Terrorismebestrijding en informationele privacy

Het spanningsveld tussen veiligheid en privacy vertaald naar het archiveringssysteem van opsporings- en veiligheidsdiensten

11 augustus 2008

Karel Renders
Het Zool 23
8939 BL Leeuwarden
stud.nr. 5626129

Masterscriptie
MA Archiefwetenschap
Universiteit van Amsterdam

Begeleider:
Drs. H. Waalwijk
Tweede beoordelaar:
Prof. dr. F.C.J. Ketelaar

INHOUD

1. INLEIDING

1.1. Informatie als grondstof: de strijd om de gegevens

De afgelopen jaren is het domein van de terrorismebestrijding prominent op de voorgrond getreden. Veel partijen zijn betrokken bij de bestrijding van terrorisme.[1] Door de Nederlandse regering zijn maatregelen genomen en is wetgeving ontwikkeld (of in ontwikkeling) die justitie, politie en inlichtingen- en veiligheidsdiensten meer bevoegdheden geven om de kans op een terroristische aanslag te verkleinen.

Centraal in veel antiterreurmaatregelen staat de wens van de bij terreurbestrijding betrokken overheidsorganen om de beschikking te hebben over 'informatie' en hiermee samenhangend over 'gegevens' of 'data', die immers ten grondslag liggen aan 'informatie'. De ministers van BZK en Justitie noemen 'het doelmatig verkrijgen en gebruiken van informatie' als één van de bepalende factoren voor het vermogen van de overheid om de dreiging van terrorisme doeltreffend aan te pakken: informatie is de belangrijkste 'grondstof' voor terrorismebestrijding.[2]

Ontwikkelingen in de informatietechnologie hebben er de laatste jaren toe geleid dat publieke en private organisaties in gedigitaliseerde vorm steeds meer gegevens over burgers verzamelen en verwerken die nuttig zijn voor speurders en terreurbestrijders. Gevoegd bij de ontwikkeling van nieuwe technologieën op het terrein van informatieverwerking, zoals het koppelen van bestanden en *datamining*-technieken, heeft dit ertoe geleid dat de belangstelling van opsporings- en veiligheidsdiensten voor deze gegevens sterk is toegenomen.

De wens te kunnen beschikken over informatie vertaalt zich in wetten en voorstellen die de bevoegdheden van opsporings- en beveiligingsdiensten tot het raadplegen, ter beschikking krijgen of vorderen van bij derden berustende gegevens uitbreiden en die de diensten meer armslag geven tot het (verder) verwerken van persoonsgegevens. Keerzijde hiervan is echter dat dit ten koste kan gaan van de grondwettelijk vastgelegde en in privacywetgeving uitgewerkte bescherming van de informationele privacy van degenen op wie de gegevens betrekking hebben. In dit verband dringt de vraag zich op welke risico's de maatregelen met zich mee kunnen brengen voor een verstoring van de balans tussen opsporing/veiligheid en privacy.

De (antiterreur)maatregelen -met betrekking tot gegevensverwerking- en de privacywetgeving zijn omgevingselementen (en als zodanig deel van de zogenaamde maatschappelijke context) waarbinnen archiveringssystemen opereren. De vraag treedt dan ook op de voorgrond hoe de archiveringssystemen van opsporings- en veiligheidsdiensten kunnen reageren op deze (wijzigingen in) omgevingsfactoren om ervoor te zorgen dat de bescherming van de informationele privacy niet het kind van de rekening wordt.

1.2. Probleemstelling

Vanuit deze achtergrond is voor dit onderzoek de volgende probleemstelling geformuleerd:

Wat betekenen de in Nederland in het kader van de terreurbestrijding van kracht geworden wettelijke bevoegdheden van opsporings- en veiligheidsdiensten inzake verwerking van persoonsgegevens voor de informationele privacy van onderzoekssubjecten en hoe kan het archiveringssysteem van opsporings- en veiligheidsdiensten ervoor zorgen dat deze privacy wordt beschermd?

[1] In *Bijlage I* is een schets gegeven van de organisatie van de terreurbestrijding.
[2] Brief van de Ministers van Justitie en van BZK aan de Voorzitter van de Tweede Kamer der Staten-Generaal over Terrorismebestrijding (10 september 2004), TK 2003-2004, 29 754, nr.1, p. 5, 7.

Definities en uitgangspunten

Bij de probleemstelling zijn de volgende definities en uitgangspunten gehanteerd:

- *In het kader van de terreurbestrijding*: dit mag ook gelezen worden als 'onder het voorwendsel van de terreurbestrijding' daar veel wetsvoorstellen terzake al vóór '9/11' voorbereid zijn. Voor het onderzoek is niet de motivering voor de wetgeving van belang, maar de wetgeving *an sich* en de betekenis ervan voor de informationele privacy en de hieruit voortvloeiende gevolgen voor de inrichting van een archiveringssysteem.

-*Verwerking van persoonsgegevens*: het onderzoek hanteert de in de Wet bescherming persoonsgegevens (Wbp) geformuleerde definitie: 'elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens'.[3]

- *Persoonsgegevens*: het onderzoek hanteert de in de Wbp geformuleerde definitie: 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon'.[4] Persoonsgegevens worden in het onderzoek beschouwd als (digitale) archiefbescheiden of '*records'*.[5]

- *Informationele privacy*: deze term duidt het facet van de eerbiediging van de persoonlijke levenssfeer aan dat ziet op de verwerking van persoonsgegevens, zoals deze is geformuleerd in het eerste en tweede lid van artikel 10 van de Nederlandse Grondwet en in artikel 8 van het Europees verdrag voor de rechten van de mens (EVRM).

- *Onderzoekssubjecten*: deze term wordt gebruikt om de persoon aan te duiden die voorwerp is van een opsporings- of veiligheidsonderzoek. De term is neutraler dan 'verdachte'; ook (nog) niet-verdachten kunnen immers voorwerp van onderzoek zijn.[6]

- *Archiveringssysteem*: het geheel van procedures, methoden, kennis, mensen, middelen en documenten, waarmee een organisatie de archiveringsfunctie vorm geeft. Deze archiveringsfunctie is de functie met als doel het beheer en de beschikbaarstelling van procesgebonden informatie die de organisatie nodig heeft voor de uitvoering van taken of het afleggen van verantwoording.[7]

Afbakening

- *het archiveringssysteem van opsporings- en veiligheidsdiensten:* gezien de veelheid aan concrete, specifieke archiveringssystemen binnen het opsporings- en veiligheidsdomein gaat het onderzoek uit van een abstracte, ideaaltypische benadering

[3] De Wet bescherming persoonsgegevens (Wbp) definieert de verwerking van persoonsgegevens als 'elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens (elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon), 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.' Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), Stb. *302*, artikel 1, lid b.

[4] Ibidem, artikel 1, lid a.

[5] E. Shepherd en G. Yeo, *Managing records. A handbook of principles and practice* (Londen 2003), 15-16: 'Data in electronic transaction systems are records. (…) Evidentiary data need to be fixed in time.'

[6] De term 'onderzoekssubject' wordt gebruikt door E.C. Mac Gillavry in het artikel 'Heeft u even voor de nieuwe Wet politiegegevens?' in: A. Harteveld, D.H. de Jong en E. Stamhuis, E. (red.) in: *Systeem in ontwikkeling, Liber amicorum G. Knigge* (Nijmegen 2005; http://irs.ub.rug.nl/ppn/296127892) 385-416, aldaar 387.

[7] P.J. Horsman, *Archiveren. Een inleiding* ('s Gravenhage 2004), 39.

van een archiveringssysteem van (samenwerkingsverbanden van) diensten die onder de werking van de Wet politiegegevens (Wpolg) of Wet op de inlichtingen- en veiligheidsdiensten (Wiv) 2002 vallen. Hoewel de verschillen tussen de bevoegdheden op het gebied van gegevensverwerking (en hiermee samenhangend de inrichting van archiveringssystemen) van de diensten vallend onder de Wpolg en de Wiv 2002 soms aanzienlijk zijn, is de uitdaging die gesteld wordt aan een privacybeschermende inrichting van systemen dermate algemeen en generiek dat een ideaaltypische invalshoek gerechtvaardigd is.

- *van kracht geworden wettelijke bevoegdheden van opsporings- en veiligheidsdiensten inzake verwerking van persoonsgegevens*: het onderzoek beperkt zich in dit verband tot de volgende wetten: inlichtingen- en veiligheidsdiensten (Wiv 2002), justitiële en strafvorderlijke gegevens, politiegegevens, vorderen gegevens telecommunicatie, bevoegdheden vorderen gegevens en verruiming mogelijkheden opsporing en vervolging terroristische misdrijven. De looptijd van het onderzoek betreft de periode vanaf '9/11' (september 2001) tot 1 april 2008.

1.3. Onderzoeksmethodiek en opbouw

Ter beantwoording van de probleemstelling start de paper met het schetsen van de maatschappelijk-juridische context van privacywetgeving en antiterreurmaatregelen inzake gegevensverwerking door opsporings- en veiligheidsdiensten. Dit gebeurt aan de hand van een grammaticale, wethistorische en systematische interpretatie van de relevante wet- en regelgeving op dit terrein.

Na een bespreking van de generieke privacywetgeving (de Wet bescherming persoonsgegevens) in hoofdstuk 2, komen in de hoofdstukken 3 en 4 de verzameling (gereguleerd via het Wetboek van Strafvordering) respectievelijk de - verdere - verwerking van persoonsgegevens (vastgelegd in sectorale privacywetgeving) door opsporingsdiensten aan bod. De paper volgt de steeds verdere verruiming van de bevoegdheden gegevens te verzamelen en te vorderen en belicht door een bespreking van de Wet politiegegevens de wetgeving met betrekking tot gegevensverwerking door een prominente speler binnen het opsporingsdomein. In hoofdstuk 5 komt de verzameling en verwerking van gegevens door inlichtingen- en veiligheidsdiensten aan bod, die in één wet is geregeld, de Wet op de inlichtingen- en veiligheidsdiensten 2002.

Vervolgens behandelt de paper in hoofdstuk 6 de systematiek van verzameling en uitwisseling van gegevens door en tussen opsporings- en veiligheidsdiensten. Dit gebeurt door een beschrijving van een tweetal vormen van verzameling en uitwisseling en aan de hand van een bespreking van een onderzoeksrapport over de systematiek.

Hoofdstuk 7 schetst het spanningsveld tussen veiligheid en privacy dat voortvloeit uit de in de voorgaande hoofdstukken geconstrueerde juridisch-maatschappelijke context. Hiertoe benoemt de paper de waarborgen en risico's voor de informationele privacy.

Het laatste deel van de paper belicht de gevolgen van de (gewijzigde) maatschappelijk-juridische context en de eruit voortvloeiende privacyrisico's voor de inrichting van het archiveringssysteem van opsporings- en veiligheidsdiensten ter bescherming van de informationele privacy. Er vindt aan de hand van archivistische inzichten, wettelijke bepalingen en toetsingskaders als het ware een archivistische vertaling plaats van de vereiste privacywaarborgen. Hiertoe worden de verschillende archiveringssystemen in één ideaaltypische verschijningsvorm beschouwd. De bespreking van de implicaties heeft daardoor een theoretisch-reflecterend karakter.

Hoofdstuk 8 stelt de kaders waarbinnen de vertaalslag uitgevoerd wordt. De hoofdstukken 9 en 10 reflecteren over de aspecten, uitdagingen en dilemma's waarmee het archiveringssysteem wordt geconfronteerd bij het beschermen van de informationele privacy. Elementen die hierbij de revue passeren zijn archivistische

concepten als kwaliteit en integriteit, metadata, context en contextualisering, technische en organisatorische maatregelen voor toegangsbeveiliging

De paper sluit af met een conclusie, gevolgd door een uitgebreid overzicht van de geraadpleegde bronnen. Enkele bijlagen, waaronder een overzicht van relevante wetgeving en gebruikte afkortingen, completeren het geheel.

2. GENERIEKE INFORMATIONELE PRIVACYWETGEVING: WBP

Dit hoofdstuk behandelt de in de Nederlandse grondwet vastgelegde en in de generieke Wet bescherming persoonsgegevens (Wbp) uitgewerkte bescherming van de informationele privacy van degenen op wie persoonsgegevens betrekking hebben. Het Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM), waarvan artikel 8 bepalingen omvat over de informationele privacy, is in *Bijlage II* kort beschreven. Sectorale en/of aanvullende wetgeving op dit vlak, dat gegevensverwerking reguleert die plaatsvindt binnen opsporings- en inlichtingendiensten, komt in de hoofdstukken 4 en 5 aan de orde.

Wet bescherming persoonsgegevens (Wbp) [8]

Binnen het geheel van de privacywetgeving in Nederland is de in 2001 in werking getreden Wet bescherming persoonsgegevens (Wbp) van groot belang. Deze wet is de vormgeving van artikel 10 van de Grondwet, dat gewijd is aan de informationele privacybescherming.[9]

De Wbp regelt de bescherming van de persoonlijke levenssfeer in verband met het verwerken van persoonsgegevens.[10] Anders dan de voorganger, de Wet Persoonsregistraties (Wpr), regelt de Wbp niet alleen de *registratie* van persoonsgegevens, maar veel ruimer de *verwerking* ervan: *elke* handeling of elk geheel van handelen met betrekking tot persoonsgegevens. De Wbp legt de verantwoordelijke[11] voor het verwerken van persoonsgegevens verplichtingen op en

---

[8] Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), Stb. 302. De Wbp is een implementatie van de Europese richtlijn nr. 95/46/EG. Dit hoofdstuk over de Wbp is gebaseerd op de Wetstekst (Stb. 2000, 302), de Memorie van Toelichting - MvT (TK 1997-1998, 25 892, nr.3), de publicatie *Wet bescherming persoonsgegevens. Handleiding voor verwerkers van persoonsgegevens* (Den Haag: Ministerie van Justitie, april 2002) en F.C.J. Ketelaar en C.G.M. Noordam, Archiefrecht, een inleiding (Amsterdam: Archiefschool, 2005) 66-72.

[9] Grondwet, artikel 10:
lid 1: Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer;
lid 2: De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens;
lid 3: De wet stelt regels inzake de aanspraken van personen op kennisneming van over hem vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

[10] Zoals Ketelaar terecht opmerkt is het terrein van de eerbiediging van de persoonlijke levenssfeer ruimer dan alleen de bescherming met betrekking tot de verwerking van persoonsgegevens, hetgeen duidelijk wordt als het recht op privacy omschreven wordt in de klassieke definitie *'The right to be left alone'*, zie hiervoor: F.C.J. Ketelaar, 'Elke handeling telt. Archiefdiensten en de Wet Bescherming Persoonsgegevens' (geactualiseerde versie van 6 augustus 2001 van een artikel, verschenen in het Archievenblad 104/3 (mei 2000) 18-23 en 104/4 (juni 2000) 26-29) 1. P.H. Blok laat in z'n dissertatie *Het recht op privacy* zien dat het bij de bescherming van de informationele privacy om andere waarden gaat dan bij de zogenaamde 'kernfacetten' van het recht op eerbieding van de persoonlijke levenssfeer. Bij de kernfacetten (zoals bescherming van de woning, het lichaam of het intieme leven) staat de bescherming tegen invloeden van buitenaf centraal en gaat het in essentie om een *principiële onschendbaarheid*. In het kader van de informationele privacy is het doel een oplossing te vinden voor de problematiek van de informatiemacht die samenhangt met het verzamelen, de opslag en het gebruik van persoonsgegevens. In de kern gaat het hierbij om een *belangenafweging* en *zorgvuldigheidsnormen*; zie: E.C. Mac Gillavry, 'Heeft u even voor de nieuwe Wet politiegegevens?' 387.

