevast worden afgewezen: Rb. Gelderland 20 oktober 2021, ECLI:NL:RBGEL:2021:5612; Rb. Gelderland 8 december 2021, ECLI:NL:RBGEL:2021:6584; Rb. Oost-Brabant 15 december 2021, ECLI:NL:RBOBR:2021:6861; Rb. Amsterdam 22 december 2021, ECLI:NL:RBAMS:2021:7553 en Rb. Amsterdam 11 mei 2022, ECLI:NL:RBAMS:2022:2453.

536 Zie in dit verband ook HR 1 december 2020, ECLI:NL:HR:2020:1889, *NJ* 2021/169 m.nt. Jörg, r.o. 2.3.1.

537 De respondenten bevestigen dat het in de praktijk vooral om systeemtoezicht gaat, mede ingegeven door verschillende (capaciteits)overwegingen.

gespecialiseerde gegevensbeschermingsautoriteit kunnen oprichten die specifiek toezicht houdt op gegevensverwerking door de opsporingsautoriteiten. Lidstaten kunnen immers meer dan één toezichthoudende autoriteit in het leven roepen.[538] Deze beschermingsautoriteit functioneert dan als waakhond en ziet toe op de naleving van de Wpg en de naleving van het (gemoderniseerde) WvSv, daar waar het gegevensverwerking door de politie betreft. De beschermingsautoriteit functioneert voorts naast de strafrechter, die vanzelfsprekend binnen een strafproces toezicht houdt op de naleving van de wet. De WP29 pleit echter voor één gegevensbeschermingsautoriteit die zowel toezicht houdt op de naleving van de AVG als de Richtlijn 2016/680. De keuze voor één autoriteit zorgt er volgens de Uniewetgever voor dat wordt gegarandeerd dat de gemeenschappelijke beginselen en begrippen zoveel mogelijk homogeen worden uitgelegd en dat een consistente gegevensbescherming in beleid en praktijk wordt gewaarborgd.[539] Bovendien is het voordeel van één gegevensbeschermingsautoriteit dat slechts één partij aan tafel zit in de EU. Een andere toezichthouder naast de AP die zich weliswaar specifiek zou richten op gegevensverwerking door de politie is in dat opzicht niet wenselijk. De Uniewetgever spreekt echter een voorkeur uit, maar dwingt niet tot slechts één gegevensbeschermingsautoriteit.

Een andere optie houdt in dat het toezicht binnen het strafvorderlijke kader wordt versterkt door naast het huidige AP en de strafrechter, een toezichthoudend orgaan op te richten naar het voorbeeld van de CTIVD dat toezicht uitoefent op het optreden van de inlichtingen- en veiligheidsdiensten. De CTIVD oefent immers toezicht uit zowel tijdens de uitoefening van de bevoegdheden als achteraf. Over dit toezicht brengt de CTIVD verslag uit in openbare rapporten. Verder kan de CTIVD de relevante actoren (in de Wiv 2017 is dat de betrokken minister) gevraagd en ongevraagd adviseren. Om deze toezichthoudende taak uit te voeren, heeft de CTIVD ook allerlei (vergaande) bevoegdheden. Zo heeft zij rechtstreeks toegang tot alle relevante systemen van de AIVD en de MIVD, kan zij medewerkers horen en deskundigen inschakelen. Het voordeel van het in het leven roepen van een met de CTIVD vergelijkbaar orgaan boven een specialistische gegevensbeschermingsautoriteit, is dat de eerste een bredere taakopdracht kan worden toebedeeld binnen het strafvorderlijke kader, een taak die verder gaat dan die van een

538 Zie Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) – wp258, p. 37. Beschikbaar via: https://ec.europa.eu/newsroom/article29/items/610178.

539 Overigens is de vraag of het altijd wenselijk is om te streven naar homogeniteit van de uitleg van normen in de AVG en de Richtlijn 2016/680. Sommige beginselen in de Richtlijn 2016/680 kennen reeds een wat van de AVG afwijkende uitleg omdat de context zo verschillend is.

waakhondfunctie. Daardoor kan dit toezichthoudende orgaan ook een belangrijke rol vervullen op het gebied van normprecisering. Dit orgaan zou wat ons betreft bovendien als klankbord kunnen fungeren bij vragen van de politie over de verwerking van gegevens gedurende de opsporing. Zo kan ook buiten de rechter om worden geborgd dat fundamentele rechten voldoende zijn beschermd alsmede dat de opsporing werkbaar blijft.

Meer ex durante toezicht?

Naast de vraag *wie* toezicht moet houden, is vanzelfsprekend van belang *hoe* toezicht moet worden gehouden. Deze twee vragen hangen met elkaar samen; zo is rechterlijke toetsing vaak meer statisch van aard en zaakspecifiek, terwijl een toezichthouder een beeld kan vormen over meerdere zaken en meer dynamisch toezicht kan houden. Goed toezicht wil echter niet zeggen dat elke (verwerkings)handeling vooraf gefiatteerd of achteraf bekeken moet worden; er zijn andere manieren om de vereiste volledigheid van het toezicht te realiseren. Waar het momenteel vooral aan lijkt te ontbreken is een onafhankelijke toezichthouder die *real-time* mee kan kijken bij de uitoefening van digitale opsporingsbevoegdheden en waar nodig kan interfereren (en dat ook doet). Nu wordt bij onderzoek aan bulkgegevens op *ad hoc* basis de rechter-commissaris betrokken, maar dat lijkt niet een erg effectieve vorm van toezicht of rechtsbescherming te zijn. Immers, vaak is vooraf nog niet precies duidelijk wat men gaat tegenkomen in de bulk met gegevens. Bovendien is niet alleen bij onderzoek aan bulkgegevens *real-time* toezicht wenselijk, ook bij andere (complexe) gegevensverwerkingen die in het kader van de opsporing worden uitgeoefend. Waar bij andersoortig strafvorderlijk optreden – bijvoorbeeld een stelselmatige observatie – een dergelijk *ex durante* toezicht soms lastig kan worden vormgegeven, moet dit voor wat betreft digitale opsporing eenvoudiger te realiseren te zijn. Ondersteuning voor het uitvoeren van *ex durante* toezicht kan mogelijk mede worden gevonden in de techniek. In het kader van de Wiv 2017 en de plannen tot hervorming van die regeling, denkt men momenteel na hoe een dergelijke vorm van toezicht gestalte kan krijgen.

De trend naar meer *ex durante* en *ex post* toezicht is ook in de jurisprudentie van het EHRM te zien, ook al formuleert het EHRM weinig harde eisen. Dat laat onverlet dat er alle aanleiding is om het stelsel van toezicht zoals we dat in Nederland kennen, te verstevigen. Op deze manier kan aan zorgen van burgers tegemoet worden gekomen en kunnen de belangen van de verdachte voldoende worden gewaarborgd.

6.4 SLOTSOM

Dit onderzoek behelst een verkenning van de wettelijke waarborgen bij strafvorderlijke vergaring van gegevens en de mate waarin vervolgens in waarborgen moet worden voorzien bij de daaropvolgende (verdere) verwerking van die gegevens. Het onderzoek inventariseert welke eisen en waarborgen het Europese recht stelt aan de normering van het verwerken van gegevens voor de opsporing en identificeert een viertal juridische knel- en aandachtspunten in het huidige wettelijke kader. Voor een overdenking van de wenselijke normering van (verdere) verwerking van gegevens vergaard in het kader van opsporing put het onderzoek inspiratie uit de Wiv 2017 en het recht in België, Duitsland en Noorwegen.

Alles overziend komen we tot volgende aanbevelingen die de wetgever voor de inrichting van de nieuwe wettelijke regeling ten aanzien van strafvorderlijke gegevensbescherming in acht kan nemen.

1. De *verwerking* van gegevens met een strafvorderlijk doel dient nader in het WvS te worden genormeerd door het creëren van een normeringskader in aanvulling op de regels die reeds gelden voor de *vergaring* van gegevens. Uitgangspunt zou moeten zijn dat het WvSv zowel de *inzet* als de *uitoefening* van opsporingsbevoegdheden normeert en de Wpg de omgang met persoonsgegevens in algemenere zin. Meer concreet betekent dit het volgende.
   a) In het normeringskader zouden de belangrijkste normen en/of beginselen op het gebied van gegevensverwerking een eigen plek moeten krijgen.
   b) Voor vormen van strafvorderlijke gegevensverwerking waarmee een meer dan beperkte inbreuk op de persoonlijke levenssfeer wordt gemaakt, dient een expliciete wettelijke grondslag te worden gecreëerd in het WvSv met bijbehorende waarborgen.
   c) Bijzondere aandacht dient worden besteed aan het doen van onderzoek aan gegevens die in bulk zijn vergaard. Daaraan dienen nadere waarborgen te worden verbonden in de vorm van een verzwaarde noodzakelijkheidtoets en een relevantietoets door analisten die niet bij het opsporingsonderzoek zijn betrokken.
2. De wetgever dient de huidige wettelijke grondslagen (bijvoorbeeld art. 126dd Sv; art. 9 lid 3 Wpg; art. 11 Wpg) voor doelafwijkend gebruik van in de opsporing verkregen gegevens te herzien. Hierbij dient in het bijzonder aandacht te worden besteed aan de vraag of de voorwaarden waaronder

doelafwijkend gebruik is toegestaan moeten worden verzwaard, opdat de proportionaliteit van dit doelafwijkende gebruik voldoende is geborgd.

3. Het toezicht op de verwerking van gegevens binnen de opsporing moet worden versterkt.
   a) Er moet een Commissie van Toezicht komen die specifiek toeziet op gegevensbescherming bij het verwerken van gegevens ten behoeve van strafvordering.
   b) Deze Commissie van Toezicht moet *ex durante* en *ex post* toezicht kunnen houden. Gelet op de aard van de activiteit kan niet worden volstaan met een statische *ex ante* toetsing. De Commissie moet kunnen meekijken met de uitoefening van bevoegdheden door de politie en zo nodig verwerkingshandelingen kunnen stopzetten.

Samenvatting

De digitalisering van de maatschappij heeft de mogelijkheden tot het vergaren van gegevens door de opsporingsautoriteiten aanzienlijk vergroot. Illustratief zijn recente zaken waarin de autoriteiten toegang hebben gekregen tot miljoenen versleutelde berichten van verschillende servers, zoals Ennetcom, EncroChat, Sky Global. Door inbeslagname van grote gegevensdragers of door het hacken van servers komt informatie steeds vaker in bulk bij de politie terecht. Deze bulkdatasets worden evenwel pas relevant wanneer de opsporingsautoriteiten deze gegevens analyseren en in verband brengen met andere gegevens. Daarmee komt het zwaartepunt van de door de overheid gemaakte inbreuk op de privacy van burgers naast vergaring, nadrukkelijk bij de verdere verwerking van die gegevens te liggen. Ook bestaat bij de opsporingsautoriteiten steeds meer behoefte om gegevens die reeds in politiesystemen zijn opgeslagen nader te onderzoeken met behulp van slimme *AI*-systemen met als doel daaraan nieuwe informatie te ontlenen. Deze ontwikkelingen roepen vragen op wat betreft de nadere normering van het onderzoeken van (bulk)gegevens voor strafvorderlijke doeleinden. Het voorgaande vormt voor de wetgever aanleiding het *vergaren* en het *verwerken* van gegevens in de opsporing in samenhang nader te doen onderzoeken. De wetgever is voornemens de wettelijke regeling inzake de bevoegdheden ter gegevensverwerking in het Wetboek van Strafvordering (WvSv) en de Wet politiegegevens (Wpg) te herschikken en waar nodig aan te passen. Met het doel bij te dragen aan het nader doordenken van de wijze van normeren van het onderzoek van gegevens voor strafvorderlijke doeleinden, stelt deze studie drie vragen centraal:

1. Waar liggen de juridische knelpunten in het huidige wettelijke kader ter zake van het doen van onderzoek aan vergaarde (persoons)gegevens voor strafvorderlijke doeleinden?
2. Welke eisen en waarborgen stellen relevante Europeesrechtelijke rechtsbronnen aan de normering van het verwerken van (persoons)gegevens voor strafvorderlijke doeleinden?
3. Welke voor deze normering relevante gezichtspunten kunnen worden ontleend aan de Wiv 2017 en het recht in België, Duitsland en Noorwegen?

Voor de beantwoording van de vragen is gebruik gemaakt van (primair juridisch) *deskresearch* dat is aangevuld door verdiepende interviews en een expertmeeting.

Hoofdstuk 2 bevat een uiteenzetting van het huidige juridische kader dat het onderzoek aan gegevens normeert. Dit kader is neergelegd in de Wpg en het WvSv. Ook wordt ingegaan op de plannen van de wetgever in het kader van de modernisering van het WvSv voor aanpassing van de wettelijke regeling. Bij deze uiteenzetting zijn vier met elkaar samenhangende knel- of aandachtspunten geïdentificeerd.

Punt 1 betreft de wetssystematische keuze om de *vergaring* van gegevens vooral in het WvSv te regelen, terwijl de *verwerking* van gegevens in een gegevensbeschermingswet (thans Wpg) wordt geregeld. De wetgever is voornemens deze scheiding nadrukkelijk in het nieuwe WvSv door te trekken. Nadere reflectie op deze keuze of eerdere keuzes om bepaalde vormen van gegevensverwerking toch in het WvSv te regelen (bv. het huidige art. 126dd WvSv) heeft echter nauwelijks plaatsgevonden. De vraag is of beide activiteiten – het vergaren en het (verder) verwerken – zich wel goed laten scheiden en wat de mogelijke implicaties zijn van een dergelijke separate normering. Bovendien lijkt de verhouding tussen de Wpg en het WvSv niet altijd logisch, nu de Wpg ook veel voor de opsporing relevante normen bevat, terwijl deze wet primair is bedoeld om de omgang met gegevens te normeren – en dus niet de opsporing van strafbare feiten.

Punt 2 betreft de vraag naar de normering van onderzoek aan bulkgegevens die door verschillende (heimelijke) opsporingsbevoegdheden kunnen worden vergaard. Het vergaren van bulkgegevens ligt vanuit het oogpunt van het recht op privacy veel gevoeliger dan meer gerichte vormen van gegevensvergaring. Recente zaken waarin bulkgegevens zijn vergaard, zoals Ennetcom, EncroChat, Sky Global, leiden tot discussie over de vraag hoe onderzoek aan bulkgegevens mag worden uitgevoerd, nu wettelijke normering hieromtrent ontbreekt.

Punt 3 betreft de vraag naar de invulling van het gegevensbeschermingsrechtelijke doelbindingsbeginsel en daarmee de reikwijdte van de mogelijkheden tot doelafwijkend gebruik van gegevens. De behoefte van de opsporingsautoriteiten om reeds in de politiesystemen opgeslagen gegevens te combineren, te verrijken en met elkaar in verband te brengen, neemt de laatste jaren sterk toe. Niet alleen omdat hiertoe steeds meer technologische mogelijkheden bestaan, ook omdat hiermee proactief – los van een concreet opsporingsonderzoek – een informatiepositie kan worden opgebouwd. Bij dit soort gegevensverwerkingen worden gegevens die voor bepaalde doelen zijn vergaard en opgeslagen, opnieuw gebruikt voor andere doelen zoals het opbouwen van een informatiepositie. Hoewel

doelafwijkend gebruik van gegevens onder omstandigheden toelaatbaar is, rijst de vraag hoe op een zinvolle wijze invulling kan worden gegeven aan het doelbindingsbeginsel en doelafwijkend gebruik, waarbij zowel recht wordt gedaan aan het waarborgkarakter van het beginsel alsook aan de werkbaarheid van de opsporing.

Punt 4 betreft het toezicht op gegevensverwerking voor strafvorderlijke doeleinden, hetgeen onlosmakelijk met de normering is verbonden is. In theorie houden verschillende, zowel interne als externe toezichtsorganen (AP, gegevensbeschermingsfunctionaris, privacyfunctionaris, OM, strafrechter) toezicht op de verwerking van gegevens in de opsporing. Het huidige toezichthoudende kader kent evenwel tekortkomingen, onder meer vanwege de taakopvatting van sommige toezichthouders alsmede verschillende capaciteitsoverwegingen. De vraag is hoe het toezichthoudende kader kan worden versterkt.

Hoofdstuk 3 brengt de eisen en waarborgen met betrekking tot het normeren van gegevensverwerking op grond van een drietal relevante Europese rechtsbronnen in kaart: de EU Richtlijn 2016/680, artikel 8 Europees Verdrag voor de Rechten van de Mens (EVRM) en artikel 7 en 8 Handvest van de Grondrechten van de Europese Unie (HGEU) en de relevante jurisprudentie van het Europees Hof voor de Rechten van de Mens (EHRM) en het Hof van Justitie EU (HvJ EU).

De **Richtlijn 2016/680** regelt uitsluitend de verwerking van persoonsgegevens in het kader van de voorkoming, het onderzoek, de opsporing en de vervolging van strafbare feiten, tenuitvoerlegging van straffen en bescherming tegen en voorkoming van gevaren voor de openbare veiligheid. Het is gericht op minimumharmonisatie van de regelgeving in EU-lidstaten. Deze richtlijn formuleert een aantal belangrijke beginselen en uitgangspunten voor de verwerking van persoonsgegevens. De specifieke invulling van de beginselen laat de richtlijn aan lidstaten over; dit geldt ook voor het in dit onderzoek belangrijke doelbindingsbeginsel. Dit beginsel kent twee componenten: 1) *doelspecificatie* en 2) *verenigbaar gebruik*. Voor wat betreft de invulling van doelspecificatie moet ervan uit worden gegaan dat de doelen waarop de richtlijn ziet (voorkoming, onderzoek, opsporing en vervolging van strafbare feiten, tenuitvoerlegging van straffen en bescherming van openbare veiligheid) onvoldoende specifiek zijn om als concrete verwerkingsdoeleinden te kunnen dienen. Voor een zinvolle invulling van het doelbindingbeginsel alsmede de hieraan verwante beginselen van dataminimalisatie en opslagbeperking, moeten staten deze algemene doeleinden in nationale wetgeving nader specificeren. De Richtlijn is ook weinig helder over de rol van de verenigbaarheidstoets in artikel 4

lid 1 en de betekenis van een 'ander doel' in artikel 4 lid 2 Richtlijn 2016/680. In het licht van de ratio van het doelbindingsbeginsel – namelijk het bieden van voldoende rechtszekerheid voor betrokkene en voorzienbaarheid van de wetgeving inzake gegevensverwerking – is verdedigbaar dat de verenigbaarheidstoets in artikel 4 lid 2 Richtlijn 2016/680 moet worden ingelezen in de daarin vereiste proportionaliteitstoets. Van belang is voorts dat de Richtlijn lidstaten verplicht tot het tot stand brengen van een toezichthoudend kader voor de gegevensverwerking door strafvorderlijke autoriteiten. De randvoorwaarden die de Richtlijn 2016/680 voor de inrichting van dit kader stelt zijn: (1) het toezicht dient zowel op intern als extern niveau plaats te vinden; (2) het toezicht moet 'onafhankelijk' zijn; (3) de toezichthouders moeten voldoende bevoegdheden hebben om te kunnen spreken van 'effectief' toezicht.

Het **artikel 8 EVRM** alsmede de **artikelen 7 en 8 HGEU** vormen een belangrijk kader voor de invulling van het recht op privacy. Relevante jurisprudentie inzake artikel 8 EVRM leert dat verschillende verwerkingshandelingen, zoals de vergaring, opslag en verdere verwerking van gegevens – die op zichzelf of in combinatie met andere gegevens iets over het privéleven kunnen zeggen – inbreuk maken op het recht op privacy. Deze inbreuken moeten daarom van een wettelijke basis worden voorzien met voldoende waarborgen tegen misbruik. Cruciale waarborgen zijn het specificeren van een doel en doelbinding, opslagbeperkingen, dataminimalisatie (irrelevante gegevens moeten zo snel mogelijk worden verwijderd) en effectief (rechterlijk) toezicht. Jurisprudentie van het **EHRM** waarin specifiek de vergaring en verwerking van bulkgegevens werd getoetst, laat voorts zien dat het EHRM niet afwijzend staat tegenover ongerichte bulkgegevensverwerking in het belang van de nationale veiligheid of de bestrijding van zeer ernstige criminaliteit. Het EHRM onderscheidt in het proces van bulkgegevensverwerking verschillende stappen – van vergaring naar (verdere) verwerking – maar beschouwt de gegevensverwerking niettemin als één proces. Dit gehele proces moet met voldoende waarborgen zijn omgeven. Nationale wetgeving moet onder meer omschrijven op basis van welke gronden en onder welke omstandigheden bulkinterceptie is toegestaan; hoe het proces van selectie, analyse en gebruik vorm krijgt; wat de beperkingen en duur van de interceptie zijn en onder welke omstandigheden de gegevens moeten worden vernietigd. Voorts moet duidelijk zijn wie bevoegd is tot het verlenen van autorisatie en moet er zowel voorafgaand, tijdens als achteraf toezicht bestaan.

Het **HvJ EU** benadert het privacybegrip op een vergelijkbare manier als het EHRM en beoordeelt de vraag of inbreuk is gemaakt op privacy niet alleen aan de hand van de aard van de gegevens, maar aan de hand van wat gegevens in

combinatie over het privéleven kunnen prijsgeven. Het HvJ EU laat (vooralsnog) geen ruimte om de normering van de opslagfase afhankelijk te stellen van de normering van de toegang tot (en het latere gebruik van) gegevens – of vice versa. Minder strenge normering van één fase kan dus niet worden gecompenseerd door strengere normering van de andere fase. Met betrekking tot het verlenen van toegang door overheidsinstanties tot de bij de telecommunicatiediensten bewaarde verkeers- en locatiegegevens (niet zijnde slechts identificerende gegevens) stelt het HvJ EU een vijftal eisen, die zien op doelbinding, de kring van personen, voorafgaand onafhankelijke rechterlijke of bestuurlijk toetsing; notificatieverplichting, en beveiliging en bescherming van gegevens.

Hoofdstuk 4 bevat een interne rechtsvergelijking met de Wiv 2017. De context waarin de diensten werken, is weliswaar anders, maar in het kader van de Wiv 2017 spelen op het gebied van de normering van gegevensverwerking in het algemeen, en bulkgegevens in bijzonder, deels vergelijkbare vragen en problemen als in strafvordering. Voorts kent de Wiv 2017 een uitgebreid toezichthoudend kader dat voor strafvordering als inspiratie kan dienen.

Uit dit hoofdstuk komt allereerst naar voren dat gegevensverwerking binnen de Wiv 2017 is genormeerd aan de hand van een aantal algemene beginselen zoals het noodzakelijkheidsbeginsel, het doelbindingsbeginsel en de relevantietoets. Deze beginselen zijn van toepassing ongeacht de wijze waarop de gegevens zijn verkregen. Een belangrijk voordeel hiervan is dat de normering van gegevensverwerking niet specifiek is gekoppeld aan een of enkele specifieke bevoegdheden en deze algemene beginselen voor verschillende gevallen een normerend kader bieden. Daarbij gelden voor de *inzet* van bijzondere bevoegdheden nog wel aanvullende waarborgen. Voor de bevoegdheid tot bulkinterceptie via artikel 48 Wiv 2017 geldt een speciaal normeringsregime. Het is probleem is echter dat bulkgegevens ook met andere bevoegdheden kunnen worden vergaard. In dat geval zijn de aanvullende waarborgen die gelden voor de verdere verwerking niet van toepassing. Ervaringen met de Wiv leren dat het verstandig is om de normering van gegevensverwerking niet uitsluitend afhankelijk te maken van de specifieke wijze waarop gegevens zijn vergaard, maar de normering aan te passen aan de handelingen of activiteiten die met de gegevens worden verricht.