[11] Anders dan de Wpr richt de Wbp zich primair tot de 'verantwoordelijke' (voor het proces 'gegevensverwerking', als object van regelgeving) in plaats van tot de 'houder ' (van de zaak 'persoonsregistratie', als object van regelgeving). Om te bepalen wie de verantwoordelijke is, moet allereerst worden gekeken welke natuurlijke persoon, rechtspersoon of bestuursorgaan *formeel-juridisch* (in plaats van *feitelijk*) de bevoegdheid heeft om het doel en de middelen van de gegevensverwerking vast te stellen (Wbp, artikel 1, vierde lid). Pas als onduidelijk is wie die bevoegdheid heeft (bijvoorbeeld als meerdere actoren bij de gegevensverwerking zijn betrokken), moet worden gekeken aan wie die bevoegdheid moet worden toegerekend 'naar de maatstaven die in het maatschappelijk verkeer gelden'. Een verantwoordelijke hoeft niet *feitelijk* zelf de gegevens te verwerken. De 'bewerker' is degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt, zonder onder diens rechtstreeks gezag te

verschaft rechten aan degene, wiens persoonsgegevens worden verwerkt. Overigens stelt niet alleen de Wbp eisen aan de verwerking van persoonsgegevens. Soms bevatten andere wetten specifieke bepalingen over gegevensverwerking. Deze hebben dan geheel of gedeeltelijk voorrang op de Wbp.[12]

Institutionele reikwijdte van de Wbp

De wet geldt zowel voor de overheid als voor particulieren die persoonsgegevens verwerken, maar is onder meer níet van toepassing op de verwerking van persoonsgegevens door en ten behoeve van de inlichtingen- en veiligheidsdiensten en ten behoeve van de uitvoering van de politietaak. De belangrijkste spelers in de strijd tegen misdaad en terreur, te weten politie, justitie en veiligheids- en inlichtingendiensten, vallen met betrekking tot de verwerking van persoonsgegevens onder het regime van specifieke, sectorale privacywetten.[13]

Definities persoonsgegeven, verwerking en bestand

Onder 'persoonsgegeven' verstaat de Wbp 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon' (Wbp, artikel 1, eerste lid). Om persoonsgegeven te zijn moet het gegeven (direct of indirect) informatie verschaffen over een persoon en de persoon moet (direct of indirect) identificeerbaar zijn.[14]

Verwerking van persoonsgegevens wordt omschreven als 'elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, 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 beschikbaarstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens' (Wbp, artikel 1, tweede lid). Het begrip gegevensverwerking omvat het gehele proces dat een

---

zijn onderworpen (Wbp, artikel 1, vijfde lid; indien wel onderwerping aan rechtstreeks gezag aan de orde is, dan is sprake van 'intern beheer' in plaats van 'bewerker'). De bewerker heeft geen zeggenschap over de gegevensverwerking, maar handelt naar de instructies en onder verantwoordelijkheid van de 'verantwoordelijke'. Zie hiervoor: Wbp, MvT, 55-61.

[12] *Wbp. Handleiding*, 19. Voorbeelden hiervan zijn de Telecommunicatiewet (Tw), de Wet geneeskundige behandelingsovereenkomst (WGBO) en de Wet justitiële en strafvorderlijke gegevens (Wjsv).

[13] Wbp, artikel 2, tweede en derde lid, bepaalt dat de Wbp niet van toepassing is:
- op de verwerking van persoonsgegevens ten behoeve van activiteiten met uitsluitend persoonlijke of huishoudelijke doeleinden;
- door en ten behoeve van de inlichtingen- en veiligheidsdiensten, bedoeld in de Wiv 2002;
- ten behoeve van de uitvoering van de politietaak, bedoeld in de Wet politiegegevens (Wpolg)(voorheen de Wet politieregisters - Wpolr);
- die is geregeld bij of krachtens de Wet gemeenschappelijke basisadministratie persoonsgegevens (Wgba);
- ten behoeve van de uitvoering van de Wet justitiële en strafvorderlijke gegevens (Wjsv);
- ten behoeve van de uitvoering van de Kieswet;
- ten behoeve van defensiedoeleinden.

[14] Gegevens die informatie over personen verschaffen kunnen zeer divers zijn, variërend van telefoonnummers, nummerplaten en BurgerServiceNummer tot unieke biometrische gegevens zoals stem, vingerafdruk of DNA-profiel (Wbp, MvT, 46-48). Bij de identificeerbaarheid van de persoon (één van de elementen die bepalend is voor de vraag of sprake is van persoonsgegevens) is het uitgangspunt dat een persoon identificeerbaar is, indien zijn identiteit redelijkerwijs,'zonder onevenredige inspanning', vastgesteld kan worden (Wbp, MvT, 47). De MvT vervolgt: 'Bij het voortschrijden van informatietechnologie moet rekening worden gehouden met het feit dat waar voorheen wellicht nog sprake was van een onevenredige inspanning (en dus niet van een persoonsgegeven), deze inspanning geringer wordt met het beschikbaar komen van nieuwe technieken. De desbetreffende gegevens kunnen daardoor onder het bereik van het wetsvoorstel [Wbp, *KR*] komen te vallen. (...) Wat bij een bepaalde stand van de techniek als anoniem, want redelijkerwijs niet op een persoon herleidbaar gegeven, kan worden beschouwd, kan door technische ontwikkelingen alsnog een persoonsgegeven worden gelet op de toegenomen mogelijkheden tot herleiding.' (Wbp, MvT, 49).

gegeven doormaakt vanaf het moment van verzamelen tot aan het moment van vernietiging.[15]

De wet is van toepassing op 'de geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens, alsmede de niet geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen' (Wbp, artikel 2, eerste lid).[16]

Voorwaarden voor rechtmatige verwerking

De Wbp stelt voorwaarden voor de rechtmatigheid van de verwerking van persoonsgegevens. Persoonsgegevens dienen 'toereikend, ter zake dienend en niet bovenmatig' en 'juist en nauwkeurig' te zijn en 'in overeenstemming met de wet' en 'op behoorlijke en zorgvuldige wijze' verwerkt te worden voor 'welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden' (Wbp, artikelen 6, 7 en 11). De verwerking van persoonsgegevens dient 'noodzakelijk' te zijn voor deze doeleinden. Deze doelbinding dient reeds bij het verzamelen van de gegevens aanwezig te zijn. Persoonsgegevens mogen 'niet verder verwerkt worden op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen' (Wbp, artikel 9, eerste lid).[17]

Gegevensverwerking is toelaatbaar (Wbp, artikel 8) indien betrokkene 'ondubbelzinnig toestemming' heeft verleend of indien de verwerking bijvoorbeeld noodzakelijk is om aan een wettelijke verplichting te voldoen.[18] Bij elke toegestane verwerking dient voldaan te zijn aan de mede op de grondrechten en de EVRM gebaseerde beginselen van proportionaliteit en subsidiariteit (zie *Bijlage II*).[19]

De verantwoordelijke voor de verwerking legt 'passende technische en organisatorische maatregelen' ten uitvoer om persoonsgegevens te beveiligen tegen verlies of enige andere vorm van onrechtmatige verwerking. Deze maatregelen zijn er tevens op gericht onnodige verzameling en verdere verwerking van persoonsgegevens te voorkomen (Wbp, artikel 13).[20] Persoonsgegevens mogen 'niet langer bewaard

---

[15] Wbp, MvT, 52.

[16] Een 'bestand' is hierbij 'elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen' (Wbp, artikel 1, derde lid). Persoonsgegevens hebben een onlosmakelijke relatie met een bestand. Losse gegevens over personen die níet zijn opgenomen in een bestand of níet zijn voorbestemd om opgenomen te worden in een bestand, zijn derhalve geen persoonsgegevens in de zin van de Wbp!

[17] Bij het beoordelen van onverenigbaarheid wordt onder meer meegewogen hoe de gegevens zijn verkregen, wat de gevolgen voor de betrokkene kunnen zijn en in welke mate de betrokkene wordt voorzien in passende waarborgen (Wbp, artikel 9, tweede lid). Verdere verwerking van de gegevens voor historische, statistische of wetenschappelijke doeleinden wordt niet als onverenigbaar beschouwd, indien de verantwoordelijke de nodige voorzieningen heeft getroffen ten einde te verzekeren dat de verdere verwerking uitsluitend geschiedt ten behoeve van deze specifieke doeleinden (Wbp, artikel 9, derde lid).

[18] Artikel 8 bepaalt dat gegevensverwerking toelaatbaar is (met andere woorden: van 'gerechtvaardigde doeleinden' is sprake) indien betrokkene 'ondubbelzinnig toestemming' heeft verleend of indien de verwerking bijvoorbeeld noodzakelijk is ter vrijwaring van een vitaal belang van betrokkene, tot uitvoering van een overeenkomst, om aan een wettelijke verplichting te voldoen, of voor een goede vervulling van een publiekrechtelijke taak. Verwerking is ook toegestaan voor 'de behartiging van het gerechtvaardigde belang van de verantwoordelijke of van een derde aan wie de gegevens worden verstrekt, tenzij het belang of de fundamentele rechten en vrijheden van de betrokkene, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer, prevaleert.' Deze laatste bepaling houdt een belangenafweging in en impliceert een motiveringsplicht.

[19] Wpb, MvT, 8-9, 80. Het proportionaliteits- of evenredigheidsbeginsel houdt in dat de inbreuk op de belangen van de betrokkene niet onevenredig mag zijn in verhouding tot het doel van de verwerking. Dit veronderstelt dus een belangenafweging aan de hand van de omstandigheden van een concreet geval. Het subsidiariteitsbeginsel houdt in dat het doel van de verwerking niet op een andere, voor betrokkene minder nadelige wijze kan worden verwerkelijkt

[20] De technische en organisatorische maatregelen moeten een passend beveiligingsniveau garanderen. Organisatorische maatregelen kunnen bijvoorbeeld inhouden dat maar een beperkt aantal personen toegang heeft tot een computersysteem; technische maatregelen kunnen bijvoorbeeld gericht zijn op de versleuteling van persoonsgegevens.

worden in een vorm die het mogelijk maakt de betrokkene te identificeren, dan noodzakelijk is voor de verwerking van de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt' (Wbp, artikel 10, eerste lid).[21]

De aard van sommige persoonsgegevens maakt dat de verwerking ervan een grote inbreuk kan vormen op de persoonlijke levenssfeer van de betrokkene, omdat die gegevens gevoelige informatie over iemand verschaffen. Enkele uitzonderingen daargelaten verbiedt de Wbp de verwerking van deze gevoelige, zogenaamde 'bijzondere persoonsgegevens' (Wbp, artikel 16). [22] Dit zijn persoonsgegevens betreffende iemands godsdienst of levensovertuiging, ras, politieke gezindheid, gezondheid, seksuele leven of lidmaatschap van een vakvereniging, maar ook strafrechtelijke persoonsgegevens.[23]

Plichten van de verantwoordelijke en rechten van de betrokkene

De verantwoordelijke voor de verwerking van persoonsgegevens dient deze verwerking te melden bij de wettelijk bepaalde toezichthouder, het College Bescherming Persoonsgegevens (CBP), of bij een speciaal benoemde functionaris voor de gegevensbescherming. Deze melding moet gedaan worden voorafgaand aan de verwerking en dus ook voorafgaand aan de verzameling (Wbp, artikel 27).

Standaardgegevensverwerkingen zijn van de meldingsplicht uitgesloten. Hiervoor heeft de wetgever een zogenaamd Vrijstellingsbesluit opgesteld, waarin de vrijgestelde gegevensverwerkingen zijn opgesomd en tevens de maximale bewaarperiode van gegevens is opgenomen.[24]

Een persoon wiens gegevens worden verwerkt, moet kunnen nagaan wat er met de gegevens gebeurt. De Wbp bevat daarom een regeling over informatieverstrekking aan

---

[21] Als het voor het doel dus niet meer noodzakelijk is persoonsgegevens te bewaren, moeten de gegevens zelf of alle identificerende kenmerken worden *verwijderd*. Hoelang gegevens feitelijk bewaard mogen worden, hangt dus af van het doel waarvoor ze zijn verzameld en verder verwerkt. Dit kan per situatie verschillen; er is dus geen vaste bewaartermijn. Het doelbindingsbeginsel betekent echter niet dat archiefbescheiden die persoonsgegevens bevatten *altijd* vernietigd moeten worden. Een specifieke uitzondering geldt namelijk onder bepaalde voorwaarden de gegevens die uitsluitend voor historische, statistische of wetenschappelijke doeleinden worden gebruikt (Wbp, artikel 10. tweede lid; zie hiervoor het rapport *Persoonsdossiers: een geval apart* (Den Haag: Nationaal Archief, 2006) 9, 23-24). Voor de (soms) botsende belangen tussen gegevensvernietiging uit privacybescherming en bewaring van dezelfde gegevens ten behoeve van het collectieve geheugen van de samenleving en de toekomstige reconstructie van het verleden, zie: P.M.M. Klep, 'Verschuivende visies en praktijken. Archieven bewaren voor onderzoek en cultuur' in: P. Brood, e.a. (red), *Selectie. Waardering, selectie en acquisitie van archieven* ('s Gravenhage 2004) 84-105 en (voor Canada) T. Cook,'Archives and privacy in a wired world: the impact of the *Personal Information Act* on archives', *Archivaria* 53 (2002) 94-114.
Voor specifieke, van de meldingsplicht vrijgestelde gegevensverwerkingen, kunnen maximale bewaartermijnen opgenomen zijn in het zogenaamde *Vrijstellingsbesluit*. Soms verplicht een wet bepaalde gegevens gedurende een bepaalde periode te bewaren (zoals de WGBO of Wgba). De Archiefwet 1995 en de daarop berustende besluiten vormen een nadere invulling van artikel 10 van de Wbp voor de bewaartermijn van persoonsgegevens. Vernietiging van archieven met persoonsgegevens is toegestaan *tenzij* het bepaalde bij of krachtens de Archiefwet zich tegen vernietiging verzet. Het zijn uiteindelijk de selectielijsten die bepalen of persoonsgegevens door de overheid naar een archiefbewaarplaats moeten worden overgebracht. Is in een selectielijst vastgelegd dat de neerslag voor bewaren in aanmerking komt, dan heeft deze bewaarplicht voorrang boven de plicht tot vernietigen van de Wbp.