Voorts biedt de Wiv 2017 inspiratie voor het ontwikkelen van waarborgen inzake de verwerking van bulkgegevens. Zo wordt bij de verwerking van bulkgegevens in de Wiv 2017 veel waarde toegekend aan een relevantietoets met functiescheiding. Dit houdt in dat na de vergaring van bulkgegevens eerst door andere personen dan die daadwerkelijk inlichtingen inwinnen, wordt beoordeeld welke

gegevens al dan niet relevant zijn. Zo kan de proportionaliteit van onderzoek aan bulkgegevens worden geborgd.

Tot slot levert het perspectief van de Wiv 2017 belangrijke inzichten voor de inrichting van het toezicht. Weliswaar is de discussie over de inrichting van het toezicht binnen de Wiv 2017 in volle gang, duidelijk is wel dat de aard van het toezicht niet los kan worden gezien van het soort bevoegdheid dat wordt ingezet. Voortbordurend hierop wordt duidelijk dat het dynamische proces van gegevensverwerking voor onderzoeksdoeleinden zich minder goed laat vangen in harde regels en een statische *ex ante* toetsing. Met dit aspect dient tevens rekening te worden gehouden in het kader van strafvordering.

Hoofdstuk 5 bevat een blik over de grens en kent daarmee een extern rechtsvergelijkend perspectief. In dit hoofdstuk is verkend op welke punten de wettelijke kaders voor gegevensverwerking voor strafvorderlijke doeleinden in drie naburige landen (België, Duitsland en Noorwegen) inspiratie kunnen bieden voor Nederland met betrekking tot de normering van gegevensverwerking voor strafvorderlijke doeleinden.

Ten eerste laat de blik over de grens zien dat het zinvol kan zijn onderscheid te maken tussen normering van opsporingsactiviteiten in het WvSv, waaronder zowel de vergaring als verwerking van gegevens wordt verstaan, en de normering van de verdere omgang met deze gegevens. Duidelijker dan in Nederland, wordt dit onderscheid bijvoorbeeld in Duitsland gemaakt. Daar is ervoor gekozen om een algemene regeling inzake de verwerking van gegevens door zowel de rechterlijke macht als het openbaar ministerie in StPO op te nemen. Daarnaast bevat StPO een aantal op verschillende bijzondere opsporingsbevoegdheden toegespitste regels inzake het gebruik van gegevens, terwijl het Duitse recht ook in meer algemene kaderwetten terzake van gegevensbescherming kent waarop kan worden teruggevallen als StPO niets regelt.

Ten tweede regelen landen elk op verschillende manieren de invulling van het doelbindingsbeginsel en daarmee de mogelijkheden tot doelafwijkend gebruik. Duitsland kent op het gebied van doelbinding een uitgebreide doctrine. Elke verdere verwerking van gegevens (waaronder ook doelafwijkend gebruik) dient daar op een wettelijke grondslag te berusten. In het algemeen geldt dat gegevens die met voor de persoonlijk levenssfeer ingrijpende bevoegdheden zijn verkregen, alleen voor vergelijkbare andere doelen kunnen worden verwerkt. Vanuit het perspectief van bescherming van het privéleven kan deze regeling positief worden gewaardeerd. Het nadeel van de regeling is dat het tamelijk complex is. In Noorwegen is daarentegen gekozen om doelafwijking in beginsel toe te staan, tenzij de

wet dat expliciet beperkt. Deze beperking geldt in beginsel voor de verwerking van gegevens die met opsporingsbevoegdheden in concrete onderzoeken zijn verkregen. Doelafwijkend gebruik van deze gegevens, bijvoorbeeld voor preventieve doeleinden, is slechts toegestaan op grond van in de wet geregelde gevallen die zien op specifieke categorieën personen of op grond van toestemming van betrokkene.

Ten derde toont de analyse van de rechtspraktijk in de drie landen dat toezicht niet vanzelfsprekend hoeft te worden neergelegd bij een gegevensbeschermingsautoriteit die tevens op de naleving van de AVG toeziet. België kent bijvoorbeeld een toezichthouder die zich specifiek bezighoudt met toezicht op gegevensverwerking door de politie. Noorwegen kent een toezichtscommissie die naleving van de uitoefening van enkele bijzondere opsporingsbevoegdheden controleert. Het voordeel van zo'n commissie is dat op structurele basis toezicht wordt gehouden op de toepassing van bijzondere opsporingsbevoegdheden waarbij specifiek rekening kan worden gehouden met enerzijds de belangen van gegevensbescherming en anderzijds de belangen van criminaliteitsbestrijding.

Hoofdstuk 6 brengt de inzichten uit voorgaande hoofdstukken met elkaar in verband. Het bevat een reflectie op de *systematiek* en de *inhoud* van de normering van onderzoek van gegevens voor strafvorderlijke doeleinden, mede aan de hand van de in hoofdstuk 2 gesignaleerde aandachtspunten.

Voor wat betreft de *systematiek* geldt dat de verhouding tussen het WvSv en de Wpg niet kan worden vormgegeven aan de hand van de verwerkingshandeling – vergaren of verwerken – die wordt verricht. Om te bepalen in welke wet welk onderwerp thuishoort, is het doel en de context waarin de verwerkingsactiviteit wordt verricht van belang. Uitgangspunt zou volgens ons moeten zijn dat verwerkingshandelingen die zijn gericht op kennisvermeerdering én een strafvorderlijk doel dienen in het WvSv worden genormeerd. Dit uitgangspunt is nog onvoldoende te herkennen in het gemoderniseerde WvSv. Dat geldt in het bijzonder voor bevoegdheden waarmee onderzoekshandelingen kunnen worden verricht ten aanzien van computergegevens, ofwel digitale opsporingsbevoegdheden. In het gemoderniseerde WvSv is voornamelijk aandacht besteed aan de normering van de *inzet* van digitale opsporingsbevoegdheden door voor te schrijven in welke gevallen, voor welke doelen en met toestemming van welke autoriteit gegevens mogen worden vergaard. De *uitoefening* van deze opsporingsbevoegdheden waarbij veelal gegevens (verder) worden verwerkt is onderbelicht gebleven. Met het oog daarop verdient het aanbeveling sommige onderwerpen die thans in de Wpg zijn ondergebracht in het WvSv te regelen.

De *inhoud* van de normering kan op vier onderdelen worden verbeterd.

Ten eerste zou de wetgever in het WvSv in een algemene titel een normeringskader moeten ontwikkelen dat van toepassing is op het verwerken van gegevens tijdens de uitoefening van digitale opsporingsbevoegdheden. Een belangrijk voordeel van één normeringskader is dat het niet slechts van toepassing is op één of enkele specifieke bevoegdheden, maar in het algemeen gelding heeft. In dit normeringskader zouden de belangrijkste normen op het gebied van gegevensverwerking een plek moeten krijgen. Zo zou in deze titel minstens tot uitdrukking moeten worden gebracht dat voorafgaand aan het uitvoeren van gegevensonderzoek het doel van dat onderzoek moet worden vastgelegd; dat gegevens die niet relevant zijn voor dit doel moeten worden verwijderd c.q. ontoegankelijk moeten worden gemaakt; in welke gevallen en met inachtneming van welke waarborgen gegevens voor een ander doel dan het doel van vergaring kunnen worden gebruikt; alsmede dat alle handelingen die in het kader van dit onderzoek worden verricht, moeten worden gelogd.

Ten tweede dient de wetgever, naast een algemene titel waarin de belangrijkste normen inzake gegevensverwerking worden neergelegd, ook een specifiek normatief kader te creëren voor het strafvorderlijk onderzoek aan bulkgegevens. In het huidige noch in het gemoderniseerde WvSv wordt dit onderzoek expliciet genormeerd. Hierdoor ontstaat al snel spanning met het recht op privacy als bedoeld in artikel 8 EVRM en artikel 7 HGEU. Uit dit recht vloeit immers voort dat het gehele proces van bulkgegevensverwerking moet worden genormeerd. In dit verband verdient aanbeveling dat de wetgever nadenkt over nieuwe waarborgen, bijvoorbeeld een verzwaarde noodzakelijkheidstoets en een bewaartermijn in combinatie met verplichte functiescheiding.

Ten derde verdienen de bepalingen die doelafwijkend gebruik van in de opsporing verkregen gegevens mogelijk maken nadere doordenking. Daarbij gaat het in elk geval om artikel 126dd Sv, artikel 9 lid 3 Wpg en artikel 11 Wpg. Deze bepalingen maken het mogelijk gegevens die met opsporingsbevoegdheden zijn verkregen voor andere doelen te verwerken dan het doel waarvoor de bevoegdheid is ingezet. Zo kunnen gegevens die zijn verwerkt voor de opsporing van een strafbaar feit bijvoorbeeld worden gebruikt voor een ander doel zoals het opbouwen van een informatiepositie. Hoewel het Europese recht het gebruik van gegevens voor andere doelen dan waarvoor ze zijn verkregen niet verbiedt, stelt het hieraan wel beperkingen. Doelafwijkend gebruik dient immers noodzakelijk en proportioneel te zijn. Niet in alle bepalingen die doelafwijkend gebruik mogelijk maken, lijkt de proportionaliteit voldoende te zijn geborgd.

Ten vierde dient het toezicht op het verwerken van gegevens voor strafvorderlijke doeleinden te worden versterkt door het oprichten van een commissie van toezicht op de politiediensten en het OM. Hoewel verschillende actoren reeds toezicht houden op gegevensverwerking voor strafvorderlijke doeleinden, verdient het oprichten van een nieuw orgaan dat toezicht kan houden op de verwerking van gegevens door de politie en het OM (vergelijkbaar met de CTIVD die de AIVD en de MIVD controleert) om verschillende redenen aanbeveling. Allereerst wordt hiermee beter tegemoetgekomen aan de eisen die vanuit het Europese recht worden gesteld. Zowel uit de richtlijn 2016/680 als de jurisprudentie van het EHRM en het HvJ EU volgt de eis van effectief toezicht. Dat geldt in het bijzonder als gegevensverwerking heimelijk plaatsvindt, hetgeen in opsporing doorgaans het geval is. Verder kan een specialistische toezichthouder een belangrijke rol vervullen op het gebied van normprecisering. Tot slot kan een nieuw op te richten toezichtsorgaan voor een breder publiek inzichtelijk maken welke nieuwe vragen en dilemma's zich in het veranderend domein opsporing voordoen, zodat hierover ook maatschappelijk en politiek debat kan plaatsvinden.

Summary

The digitization of society has significantly increased the possibilities for collecting data by the law enforcement authorities. This is illustrated by recent cases in which the authorities obtained access to millions of encrypted messages on various servers, such as Ennetcom, EncroChat and Sky Global. Through the seizure of huge data carriers or by hacking into servers, information in bulk increasingly often ends up in the hands of the police. However, these bulk datasets only become relevant if the investigation authorities analyse these data and manage to connect them with other data. This means that the severity of the government's interference with citizens' privacy, apart from the actual collection of the data, becomes explicitly tied in with the subsequent processing of those data. There is also a growing need among investigation authorities for further analysis of data already stored in police systems by using smart AI systems with a view to gleaning new information. These developments raise questions about further regulation of analysing (bulk) data for criminal procedure purposes.[540] The foregoing impels the Dutch legislator to commission further research into *collecting* and *processing* data in criminal investigations and the way in which these are interconnected. The legislator intends to recast and, where necessary, amend the statutory provisions regarding the powers of data processing as laid down in the Dutch Code of Criminal Procedure (CCP) and the Dutch Police Data Act (DPDA). Aiming to make a contribution to the rethinking of the way in which the processing of data for the sake of criminal procedure purposes needs to be regulated, we pose three key questions in this study:

1. Where are the legal bottlenecks in the current legal framework with regard to examining data collected for criminal procedure purposes?
2. Which requirements and safeguards do the relevant European law sources set for the regulation of the processing of data for the benefit of criminal procedure purposes?
3. Which of the points of view that are relevant to this regulation are derived from the Dutch Intelligence and Security Services Act 2017 (ISS Act 2017) and the law in a few nearby countries (Belgium, Germany and Norway)?