[22] Verwerking van bijzondere persoonsgegevens is toegestaan als dit geschiedt met 'uitdrukkelijke toestemming' van de betrokkene, de gegevens door de betrokkene duidelijk openbaar zijn gemaakt of als de verwerking noodzakelijk is voor de vaststelling, uitoefening of verdediging van een recht in rechte, ter voldoening van een volkenrechtelijke verplichting of met het oog op 'een zwaarwegend algemeen belang' en passende waarborgen worden geboden ter bescherming van de persoonlijke levenssfeer en dit bij wet wordt bepaald (Wbp, artikel 23).

[23] Het verbod op verwerking van strafrechtelijke persoonsgegevens is overigens niet van toepassing indien de verwerking geschiedt door organen die krachtens de wet zijn belast met de toepassing van het strafrecht, alsmede door verantwoordelijken die deze hebben verkregen krachtens de Wet politiegegevens of de Wjsg (Wbp, artikel 22, eerste lid).

[24] *Wbp. Handleiding,* 31. Het Vrijstellingsbesluit geeft uitvoering aan Wbp, artikel 29, eerste en twee lid en poogt onder meer de administratieve lasten van bedrijven en overheden te beperken.

de betrokkene.[25] De rechten van betrokkenen zijn het recht van mededeling inzake verwerking van persoonsgegevens, recht op verbetering, aanvulling, verwijdering en afscherming van gegevens indien deze feitelijk onjuist zijn of onvolledig of niet ter zake dienend zijn voor het doel van de verwerking en het recht van verzet tegen verwerking in verband met bijzondere persoonlijke omstandigheden (Wbp, artikelen 35 t/m 42).

Uitzonderingsartikel 43

Belangrijk in het kader van activiteiten samenhangend met terrorismebestrijding is uitzonderingsartikel 43, dat bepaalt dat de verantwoordelijke de verplichting om gegevens niet verder te verwerken op een wijze die onverenigbaar is met het doel waarvoor ze verkregen zijn en de informatie- en inzageverplichtingen richting betrokkenen buiten toepassing kunnen laten, voorzover dit 'noodzakelijk' is in het belang van onder meer:
- de veiligheid van de staat;
- de voorkoming, opsporing en vervolging van strafbare feiten;
- gewichtige economische en financiële belangen van de staat en andere openbare lichamen;
- de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

In deze gevallen berust de verantwoordelijkheid voor de beslissing om gegevens verder te verwerken (bijvoorbeeld te verstrekken) bij de instelling die de desbetreffende registratie voert. De verantwoordelijke dient te oordelen over de 'noodzakelijkheid' van een verdere verwerking waartoe verzocht is. Bovendien is hij verantwoordelijk voor de verstrekking en aansprakelijk voor eventuele schade aan personen wiens gegevens worden verstrekt, mocht de beoordeling achteraf onjuist blijken. Zijn er echter *wettelijke verplichtingen* van kracht om gegevens aan derden (bijvoorbeeld politie, justitie en veiligheidsdiensten) te verstrekken (Wbp, artikel 8), dan ligt de verantwoordelijkheid voor de afweging en de verwerking (bijvoorbeeld verstrekking) niet meer bij de registratiehouder (de verantwoordelijke), maar bij bijvoorbeeld de politie, justitie of de veiligheidsdienst.

[25] Met betrekking tot de informatieverstrekking aan betrokkenen maakt de Wbp onderscheid tussen de situatie dat de gegevens bij de betrokkene zelf worden verkregen en de situatie dat de gegevens op een andere manier, via derden, worden verkregen. Worden de gegevens van de betrokkene verkregen, dan moet de betrokkene geïnformeerd worden vóór de verkrijging. Bij verkrijging buiten de betrokkene om moet informatieverstrekking hierover plaatsvinden op het moment van vastlegging van de gegevens. Worden de gegevens buiten de betrokkene om verzameld om deze aan een derde te verstrekken, dan moet de betrokkene geïnformeerd worden uiterlijk op het moment van eerste verstrekking aan die derde (Wbp, artikelen 33 en 34).

3. GEGEVENSVERZAMELING DOOR OPSPORINGSDIENSTEN

Vanaf 2000 is er een versnellingsproces opgetreden wat betreft de verruiming van de mogelijkheden van opsporings- en veiligheidsdiensten om de beschikking te krijgen over bij derden berustende gegevens om deze vervolgens verder te kunnen verwerken. Wetten om verplichte verstrekking van telecommunicatiegegevens, financiële gegevens en uiteindelijk zelfs van in principe *alle* soorten gegevens van maatschappelijke instellingen en bedrijven mogelijk te maken, zijn elkaar in het kader van (of zo men wil: onder het mom van) terrorismebestrijding in rap tempo opgevolgd.

Dit hoofdstuk schetst een beeld van de ontwikkeling in de verruiming van de bevoegdheden tot het verkrijgen (vorderen) van gegevens door opsporingsdiensten (politie en justitie). Dit gebeurt, vertrekkend vanuit de Wet bijzondere opsporingsbevoegdheden, aan de hand van een bespreking van de wetgeving met betrekking tot het verstrekken van telecommunicatiegegevens, de algemene wet tot het vorderen van gegevens en de meest recente verruiming van mogelijkheden tot opsporing en vervolging van terroristische misdrijven. De mogelijkheden die inlichtingen- en veiligheidsdiensten hiertoe hebben, komen in hoofdstuk 5 aan bod.

3.1. Wet bijzondere opsporingsbevoegdheden (BOB)

De Wet BOB uit 2000 beoogt de opsporingsonderzoeken te normeren en beter controleerbaar te maken. De wet heeft betrekking op een breed scala aan zogenaamde bijzondere opsporingsmethoden[26], die uitsluitend mogen worden toegepast voor de opsporing en strafrechtelijke afdoening van strafbare feiten. Andere doeleinden, zoals het verbeteren van de informatiepositie van de politie,[27] of het ontmantelen van een criminele organisatie, zonder dat dit leidt tot strafrechtelijke afdoening, vallen hier dus buiten. Ook moet het misdrijf 'een ernstige inbreuk op de rechtsorde' vormen; in geval van het inzetten van bijzondere bevoegdheden voor het onderzoek naar het beramen of plegen van ernstige misdrijven in georganiseerd verband moet een uit feiten en omstandigheden voortvloeiend 'redelijk vermoeden' aanwezig zijn.[28]

De Wet BOB bepaalt dat de officier van justitie leider is van het opsporingsonderzoek, beslist over de toepassing van een bijzondere opsporingsbevoegdheid en zorg draagt voor het bewaren en vernietigen van de aldus verkregen gegevens.[29] Alleen in geval van 'het opnemen van vertrouwelijke communicatie'[30] en 'het onderzoeken van

[26] Als bijzondere opsporingmethoden noemt de Wet BOB observatie, infiltratie, pseudo-aankoop of -dienstverlening, stelselmatige inwinning van informatie, bevoegdheden in een besloten plaats, opnemen van vertrouwelijke communicatie met een technisch hulpmiddel en onderzoek van telecommunicatie (Wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), TK 1996-1997, 25 403, nr. 1-2, artikelen 126g t/m 126m (2000)).

[27] Voor gegevensverwerking (níet verkrijging of vordering) ten behoeve van het verbeteren van de informatiepositie van de politie, zie hoofdstuk 4 over de Wet politiegegevens.

[28] *Factsheet Wet bijzondere opsporingsbevoegdheden (BOB)* ('s Gravenhage: Ministerie van Justitie, z.j.).

[29] Gegevens die zijn verkregen door taps, observatie en direct afluisteren doet de officier van justitie twee maanden na beëindiging van de zaak vernietigen (Wet BOB, artikel126cc (2000)). Gegevens kunnen ook voor een ander strafrechtelijk onderzoek worden gebruikt dan waartoe de bevoegdheid is uitgeoefend, vernietiging is dan pas aan de orde indien dit andere onderzoek is afgerond (Wet BOB, artikel 126dd (2000)). Ten opzichte van voorgaande wetgeving betekent dit een versoepeling van de vernietigingsplicht. Koops noemt dit een verschuiving in de richting van opsporing ten koste van privacy, omdat het langer bewaren van (tap)gegevens een groter risico voor de privacy inhoudt, zie: B.-J. Koops, *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy* (Deventer 2002) 155.

[30] Koops wijst op onvolkomenheden in de Wet BOB met betrekking tot de afstemming tussen de bevoegdheid en de strafbepaling van het 'opnemen van vertrouwelijke communicatie'. Omdat de Wet BOB justitieel direct afluisteren mogelijk maakt betekent deze wet op dit aspect volgens Koops een belangrijke

telecommunicatie'[31] is een voorafgaande machtiging van de rechter-commissaris nodig.

Indien relevant voor het onderzoek mogen de bijzondere bevoegdheden worden ingezet tegen zowel verdachten als niet-verdachten.[32] Zo is bij het aftappen van telecommunicatie de voorwaarde komen te vervallen dat de verdachte zelf aan de communicatie moet deelnemen.[33] Wel is in de Wet BOB de zogenaamde notificatieplicht opgenomen, wat inhoudt dat degene die onderwerp is van een bijzondere opsporingsbevoegdheid hierover -zodra het onderzoeksbelang het toelaat- wordt geïnformeerd.[34]

In het kader van onderzoek naar de georganiseerde misdaad geeft de Wet BOB het zogenaamde 'verkennend onderzoek' een plaats in het Wetboek voor Strafvordering. Dit houdt in dat opsporingsdiensten behalve uit politieregisters ook uit andere registers gegevens kunnen verzamelen, combineren en analyseren - ook van niet-verdachten. Het verkennend onderzoek is geen *opsporings*onderzoek, maar dient ter *voorbereiding* van de opsporing. Derhalve mogen in een verkennend onderzoek geen bijzondere opsporingsbevoegdheden of dwangmiddelen worden toegepast.[35]

3.2. De slag om de telecommunicatiegegevens

In de Wet BOB zijn de voorwaarden en vormvereisten van de tapbevoegdheid herzien in vergelijking met de voorafgaande periode. Hoewel het gedurende een groot deel van de 20ste eeuw mogelijk was om op ad hoc-basis kennis te nemen van telefoongesprekken, bestaat pas sinds 1971 een structurele bevoegdheid voor opsporingsdiensten om telefoons af te luisteren. Hieraan werden wel beperkende voorwaarden gesteld. Zo was toestemming van de rechter-commissaris noodzakelijk en mochten slechts gesprekken worden afgeluisterd waaraan de verdachte vermoedelijk deelnam.[36] De Wet Computercriminaliteit (1993) breidde het object van de tapbevoegdheid uit tot alle vormen van telecommunicatie.

Mede als reactie op de privatisering en liberalisering van telecommunicatiediensten zijn de aanbieders van openbare telecommunicatienetwerken- en diensten vervolgens via de Telecommunicatiewet, artikel 13, verplicht gesteld ervoor te zorgen hun telecommunicatie (waaronder internet) vanaf het moment van introductie technisch aftapbaar is.[37] Daarnaast zijn de aanbieders verplicht gehoor te geven aan bevelen van

---

verschuiving in de richting van opsporing ten nadele van de privacy, zie: Koops, *Strafvorderlijk onderzoek van (tele)communicatie*, 194, 198, 200.

[31] Bij 'het onderzoek van telecommunicatie' gaat het om de telecommunicatietap en de vordering van zogenaamde verkeersgegevens, dit zijn gegevens over telecommunicatie die heeft plaatsgevonden of zal plaatsvinden. In tegenstelling tot de telecommunicatietap is de bevoegdheid tot het vorderen van verkeersgegevens in de Wet BOB inhoudelijk niet gewijzigd. De officier van justitie kan 'inlichtingen terzake' van verkeer vorderen dat over een openbaar telecommunicatienetwerk, dan wel met gebruikmaking van openbare telecommunicatiediensten heeft *plaatsgevonden* en waarvan het vermoeden bestaat dat 'de verdachte van misdrijf' of 'een persoon ten aanzien van wie een redelijk vermoeden bestaat dat deze betrokken is bij het in het georganiseerd verband beramen of plegen van misdrijven' eraan heeft deelgenomen (Wet BOB, artikel 126n Sv (2000) en artikel 126u Sv (2000)).

[32] Dit geldt echter niet voor de bevoegdheid tot het vorderen van inlichtingen terzake van alle telecommunicatie*verkeer*; zie vorige noot.

[33] Over de totstandkoming van de Wet BOB in relatie tot de telecommunicatietap, zie: Koops, *Strafvorderlijk onderzoek van (tele)communicatie*, 149-157. Koops' conclusie luidt in dit verband dat de verruimingen van de bevoegdheid (met name de uitbreiding met gevallen van beraamde georganiseerde misdaad en het kunnen aftappen van niet-verdachten) het voor justitie mogelijk hebben gemaakt om in steeds meer gevallen te tappen en dat het grensvlak tussen opsporing en privacy in 2000 grotendeels is opgeschoven in de richting van opsporing (Ibidem, 157).

[34] *Factsheet Wet BOB*, 1.

[35] Ibidem, 5. Vgl. noot 69 en 99.

[36] Koops, *Strafvorderlijk onderzoek van (tele)communicatie*, 145-146.

[37] Deze verplichting is in 1994 ingevoerd voor de mobiele telefonie, in 1998 voor alle vormen van openbare telecommunicatie (Telecommunicatiewet, hoofdstuk 13; zie ook hoofdstuk 5 en noot 129) en

justitie en veiligheidsdiensten tot aftappen en tot overhandigen van gebruikers- en verkeersgegevens.[38]

Wet vorderen gegevens telecommunicatie (Wvgt)

In september 2004 is de Wet vorderen gegevens telecommunicatie[39] in werking getreden. Deze geeft de officier van justitie de bevoegdheid richting aanbieders van openbare telecommunicatienetwerken en/of -diensten 'een vordering [te] doen gegevens te verstrekken over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker'.[40] Deze vordering kan gedaan worden in geval van verdenking van het beramen of plegen van een ernstig misdrijf in georganiseerd verband dat een ernstige inbreuk op de rechtsorde kan opleveren. Anders dan bepaald in de Wet BOB kunnen de verplicht te verstrekken gegevens betrekking hebben op zowel verdachten als niet-verdachten[41] en kunnen de verkeersgegevens zowel historische als toekomstige gegevens betreffen.[42]

De door de officier van justitie te vorderen verkeersgegevens omvatten onder meer NAW- en nummergegevens van de verzender en de ontvanger van de communicatie en locatie, duur en tijdstip van het telecommunicatieverkeer (waaronder -mobiele-telefonie en internetverkeer).[43] Van de uitoefening van de bevoegdheid tot het vorderen

---

sinds 2001 geldt ze ook voor internetproviders (Regeling aftappen openbare telecommunicatienetwerken en -diensten).

[38] De verkeersgegevens dienen volgens Tw, artikel 11.5 bij beëindiging van de oproep verwijderd of geanonimiseerd te worden; verwerking is daarna slechts nog mogelijk voor bepaalde doelen, zoals het opstellen van een nota voor een abonnee. Zie voor de verkeersgegevens ook noot 43 en 129. Voor een beschouwing over de verwijderingplicht van verkeersgegevens in Tw, artikel 11.5, zie: Koops, *Strafvorderlijk onderzoek*, 134-135. In Tw, artikel 13.4, tweede lid (aangepaste versie op basis van Wet vorderen gegevens telecommunicatie, 2004) is echter ten behoeve van het maken van bestandsanalyses een bewaarplicht (drie maanden) opgenomen voor een (bij Besluit bijzondere vergaring nummergegevens telecommunicatie in artikel 7 aangewezen) beperkte set (verkeers)gegevens, te weten de tijdstippen van communicatie, nummers (van beller en gebelde) en het basisstation, met als uitsluitend doel het achterhalen van een nummer van een gebruiker van prepaid kaarten. Over de geschiedenis van de bewaarplicht van verkeersgegevens, vooruitlopend op de huidige wetsvoorstellen (zie noot 45) op dit terrein, zie: Koops, *Strafvorderlijk onderzoek*, 131-144.

[39] Wet van 18 maart 2004 tot wijziging van het Wetboek van Strafvordering en andere wetten in verband met de aanpassing van de bevoegdheden tot het vorderen van gegevens terzake van telecommunicatie (vorderen gegevens telecommunicatie) [Wvgt], Stb. 2004, 105.

[40] Voor het 'onderzoeken van telecommunicatie' (waaronder verkeersgegevens) had de officier van justitie in de Wet BOB nog een voorafgaande machtiging van de rechter-commissaris nodig.

[41] Wvgt, artikel 126n en 126u. De in de Wet BOB geformuleerde eis van vermoedelijke deelname van de verdachte aan dit verkeer is geschrapt. Hiermee is deze bevoegdheid gelijk getrokken aan de tapbevoegdheid in de Wet BOB, die immers ook jegens andere personen dan de verdachte ingezet kan worden (Wijziging van het Wetboek van Strafvordering en andere wetten in verband met de aanpassing van de bevoegdheden tot het vorderen van gegevens terzake van telecommunicatie (vorderen gegevens telecommunicatie) [Wvgt], Memorie van Toelichting, TK 2001-2002, 28 059, nr. 3, p. 9).

[42] Wvgt, artikel 126n (en 126u), eerste lid, onder b. Deze uitbreiding naar *toekomstige* gegevens is niet onbelangrijk, daar het de weg opent voor verzoeken om gegevens vanaf een zeker moment vast te leggen, zodat de afhankelijkheid van de al dan niet toevallige vastlegging door telecomaanbieders omzeild kan worden. De Memorie van Toelichting stelt nadrukkelijk dat het bij toekomstige gegevens uitsluitend gaat om gegevens die de aanbieder op enig moment voorhanden heeft; de bevoegdheid voorziet niet in een plicht tot medewerking betreffende het *vergaren* van gegevens die de aanbieder bij de normale bedrijfsuitvoering niet ter beschikking krijgt. (Wvgt, MvT, 10).

[43] Besluit vorderen gegevens telecommunicatie van 3 augustus 2004, Stb., 394. Het begrip verkeersgegevens omvat dus tevens gebruikersgegevens en is hiermee ruimer dan het begrip zoals dat in de Tw wordt gehanteerd. In de Memorie van Toelichting van de Wvgt wordt het plaatsen van de gebruikersgegevens onder de categorie verkeersgegevens ingegeven door het feit dat de bevoegdheid tot het vorderen van NAW- en andere gebruikersgegevens ook onder de bevoegdheid tot het vorderen van verkeersgegevens begrepen dient te worden (Wvgt, MvT, 7). In de Wvgt wordt ook bepaald dat de AIVD/MIVD bij AMvB aan te wijzen 'gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot die gebruiker' kan vorderen. Deze aanwijzing is neergelegd in het Besluit ex artikel 28 Wiv 2002 van 19 mei 2005 en betreft dezelfde gegevens als opgesomd in het Besluit vorderen gegevens telecommunicatie, zie hiervoor noot 129. Er is overigens veel discussie over de reikwijdte van de 'verkeersgegevens' (zie ook noot 38). Koops verstaat onder verkeersgegevens 'gegevens over

van verkeersgegevens doet de officier van justitie mededeling aan de betrokkene, zodra het belang van het onderzoek dat toelaat (notificatieplicht).

De wet regelt tevens de bevoegdheid tot het vorderen van identificerende gegevens of gebruikersgegevens betreffende NAW, nummer en soort dienst door een opsporingsambtenaar in geval van verdenking van een misdaad.[44] Hierbij moet proces-verbaal opgemaakt worden door de officier van justitie; de notificatieplicht geldt niet bij de uitoefening van deze bevoegdheid.

Vordering versus vrijwillige verstrekking

Zoals in hoofdstuk 2 is opgemerkt, biedt de Wbp in artikel 43 de mogelijkheid om op *vrijwillige* basis gegevens te verstrekken aan opsporingsinstanties, indien deze daar om verzoeken. De verantwoordelijke tot wie het verzoek wordt gericht, dient in deze gevallen te beslissen over de noodzakelijkheid van de verstrekking en is aansprakelijk, indien een betrokkene door een eventuele onrechtmatige verstrekking schade ondervindt. Artikel 8 van de Wbp bepaalt dat gegevensverwerking (waaronder verstrekking) toelaatbaar is, als er sprake is van een *wettelijke verplichting*. De Wet vorderen gegevens telecommunicatie is een dergelijke wettelijke verplichting. Met de inwerkingtreding van deze vorderingswet is het de vorderende partij die verantwoordelijk is voor de afweging die ten grondslag ligt aan de verstrekking.[45]

3.3. Algemene vorderingswet: Wet bevoegdheden vorderen gegevens (Wbvg)

Een in 2001 gepubliceerd rapport over strafvorderlijke gegevensgaring van de Commissie Mevis (zie *Bijlage III*) ligt ten grondslag aan de maatregelen die nadien door de regering genomen zijn ter verruiming van de gegevensverstrekking. De besproken Wet vorderen gegevens telecommunicatie is een uitwerking van in het Mevis rapport geformuleerde uitgangspunten. Begin 2004 is een wet van kracht geworden die justitiële autoriteiten in verband met de opsporing van terroristische misdrijven bevoegdheden toekent gegevens van instellingen in de financiële sector te

---

telecommunicatie die heeft plaatsgevonden of zal plaatsvinden' (Koops*, Strafvorderlijk onderzoek,* 108). Volgens de Memorie van Toelichting van de Wvgt gaat het bij deze gegevens om de 'uiterlijke kenmerken van telecommunicatie en niet om de inhoud van hetgeen via het telecommunicatieverkeer wordt uitgewisseld' (Wvgt, MvT, 7). Ook de aanduiding van bijvoorbeeld een (pagina binnen een) website of een email-bericht met *header* worden in de Memorie van Toelichting tot verkeersgegevens gerekend. De vraag is natuurlijk of in deze gevallen inhoud en locatie (verkeer) wel van elkaar te scheiden zijn. In deze paper zal op deze kwestie niet nader in worden gegaan, hoewel dit in het kader van de debatten rond het Wetsvoorstel bewaarplicht telecommunicatiegegevens (dataretentie) (zie noot 45) een belangrijk vraagstuk is.

[44] Deze bevoegdheid was voorheen voorbehouden aan de officier van justitie. De aanvankelijk voorgenomen uitbreiding van de bevoegdheid gegevens te vorderen in een verkennend onderzoek is na kritiek van de Raad van State en het CBP uiteindelijk uit het wetsvoorstel Wvgt geschrapt.

[45] Wvgt, MvT,3. Vordering van telecommunicatiegegevens (waaronder verkeersgegevens) is alleen zinvol indien deze gegevens (een minimale periode) beschikbaar zijn bij de telecomaanbieder. Hiertoe is medio 2006 een Europese Richtlijn in werking getreden (Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006), waarin de lidstaten een bewaarplicht voor verkeersgegevens door telecom- en internetproviders zijn overeengekomen van minimaal zes maanden en ten hoogste twee jaar. Het wetsvoorstel bewaarplicht verkeersgegevens ter implementatie van de richtlijn is momenteel nog in behandeling en valt daarmee buiten het domein van deze paper. Voor het wetsvoorstel, zie: Wet bewaarplicht telecommunicatiegegevens, Voorstel van Wet, TK 2006-2007, 31 145, nr. 2 en Wet bewaarplicht telecommunicatiegegevens, Memorie van Toelichting, TK 2006-2007, 31 145, nr. 3. Het wetsvoorstel heeft ingrijpende gevolgen voor de informationele privacy en is daarmee nogal controversieel. Zie: Bits of Freedom, Dossier verkeersgegevens (2005) (www.bof.nl/verkeersgegevens.html); CBP, *Advies Wetsontwerp implementatie Europese Richtlijn Dataretentie* (22 januari 2007); Erasmus Universiteit Rotterdam, *Wie wat bewaart, heeft wat* (Rotterdam 2005); Stratix Consulting Group B.V., *Onderzoek "Bewaren verkeersgegevens door telecommunicatie-aanbieders".* Eindrapport uitgebracht aan het WODC (Schiphol, augustus 2003); W. Steenbruggen, 'I know what you did last summer! Over grenzeloze en ongegeneerde verwerking van verkeersgegevens in de informatiemaatschappij', JAVI, 3 (december 2002) 89-97.

vorderen. Tot dan toe kon een financiële instelling op basis van de Wbp zelf beslissen om gegevens al dan niet te verstrekken.[46]

De Wet vorderen gegevens financiële sector is inmiddels al weer opgevolgd door de in 2006 in werking getreden Wet bevoegdheden vorderen gegevens (Wbvg).[47] Deze op de voorstellen van de Commissie Mevis gebaseerde wet geeft politie en justitie bevoegdheden om persoonsgegevens te vorderen bij maatschappelijke instellingen en bedrijven.[48]

De nieuwe algemene vorderingswet maakt het in beginsel mogelijk dat *elk* geregistreerd gegeven berustend bij maatschappelijke instellingen en bedrijven (waaronder de financiële sector) ter beschikking kan komen in het belang van een opsporingsonderzoek. De wettelijke *verplichting* tot verstrekking maakt dat de verantwoordelijke tot wie een verzoek tot verstrekking wordt gericht niet meer op basis van Wbp, artikel 43 zelf een afweging hoeft (of kan) te maken omtrent de 'noodzaak' van de verstrekking.[49]

Driedeling categorieën gegevens

Overeenkomstig de voorstellen van de Commissie Mevis kent de wet een driedeling in de bevoegdheden tot het vorderen van 'gegevens'[50], te weten het vorderen van 'identificerende gegevens' (Sv, artikelen 126nc en 126 uc), 'ook andere dan identificerende gegevens' (Sv, artikelen 126nd en 126 ud) en 'gevoelige gegevens' (Sv, artikelen 126nf en uf). Al naar gelang de categorie van gegevens ingrijpender is voor

[46] Wijziging Wetboek Strafvordering i.v.m. regeling bevoegdheden tot vorderen gegevens financiële sector (Wet vorderen gegevens financiële sector), TK 2001-2002, 28 353. Wel is (en blijft) een ieder die beroepsmatig financiële transacties verricht op grond van de Wet melding ongebruikelijke transacties bij financiële dienstverlening (Wet van 16 december 1993) verplicht ongebruikelijke financiële transacties te melden aan het Meldpunt Ongebruikelijke Transacties (MOT). Het MOT analyseert de meldingen en meldt deze door aan het Openbaar Ministerie in het geval de transactie daadwerkelijk als verdacht aangemerkt moeten worden.

[47] Wet van 16 juli 2005 tot wijziging van het Wetboek van Strafvordering en enkele andere wetten i.v.m. de regeling van bevoegdheden tot het vorderen van gegevens (bevoegdheden vorderen gegevens) [Wbvg], Stb. 2005, 380.

[48] De Wet vorderen gegevens financiële instellingen is bij het inwerkingtreden van de Wet bevoegdheden vorderen gegevens komen te vervallen. De bevoegdheid telecommunicatiegegevens te vorderen is vastgelegd in de besproken Wet vorderen gegevens telecommunicatie. Gegevens die beschikbaar zijn bij de aanbieders van telecommunicatie en die niet gevorderd kunnen worden op grond van de Wet vorderen gegevens telecommunicatie kunnen wel door toepassing van de bevoegdheden van de nieuwe algemene vorderingswet gevorderd worden. Een bijzondere categorie in dit verband zijn de gegevens betreffende de inhoud van een e-mail die is opgeslagen bij een internetaanbieder. (Wijziging van het Wetboek van Strafvordering en enkele andere wetten i.v.m. de regeling van bevoegdheden tot het vorderen van gegevens (bevoegdheden vorderen gegevens) [Wbvg], Memorie van Toelichting, TK 2003-2004, 29 441, nr. 3, p. 13-14).

[49] Wél kan de verantwoordelijke toetsen of de vordering aan de formele voorwaarden voldoet, zoals of de vordering door de bevoegde instantie is gedaan en of de opgevraagde gegevens voldoende gespecificeerd zijn. Jeloschek en de Vries betogen dat bij de Wbvg niet altijd duidelijk is op grond van welk lid van Wbp, artikel 8 gegevens kunnen worden verstrekt; bovendien moet de verantwoordelijke derde altijd nog toetsen of de vordering correct is ingekleed en voldoende bepaald is. De derde zou volgens hen hierdoor nog steeds met een beroep op de Wbp aansprakelijk kunnen worden gesteld voor onrechtmatige gegevensverstrekking, zie: C. Jeloschek en H.H. de Vries, 'Het spanningsveld tussen het vorderen en het beschermen van persoonsgegevens', *NJB, 2 (*12 januari 2007) 86-91, passim. M. Jongeneel-van Amerongen stelt hier tegenover dat naleving van vorderingen op grond van het Wetboek van Strafvordering evident onder Wbp, artikel 8, lid c ('wettelijke verplichting') valt en dat zowel de verantwoordelijkheid als de *aansprakelijkheid* voor de afweging of gegevens verstrekt moeten worden in dit geval weg wordt gehaald bij de derde. Ook is ontheffing van het CBP voor het verwerken van gegevens in geval van de vordering niet meer nodig, zie: M. Jongeneel-van Amerongen, 'Geen spanningsveld tussen het vorderen van gegevens en de Wet bescherming persoonsgegevens', *NJB*, 28 (3 augustus 2007) 1755. Anders dan in de Wbvg is aan deze kwestie in de Wiv 2002 expliciet artikel 17, derde lid gewijd: 'De bij of krachtens de wet geldende voorschriften voor de verantwoordelijke voor een gegevensverwerking betreffende de verstrekking van zodanige gegevens zijn niet van toepassing op verstrekkingen gedaan ingevolge van een verzoek [van de AIVD/MIVD]', zie noot 123.