540 In this study we focus on the processing of data for the detection and investigation of criminal acts by the police. The detection and investigation of criminal acts include the collection of evidence and the so-called law enforcement intelligence.

To answer these questions, (primarily legal) *desk research* was used, which was supplemented by in-depth interviews and an expert meeting.

Chapter 2 contains an explanation of the current Dutch legal framework which regulates the use of data for criminal procedure purposes. This framework was laid down in the DPDA and the CCP. It also discusses the plans of the legislator with regard to modernizing the CCP for amending the statutory provisions. Four interconnected bottlenecks have been identified in this explanation.

Point 1 relates to the legal systemic choice to lay down the *collection* of data primarily in the CCP, whereas the *processing* of data was laid down in a data protection act (currently the DPDA). The legislator intends to continue this separation emphatically in the new CCP. However, there has been hardly any further reflection on this choice or previous choices to lay down certain forms of data processing in the CCP after all (for example the current article 126dd CCP). The question is whether both activities – collecting and (further) processing – can be separated properly and what the possible implications are of such separate regulation. Furthermore, the relation between the DPDA and the CCP does not always seem to be logical, because the DPDA also contains standards relevant to investigations, whereas this Act is primarily intended to regulate the handling of data – instead of the investigation of criminal offences.

Point 2 concerns the demand for regulation of examination of bulk data which can be collected using various (secret) investigative powers. Collecting bulk data is a much more sensitive matter from the perspective of the right to privacy than more targeted forms of data collection. Recent cases in which bulk data were collected, such as those involving Ennetcom, EncroChat and Sky Global, lead to discussions about the question how examination of bulk data is allowed to be conducted, in the absence of statutory regulation about this.

Point 3 is to do with the question of purpose limitation with regard to data protection laws and by extension the scope of the possibilities to use data for different purposes. Over the past few years, there has been a sharp increase in the need of the investigation authorities to combine, enrich and correlate data already stored in police systems. This is not only because there are more and more technological tools to do so, but also because it enables the authorities proactively – apart from a specific criminal investigation – to create useful *intelligence*. With this type of data processing, data which were collected and stored for certain purposes, are re-used for different purposes such as building an information position. Although the use of data for different purposes is permissible under certain circumstances, the question arises how the principle of purpose limitation and the use of data for

different purpose(s) can be reconciled in a meaningful way, so that the principle's rational as a safeguard is honoured while taking into account the efficacy of the investigation.

Point 4 concerns the monitoring of data processing for criminal procedure purposes, which is inextricably linked to the regulation of the processing of data. In theory, various supervisory authorities (both internal and external) such as the Dutch Data Protection Authority (DPA), the data protection official, chief privacy officer, the Dutch Public Prosecution Office, and the criminal court, monitor the processing of data during a criminal investigation. The present supervisory framework has a number of shortcomings though, among other things because of the way some supervisors interpret their mandate and also because of the capacity for supervision. The question is how the supervisory framework can be strengthened.

Chapter 3 maps the requirements and safeguards with regard to the regulation of data processing on the basis of three relevant European legal sources: the EU Directive 2016/680, Article 8 of the European Convention on Human Rights (ECHR) as well as Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU) and the relevant case law of the European Court of Human Rights (ECtHR) and the European Court of Justice (CJEU).

The **Directive 2016/680** only deals with the processing of personal data in the context of the prevention, investigation, detection and prosecution of criminal offences, execution of criminal penalties and safeguarding against and the prevention of threats to public security. It is aimed at minimum harmonization of regulations in EU member states. This Directive contains a number of important principles and starting points for the processing of personal data. The specific way in which the principles are put into practice is left to the member states; this also applies to the principle of purpose limitation, which is important to this study. This principle has two components: 1) *purpose specification* and 2) *compatible use*. As far as the exact nature of the purpose specification is concerned, it must be assumed that the purposes that the Directive relates to (prevention, investigation, detection and prosecution of criminal offences, the execution of criminal penalties and the protection of public safety) are insufficiently specific to be used as concrete processing purposes. For a meaningful specification of the principle of purpose limitation as well as the associated principles of data minimization and storage limitation, member states must specify these general purposes in more detail in their own national legislation. The Directive is not particularly clear either about the role of the compatibility test in Article 4 paragraph 1 and the meaning of an 'other purpose' in Article 4 paragraph 2 of Directive 2016/680. In the light of the rational of

the purpose limitation principle – i.e., offering adequate legal certainty for the data subject and foreseeability of the legislation – one can argue that the compatibility check should be made part of the proportionality test in Article 4 paragraph 2 of Directive 2016/680. It is also important that the Directive requires member states to bring about a supervisory framework for data processing by criminal proceedings authorities. The prerequisites set out by the Directive 2016/680 for the creation of this framework are as follows: (1) supervision must take place at both an internal and an external level; (2) supervision must be 'independent'; (3) supervisors must have sufficient powers for the supervision to be called 'effective'.

Article 8 ECHR as well as **Articles 7 and 8 CFREU** constitute an important framework for defining the particulars of the right to privacy. Relevant case law regarding Article 8 ECHR shows that various processing operations, such as the collection, storage and further processing of data – which on their own or in combination with other data may reveal information about someone's private life – interfere with the right to privacy. These interferences must therefore be given a legal basis with sufficient safeguards to prevent abuse. Crucial safeguards are the specification of a purpose and purpose limitation, storage limitations, data minimization (irrelevant details must be deleted as soon as possible) and effective (judicial) supervision. Case law of the ECtHR in which the collection and processing of bulk data was specifically scrutinized also shows that the ECtHR is not opposed to untargeted processing of bulk data in the interest of national security or the fight against very serious crime. The ECtHR distinguishes between various steps in the processing of bulk data – from collection to (further) processing – yet it treats data processing as one process. The entire process must be surrounded by sufficient safeguards. Among other things, national legislation must describe on which grounds and under which circumstances wholesale interception of data is permitted; how the process of selection, analysis and use takes shape; what are the limits and the duration of the interception and under which circumstances must the data be destroyed. Additionally, it must be clear who has the power to grant authorization and there will have to be supervision before, during and after the process from interception to processing of data.

The **CJEU** approaches the concept of privacy in a way similar to that of the ECtHR and it looks at the question of whether there has been an interference with privacy not merely on the basis of the nature of the data but also on the basis of what data may reveal about someone's private life when combined. For the time being, the CJEU does not leave any room to make regulation of the data retention phase dependent on the regulation of access to (and later use of) data – or vice versa. A less rigorous regulation of one phase can therefore not be compensated by

more rigorous regulation of the other phase. As regards the granting of access by government bodies for criminal procedure purposes to traffic and location data (which are not merely identifying data) stored by telecommunication services, the CJEU applies a set of five requirements, relating to purpose limitation, the circle of people, previous independent judicial or administrative review; an obligation of notification, and security and protection of data.

Chapter 4 contains an internal comparison with the ISS Act 2017. Admittedly, the context in which the services operate is different, but within the framework of the ISS Act 2017, the questions and problems presenting themselves there in the area of regulation of data processing in general and bulk data in particular are to some extent similar to those in criminal investigations. Furthermore, the ISS Act 2017 features an elaborate supervisory framework that can serve as a model for criminal procedure.

What becomes clear in this chapter is first and foremost that data processing within the ISS Act 2017 has been regulated on the basis of a number of general principles, such as the necessity principle, the principle of purpose limitation and the relevance test. These principles apply irrespective of the manner in which the data were collected. An important advantage of this is that the regulation of data processing is not specifically linked to one power or some specific powers and these general principles provide a regulatory framework for various cases. Nevertheless, additional safeguards apply for the *deployment* of special powers. With regard to the power of bulk interception based on article 48 the ISS Act 2017, a special regulation regime applies. The problem, though, is that bulk data can also be collected using other powers. In that case, the additional safeguards that are relied on for further processing do not apply. Experience with the ISS Act 2017 shows that it is a good idea not to make the regulation of data processing solely dependent on the specific manner in which data have been collected, but to adapt regulation to the operations or activities carried out with the data.

Furthermore, the ISS Act 2017 provides inspiration for the development of safeguards with respect to the processing of bulk data. For example, the ISS Act 2017 sets great store by a relevance check with segregation of functions in the processing of bulk data. This means that after the collection of bulk data, persons other than those who actually garnered the data first assess which data are relevant and which are not. This ensures the proportionality of examination of bulk data.

Finally, the perspective of the ISS Act 2017 offers important insights in the way supervision may be set up. While it is true that the discussion about the set-up of supervision within the ISS Act 2017 is well under way, it is clear that the nature of the supervision cannot be isolated from the type of power deployed. Building on this, it becomes clear that the dynamic process of data processing for

investigative purposes does not lend itself so well to being captured in hard and fast rules and to a static *ex ante* test. This aspect must also be taken into account in the context of criminal procedure.

Chapter 5 offers a view across the border for an external comparative perspective. This chapter is an exploration of the areas in which the legal frameworks for data processing for criminal procedure purposes in three nearby countries (Belgium, Germany and Norway) may offer inspiration to the Netherlands in respect of the regulation of data processing in criminal investigations.

First of all, peering across the border reveals that it may be useful to distinguish between regulation of investigation activities in the CCP, which is meant to be understood as both collecting and processing of data, and the regulation of further handling of these data. This distinction is made more clearly in Germany for example than in the Netherlands. The authorities there opted for a general regulation regarding the processing of data, by including both the judiciary and the public prosecution department in StPO (the German Code of Criminal Procedures). Additionally, StPO contains a few rules aimed at various special investigative powers regarding the use of data, while German law also provides more generic framework laws in respect of data protection that can be resorted to in case StPO offers no succour.

Secondly, each country has its own way of implementing the purpose limitation principle and consequently the possibilities for uses that deviate from this principle. Germany has an extensive doctrine on the subject of purpose limitation. Every subsequent processing of data (including for (a) different purpose(s)) must have a legal ground there. In general, data that have been obtained using powers that interfere with a person's privacy can only be processed for similar other purposes. From the perspective of protecting an individual's privacy, this arrangement can be considered positive. However, the drawback of this arrangement is that is fairly complex. In Norway, on the other hand, it was decided to permit deviation from the original purpose(s) in principle, unless expressly prohibited by law. This restriction applies in principle to the processing of data that have been obtained with investigative powers in concrete investigations. Any use of these data for other purposes, for example for prevention purposes, is only permitted on the basis of cases set out in law which relate to specific categories of persons or on the basis of permission of the data subject involved.

Thirdly, the analysis of legal practice in the three countries shows that supervision does not necessarily need to be entrusted with a data protection authority that also supervises compliance with the General Data Protection Regulation (GDPR). Belgium for example has a supervisor that specifically concerns itself with the supervision of data processing by the police. Norway has a supervisory committee that checks compliance with respect to the exercise of certain special

investigative powers. The advantage of such a committee is that supervision of the deployment of special investigative powers occurs on a structural basis, where the interests of data protection on the one hand and the interests of law enforcement on the other hand can specifically be taken into account.

Chapter 6 synthesizes the insights gained in the previous chapters. It contains a reflection on the *system* and the *content* of the regulation of the examination of data for criminal procedure purposes, partly on the basis of the items of interest highlighted in Chapter 2.

As far as the *system* is concerned, the relation between the CCP and the DPDA cannot be shaped based on the processing operation – collecting or processing of data – that is carried out. The purpose and the context in which the processing operation takes place play an important part in determining which processing operation belongs to which Act. We argue that the starting point should be that the processing of data that is deployed for criminal procedure purposes and is exercised with the aim of gaining new information (for specific criminal investigations as well as for building intelligence) should be regulated in the CCP. As yet, this starting point is not sufficiently prominent in the modernized CCP. This applies in particular to powers with which investigations can be carried out with regard to computer data, in other words digital investigative powers. The main focus in the modernized CCP has been on regulating the *deployment* of digital investigative powers by prescribing in which cases, for which purposes and with the approval of which authorities data are allowed to be collected. The *exercise* of these investigative powers through which mostly data are processed (further) has received too little attention. In view of this, it is recommended that certain areas that are currently covered by the DPDA be regulated in the CCP.
The *content* of the regulation can be improved in four areas.

Firstly, the legislator would have to develop a regulatory framework in the CCP in a general title that applies to the processing of data during the exercise of digital investigative powers. An important advantage of having one regulatory framework is that it does not apply merely to one investigatory power or a few specific powers, but is applicable generally. The most important standards with regard to data processing would have to be incorporated in this regulatory framework. This title would need to express the notion that prior to an examination of data, the purpose of that examination must be established; that data which are not relevant for that purpose must be deleted and/or made inaccessible; in which cases and with due consideration for the question which safeguards data can be used for a purpose other than the purpose of collection; and that all operations carried out in the context of that examination must be registered.

Secondly, in addition to a general title in which the most important standards regarding data processing have been laid down, the legislator must also create

a specific normative framework for the examination of bulk data for criminal procedure purposes. This type of examination has not been regulated explicitly in either the present or the modernized CCP. This will soon interfere with the right to privacy as referred to in Article 8 ECHR and Article 7 CFREU. After all, it follows from this right that the entire process of bulk data processing must be regulated. In this context, it is to be recommended that the legislator reflects on new safeguards, for example a beefed-up necessity test and a retention period in combination with mandatory segregation of functions.

Thirdly, the provisions allowing the data obtained in the investigation to be used for entirely different purposes deserve to be thought in further detail. This concerns at any rate Article 126dd CCP, Article 9 paragraph 3 DPDA and Article 11 DPDA. These provisions make it possible for data obtained thanks to investigative powers to be processed for purposes other than the one for which the power was exercised. For example, data processed for the investigation of a criminal offence can be used for another purpose such as building an information position. Although European law does not prohibit the use of data for purposes other than for which they were obtained, it certainly imposes restrictions on this. After all, any use of data for different purposes has to be necessary and proportional. It would appear that the proportionality principle is not sufficiently guaranteed in all the provisions permitting the use of data for different purposes.

Fourthly, the supervision of processing data for criminal investigation purposes will have to be tightened by the creation of a committee supervising the police forces and the Public Prosecution Office. Although various actors already supervise the processing of data for criminal procedure purposes, it is recommended for a variety of reasons that a new body is created to monitor the processing of data by the police and the public prosecution department (comparable with the Dutch CTIVD (Committee for the Supervision of the Intelligence and Security Services) which monitors the AIVD, i,e., the General Intelligence and Security Service, and the MIVD, i.e., the Military Intelligence and Security Service). First of all, this better meets the requirements set by European law. The requirement of effective supervision ensues from both EU Directive 2016/680 and the case law of the ECtHR and the CJEU. This applies particularly if the processing of data is carried out covertly, which tends to be the case in criminal proceedings. Furthermore, a specialist supervisor may play an important role in improving the definition of standards. Finally, a new supervisory body to be established can furnish a wider public with insights into which new questions and dilemmas present themselves in the ever-changing domain of criminal investigations, thereby enabling a broader social and political debate about these matters.

Bronnen

1. Regelgeving en parlementaire documenten

Kamerstukken

Kamerstukken II 1996/97, 25403, 3.
Kamerstukken II 1997/98, 25877, 3 (MvT Wiv 2002).
Kamerstukken II 2005/06, 30327, 3.
Kamerstukken II 2012/13, 33542, 3.
Kamerstukken II 2013/14, 33820, 2.
Kamerstukken II 2013/14, 33842, 2.
Kamerstukken II 2016/17, 34588, 3 (MvT Wiv 2017).
Kamerstukken II 2016/17, 34 588,18 (Nota naar aanleiding van het Verslag Wiv 2017).
Kamerstukken II 2016/17, 34588, 66.
Kamerstukken II 2017/18, 34588, 70.
Kamerstukken II 2017/18, 34889, 2.
Kamerstukken II 2017/18, 34889, 6.
Kamerstukken II 2018/19, 29924,173.
Kamerstukken II 2018/19, 34242, 3 (MvT Wijzingswet Wiv 2017).
Kamerstukken II 2021/22, 34588, 91.

Regelgeving

België

Wet van 17 november 1808, Wetboek van Strafvordering, Belgisch Staatsblad, dossiernr. 1808-11-17/30.

Wet van 5 augustus 1992, Wet op het Politieambt, Belgisch Staatsblad, dossiernr. 1992-08-05/52.

Wet van 11 december 1998, Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, Belgisch Staatsblad, dossiernr. 1992-12-08/32.

Wet van 25 december 2016 houdende diverse wijzigingen van het Wetboek van strafvordering en het Strafwetboek, met het oog op de verbetering van de bijzondere opsporingsmethoden en bepaalde onderzoeksmethoden met betrekking tot

internet en elektronische en telecommunicaties en tot oprichting van een gegevensbank stemafdrukken, Belgisch Staatsblad, Numac nr. 2017030017.

Duitsland

Wet van 23 mei 1949, Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100-1.

Wet van 1 juni 2017, Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz - BKAG), BGBl. I S. 1354; 2019 I S. 400.

Wet van 7 april 1987, Strafprozeßordnung (StPO), BGBl. I S. 1074, 1319.

Wet van 25 juli 2003, Polizeigesetz des Landes Nordrhein-Westfalen (PolG NRW), GV. NRW. P. 441.

Wet van 30 juni 2017, Bundesdatenschutzgesetz, BGBl. I S. 2097.

Europese Unie

Handvest van de Grondrechten van de Europese Unie van 18 december 2000 (2000/C 364/01) (PbEG 2000, L 320).

Kaderbesluit 2008/977/JBZ van de Raad van 27 november 2008 over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken (PbEU 2008, L 350).

Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie) (PbEG 2002, L 201).

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 en tot intrekking van Kaderbesluit 2008/977/JBZ van de Raad (PbEU 2016, L 119).

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) (PbEU 2016, L 119).

Nederland

***Stb*. 1921, 14**
Wet van 15 januari 1921, Wetboek van Strafvordering, *Stb*. 1921, 14.

***Stb*. 1987/635**
Wet van 3 december 1987 houdende regels betreffende de inlichtingen- en veiligheidsdiensten (Wet op de inlichtingen- en veiligheidsdiensten), *Stb*. 1987, 635.

***Stb*. 1993, 33**
Wet van 23 december 1992 tot wijziging van het Wetboek van Strafrecht en van het Wetboek van Strafvordering in verband met de voortschrijdende toepassing van informatietechniek (Wet computercriminaliteit), *Stb*. 1993, 33.

***Stb*. 1999, 245**
Wet van 27 mei 1999 tot wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden tot opsporing en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), *Stb*. 1999, 245.

***Stb*. 2001, 180**
Wet van 5 april 2001 tot wijziging van bepalingen met betrekking tot de verwerking van persoonsgegevens, *Stb*. 2001, 180.

***Stb*. 2006, 300**
Wet van 1 juni 2006 tot wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (Wet computercriminaliteit II), *Stb*. 2006, 300.

***Stb*. 2002, 552**
Wet van 7 november 2002 tot wijziging van de regels betreffende de verwerking van justitiële gegevens en het stellen van regels met betrekking tot de verwerking *van persoonsgegevens in persoonsdossiers (Wet justitiële gegevens), Stb. 2002, 552.*

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

***Stb*. 2012, 315**
Wet van 12 juli 2012 tot vaststelling van een nieuwe Politiewet *(Politiewet 2012), Stb.* 2012, 315.

***Stb.* 2017, 317**
Wet van 26 juli 2017, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten *(Wet op de inlichtingen- en veiligheidsdiensten 2017), Stb.* 2017, 317.

***Stb.* 2017, 462**
Wet van 22 november 2017 tot wijziging van het Wetboek van Strafvordering in verband met de regeling van het vastleggen en bewaren van kentekengegevens door de politie, Stb. 2017, 462.

***Stcrt.* 2018, 24397**
Besluit van de Minister van Binnenlandse Zaken en Koninkrijksrelaties en de Minister van Defensie van 25 april 2018, nr. 2018-0000251025, houdende vaststelling van beleidsregels met betrekking tot de uitvoering van de Wiv 2017 *(Beleidsregels Wiv 2017), Stcrt. 2018, 24397.*

***Stcrt.* 2018, 36060**
Aanwijzing wet politiegegevens en de rol van de officier van justitie van 29 juni 2018, *Stcrt.* 2018, 36060.

***Trb.* 1951, 154**
Verdrag van 4 november 1950 tot bescherming van de rechten van de mens en de fundamentele vrijheden *(EVRM).*

Voorstel van wet
Memorie van toelichting van juli 2020 bij het wetsvoorstel tot vaststelling van het nieuwe Wetboek van Strafvordering *(ambtelijke versie).*

Noorwegen

Regeling van 20 september 2013, Forskrift om behandling av opplysninger i politiet og påtalemyndigheten (*politiregisterforskriften*).

Wet van 1 januari 1986, Lov om rettergangsmåten i straffesaker (*Straffeprosessloven*).

Wet van 28 mei 2010, Lov om behandling av opplysninger i politiet og påtalemyndigheten (*politiregisterloven*).

Wet van 1 oktober 1995, Lov om politiet (*politiloven*).

2. Jurisprudentie

Rb. Amsterdam 19 april 2018, ECLI:NL:RBAMS:2018:2504.
Rb. Amsterdam 7 december 2018, ECLI:NL:RBAMS:2018:8698.
Rb. Amsterdam, 30 april 2021, ECLI:NL:RBAMS:2021:2161.
Rb. Amsterdam 3 juli 2021, ECLI:NL:BRAMS:2021:3825.
Rb. Amsterdam 14 september 2021, ECLI:NL:RBAMS:2021:5460.
Rb. Amsterdam 30 september 2021, ECLI:NL:RBAMS:2021:5520.
Rb. Amsterdam 22 december 2021, ECLI:NL:RBAMS:2021:7553.
Rb. Amsterdam 5 januari 2022, ECLI:NL:RBAMS:2022:131.
Rb. Amsterdam 17 maart 2022, ECLI:NL:RBAMS:2022:1273.
Rb. Amsterdam 11 mei 2022, ECLI:NL:RBAMS:2022:2453.

Rb. Den Haag 20 januari 2021, ECLI:NL:RBDHA:2021:284.

Rb. Gelderland 20 oktober 2021, ECLI:NL:RBGEL:2021:5621.
Rb. Gelderland 8 december 2021, ECLI:NL:RBGEL:2021:6584.

Rb. Limburg 26 januari 2022, ECLI:NL:RBLIM:2022:558.

Rb. Midden-Nederland 17 juni 2021, ECLI:NL:RBMNE:2021:2570.

Rb. Noord-Holland 4 mei 2022, ECLI:NL:RBNHO:2022:3899.

Rb. Oost-Brabant 25 maart 2021, ECLI:NL:RBOBR:2021:1272.
Rb. Oost-Brabant 8 juli 2021, ECLI:NL:RBOBR:2021:3249.
Rb. Oost-Brabant 15 december 2021, ECLI:NL:RBOBR:2021:6861.
Rb. Oost-Brabant 2 februari 2022, ECLI:NL:RBOBR:2022:312.

Rb. Rotterdam 9 juni 2020, ECLI:NL:RBROT:2020:11875.
Rb. Rotterdam 15 oktober 2021, ECLI:NL:RBROT:2021:10180.

Rb. Zeeland-West-Brabant 24 februari 2021, ECLI:NL:RBZWB:2021:735.
Rb. Zeeland-West-Brabant 6 juli 2021, ECLI:NL:RBZWB:2021:3406.

HR 19 december 1995, ECLI:NL:HR:1995:ZD0328, NJ 1996/249, m.nt. Schalken.
HR 28 oktober 2008, 2009/224, ECLI:NL:HR:2008:BE9817.
HR 20 januari 2009, ECLI:NL:HR:2009:BF5603, NJ 2009/225, m.nt. Borgers.