[50] Onder het begrip 'gegeven' verstaat de wet: 'informatie die is vastgelegd of opgeslagen op een gegevensdrager, hetzij op schrift, hetzij in elektronische vorm' (Wbvg, MvT, 7).

de persoonlijke levenssfeer van betrokkenen en meer handelingen vereist van de verstrekkers gelden zwaardere voorwaarden en waarborgen met betrekking tot de uitoefening van de bevoegdheid.[51]

De categorie *'identificerende gegevens'* betreft NAW-gegevens, geboortedatum, geslacht en administratieve kenmerken (bijvoorbeeld klant-, polis-, lidmaatschap- of bankrekeningnummer). Deze gegevens kunnen door elke opsporingsambtenaar worden gevorderd in geval van een verdenking van een misdrijf of het in georganiseerd verband beramen of plegen van misdrijven die een ernstige inbreuk op de rechtsorde opleveren. Per politieregio worden hiertoe opsporingsambtenaren aangewezen die geautoriseerd zijn identificerende gegevens te vorderen.[52]

Bij de categorie *'ook andere dan identificerende gegevens'* gaat het om *alle* gegevens (inclusief de identificerende) van een persoon of groep van personen met uitzondering van de 'gevoelige gegevens'. Hierbij moet gedacht worden aan gegevens over diensten die zijn verleend, zoals de duur, data, de plaats en de aard van de dienstverlening en rekening- en betalingsgegevens.[53] Omdat deze gegevens een grote inbreuk op de persoonlijke levenssfeer van betrokkenen met zich meebrengen, ligt de bevoegdheid tot de vordering bij de de officier van justitie en moet er sprake zijn van een verdenking van (het in georganiseerd verband beramen of plegen van) een ernstig misdrijf dat een grote inbreuk op de de rechtsorde kan opleveren. [54]

Naast het vorderen van reeds bestaande (vooraf bepaalde) gegevens kunnen met betrekking tot 'andere dan gevoelige gegevens' door de officier van justitie ook (vooraf bepaalde) *toekomstige* gegevens worden gevorderd (Sv, artikelen 126ne en 126ue), dit zijn gegevens die op het moment van vordering nog niet aanwezig zijn bij het bedrijf of de instelling die ze verwerkt.[55] In 'dringend noodzakelijke gevallen' kan de officier van justitie in de vordering bepalen dat de toekomstige gegevens direct na de eerste verwerking worden verstrekt. Daar deze directe verstrekking extra belastend is voor de derde en verder af staat van het doel waartoe de gegevens oorspronkelijk zijn verwerkt is voor deze vordering een machtiging van de rechter-commissaris nodig.[56]

Ook de vordering van *'gevoelige gegevens'*, de zogenaamde 'bijzondere persoonsgegevens' van artikel 16 van de Wbp, is een bevoegdheid van de officier van justitie. Hiervoor is eveneens een machtiging van de rechter-commissaris vereist.[57]

---

[51] Wbvg, MvT, 4-5.
[52] Ibidem, 7-8, 20-23.
[53] Het gaat hier om een veelheid aan zeer privacygevoelige gegevens van zowel verdachte als niet-verdachte personen, bijvoorbeeld informatie over het soort videobanden dat iemand geleend heeft, welke boeken iemand hoe lang heeft geleend bij de bibliotheek, welke stukken iemand heeft aangevraagd in een archiefinstelling of hoeveel boodschappen iemand de afgelopen maand heeft afgerekend met zijn klantenkaart en ook - als de supermarkt dat bijhoudt - welke boodschappen dat precies waren. Anders dan bij de archiefsecter, is vanuit de bibliotheeksector door de koepelorganisatie FOBID (tevergeefs) opgeroepen het wetsvoorstel niet te aanvaarden, omdat de wet inbreuk zou maken op de persoonlijke levenssfeer van de burger die gebruik maakt van een bibliotheek en de vrije toegang tot informatie zou ondermijnen. In de *InformatieProfessional*-nummers van 2005 en 2006 zijn verschillende artikelen gepubliceerd over de (gevolgen van de) Wbvg voor de bibliotheeksector.
[54] Wbvg, MvT, 8-9, 23-24.
[55] Het gaat hier om de bevoegdheid tot het vorderen van *vooraf bepaalde* gegevens die op een later tijdstip toch al zouden worden verwerkt en níet tot het vorderen dat bepaalde gegevens worden verwerkt of vergaard die normaliter niet zouden worden verwerkt (hierin gaat de Wbvg dus iets minder ver dan het voorstel van de Commissie Mevis, vgl. *Bijlage III,* noot 222). In de vordering vermeldt de officier van justitie de termijn waarbinnen de gegevens moeten worden verstrekt. Het kan gaan om een termijn die langer is dan de periode gedurende welke de derde de gegevens voor de uitvoering van de eigen taken zou bewaren. Dit betekent dat van de derde kan worden gevraagd gegevens die hij normaliter niet zo lang zou bewaren, ten behoeve van het opsporingsonderzoek te bewaren tot het moment van verstrekking (ibidem, 9-10, 25).
[56] Wbvg, MvT, 9-10, 24-25.
[57] Ibidem, 10, 25.

Personele reikwijdte, procedures en rechten onderzoekssubjecten

De kring van personen over wie gegevens gevorderd kunnen worden, wordt begrensd door het belang van het opsporingsonderzoek; ook over 'anderen dan de verdachte' kunnen gegevens worden gevorderd.[58]

De Wbvg bepaalt dat een vordering tot verstrekking van gegevens schriftelijk moet zijn; de te vorderen gegevens dienen *vooraf bepaald* te zijn en zo specifiek mogelijk te zijn omschreven. Van de verstrekking dient een proces-verbaal te worden opgemaakt.[59]

Aan de persoon over wie de gegevens zijn gevorderd, dient, zodra het belang van het onderzoek het toelaat, mededeling te worden gedaan over de toepassing van de bevoegdheid (de notificatieplicht).[60] Degenen van wie gegevens opgevraagd zijn, kunnen een klacht indienen bij de rechtbank (klachtrecht); indien nodig kunnen achteraf de gevolgen van een verstrekking ongedaan worden gemaakt.[61]

Bezwaren tegen de Wbvg

Belangrijk kritiekpunt op de uitbreiding van de bevoegdheden tot het vorderen van gegevens is de inbreuk op de privacy van (onverdachte) burgers die ermee gepaard gaat. De pijlen richten zich vooral op de alomvattendheid van de bevoegdheden. Zo kan in beginsel elk geregistreerd gegeven van zowel verdachte als niet-verdachte burgers gevorderd worden ('wie niets te verbergen heeft, heeft immers niets te verliezen'). En elk gegeven wordt wel ergens geregistreerd. Vanwege de grootschaligheid van opgeslagen computergegevens komen burgers hierdoor sneller dan voorheen in het vizier van justitie. Er zijn echter veel gevallen denkbaar waarin niet-verdachte burgers wel degelijk wat te vrezen hebben van een onderzoek, zoals verlies van hun goede naam.[62]

Een ander kritiekpunt is dat de gevoeligheid van gegevens vooraf vaak niet kenbaar zal zijn. Bij het gewoon opvragen van alle gegevens kunnen eventuele 'gevoelige gegevens' als 'bijvangst' worden geteld.[63]

De vraag is ook of de vereisten van schriftelijkheid bij vordering, verbaliseringsplicht en notificatie de burgers voldoende rechtsbescherming bieden. Naar het oordeel van de CBP leert de ervaring dat dit slechts papieren garanties zijn.[64]

3.4. Wet verruiming mogelijkheden tot opsporing en vervolging van terroristische misdrijven (Wvm)

Vanaf 1 februari 2007 zijn door een aanpassing van het Wetboek van Strafvordering de mogelijkheden tot opsporing en vervolging van terroristische misdrijven opnieuw aanzienlijk verruimd.[65] Bijzondere opsporingsmethoden kunnen in het vervolg ingezet

---

[58] Ibidem, 6. De Memorie van Toelichting vermeldt dat bij de toepassing van de bevoegdheden ter verkrijging van gegevens van niet-verdachte personen 'grotere terughoudendheid' is geboden en dat hierover in het proces-verbaal verantwoording dient te worden afgelegd.

[59] Ibidem, 17. Bij of krachtens AMvB kunnen regels worden gesteld met betrekking tot de wijze waarop de gegevens worden gevorderd en verstrekt.

[60] Ibidem, 5. Deze notificatieplicht geldt niet voor de bevoegdheid tot het vorderen van identificerende gegevens.

[61] Ibidem, 4-5, 16, 27. Het beklagrecht heeft echter geen opschortende werking.

[62] Voor de inbreuk op de privacy als kritiekpunt op de Wbvg, zie: L. Stevens, B.-J. Koops en P. Wiemans, 'Een strafvorderlijke gegevensgaring nieuwe stijl', *NJB*, 32 (10 september 2004) 1680-1686, aldaar 1683, 1686.

[63] Stevens, e.a., 'Strafvorderlijke gegevensgaring nieuwe stijl', 1681.

[64] Ibidem, 1684.

[65] Wet van 20 november 2006 tot wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven, Stb. 2006, 580.

worden bij aanwijzingen dat een terroristische aanslag wordt voorbereid. Daarnaast zijn de mogelijkheden uitgebreid om informatie te verzamelen in het kader van een verkennend onderzoek, personen in bewaring te nemen en preventief te fouilleren.

Bijzondere opsporingsmethoden bij aanwijzingen terroristisch misdrijf

Voor het inzetten van bijzondere opsporingsmethoden is niet langer in alle gevallen een 'redelijk vermoeden' van een strafbaar feit noodzakelijk. Bij terrorisme zijn 'aanwijzingen' dat een 'terroristisch misdrijf' wordt voorbereid voldoende voor het inzetten van bijzondere opsporingsmethoden (waaronder ook de 'nieuwe' bevoegdheid tot het vorderen van gegevens!)[66] tegen een ieder, ook jegens personen die (nog) niet als verdachte worden aangemerkt.[67]

De toestemming voor het inzetten van bijzondere opsporingsmethoden door opsporingsambtenaren moet (schriftelijk) komen van de officier van justitie; bij het opnemen van vertrouwelijke communicatie en telecommunicatie en het vorderen van historische en toekomstige gegevens over een gebruiker en het telecommunicatieverkeer met betrekking tot de gebruiker is een machtiging van de rechter-commissaris nodig.[68]

Gegevensvordering bij verkennend onderzoek naar terroristische misdrijven

De mogelijkheden zijn verruimd om in een verkennend onderzoek informatie te verzamelen over groepen van personen waarbinnen mogelijk een aanslag wordt beraamd. De bevoegdheid tot het vorderen van identificerende gegevens en de bevoegdheid tot het vorderen van telecommunicatiegegevens mogen nu ook toegepast worden in een *verkennend* onderzoek naar terroristische misdrijven op basis van 'aanwijzingen' dat binnen verzamelingen van personen terroristische misdrijven worden beraamd of gepleegd.[69] Ten behoeve van dit verkennend onderzoek kunnen niet alleen gegevens, maar (delen van) volledige gegevensbestanden[70] van publieke en particuliere organisaties worden gevorderd, teneinde de daarin opgenomen gegevens te kunnen bewerken, d.w.z. aan elkaar te koppelen, te doorzoeken aan de hand van profielen en met elkaar en met andere bestanden te vergelijken met het oog op het opsporen van bepaalde patronen. Door deze bewerking ontstaan *nieuwe* gegevens.[71]

---

[66] Ibidem, Sv, Artikelen 126zk t/m 126zp. Wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven [Wvm], Memorie van Toelichting, TK 2004-2005, 30 164, nr. 3, p. 51.

[67] Wvm, MvT, 8-12. Van dergelijke 'aanwijzingen' is sprake, als 'de beschikbare informatie feiten en omstandigheden bevat die erop duiden dat daadwerkelijk een terroristisch misdrijf zou zijn of zal worden gepleegd', zoals het geval is bij moeilijk verifieerbare geruchten dat een aanslag wordt voorbereid of dat daartoe wordt samengespannen of bij uitkomsten van dreigingsanalyses van de AIVD.

[68] Ibidem, 35-42.

[69] Door de mogelijkheid om *bijzondere* opsporingsbevoegdheden en *dwang*middelen toe te passen tijdens een verkennend onderzoek naar terroristische misdrijven zijn de uitgangspunten aangaande het verkennend onderzoek zoals geformuleerd in de BOB verlaten; vgl. paragraaf 3.1. en noot 35 en 99.

[70] Onder 'bestand' wordt in de Memorie van Toelichting verstaan 'een gestructureerd geheel van persoonsgegevens, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen' (Wvm, MvT, 47). Ogenschijnlijk reflecteert deze formulering de bestandsdefinitie van de Wbp. Daar waar het begrip ‘bestand’ in de Wbp echter juist dient om (ook) niet-geautomatiseerde verwerkingen onder de reikwijdte van de wet te brengen, gaat het in de Wvm daarentegen expliciet om *geautomatiseerde* bestanden, zie: CBP, *Advies conceptwetsvoorstel bijzondere bevoegdheden tot opsporing van terroristische misdrijven*, Brief van de Minister van Justitie (22 december 2004) 1-12, aldaar 10.

[71] Wvm, MvT, 18-21, 47-48. De in de voorgaande paragraaf besproken bevoegdheden tot het vorderen van (identificerende) gegevens hebben betrekking *op vooraf bepaalde* gegevens over personen die van betekenis zijn voor de *opheldering van een misdrijf*. De toekenning tot het vorderen van geautomatiseerde gegevensbestanden in het kader van een *verkennend* onderzoek naar terroristische misdrijven strekt daarentegen tot het vorderen van *volledige bestanden of delen daarvan* waarbij het in het belang van de bewerking juist *níet* gaat om vooraf bepaalde gegevens. Juist het doorzoeken en bewerken van vooraf niet geselecteerde gegevens aan de hand van bepaalde zoeksleutels, profielen en patronen kan nieuwe

De vordering en verdere verwerking van gegevensbestanden ten behoeve van een verkennend onderzoek naar terroristische misdrijven is ingrijpend voor de persoonlijke levenssfeer van onderzoekssubjecten, omdat grote hoeveelheden gegevens worden gebruikt, ongeacht of personen zelf aanleiding geven tot onderzoek. Bij de vordering door de officier van justitie is in deze gevallen een machtiging van de rechter-commissaris nodig. De officier van justitie dient erop toe te zien dat van de bewerking een proces-verbaal wordt opgemaakt waarin wordt beschreven op welke gegevens de bewerking is uitgevoerd en op welke wijze de bewerking heeft plaatsgevonden; de politie voert het onderzoek feitelijk uit.[72]

De gegevensbewerking dient te geschieden op een wijze die de bescherming van de persoonlijke levenssfeer van personen zo veel mogelijk waarborgt.[73] Uitsluitend gegevens die het resultaat zijn van de bewerking en van betekenis zijn voor het onderzoek mogen voor het verkennend onderzoek verder worden verwerkt; gegevens die het resultaat zijn van de bewerking en niet van betekenis zijn voor het onderzoek alsmede gevorderde gegevens die geen deel uitmaken van het resultaat van de bewerking dienen te worden vernietigd.[74] Vernietiging van deze gegevens mag echter niet plaatsvinden voor zover en voor zolang de gegevens beschikbaar moeten blijven (en voor dat doel verwerkt mogen worden) om de bewerking achteraf te controleren.[75]

Bezwaren tegen de verruiming van de bevoegdheden

Kritiek van onder meer het CBP is dat de nieuwe bevoegdheden en taken die politie en justitie gekregen hebben vergelijkbaar zijn met die van de AIVD. De AIVD is volgens het CBP bij uitstek toegerust voor het inlichtingenwerk op het specialistische terrein van de terrorismebestrijding en op het afschermen van 'zachte' informatie. En het is juist in deze (steeds verder vervagende) scheiding van taken en bevoegdheden tussen de AIVD en de politie (die tot samenwerking noopt) waar volgens het CBP een belangrijke waarborg schuilt voor een adequate bescherming van persoonsgegevens.[76]

Een ander door het CBP geuit bezwaar is dat het verkennend onderzoek niet onder het bereik van de notificatieplicht valt. Hierdoor blijft de burger in beginsel onwetend (indien het onderzoek niet in een strafrechterlijke vervolging resulteert), waardoor hij ook geen

---

verbanden blootleggen en onverwachte inzichten opleveren, hetgeen in het kader van een verkennend onderzoek effectief kan zijn. De Wet bevoegdheden vorderen gegevens voorziet hierin niet. (Wvm, MvT, 24). De toepassing van de strafvorderlijke bevoegdheid bestanden te vorderen doorbreekt het regime van de Wbp dat eventueel van toepassing zou zijn op de bestanden indien deze niet gevorderd zouden zijn. (Wvm, MvT, 48).

[72] Ibidem, 21-22, 25. De officier van justitie stelt, op basis van het doel van het verkennend onderzoek, de profielen, patronen of sleutels vast aan de hand waarvan de gegevens worden bewerkt.

[73] De bescherming van de persoonlijke levenssfeer kan volgens de Memorie van Toelichting het beste gewaarborgd worden door de gegevensbewerking volledig geautomatiseerd te laten plaatsvinden, waarbij alleen van de resultaten van de bewerking kennis genomen kan worden. (Wvm, MvT, 22).

[74] De officier van justitie moet toezien op deze verdere verwerking en vernietiging. De Memorie van Toelichting meldt dat voor het verdere gebruik en de vernietiging voorschriften moeten worden gegeven. (Wvm, MvT, 22).

[75] Ibidem, 22, 48.

[76] CBP, *Advies conceptwetsvoorstel bijzondere bevoegdheden tot opsporing van terroristische misdrijven*, 1, 7. In de Memorie van Toelichting van het wetsvoorstel Wvm wordt de verhouding tussen opsporingsinstanties en inlichtingen- en veiligheidsdiensten na verruiming van de bevoegdheden van de eerste als volgt geformuleerd. In de operationele sfeer wordt, vanuit een verschillende invalshoek, de bestrijding van terrorisme (met inbegrip van het voorkomen ervan) primair door de inlichtingen- en veiligheidsdiensten en door de met opsporing en vervolging van strafbare feiten belaste instanties uitgevoerd. Inlichtingen- en veiligheidsdiensten richten zich op het tijdig onderkennen en waar mogelijk voorkomen van (de realisatie van) terroristische dreigingen. De opsporingsinstanties hebben een strafrechtelijke invalshoek bij hun optreden: hun focus is gericht op het opsporen en vervolgen van strafbare feiten. Door de verruiming van de mogelijkheid om in het kader van terrorismebestrijding in een eerder stadium strafvorderlijk op te treden, zullen eerder dan voorheen onderzoeken naar personen en organisaties in het door de Wiv 2002 beheerste domein 'over kunnen gaan' naar het strafvorderlijke domein. (Wvm, MvT, 33).

rechterlijke toetsing kan inroepen.[77] Voor de bewerkingen die wel onder de notificatieplicht vallen, constateert het CBP dat de naleving van deze plicht tekort schiet en dat onafhankelijk toezicht op naleving ervan onontbeerlijk is. Voor dit toezicht, alsook voor het op structurele basis toezien op de uitvoeringspraktijk van politie en justitie inzake verwerking van persoonsgegevens, ontbreekt het het CBP echter aan middelen.[78]

Risico's datamining

Het CBP plaatst vraagtekens bij de algemene deugdelijkheid van de methodiek van profilering en *datamining*. De waarde van dergelijke instrumenten wordt bepaald door de kwaliteit van de gegevens en de profielen en sleutels die als uitgangspunt voor de bewerking worden gekozen. De politie zal in veel gevallen niet voor de juistheid of volledigheid van de gebruikte gegevens kunnen instaan. In voorkomende gevallen zal de politie de kwaliteit van de gegevens zelfs niet kúnnen kennen, omdat deze gegevens oorspronkelijk door andere partijen voor andere doeleinden werden verwerkt. Profielen en sleutels zijn ongeschikt om gebreken in de gebruikte databestanden te compenseren. Op z'n minst zou acht geslagen moeten worden op de zeer uiteenlopende herkomst en mate van betrouwbaarheid van gebruikte gegevens.[79]

Ook in reactie op andere wetsvoorstellen, zoals het voorstel tot verruiming van de bevoegdheden van de inlichtingen- en veiligheidsdiensten dat momenteel in behandeling is, wijst het CBP bovenal op de risico's en nadelen van data-analyse. Diensten zullen steeds meer gegevens moeten analyseren om de eenvoudige reden dat steeds meer gegevens beschikbaar komen; dit 'zoeken naar een spel in een hooiberg' is allerminst bevorderlijk voor de effectiviteit van het doorzoeken van informatie.[80]

Daarnaast is volgens het CBP niet gegarandeerd dat de gegevens die door overheden en bedrijven worden verstrekt zodanig van kwaliteit zijn, dat daaruit, 'op zichzelf, of in samenhang met andere gegevens bezien, conclusies kunnen worden getrokken die overeenkomen met de werkelijkheid' Hierin schuilt een groot risico voor de burgers. Gegevens kunnen immers in een andere context dan waarin zij verzameld zijn of bewaard worden, een volstrekt onjuist beeld geven van die (groep) burger(s); het risico op zogenaamde 'valse positieve' of 'valse negatieve uitkomsten' is aanzienlijk.[81]

Bovendien bergt data-analyse het risico van zogenaamde *function creep* met betrekking tot zowel personen/onderzoeksubject als doelbinding in zich: enerzijds worden technologieën die aanvankelijk gericht zijn op bepaalde groepen gaandeweg toegepast op (bijna) iedereen (ook op onverdachte personen), terwijl anderzijds verzamelde gegevens voor een bepaald doel ten behoeve van een ander doel (verplicht) verstrekt en verwerkt worden.[82]

---

[77] CBP*, Wetsvoorstel tot verruiming van de mogelijkheden ter opsporing en vervolging van terroristische misdrijven*. Brief aan de Vaste commissie voor Justitie van de Eerste Kamer (2 november 2006) 1-5, aldaar 3.
[78] CBP, *Advies conceptwetsvoorstel bijzondere bevoegdheden*, 2, 11.
[79] CBP, *Advies conceptwetsvoorstel bijzondere bevoegdheden*, 10-11; CBP, *Wetsvoorstel tot verruiming van de mogelijkheden*, 3.
[80] CBP, *Advies wetsvoorstel 30 533*, Brief aan voorzitter van de Tweede Kamer (20 december 2007) 10. Voor dezelfde argumentatie zie Buruma's opmerkingen over de verhouding tussen *actionable intelligence* en *noise* in noot 102.
[81] Ibidem, 11.
[82] Ibidem.

4. SECTORALE WETGEVING GEGEVENSVERWERKING OPSPORINGSDIENSTEN: WPOLG

In het voorgaande hoofdstuk zijn de (verruimingen van de) bevoegdheden van opsporingsdiensten om gegevens te verzamelen (of te vorderen) de revue gepasseerd. Na de behandeling in hoofdstuk 2 van de generieke informationele privacywetgeving gaat dit hoofdstuk dieper in op de regels die in sectorale en aanvullende wetgeving gesteld zijn aan de verwerking van (verzamelde/gevorderde) gegevens door opsporingsdiensten (politie en justitie). Dit gebeurt aan de hand van een uitgebreide analyse van de Wet politiegegevens (Wpolg). Een korte weergave van de Wet justitiële en strafvorderlijke gegevens (Wjsg) is in *Bijlage IV* opgenomen.

Wet politiegegevens (Wpolg)

De Wbp is niet van toepassing op verwerking van persoonsgegevens door de politie. Een dergelijke verwerking is volgens de wetgever zodanig specifiek van aard dat een aparte regeling noodzakelijk is, die 'enerzijds meer ruimte biedt voor het gegevensverkeer binnen de politie en een meer geclausureerd recht op kennisneming en correctie inhoudt dan mogelijk zou zijn onder het regime van de Wbp en die anderzijds rekening houdt met de gevoeligheid van de gegevens'.[83] Deze aparte regeling is de Wet politieregisters (Wpolr) die met ingang van 1 januari 2008 vervangen is door de Wet politiegegevens (Wpolg).[84] De nieuwe wet wordt geïmplementeerd in samenhang met de invoering van een nieuwe landelijke informatiehuishouding bij de politie.[85]

Aanleiding herziening Wpolr

De herziening van de Wpolr achtte de wetgever noodzakelijk om tegemoet te kunnen komen aan nieuwe werkwijzen van de politie met betrekking tot het verwerken en

[83] Regels inzake de verwerking van politiegegevens (Wet politiegegevens), Memorie van Toelichting, TK 2005-2006, 30 327, nr. 3, p.3.
[84] Wet van 21 juni 1990, houdende regels ter bescherming van de persoonlijke levenssfeer in verband met politieregisters (Wet politieregisters), Stb, 1990, 414 en Wet van 21 juli 2007, houdende regels inzake de verwerking van politiegegevens (Wet politiegegevens) [Wpolg], Stb. 2007, 300.
[85] In 2003 concludeerde de Algemene Rekenkamer in een onderzoek naar de uitwisseling van opsporings- en terrorisme-informatie dat de verzameling en uitwisselingen van informatie over (potentiële) criminele activiteiten alsook op het gebied van terrorismebestrijding binnen de politieorganisatie tekortkomingen vertoonde, die terug te voeren waren op een te kort schietende organisatie en opzet van de informatiehuishouding van de politie. Voor het terrorismedomein ontbrak bij het KLPD zelfs een specifiek informatiesysteem voor het terrorismedomein. De Algemene Rekenkamer adviseerde dat het KLPD een voor de opsporingsdiensten beschikbaar en bruikbaar informatiesysteem voor het beleidsveld terrorisme diende te ontwikkelen, dat alle informatie zou bevatten die opsporingsdiensten verzamelden en de indicatie 'terrorisme' had meegekregen. Dit systeem zou uitsluitend door aangewezen functionarissen binnen de gehele politieorganisatie te raadplegen moeten zijn. De systeembeschrijving ervan zou moeten aangeven welke informatie vanuit welke kanalen op welke wijze aangeleverd zou moeten worden. Met betrekking tot de uitwisseling van terrorisme-informatie tussen KLPD en AIVD constateerde de Algemene Rekenkamer dat, hoewel beide organisaties informatie verzamelen op het terrein van terrorisme, een geautomatiseerde afstemming van de gegevens niet plaats vond. Derhalve bestond er geen zekerheid over de volledigheid van relevante informatie op centraal niveau. In een *follow up* op haar rapportage stelde de Algemene Rekenkamer vast dat het KLPD de nodige stappen heeft gezet in de ontwikkeling van een geautomatiseerd informatiesysteem waarin terrorisme-informatie opgeslagen is. De wettelijke grondslag voor opslag van deze informatie (onder meer het langer dan vier maanden bewaren van gegevens over onverdachte personen en het aanleggen van themaregisters) ontbrak echter nog en zou pas in de nieuwe Wet politiegegevens zijn beslag krijgen. Ook oordeelde de Rekenkamer positief over de ontwikkelingen rond de zogenaamde CT-Infobox (zie hoofdstuk 6.2.), die een betere afstemming of uitwisseling van terrorisme-informatie mogelijk zou maken. Zie: *Uitwisseling van opsporings- en terrorisme-informatie*, Rapport Algemene Rekenkamer, TK 2002-2003, 28 845, nr. 2, p. 5-6, 34-38 en Algemene Rekenkamer, *Terugblik 2005. Elf onderzoeken nader beschouwd* (Den Haag, 24 maart 2005) 20-30.

veredelen van informatie. Met de ontwikkelingen in de informatie- en communicatietechnologie zijn de mogelijkheden tot het leggen van verbanden tussen gegevens sterk toegenomen. De politie maakt hierdoor steeds meer gebruik van 'informatiegestuurde opsporing', dit is opsporing die plaatsvindt door onder andere eenmaal verzamelde gegevens langs elektronische weg met elkaar in verband te brengen.[86] Daarnaast werkt de politie bij de uitoefening van de politietaken steeds vaker samen met andere instanties, wat leidt tot een toenemende behoefte aan informatie-uitwisseling met derden. Ook de aandacht voor terroristische activiteiten wordt als één van de redenen genoemd voor de herziening.[87]

Uitbreiding verwerkingsmogelijkheden politiegegevens

Ten opzichte van de Wpolr verruimt de Wpolg de mogelijkheden van de politie tot het verwerken van gegevens over personen die (nog) niet als verdachte zijn aangemerkt. Daarnaast biedt de Wpolg de politie de mogelijkheid meer permanent gegevens te verwerken, ook betreffende onverdachte personen, die relevant kunnen zijn voor het inzicht in bijvoorbeeld terroristische activiteiten; deze gegevens mogen bovendien langer bewaard worden dan voorheen. Voorts mag de politie krachtens de Wpolg verzamelde gegevens van onverdachte personen uit een bepaald onderzoek zonodig gaan gebruiken voor andere onderzoeken en verruimt het de zoekmogelijkheden in databestanden en het gebruik van *datamining*-technieken. Verder is het verstrekkingsregime minder gesloten dan dat van de Wpolr en zijn er meer mogelijkheden om gegevens te verstrekken aan derden waarmee de politie samenwerkt.[88]

Verhouding Wpolg en Wbp

Net als de Wpolr stelt de Wpolg regels inzake de verwerking van politiegegevens, dat wil zeggen van persoonsgegevens die opgenomen zijn in politieregisters ten behoeve van de uitvoering van de politietaak.[89] De Wpolg steunt, net als zijn voorganger, rechtstreeks op artikel 10 van de Grondwet en geeft invulling aan de informationele privacy van onderzoekssubjecten; de Wpolg is daarmee het politiële equivalent van de Wbp.[90]

Evenmin als de Wpolr beoogt de Wpolg bevoegdheden te regelen tot het 'verkrijgen' van politiegegevens. Dergelijke bevoegdheden worden geregeld in andere wetten,

---

[86] In 2004 is dit idee van de 'informatiegestuurde opsporing' (naar voorbeeld van het Britse *intelligence-led policing*) in een rapport van de Raad van Hoofdcommissarissen gelanceerd. Toepassing van geavanceerde technologieën en een goed informatiebeheer zouden de politie in staat moeten stellen het opsporingswerk optimaal te sturen; een zorgvuldige analyse van de opsporingsinformatie staat daarbij centraal. Het begrip 'opsporing' moest hierbij ruim worden geïnterpreteerd: behalve voor de traditionele, reactieve opsporing, zou er meer ruimte moeten komen voor proactieve en op preventie gerichte opsporingsactiviteiten. Hierbij zou de politie zich veel meer gaan richten op groepen van potentiële verdachten dan op individuen; zie A. Vedder, L. v.d. Wees, B.-J. Koops en P. de Hert, *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw* (Den Haag: Rathenau Instituut, 2007) 44.