HR 6 oktober 2009, ECLI:NL:HR:2009:BI7084, NJ 2009/503.
HR 1 juli 2014, ECLI:NL:HR:2014:1562, NJ 2015/114, m.nt. Van Kempen.
HR 1 juli 2014, ECLI:NL:HR:2014:1569, NJ 2015/115, m.nt. Van Kempen.
HR 11 november 2014, ECLI:NL:HR:2014:3142, NJ 2015/296, m.nt. Borgers.
HR 1 december 2020, ECLI:NL:HR:2020:1890, NJ 2021/170, m.nt. Jörg.
HR 5 april 2022, ECLI:NL:HR:2022:475.
HR 28 juni 2022, ECLI:NL:HR:2022:900.

A-G PHR 21 december 2021, ECLI:NL:PHR:2021:1184.

Hof van Cassatie van België, 29 maart 2022, P.22.0078.N/1.

GwH 6 december 2018, nr. 174/2018, ECLI:BE:GHCC:2018:ARR.174.

BVerfG 15 februari 1983, BvR 209/83.
BVerfG 4 april 2006 - 1 BvR 518/02.

EHRM 6 september 1978, nr. 5029/71 (Klass e.a./Duitsland).
EHRM 16 april 1979, nr. 6538/74 (Sunday Times/Verenigd Koninkrijk), NJ 1980/146, m.nt. Alkema.
EHRM 25 maart 1983, nrs. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75 (Silver e.a./Verenigd Koninkrijk).
EHRM 2 augustus 1984, nr. 8691/79 (Malone/Verenigd Koninkrijk).
EHRM 26 maart 1987, nr. 9248/81 (Leander/Zweden).
EHRM 28 maart 1990, nr. 10890/84 (Groppera Radio AG e.a./Zwitserland).
EHRM 24 april 1990, nr. 11105/84 (Huvig/Frankrijk).
EHRM 25 maart 1998, nr. 23224/94 (Kopp/Zwitserland).
EHRM (GK) 16 februari 2000, nr. 27798/95 (Amann/Zwitserland).
EHRM 4 mei 2000, nr. 28341/95 (Rotaru/Roemenië), EHRC 2000/53, m.nt. Brems.
EHRM 12 mei 2000, nr. 35394/97 (Khan/Verenigd Koninkrijk), NJ 2002/180, m.nt. Schalken.
EHRM 25 september 2001, nr. 44787/98 (P.G. & J.H./Verenigd Koninkrijk), NJ 2003/670, m.nt. Dommering.
EHRM 28 januari 2003, nr. 44647/98 (Peck/Verenigd Koninkrijk).
EHRM 17 juli 2003, nr. 63737/00 (Perry/Verenigd Koninkrijk), NJ 2006/40, m.nt. Dommering.
EHRM 6 juni 2006, nr. 62332/00 (Segerstedt-Wiberg/Zweden).
EHRM 29 juni 2006, nr. 54934/00 (Weber en Saravia/Duitsland).

EHRM 1 juli 2008, nr. 58243/00 (Liberty e.a./ Verenigd Koninkrijk).
EHRM (GK) 4 december 2008, nr. 30562/04 (S. en Marper/Verenigd Koninkrijk), NJ 2009/410, m.nt. Alkema, NTM/NJCM-bull. 2009/4, m.nt. Van der Staak.
EHRM 10 maart 2009, nr. 4378/02 (Bykov/Rusland).
EHRM 17 december 2009, nr. 16428/05 (Gardel/Frankrijk).
EHRM 17 december 2009, nr. 22115/06 (M.B./Frankrijk).
EHRM 12 januari 2010, nr. 4158/05 (Gillan & Quinton/Verenigd Koninkrijk), NJ 2010/325, m.nt. Dommering.
EHRM 18 mei 2010, nr. 26839/05 (Kennedy/Verenigd Koninkrijk), NJ 2011/333.
EHRM 2 september 2010, nr. 35623/05 (Uzun/Duitsland).
EHRM 18 oktober 2011, nr. 16188/07 (Khelili/Zwitserland).
EHRM 13 november 2012, nr. 24029/07, (M.M./Verenigd Koninkrijk).
EHRM 14 maart 2013, nr. 24117/08 (Bernh Larsen Holding AS e.a./Noorwegen).
EHRM 18 april 2013, nr. 19522/09 (M.K./Frankrijk).
EHRM 4 juni 2013, nrs. 7841/08 en 57900/12 (Peruzzo en Martens/Duitsland).
EHRM 18 september 2014, nr. 21010/10 (Brunet/Frankrijk).
EHRM 27 oktober 2015, nr. 62498/11 (R.E./ Verenigd Koninkrijk).
EHRM (GK) 4 december 2015, nr. 47143/06 (Roman Zakharov/Rusland), NJ 2017/185, m.nt. Dommering.
EHRM 12 januari 2016, nr. 37138/14 (Szabó en Vissy/Hongarije).
EHRM 18 oktober 2016, nr. 61838/10 (Vukota-Bojić/Zwitserland), AB 2017/418, m.nt. Schuurmans & Uzman.
EHRM 27 juni 2017, nr. 931/13 (Satakunnan Markkinapörssi Oy and Satamedia Oy/Finland).
EHRM 8 februari 2018, nr. 31446/12 (Ben Faiza/Frankrijk).
EHRM 30 januari 2020, nr. 50001/12 (Breyer/Duitsland).
EHRM 13 februari 2020, nr. 45245/15 (Gaughran/UK), EHRC 2020/86, m.nt. Van der Sloot.
EHRM (GK) 25 mei 2021, (Centrum för Rättvisa/Zweden), JBP 2021/62, m.nt. Moyakine, EHRC Updates, m.nt. Hagens en Oerlemans.
EHRM (GK) 25 mei 2021, nrs. 58170/13, 62322/14 & 24960/15 (Big Brother Watch e.a./Verenigd Koninkrijk), NJ 2021/361, m.nt. Dommering.
EHRM 11 januari 2022, nr. 70078/12 (Ekimdzhiev e.a./Bulgarije).

HvJ EG 6 november 2003, C-101/01, ECLI:EU:C:2003:596 (Lindqvist).
HvJ EU 8 april 2014, C-293/12 en C-594/12, ECLI:EU:2014:238 (Digital Rights Ireland).
HvJ EU 6 oktober 2015, C-362/14, ECLI:EU:C:2015:650 (Schrems).

HvJ EU 21 december 2016, C-203/15 en C-698/15, ECLI:EU:C:2016:970 (Tele2 Sverige AB), EHRC 2017/79.
HvJ EU 2 oktober 2018, C-207/16, ECLI:EU:C:2018:788 (Ministerio Fiscal).
HvJ EU 6 oktober 2020, C-511/18, C-512/18, C-520/18, ECLI:EU:C:2020:791 (La Quadrature du Net).
HvJ EU 2 maart 2021, C-746/18, ECLI:EU:C:2021:152 (H.K., in tegenwoordigheid van Prokuratuur).
HvJ EU 15 juni 2021, C-645/19, ECLI:EU:C:2021:483 (Facebook/Gegevensbeschermingsautoriteit).
HvJ EU 5 april 2022, C-140/20, ECLI:EU:C:2022:258 (G.D./Commissioner An Garda Síochána).

A-G HvJ EU 15 januari 2020, C-520/18, ECLI:EU:C:2020:7 (Ordre des barreaux francophones et germanophone e.a.).
A-G HvJ EU 31 maart 2022, C-77/21, ECLI:EU:C:2022:248 (Digi Távközlési és Szolgáltató Kft./Nemzeti Adatvédelmi).
A-G HvJ EU 19 mei 2022, C-180/21, ECLI:EU:C:2022:406 (Verenigde Staten/Inspektor v Inspektorata kam Visshia sadeben savet).

3. LITERATUUR

Alves Hendriques 2020
A. Alves Hendriques, 'Data In Person-Based Predictive Policing', *whatnext.law*.

Andelbeek 2022
W. Andelbeek, 'Wat is de reikwijdte van de Wet politiegegevens?', *Privacy & Informatie* 2022, afl. 1, p. 21-30.

Bas Seyyar & Geradts 2020
M. Bas Seyyar & Z.J.M.H Geradts, 'Privacy impact assessment in large-scale digital forensic investigations', *Forensic Science International: Digital Investigation* 2020, afl. 33.

Van der Bel e.a. 2020
D. van der Bel, B. de Jonge & J.J.T.M. Pieters, *Informatie en opsporing. Handboek informatieverwerving, -verwerking en -verstrekking ten behoeve van de opsporingspraktijk*, Zeist: Kerckebosch 2020.

Berkmoes 2022
H. Berkmoes, 'Het controleorgaan op de politionele informatie', in: *Controle op de politiediensten* 2022, C47/55.

Biega & Finck 2021
A.J. Biega & Michèle Finck, 'Reviving Purpose Limitation and Data Minimisation in Data-Driven Systems', *Technology and Regulation* 2021, p. 44-61.

Bleichrodt, Mevis & Volker 2011
F.W. Bleichrodt, P.A.M. Mevis & B.W.A. Volker, *Vergroting van de slagvaardigheid van het strafrecht: een rechtsvergelijkend perspectief*, Den Haag: WODC 2011.

Borgers 2015
M.J. Borgers, 'Normering van 'lichte' opsporingshandelingen', *DD* 2015/15, p. 143-155.

Van Brakel 2020
R. van Brakel, 'Een reflectie over het huidig toezicht van het gebruik van surveillancetechnologie door de lokale politie in België', in: E. Devroe e.a. (red.), *Toezicht op de politie. Cahiers Politiestudies*, Oud-Turnhout: Gompel & Svacina 2020, p. 139-160.

Brinkhoff 2014
S. Brinkhoff, *Startinformatie in het strafproces* (dissertatie Nijmegen), Deventer: Kluwer 2014.

Brkan 2017
M. Brkan, 'The Court of Justice of the EU, privacy and data protection: Judgemade law as a leitmotif in fundamental rights protection', in: *M. Brkan & E. Psychogiopoulou, Courts, Privacy and Data Protection in the Digital Environment*, Cheltenham: Edward Elgar Publishing 2017, p. 10-31.

Brouwer 2011
E.R. Brouwer, 'Legality and Data Protection Law: The Forgotten Purpose of Purpose Limitation', in: L.F.M. Besselink, S. Prechal, F. Pennings (red.), *The Eclipse of the Legality Principle in the European Union*, Kluwer Law International: Alphen aan de Rijn 2011, p. 273-294.

Bruce 2021
I. Bruce, *Preventive Use of Surveillance Measures for the Protection of National Security. A normative and comparative study of Dutch, Norwegian and Swedish law* (diss. Oslo), 2021 (nog niet gepubliceerd).

Caruana 2017
M.M. Caruana, 'The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement', *International Review of Law, Computers & Technology* 2017, afl. 3, p. 249-270.

Conings 2017
C. Conings, *Klassiek en digitaal speuren naar strafrechtelijk bewijs* (diss. Leuven), Antwerpen: Intersentia 2017.

Corstens/Borgers & Kooijmans 2021
G.J.M. Corstens, *Het Nederlandse strafprocesrecht*, bewerkt door M.J. Borgers & T. Kooijmans, Deventer: Wolters Kluwer 2021.

Coudert 2017
F. Coudert, 'The Europol Regulation and Purpose Limitation: From the "Silo-Based Approach" to … What Exactly?', *European Data Protection Law Review* 2017, afl. 3, p. 313-324.

Custers & Ursic 2016
B. Custers & H. Ursic, 'Big Data and Data Reuse. A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection', *International Data Privacy Law* 2016(6) 1, p. 4-15.

Custers & Leiser 2019
B.H.M. Custers & M.R. Leiser, 'Persoonsgegevens in het strafrecht. Weeffouten in EU-Richtlijn 2016/680 leiden tot praktische problemen', *NJB* 2019/2017, afl. 34, p. 2490-2497.