[87] Wpolg, MvT, 2.

[88] Ibidem.

[89] Gerefereerd wordt aan de politietaak als bedoeld in art. 2 van de Politiewet 1993. Dit betekent dat de Wpolg niet alleen betrekking heeft op de strafvorderlijke gegevensverwerking, maar ook op de verwerking van gegevens voor andere taken, zoals de handhaving van de openbare orde en de hulpverlening (maar bijvoorbeeld níet op taken samenhangend met de interne bedrijfsvoering).

[90] De Wpolg sluit weliswaar zoveel mogelijk aan bij de systematiek en uitgangspunten van de Wbp, maar is geen *lex specialis* ten opzichte van de Wbp. De Wbp is niet van toepassing op politiegegevens (Wbp, artikel 2). Dit in tegenstelling tot de meeste Europese landen die de algemene privacywetgeving ook van toepassing hebben verklaard op de gegevensverwerking door politiediensten (Mac Gillavry, 'Nieuwe Wet politiegegevens', 396).

waaronder het Wetboek van Strafvordering en zijn aan de orde gekomen in het vorige hoofdstuk.[91]

De Wpolg is van toepassing op de verwerking van 'politiegegevens'[92] die in een 'bestand'[93] zijn opgenomen of die bestemd zijn daarin te worden opgenomen. Bij deze gegevensverwerking gaat de Wpolg, net als de Wbp, uit van het principe van de doelbinding en niet meer van het registerbegrip (en de hiermee samenhangende verplichting om per register een reglement op te stellen) dat het uitgangpunt van de Wpolr vormde. Ook de vermelding van het noodzakelijkheids-, rechtmatigheids- en doelbindingscriterium[94] weerspiegelt de Wbp, evenals de bepalingen aangaande het bewaren/vernietigen en de juistheid, volledigheid en beveiliging van politiegegevens.[95]

Doelbinding en verwerkingsdoelen

Het uitgangspunt dat politiegegevens alleen voor welomschreven en gerechtvaardigde doelen worden verwerkt, leidt tot het onderscheiden van een vijftal doelen binnen de politietaak, waarvoor gegevens mogen worden verwerkt.

Voor één van die doelen, de uitvoering van de dagelijkse politietaak, mogen gedurende één jaar na de datum van eerste verwerking politiegegevens van zowel verdachte als onverdachte personen vrij worden verwerkt. Onder de Wpolr was deze bewaartermijn maximaal vier maanden. Gedurende deze periode van één jaar kunnen de gegevens, waar mogelijk en noodzakelijk, geautomatiseerd met elkaar worden vergeleken en in combinatie met elkaar verder worden verwerkt, teneinde vast te stellen of verbanden bestaan tussen de gegevens. Daarna worden de gegevens 'verwijderd', dat wil zeggen 'achter het schot geplaatst' en zijn ze nog vier jaar beschikbaar voor raadpleging, indien daar aanleiding toe bestaat, alvorens 'vernietigd' te worden. Nieuw ten opzichte van de Wpolr is dat de Wpolg de mogelijkheid biedt de gegevens verder te verwerken voor een ander doel binnen de politietaak. Is dit het geval, dan geldt een andere vernietigingstermijn (Wpolg, artikel 8).[96]

---

[91] Voor een interessante verhandeling over de kwestie van de 'verkrijging' of 'verzameling' (verzamelen is een verwerkingshandeling!) van gegevens en de verhouding van de Wpolg ten opzichte van het Wetboek van Strafvordering, zie: Mac Gillavry, 'Nieuwe Wet politiegegevens', 405-409.

[92] Analoog aan de Wbp wordt onder 'politiegegeven' verstaan: 'elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon dat in het kader van de uitoefening van de politietaak wordt verwerkt' (Wpolg, artikel 1, eerste lid). Ook de definitie van 'verwerken' is gelijk aan die van de Wbp, zij het dat in de Wpolg-definitie nog de -tegen de achtergrond van data-analysetechnieken overigens niet onbelangrijke - handeling 'vergelijken' is toegevoegd.

[93] De definitie van 'bestand' is in de Wpolg identiek aan die van de Wbp.

[94] Politiegegevens mogen slechts worden verwerkt 'voor zover dit noodzakelijk is voor de bij of krachtens de wet geformuleerde doeleinden', 'voor zover zij rechtmatig zijn verkregen en, gelet op de doeleinden waarvoor zij worden verwerkt, toereikend, terzake dienend en niet bovenmatig zijn'. De gegevens mogen uitsluitend worden verwerkt voor een ander doel dan waarvoor zij zijn verkregen, 'voor zover de wet daar uitdrukkelijk in voorziet' (Wpolg, artikel 3).

[95] De verantwoordelijke treft de nodige maatregelen opdat politiegegevens 'juist en nauwkeurig' zijn en hij 'verbetert, vernietigt of vult deze aan indien hem blijkt dat deze onjuist of onvolledig zijn'; hij treft 'de nodige maatregelen' opdat politiegegevens worden verwijderd *of* vernietigd zodra zij niet langer 'noodzakelijk' zijn voor het doel waarvoor ze zijn verwerkt of dit door enige wettelijke bepaling wordt vereist. Hij treft 'passende technische en organisatorische maatregelen' om de politiegegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking (Wpolg, artikel 4). De Wpolg maakt een duidelijk onderscheid tussen 'verwijderen' (het achter een schot plaatsen) en 'vernietigen'. De Wpolr sprak in dit verband van de plicht tot verwijderen *en* vernietigen; op grond van de Wpolr betekent (enkele nauwkeurig omschreven gevallen daargelaten) verwijderen een dwingend voorgeschreven daadwerkelijke vernietiging. De *Basisselectielijst voor archiefbescheiden van (Regionale) Politieorganisaties 2004* verwijst voor de bewaartermijnen van in registratiesystemen opgenomen politiegegevens naar de Wpolr en de daaruit voortvloeiende privacyreglementen. De selectielijst merkt op dat de (destijds nog ontwerp-) Wet Politiegegevens naar verwachting zal leiden tot andere bewaartermijnen van gegevens die onder de Wpolr zo spoedig mogelijk vernietigd dienen te worden; zie: *Basisselectielijst politieorganisaties 2004*, 4, 10.

[96] Wpolg, MvT, 10-11, 38-42.

Een ander doel waarvoor de politie gegevens mag verwerken, is 'onderzoek in verband met de handhaving van de rechtsorde in een bepaald geval'. Van deze *gerichte* verwerking is sprake zodra een rechercheonderzoek is aangemeld, een *verkennend onderzoek* wordt gestart en zodra bijzondere opsporingsmethoden worden ingezet. De gegevens kunnen beschikbaar worden gesteld voor verdere bewerking ten behoeve van bepaalde andere doelen binnen de politietaak. 'Verwijdering' van de gegevens vindt plaats zodra het onderzoek is afgerond. Deze verwijdering behelst niet een onmiddellijke vernietiging (de gegevens dienen nog vijf jaar bewaard te worden), maar een apart zetten zodat ze niet langer toegankelijk zijn voor operationele doeleinden. In bijzondere gevallen kunnen de gegevens opnieuw beschikbaar komen voor operationeel gebruik (Wpolg, artikel 9).[97]

Themaverwerking

De politie mag ook gegevens gericht verwerken van zowel verdachte als onverdachte personen indien deze verwerking noodzakelijk is voor het verkrijgen van 'inzicht in de betrokkenheid van personen bij bepaalde ernstige bedreigingen van de rechtsorde' (Wpolg, artikel 10), waaronder (refererend aan terrorisme) 'handelingen die kunnen wijzen op het beramen of plegen van (...) categorieën van misdrijven die door hun ernst of hun samenhang met andere misdrijven een ernstig gevaar voor de rechtsorde opleveren', (Wpolg, artikel 10, eerst lid, onderdeel b). Verwerking van gegevens vindt in dit kader plaats omtrent 'personen die betrokken zijn bij de [bovengenoemde] handelingen' en personen, die tot deze personen 'in een bepaalde relatie staan' (Wpolg, artikel 10, derde lid). Om terroristische dreigingen het hoofd te kunnen bieden en inzicht te krijgen in 'de kring van personen die op grond van de handelingen die zij verrichten daarbij betrokken kunnen zijn', is het noodzakelijk dat ('in een zeer vroeg stadium') relevante gegevens worden verzameld en geanalyseerd.[98]

Anders dan bij Wpolg, artikel 9 staat in Wpolg, artikel 10 niet zozeer de gebeurtenis of situatie centraal, als wel de opbouw van een informatiepositie; de gegevensverwerking heeft een zogenaamde 'pro-actieve functie'. In dit kader vindt 'een min of meer permanent proces van analyse' plaats dat leidt tot het vastleggen van gegevens over (groepen van) veelal nog onverdachte personen ten aanzien van wie 'aanknopingspunten' bestaan dat zij betrokken kunnen zijn bij de hierboven omschreven handelingen. Hiermee geeft de Wpolg uitdrukking aan de aanbeveling van de werkgroep Gegevensuitwisseling en Terrorismebestrijding om zogenaamde 'themaverwerking' mogelijk te maken.[99]

---

[97] Ibidem, 11-12, 43-46.

[98] Ibidem, 46, 48-50. Problematisch voor de kwaliteit van de gegevens en voor de hiermee samenhangende privacy van betrokkenen is echter dat gegevens die in het kader van Wpolg artikel 9 en 10 worden verwerkt volgens de Memorie van Toelichting 'niet altijd op juistheid en volledigheid zijn en kunnen worden getoetst'. (Wpolg, MvT, 52). Het pleidooi van het CBP om politiegegevens te voorzien van een codering omtrent de kwaliteit van de gegevens is volgens de Memorie van Toelichting niet goed uitvoerbaar (vgl. noot 100): 'Eigen aan het werk van de politie (...) is immers dat men veelal werkt met gegevens waarvan de juistheid en volledigheid niet vaststaan.' Hierdoor zal de waarde van een code omtrent de kwaliteit van gegevens per definitie slechts zeer beperkt kunnen zijn. Wel worden ten behoeve van de kwaliteit van de gegevens de herkomst en de wijze van verkrijging vermeld. (Wpolg, MvT, 21)

[99] Wpolg, MvT, 49. De Werkgroep Gegevensuitwisseling en Terrorismebestrijding, samengesteld uit vertegenwoordigers van de Ministeries van Justitie, OM, BZK en Defensie en de KLPD, adviseerde in een in 2003 uitgebracht rapport de zogenaamde themaregisters in het leven te roepen; zie: *Gegevensuitwisseling en Terrorismebestrijding*, Werkgroep Gegevensuitwisseling en Terrorismebestrijding (6 januari 2003) en Brief van de Minister van Justitie, Bestrijding internationaal terrorisme, TK 2002-2003, 27 925, nr. 82. Mac Gilavry merkt in verband met deze themaverwerking op dat het hierbij gaat om een veel omvangrijkere gegevensverwerking dan volgens de Wet BOB bij het zogenaamde *verkennend onderzoek* toegestaan was. Dit verkennend onderzoek mocht alleen plaatsvinden als er *aanwijzingen* waren dat in *georganiseerd* verband misdrijven werden geraamd of gepleegd. Bovendien beperkte het zich tot gegevens die afkomstig waren uit *open* bronnen of die zijn verzameld op basis van *vrijwillige* medewerking van particulieren; zie; Mac Gilavry, 'Heeft u even voor de nieuwe Wet politiegegevens?' 406-407. De in het vorige hoofdstuk besproken Wet verruiming mogelijkheden tot opsporing en vervolging van terroristische misdrijven heeft echter het BOB-concept van het verkennend onderzoek al verlaten door

Gegevens die zijn verwerkt ten behoeve van een doel als geformuleerd in de artikelen 9 en 10 kunnen, indien noodzakelijk, langs geautomatiseerde weg worden vergeleken met gegevens die zijn verwerkt in een ander onderzoek. In dit verband kunnen *alle* beschikbare politiegegevens (inclusief de gegevens van onverdachte burgers die in een ander -vrijwillig of verplicht- verband zijn verzameld) in combinatie met elkaar worden verwerkt en op basis van patronen en profielen worden onderzocht. Deze zoekmogelijkheden (voorzien in Wpolg, art. 11) houden een verruiming in ten opzichte van de Wpolr.[100]

De gegevens dienen minimaal elke zes maanden te worden gecontroleerd om de noodzaak na te gaan tot verwerking voor het betreffende doel. Aangezien de permanente artikel-10-verwerking geen natuurlijke grens kent in de afsluiting van een onderzoek, is bepaald dat de gegevens uiterlijk worden verwijderd na verloop van vijf jaren na de datum van de laatste opname van gegevens die blijk geven van de noodzaak tot verwerking met het oog op het doel bedoeld in artikel 10. Verwijderde gegevens worden vervolgens nog vijf jaar 'achter het schot' bewaard en kunnen alleen in bijzondere gevallen beschikbaar worden gesteld voor hernieuwde verwerking op grond van de artikelen 9 en 10.[101]

Het is vooral deze themaverwerking, met de eraan gekoppelde zoekmogelijkheden en bewaartermijnen, die zeer ingrijpend kan zijn voor de persoonlijke levenssfeer van onverdachte personen. Hier richt zich dan ook de nodige kritiek op, nog los van de vraag naar de effectiviteit van de maatregel en het competentievraagstuk.[102] Voor een dergelijke verwerking is namelijk niet 'een redelijk vermoeden van schuld' aan ernstige strafbare feiten vereist. Alleen 'betrokkenheid bij handelingen die kunnen wijzen op' is al een voldoende en bovendien erg ruim criterium, waardoor het aantal geregistreerden fors zal toenemen. Doordat themaverwerkingen betrekking hebben op onverdachte personen in een proactieve fase, staan deze volgens het CBP op gespannen voet met de eisen van proportionaliteit en subsidiariteit. Burgers die voldoen aan de opnamecriteria voor een themaverwerking worden daarin opgenomen als potentieel dader van zeer ernstige criminaliteit. Alleen al op die grond vormt een dergelijke gegevensverwerking een groot risico voor hen. Het CBP heeft dan ook 'onoverkomelijke bezwaren' geuit tegen het op grote schaal en voortdurend verwerken

---

bijzondere opsporingsbevoegdheden en dwangmiddelen in het kader van een verkennend onderzoek naar terroristische misdrijven toe te staan. Vgl. paragraaf 3.1. en noot 35 en 69.

[100] Wpolg, MvT, 14, 51-55. Bij of krachtens AMvB worden regels gesteld over de uitvoering van deze gegevensvergelijking, die onder meer betrekking kunnen hebben op het 'oormerken' van politiegegevens naar mate van betrouwbaarheid (vgl. noot 98) en/of vertrouwelijkheid. Naast deze codering kan bij AMvB tevens worden bepaald op basis van welke categorieën van gegevens politiegegevens vergeleken kunnen worden en op welke wijze de verbanden zichtbaar gemaakt kunnen worden. Deze regels kunnen worden gesteld om de veiligheid van bijvoorbeeld getuigen of informanten te waarborgen.

[101] Ibidem, 16-17, 51.