Das & Schuilenberg 2018
A. Das & M.B. Schuilenberg, 'Predictive policing: waarom bestrijding van criminaliteit op basis van algoritmen vraagt om aanpassing van het strafprocesrecht', *Strafblad* 2018, p. 19-26.

De Hert & Gutwirth 2009
P. de Hert & S. Gutwirth, 'Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action', in: Y. Poullet, S. Gutwirht, C. de Terwanghe & P. de Hert, *Reinventing data protection?*, Berlin: Springer 2009, p. 3-45.

De Hert & Papakonstantinou 2016
P. de Hert & V. Papakonstantinou, 'The new police and criminal justice data protection directive: A first analysis', *New journal of European criminal law* 2016, afl. 3, p. 7-19.

De Hert & Malgieri 2021
P. de Hert en G. Malgieri, 'One European Legal Framework for Surveillance: The ECtHR's expanded legality testing copied by the CJEU', in: V. Mitsilegas & N. Vaoula (eds.), *Surveillance and Privacy in the Digital Age, European, Transatlantic and Global Perspectives*, Oxford: Hart Publishing 2021, p. 255-295.

De Hert & Sajfert 2018
P. de Hert & J. Sajfert, 'The role of data protection authorities in supervising police and criminal justice authorities processing personal data', in: C. Brière & A. Weyembergh (red.), *The needed balances in EU Criminal Law: past, present and future*, London: Hart 2018, p. 243-255.

De Hert & Sajfert 2021
P. De Hert & J. Sajfert, 'The fundamental right to personal data protection in criminal investigations and proceedings: framing big data policing through the purpose limitation and data minimisation principles of the Directive (EU) 2016/680', *Brussels Privacy Hub Working paper* 2021, afl. 7.

Derin & Singelnstein 2021
B. Derin & T. Singelnstein, 'Verwendung und Verwertung von Daten aus massenhaften Eingriffen in informationstechnische Systeme aus dem Ausland (Encrochat)', *NStZ* 2021, p. 449-454.

Dimitrova & De Hert 2018
D. Dimitrova & P. De Hert, 'The right of access under the Police Directive: Small steps forward', in: M. Medina e.a. (red.), *Privacy technologies and policy: 6th Annual Privacy Forum. APF 2018*, Springer International Publishing: Cham 2018, p. 111-130.

Dubelaar, Fedorova & Te Molder 2021
M.J. Dubelaar, M.I. Fedorova & R.M. te Molder, 'De vergaring en het gebruik van digitale gegevens in een strafvorderlijke context', in P.T.J. Wolters e.a. (red.), *Digitalisering en conflictoplossing*, Deventer: Wolters Kluwer 2021, p. 53-81.

Van den Eeden e.a. 2021
C.A.J. van den Eeden, J.J. van Berkel, C.C. Lankhaar & C.J. de Poot, *Opsporen, vervolgen en tegenhouden van cybercriminaliteit*, WODC Cahier 2021-13.

EDPS 2012
European Data Protection Supervisor, 'Opinion on the Data Protection Reform Package', *edps.europa.eu*, 7 maart 2012.

Eskens 2022
S.J. Eskens, 'The ever-growing complexity of the data retention discussion in the EU: An in-depth review of La Quadrature du Net and others and Privacy International', *EDPL* 2022 1(8), p. 143-155.

Eskens, Van Daalen & Van Eijk 2016
S.J. Eskens, O.L. van Daalen & N.A.N.M. van Eijk, *Geheime surveillance en opsporing. Richtsnoeren voor de inrichting van wetgeving*, Amsterdam: Instituut voor Informatierecht (IViR) 2016.

Fokkens & Kirkels-Vrijman 2009
J.W. Fokkens & N. Kirkels-Vrijman, 'De artikelen 2 Politiewet 1993 en 141 en 142 WvSv als basis voor opsporingsbevoegdheden', in: M.J. Borgers e.a. (red.), *Politie in beeld* (Liber amicorum Jan Naeyé), Nijmegen: Wolf Legal Publishers 2009, p. 105-124.

FRA 2018
European Union Agency for Fundamental Rights and Council of Europe (FRA), *Handbook on European data protection law*, Luxemburg: Publications Office of the European Union 2018.

Galič 2021
M. Galič, 'De rechten van de verdediging in de context van omvangrijke datasets en geavanceerde zoekmachines in strafzaken: een suggestie voor uitbreiding', *Boom Strafblad* 2021, afl. 2, p. 41-49.

Galič 2022
M. Galič, 'Bulkbevoegdheden en strafrechtelijk onderzoek: lessen uit de jurisprudentie van het EHRM voor de normering van grootschalige data-analyse', in: *TBS&H* 2022, nr. 2, p. 130-137.

Gerhold 2022
S.F. Gerhold, '§ 98c', in: J.P. Graf, *BeckOK StPO,* C.H. Beck: München 2022.

Gonzalez Fuster 2014
G. Gonzalez Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Cham: Springer 2014.

Von Grafenstein 2018
M. von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws. The Risk-Based Approach, Principles, and Private Standards as Elements for Regulating Innovation*, Baden-Baden: Nomos 2018.

Groenhart, in: *T&C Privacy- en gegevensbeschermingsrecht* 2020
N.W. Groenhart, commentaar op art. 34 Wpg, in: *Tekst & Commentaar Privacy- en gegevensbeschermingsrecht*, Deventer: Wolters Kluwer 2020.

Günther 2014
H.L. Günther, '§ 98a', in: C. Knauer, H. Kudlich & H Schneider (Hrsg.), *Münchener Kommentar zu Strafprozessordnung*, C.H. Beck: München 2014.

Hahn 2021
I. Hahn, 'Purpose Limitation in the Time of Data Power: Is There a Way Forward?', *EDPL* 2021, afl. 1, p. 37-38.

Von Häfen 2022
M. von Häfen, '§ 500', in: J.P. Graf, BeckOK StPO, C.H. Beck: München 2022.

Harris e.a. 2018
D.J. Harris e.a., *Harris, O'Boyle & Warbrick: Law of the European Convention on Human Rights*, Oxford: Oxford University Press 2018.

Heckmann/Scheurer 2019
D. Heckmann & M. Schreuer, '§ 49', in: P. Gola & D. Heckman, *Kommentar zu BDSG*, C.H. Beck: München 2019.

Van Hoboken 2016
J. van Hoboken, 'From Collection to Use in Privacy Regulation? A Forward-Looking Comparison of European and US Frameworks for Personal Data Processing', in: B. van der Sloot, D. Broeders & E. Schrijvers (red.), *Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press 2016, p. 231-252.

Hudobnik 2020
M.M. Hudobnik, 'Data protection and the law enforcement directive: a procrustean bed across Europe?', *ERA Forum* 2020, nr. 21, p. 485-500.

Information Commissioner's Office, *Guide to Law Enforcement processing*
Information Commissioner's Office, *Guide to Law Enforcement Processing*. Beschikbaar via: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/.

Jacobs 2016
B.P.F. Jacobs, 'Select while you collect: over de voorgestelde interceptiebevoegdheden voor inlichtingen- en veiligheidsdiensten', *NJB* 2016, p. 256-261.

Jansen 2021
R.H.T. Jansen, 'Toezicht onder de Wet op de inlichtingen- en veiligheidsdiensten 2017: een tour de force', *NTM-NJCMBull* 2021/32, p. 419-443.

Jasserand 2018a
C. Jasserand, 'Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle Purpose Limitation', *European Data Protection Law Review* 2018, afl. 2, p. 152-167.

Jasserand 2018b
C. Jasserand, 'Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?', *Computer Law and Security Review* 2018, p. 154-165.

De Keersmaecker & Van de Heyning 2021
R. de Keersmaecker & C. van de Heyning, 'De bewaarplicht van en toegang tot telecomgegevens na de arresten van het Hof van Justitie en het Grondwettelijk Hof: een nieuwe episode in de dataretentie-saga', *Tijdschrift voor strafrecht* 2021, p. 171-189.

Koning 2020
M.E. Koning, *The purpose and limitations of purpose limitation* (diss. Nijmegen), Nijmegen 2020.

Koops 2019
B.J. Koops, 'Privacyconcepten voor de 21e eeuw', *ArsAequi* 2019, p. 532-544.

Koops, Conings & Verbruggen 2016

B.J. Koops, C. Conings & F. Verbruggen, *Zoeken in computers naar Nederlands en Belgisch recht: Welke plaats hebben 'digitale plaatsen' in de systematiek van opsporingsbevoegdheden?* (Preadviezen voor de Nederlands-Vlaamse Vereniging voor Strafrecht), Nijmegen: Wolf Legal Publishers 2016.

Kranenborg & Verhey 2018
H.R. Kranenborg & L.F.M. Verhey, *De Algemene Verordening Gegevensbescherming in Europees en Nederlands perspectief (Mastermonografieën staats- en bestuursrecht*), Deventer: Wolters Kluwer 2018.

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

Loideain 2022
N.N. Loideain, 'The Approach of the European Court of Human Rights to the Interception of Communications', in: *EU Data Privacy Law and Serious Crime*, Oxford: Oxford University Press, 2022 (wordt verwacht), p. 30-73. Draft raadpleegbaar via: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3699386.

Mac Gillavry 2005
E.C. Mac Gillavry, 'Heeft u even voor de nieuwe Wet politiegegevens?', in: A. Harteveld, D.H. de Jong & E. Stamhuis, *Systeem in ontwikkeling. Liber amicorum Geert Knigge*, Nijmegen: Wolf Legal Publishers 2005, p. 385-416.

Malgieri & De Hert 2017
G. Malgieri, & P. de Hert, 'European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards Good Enough Judicial Oversight', in: D. Gray & S Henderson (eds.), *Cambridge Handbook of Surveillance Law*, Cambridge: Cambridge University Press 2017, p. 509-532.

Moerel & Prins 2016
E.M.L. Moerel en J.E.J. Prins, 'Privacy voor de homo digitalis', in: *Homo digitalis. Preadviezen* (Handelingen Nederlandse Juristen-Vereniging, deel 2016-I), Deventer: Wolters Kluwer 2016/1, p. 1-136.

Mouzakiti 2020

F. Mouzakiti, 'Cooperation between Financial Intelligence Units in the European Union: Stuck in the middle between the General Data Protection Regulation and the Police Data Protection Directive', *New Journal of European Criminal Law* 2020, afl. 3, p. 351-374.

Oerlemans & Hagens 2019
J.J. Oerlemans & M. Hagens, 'Privacy en bulkinterceptie in de Wiv 2017', *Ars Aequi* 2019, p. 560-568.

Oerlemans 2020a
J.J. Oerlemans, *Grenzen stellen aan datahonger. De bescherming van de nationale veiligheid in een democratische rechtsstaat* (oratie Utrecht) 2020.

Oerlemans 2020b
J.J. Oerlemans, 'Metadata-analyse in de Wiv 2017', *Privacy & Informatie* 2020, nr. 6, p. 260-267.

Oerlemans e.a. 2021
J.J. Oerlemans, M. Hagens & S. Royer, 'Tijd voor een nieuwe bewaarplicht?', *Computerrecht* 2021/59, afl. 2, p. 151-159.

Peters 2022
S. Peters, commentaar bij *Politiregisterloven*, 2022. Beschikbaar via: http://www.rettsdata.no.

***Rapport Commissie-Bovend'Eert* 2022**
Rapport Commissie-Bovend'Eert, Naar een duurzaam en effectief stelsel van toezicht op de inlichtingen- en veiligheidsdiensten, 2022.

***Rapport Commissie-Dessens* 2013**
Rapport Evaluatiecommissie Dessens, Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen, Den Haag 2013.

***Rapport Commissie-Jones-Bos* 2020**
Rapport Evaluatiecommissie Wiv 2017 (commissie Jones-Bos), Evaluatie 2020: wet op de inlichtingen- en veiligheidsdiensten 2017, Den Haag 2022.

***Rapport Commissie-Koops* 2018**

Rapport commissie modernisering opsporingsonderzoek in het digitale tijdperk, 2018.

Royer 2020
S. Royer, *Strafrechtelijk beslag. Digiproof en (multi)functioneel* (diss. Leuven), Antwerpen: die Keure 2020.

Sajfert & Quintel 2019
J. Sajfert & T. Quintel, *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities*. Beschikbaar via:
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4016491

Samadi 2020
M. Samadi, *Normering en toezicht in de opsporing: een onderzoek naar de normering van het strafvorderlijk optreden van opsporingsambtenaren in het voorbereidend onderzoek en het toezicht op de naleving van deze normen* (diss. Leiden), Den Haag: Boom Juridisch 2020.

Schermer 2017
B.W. Schermer, 'Het gebruik van Big Data voor opsporingsdoeleinden: tussen strafvordering en de Wet politiegegevens', *TBS&H* 2017, afl. 4, p. 207-216.

Schermer & Oerlemans 2020
B.W. Schermer & J.J. Oerlemans, 'AI, strafrecht en het recht op een eerlijk proces', *Computerrecht* 2020/3, afl. 1, p. 14-21.

Schuermans 2017
F. Schuermans, 'Politionele informatiehuishouding en cameragebruik', in: *Strafrecht en strafprocesrecht: doel of middel in een veranderde samenleving?*, Deventer: Wolters Kluwer 2017, p. 703-751.

Schuermans 2020
F. Schuermans, 'Politionele handhaving en gegevensbescherming: een beladen wedstrijd met het COC als scheidsrechter', *Tijdschrift Privacy & Persoonsgegevens* 2020/3, p. 42.

Singelnstein 2019
T. Singelnstein, **'**§ 474-499 StPO**'**, in: C. Knauer, H. Kudlich & H. Schneider (Hrsg.), *Münchener Kommentar zur Strafprozessordnung, Band 3/1*, C. H. Beck: München 2019.

Singelnstein 2020
T. Singelnstein, 'Folgen des neuen Datenschutzrechts für die Praxis des Strafverfahrens und die Beweisverbotslehre', *NStZ* 2020, p. 639.

Sholeh 2022
G.P. Sholeh, 'De betekenis van het Prokuratuur-arrest: digitale opsporing en privacy onder de loep', *DD* 2022/15, p. 227-247.

Simmelink 2017
J.B.H.M. Simmelink, 'Normering van opsporingsbevoegdheden in het gemoderniseerde Wetboek van Strafvordering', *RMThemis* 2017-6, p. 323-333.

Van der Sloot 2021
B. van der Sloot, 'Big Brother Watch and others v. the United Kingdom & Centrum för Rättvisa v. Sweden: Does the Grand Chamber Set Back the Clock in Mass Surveillance Cases?', *European Data Protection Law Review* 2021, p. 319-326.

Van der Sloot 2020
B. van der Sloot, 'The Quality of Law: how the European Court of Human Rights gradually became a European Constitutional Court for privacy cases', *JIPITEC* 2020, nr. 2, vol. 11, p. 160-185.

Van der Sloot 2017
B. van der Sloot, 'Legal Fundamentalism: Is data Protection Really a Fundamental Rights?', in: R. Leenes et al. (red.), *Data protection and privacy: (In)visibilities and Infrastructures*, Springer 2017, p. 3-30.

Van der Sloot & Kosta 2019
B. van der Sloot & E. Kosta, 'Big Brother Watch and Others v UK: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance', *European Data Protection Law Review* 2019, nr. 2, vol. 5, p. 252-261.

Stevens & Koops 2021
L. Stevens & B.J. Koops, 'Naar een Strafvordering 2030 and beyond', in: M. Braakman e.a., *Op zoek naar evenwicht. Liber amicorum Marc Groenhuijsen*, Deventer: Wolters Kluwer 2021, p. 701-713.

Stevens e.a. 2021
L. Stevens e.a., 'Strafvorderlijke normering van preventief optreden op basis van datakoppeling. Een analyse aan de hand van casus Sensingproject Outlet Roermond', *TBS&H* 2021, afl. 4, p. 234-245.

Sunde 2021
I.M. Sunde, 'Effektiv, tillitvekkende og rettssikker behandling av databevis. En straffeprosessuell utredning om ransaking, sikring og beslag i data', Avgitt til Justis- og beredskapsdepartementet, (Efficiente, betrouwbare en rechtsmatige verwerking van digitaal bewijs. Een rapport met betrekking tot doorzoeking, beveiliging en inbeslagneming van data in de strafvordering. Aangeboden aan het Ministerie van Justitie en Veiligheid, 18 juni 2021), beschikbaar via: https://phs.brage.unit.no/phs-xmlui/bitstream/handle/11250/2762721/Utredning%20databevis_Sunde.pdf?sequence=1&isAllowed=y.

TNO 2016
TNO, 'Privacy Impact Assessment Wet op de inlichtingen- en veiligheidsdiensten 20XX', *aivd.nl* 12 februari 2016.

Toe Laer 2019
A.H. Toe Laer, 'Klachtbehandeling in de Wiv 2017: een belangrijke waarborg tegen onrechtmatig handelen van de inlichtingen- en veiligheidsdiensten', *NJB* 2019, p. 734-738.

Torgersen e.a. 2016
R. Torgersen e.a., 'Proposal for a new Norwegian code of Criminal Procedure. A summary of NOU 2016: 24', *Bergen Journal of Criminal Law and Criminal Justice* 2016/2, p. 286-315.

Vis 2012
T. Vis, *Intelligence, politie en veiligheidsdienst: Verenigbare grootheden?* (diss. Tilburg University), Tilburg University 2012.

Voermans & Muller 2017
W. Voermans & E. Muller, 'Nieuwe Wet op de Inlichtingen- en Veiligheidsdiensten: een nieuw evenwicht tussen veiligheid en waarborgen', *NJB* 2017/95, p. 102-109.

Vogiatzoglou e.a. 2020
P. Vogiatzoglou e.a., 'From Theory to Practice: Exercising the Right of Access under The Law Enforcement Directive and PNR Directives', *Jipitec* 2020, 11(3), p. 274-302.

De Vries 2017
I. de Vries, 'Big Data', in: M. den Hengst, T. ten Brink & J. ter Mors (red.), *Informatiegestuurd politiewerk in de praktijk*, Deventer: Vakmedia 2017.

Van Wifferen 2003
L. van Wifferen 'Intelligence in het strafproces: over de waarde van door de inlichtingen- en veiligheidsdiensten verstrekte informatie', *NJB* 2003, p. 617-621.

Winter e.a. 2020
H.B. Winter e.a., *De verwerking van politiegegevens in vijf Europese landen*, Groningen/Den Haag: WODC 2020.

Wolters, Ruckert & Van Sloten 2016
N. Wolters, Ruckert & L. van Sloten, 'Big Data: Big Privacy Challenges', *Computerrecht* 2016, afl. 3, p. 155-159.

WP29 2013
Article 29 data protection working party, *Opinion 03/2013 of the Article 29 Data Protection Working Party on Purpose limitation*, WP 203, *ec.europe.eu*, 2 april 2013.

WP29 2015/233
Article 29 data protection working party, 'Opinion 03/2015 on the draft directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data', WP 233, *ec.europe.eu*, 1 december 2015.

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

Yperman, Royer & Verbruggen 2019

W. Yperman, S. Royer & F. Verbruggen, 'Vissen op de grote datazee: digitale informatievergaring in vooronderzoek en strafuitvoering', *Nullum Crimen* 2019, p. 389-416.

Zwenne & Schmidt 2016
G.J. Zwenne & A.H.J. Schmidt, 'Wordt de homo digitalis bestuursrechtelijk beschermd?', in: E.L.M Moerel e.a.: *Homo digitalis. Preadviezen* (Handelingen Nederlandse Juristen-Vereniging, deel 2016-I), Deventer: Wolters Kluwer 2016/1, p. 307-381.

Bijlagen: deskundigen die aan het onderzoek hebben bijgedragen

1. GEÏNTERVIEWDE PERSONEN

Dr. I. (Ingvild) Bruce, Bergen, Noorwegen

Dr.mr. C. (Charlotte) Conings, Advocaat Stibbe BV / SRL

Prof. K. (Kai) Cornelius, Universiteit Hamburg

Dr. B (Benjamin) Derin, Advocaat in Berlijn

Drs. Ing. A.E. (Sandor) Dooper, Operationeel Specialist Intelligence, eenheid Oost-Nederland

Dr. mr. C. (Catherine) Jasserand-Breeman, Centre for IT & IP Law, Leuven

Mr. D.N. (Desiree) de Jonge, strafrechtadvocaat bij Cleerdin & Hamer Advocaten te Rotterdam

J. (Jarle) Langeland, Senior Data Protection Officer, National Criminal Investigation Service (Kripos), Oslo, Noorwegen

Dr. mr. T. (Thomas) Kraniotis, Senior rechter, Rechtbank Oost-Brabant

Mr. T. (Thomas) Marquenie, Centre for IT & IP Law, KU Leuven

Medewerker van AIVD, Adviseur bij de afdeling bestuursondersteuning die zich bezighoudt met de herziening van de Wiv 2017

Mr. G. (Geertje) van Roermund, Senior informatieofficier van justitie, Arrondissementsparket Oost-Nederland

Dr.mr. S. (Sofie) Royer, Onderzoeksexpert aan het Centre for IT & IP Law, KU Leuven

Mr. J. (Juraj) Sajfert, Researcher aan de Law, Science, Technology & Society Research Group, Vrije Universiteit Brussel

Prof. T. (Tobias) Singelnstein, Ruhr-Universität Bochum

Prof. I.M. (Inger Marie) Sunde, Politihøgskolen, Norwegian Police University College, Oslo

Mr. T. (Tess) Priester, Senior Officer International Investigations bij de Autoriteit Persoonsgegevens

Mr. S. (Sylvia) Eeuwema, senior inspecteur bij de Autoriteit Persoonsgegevens

Prof. mr. F. (Frank) Verbruggen, Professor Institute of Criminal Law, KU Leuven

2. AANWEZIGEN EXPERTMEETING

Mr. W. (Wilko) Andelbeek, stafjurist/privacyfunctionaris politie Zeeland-West-Brabant

Mr. V.M. (Vincent) Cozijn, strategisch adviseur wet- en regelgeving bij de Gegevensautoriteit van de politie

Dr. mr. M. (Maša) Galič, universitair docent straf(proces)recht & privacy aan de Vrije Universiteit Amsterdam

Prof. mr. M.F.H. (Marianne) Hirsch Ballin, hoogleraar straf- en strafproces recht aan de Vrije Universiteit Amsterdam

Prof. mr. B.W. (Bart) Schermer, hoogleraar recht & digitale technologie aan eLaw, Universiteit Leiden

Mr. drs. B.A. (Birgit) Vredendaal, strategisch adviseur wet- en regelgeving bij de Gegevensautoriteit van de politie

De politie heeft vanwege de digitaliserende maatschappij steeds meer mogelijkheden om enorme hoeveelheden persoonsgegevens te verzamelen, verder te onderzoeken en met elkaar te combineren via geavanceerde technologieën. Het huidige juridische kader is echter nog onvoldoende aangepast aan deze nieuwe realiteit. In opdracht van het WODC worden in dit onderzoek de wettelijke waarborgen bij strafvorderlijke vergaring van gegevens bezien in samenhang met waarborgen die gelden voor de daaropvolgende (verdere) verwerking van die gegevens. Daartoe vindt inventarisatie plaats van de eisen en waarborgen die het Europese recht stelt aan de verwerking van gegevens voor strafvorderlijke doeleinden. Voorts wordt inspiratie geput uit ervaringen met de Wet op de Inlichtingen- en Veiligheidsdiensten 2017 en het recht in België, Duitsland en Noorwegen. Dit onderzoek biedt handvatten voor de wetgever om de wijze van normeren en de inrichting van een wettelijke regeling nader te doordenken om de privacy van burgers beter te beschermen.

ISBN 978-90-8317-899-8

9 789083 178998 >

SteR | Onderzoekcentrum voor Staat & Recht
Radboud Universiteit

iHub

Radboud Universiteit

www.ru.nl/radbouduniversitypress