[102] Kielman en Koelewijn betwijfelen of het op grote schaal verzamelen van 'zachte' gegevens werkelijk effectief zal zijn in de strijd tegen terrorisme. Zij citeren in dit verband Buruma, die erop wijst dat het verzamelen van te veel informatie het gevaar in zich heeft dat de verhouding tussen *actionable intelligence* en *noise* onaanvaardbaar scheef komt te liggen: 'Men weet dan te veel van te veel mensen om een verstandige keuze te kunnen maken tussen gegevens waar echt iets mee moet gebeuren' (vgl. de opmerkingen van het CBP inzake *datamining* in paragraaf 3.4.) Bovendien is het uitbouwen en in stand houden van een permanente informatiepositie en het uitvoeren van themaverwerkingen volgens Kielman en Koelewijn geen taak van de politie, maar van de AIVD (ook het CBP ziet hierin eerder een taak voor de AIVD weggelegd, zie: CBP, *Advies conceptwetsvoorstel inzake de verwerking van politiegegevens (Wet politiegegevens)*, Brief aan de Minister van Justitie (3 augustus 2004) 28. Deze steeds verder vervagende scheiding van taken en bevoegdheden tussen de AIVD en de politie was al een voornaam kritiekpunt van het CBP met betrekking tot de verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven, zie noot 76). De forse toename van het aantal geregistreerden en verwerkingsmogelijkheden van gegevens, vergroot het gevaar van onrechtvaardige inbreuken op de privacy. Vanwege het ontoereikende en weinig effectieve toezicht zijn Kielman en Koelewijn van mening dat het nieuwe regime van de Wpolg een andere balans inhoudt tussen het opsporingsbelang en het privacybelang, waarbij deze eerste aanmerkelijk zwaarder is gaan wegen. Zie: H.H. Kielman en W.I. Koelewijn, 'Minder registers, meer gegevens. Over gegevensverwerking betreffende zware criminaliteit', *Ars Aequi* (juni 2005) 451- 457.

van gegevens over onverdachte personen in het kader van de themaverwerkingen en, tevergeefs, 'met klem' geadviseerd af te zien van dit nieuwe wettelijke fenomeen.[103]

Uitbreiding verstrekkingsregime

Om tegemoet te komen aan de wens om gegevens uit te wisselen met derden waarmee de politie samenwerkt, is het verstrekkingsregime vergaand verruimd in vergelijking met het gesloten regime van de Wpolr. Verstrekking van politiegegevens aan derden kan plaatsvinden indien dit voortvloeit uit 'een wettelijke verplichting' (zoals de verstrekking aan gezagsdragers of bepaalde opsporingsambtenaren of zoals voortvloeiend uit de verplichting gegevens te verstrekken aan de AIVD of MIVD, conform artikelen 17 en 62 van de Wet inlichtingen- en veiligheidsdiensten (Wiv 2002)) of voor zover dit door de verantwoordelijke korpsbeheerder, in overeenstemming met het bevoegd gezag, 'noodzakelijk' wordt geacht met het oog op 'een zwaarwegend algemeen belang' (artikelen 18 t/m 20) .[104]

In enkele gevallen[105] is ook zogenaamde rechtstreekse verstrekking langs geautomatiseerde weg mogelijk, wat inhoudt dat een derde *online* inzage kan krijgen in politiebestanden. Vanuit het oogpunt van privacybescherming en afscherming van gevoelige opsporingsinformatie is rechtstreekse verstrekking uitsluitend mogelijk 'voor zover dit noodzakelijk is voor het doel waarvoor die gegevens worden verstrekt' en nadat is voldaan aan technische en organisatorische eisen ten behoeve van beveiliging. De verantwoordelijke is verplicht hiertoe passende maatregelen te treffen (Wpolg, artikelen 4 en 23).[106]

Rechtstreekse verstrekking aan de AIVD

De politie heeft op grond van artikel 62 van de Wiv 2002 een plicht tot het verstrekken van informatie die van belang kan zijn voor de inlichtingen- en veiligheidsdiensten (AIVD en MIVD). Daarnaast is in artikel 60 van de Wiv 2002 bepaald dat de korpschef van een politiekorps en de commandant van de Koninklijke marechaussee werkzaamheden (laten) verrichten voor de AIVD onder verantwoordelijkheid van de Minister van BZK en overeenkomstig de aanwijzingen van het Hoofd van de AIVD. De Regionale Inlichtingen Diensten (RID) houden zich bezig met de informatieverzameling ten behoeve van de AIVD.

---

[103] CBP, *Advies conceptwetsvoorstel Wet politiegegevens*, 28-29, 40.

[104] De Wpolr hanteerde het criterium van 'het openbare belang' voor verstrekkingen aan derden, evenals de vereiste van 'de publieke taak' (Wpolr, artikel 18, derde lid). De vervanging van het criterium van 'het openbaar belang' door het criterium van 'het zwaarwegend algemeen belang' en het vervallen van de eis van 'de publieke taak' brengen met zich mee dat de Wpolg verstrekking van politiegegevens aan particuliere instanties mogelijk maakt met het oog op 'een zwaarwegend algemeen belang' (Wpolg, MvT, 73). In geval van 'noodzakelijk' geachte verstrekking op 'een zwaarwegend algemeen belang' kan het gaan om incidentele verstrekkingen in bijzondere gevallen, dan wel verstrekkingen in het kader van een structureel samenwerkingsverband tussen een of meer politiekorpsen en andere instanties (Wpolg, MvT, 5).

[105] Deze mogelijkheid staat open voor leden van het Openbaar Ministerie, voor zover zij deze gegevens nodig hebben voor strafvorderlijke beslissingen omtrent opsporing en vervolging en de hulp aan slachtoffers van strafbare feiten. Ook enkele andere bij AMvB aangewezen instanties of personen met een publiekrechtelijke taak kunnen voor rechtstreekse verstrekking van een bepaalde categorie van politiegegevens in aanmerking komen (Wpolg, artikel 23).

[106] Wpolg, MvT, 79-80. De verantwoordelijke dient er bij deze rechtstreekse verstrekking op toe te zien dat de verstrekking van politiegegevens plaatsvindt aan de hand van de door de belanghebbende te verstrekken persoonsgegevens. Zo dient de verantwoordelijke er op toe te zien dat een derde geen eigen (schaduw)bestand van politiegegevens zou kunnen aanleggen. Hiertoe kunnen voorwaarden worden gesteld die waarborgen dat de ontvanger de verkregen politiegegevens niet zelf opslaat dan wel deze gedurende een beperkte termijn verwerkt. (Wpolg, MvT, 80). Omdat controle op naleving hiervan niet eenvoudig zal zijn, voegt de Memorie van Toelichting hier verwachtingsvol (of vertwijfeld?) aan toe dat '*op termijn* (...) *wellicht* (cursivering KR) technische voorzieningen mogelijk [zijn] die opslag door de ontvangers voorkomen'.

De Wpolg voorziet via artikel 24 in de rechtstreekse verstrekking van in beginsel alle politiegegevens[107] aan de AIVD voorzover dat 'noodzakelijk' is voor de uitvoering van de taak als bedoeld in artikel 6, tweede lid van de Wiv 2002. Gegevens die worden opgeslagen en verwerkt ten behoeve van een goede uitvoering van de politietaak kunnen (doelafwijkend) op systematische wijze zelfstandig worden geraadpleegd en verder worden verwerkt door de AIVD[108]. Deze regeling is nieuw ten opzichte van de Wpolr en beoogt tegemoet te komen aan geconstateerde tekortkomingen op het gebied van de geautomatiseerde afstemming van gegevens tussen de AIVD en de politie bij de bestrijding van terrorisme.[109]

Privacywaarborgen

Waar de Wpolg aan de ene kant uitdrukkelijk de mogelijkheden tot opslag, gebruik en verstrekking van politiegegevens verruimt, beoogt het aan de andere kant in de nodige waarborgen te voorzien voor de burger tegen ongerechtvaardigde inbreuken op zijn persoonlijke levenssfeer.

Centraal in de Wpolg staat dat meer bescherming tegen inbreuken op de privacy worden geboden, naarmate de gegevensverwerking gerichter en voor onderzoekssubjecten ingrijpender is. Dit op zijn beurt is weer afhankelijk van de doeleinden waarvoor politiegegevens mogen worden verwerkt. De Wpolg biedt waarborgen in het uitgangspunt van het doelbindings-, rechtmatigheids- en noodzakelijkheidscriterium.[110] Daarnaast voorziet het in een oplopende beperking van de toegankelijkheid voor politieambtenaren door middel van autorisaties naarmate de verwerkingen ingrijpender zijn voor betrokkenen.[111] Voorts kent de Wpolg een gedifferentieerd stelsel van (volgens het CBP te lange) bewaartermijnen dat is gerelateerd aan de verwerkingsdoeleinden.[112] Voor bepaalde verwerkingen is een machtiging vereist, al dan niet in combinatie met een opdracht van het bevoegd gezag. Uiteraard kent de Wpolg eveneens bepalingen omtrent de juistheid, volledigheid en beveiliging van politiegegevens.[113] De verantwoordelijke moet 'passende technische en

---

[107] Hieronder vallen ook de gegevens over terrorisme, die worden verzameld in het kader van de zogenaamde themaverwerking op grond van Wpolg, artikel 10, eerste lid, onderdeel b. Bij AMvB kunnen categorieën van gegevens aangewezen worden die uitgezonderd zijn rechtstreekse verstrekking (Wpolg, MvT, 82).

[108] Wpolg, MvT, 80-82. Gezien de onderlinge verwevenheid van de verschillende bestanddelen van de wettelijke taak van de AIVD, geldt de mogelijkheid van het rechtstreeks zoeken in politiegegevens door de AIVD voor de gehele taak, bedoeld in artikel 6, tweede lid, van de Wiv 2002. De rechtstreekse gegevensvergelijking vanuit de AIVD vindt plaats op basis van *hit/no hit*. In geval van een *hit* met een door de AIVD ingebracht gegeven worden de gegevens die overeenkomen, alsmede de daarmee verband houdende gegevens, rechtstreeks vertrekt aan de AIVD. De verdere verwerking van deze aan de AIVD verstrekte gegevens wordt bestreken door de Wiv 2002, waarin in hoofdstuk 3 een afzonderlijk regime wordt gegeven voor de gegevensverwerking door de AIVD. De personen op wie de gegevensverwerking betrekking kan hebben, worden opgesomd in artikel 13 van de Wiv 2002. De Wiv 2002 wordt in het volgende hoofdstuk besproken.

[109] In het op 10 april 2003 aan de Tweede Kamer aangeboden rapport *Uitwisseling van opsporings- en terrorisme-informatie* van de Algemene Rekenkamer zijn tekortkomingen gesignaleerd ten aanzien van informatieverzameling en -uitwisseling op het gebied van terrorismebestrijding. Zo zou er geen geautomatiseerde afstemming van de gegevens van politie en AIVD plaatsvinden (TK 2002-2003, 28 845, nr. 1-2). Zie ook noot 85.

[110] Voor het doelbindings-, rechtmatigheids- en noodzakelijkheidscriterium, zie noot 94.

[111] Met betrekking tot de verwerking van politiegegevens is de verantwoordelijke verplicht een systeem van autorisaties te onderhouden dat voldoet aan de vereisten van zorgvuldigheid en evenredigheid (Wpolg, artikel 6, eerste lid). Politiegegevens worden slechts verwerkt door ambtenaren van politie die daartoe door de verantwoordelijke zijn geautoriseerd en voor zover de autorisatie strekt (Wpolg, artikel 6, tweede lid).

[112] Naar het oordeel van het CBP zijn de bewaartermijnen van verwijderde gegevens veel te lang, zie: CBP, *Advies conceptwetsvoorstel Wet politiegegevens*, 40. Ook Kielman en Koelewijn bekritiseren de significante uitbreiding van de bewaartermijnen, vooral met betrekking tot de zogenaamde 'zachte' informatie die onder de Wpolr nog in een 'voorlopig register' (voorportaalfunctie) werd opgenomen, zie: Kielman en Koelewijn, 'Minder registers, meer gegevens', 455-456.

[113] Voor deze bepalingen, zie noot 95.

organisatorische maatregelen' treffen om de politiegegevens te beveiligen tegen verlies of enige vorm van onrechtmatige verwerking. Deze maatregelen moeten een 'passend beveiligingsniveau' garanderen, gelet op de risico's die de verwerking en de aard van de gegevens met zich meebrengen (Wpolg, artikel 4, derde lid).

Rechten betrokkenen

De regeling over informatieverstrekking aan de betrokkene is in de Wpolg gezien de aard van de taken van de politie afwijkend van die van de Wbp. In de sfeer van de rechtsbescherming kent Wpolg de burger het recht toe om een schriftelijk verzoek tot kennisneming in te dienen aangaande de gegevens die de politie mogelijk over hem verwerkt en de mogelijkheid in rechte op te komen tegen een weigering (Wpolg, artikel 25)[114]. Een verzoek om kennisgeving kan eventueel worden gevolgd door een verzoek tot wijziging (Wpolg, artikel 28).

De vraag dringt zich natuurlijk op wat dit recht op kennisneming in de praktijk oplevert. Burgers weten vaak namelijk helemaal niet dat er gegevens over hen worden verzameld en verwerkt. Dit geldt in nog sterkere mate voor die groepen onverdachte burgers, waarover in het kader van de themaverwerkingen op grote schaal gegevens worden verwerkt.[115]

Controle en toezicht

Tenslotte zijn in de Wpolg waarborgen opgenomen voor controle en toezicht. Deze houden in dat de verantwoordelijke verplicht is een privacyfunctionaris aan te wijzen en periodiek *privacy-audits* te laten uitvoeren (Wpolg, artikelen 33 en 34). Het CBP is belast met het toezicht op de naleving van de wet (Wpolg, artikel 35). Om de beoogde controle en toezicht te kunnen effectueren, verplicht de Wpolg tot het schriftelijk vastleggen van bepaalde gegevensverwerkingen, onderzoeksdoelen en autorisatietoekenningen, de zogenaamde 'protocolplicht' (Wpolg, artikel 32). Over de effectiviteit van deze waarborgen wordt echter nogal verschillend gedacht.[116]

[114] Een verzoek om kennisgeving kan afgewezen worden voor zover het onthouden van kennisneming noodzakelijk is in het belang van de goede uitvoering van de politietaak, gewichtige belangen van anderen of de veiligheid van de staat (Wpolg, artikel 27).

[115] A. Vedder, L. v.d. Wees en B.-J. Koops, 'Big Brother's bevoegdheden zijn er - nu hij zelf nog?' *NJB*, 41 (17 november 2006) 2356-2360, aldaar 2360. Kielman en Koelewijn merken in dit verband op dat evaluatieonderzoeken hebben aangetoond dat van het kennisnemingsrecht weinig of geen gebruik wordt gemaakt en dat zelfs advocaten in veel gevallen niet op de hoogte zijn van deze rechten, Kielman en Koelewijn, 'Minder registers, meer gegevens', 456.

[116] Kielman en Koelewijn zetten vraagtekens bij de effectiviteit van deze waarborgen: de controlerende taak van de privacyfunctionaris zou conflicteren met zijn andere taken, het CBP zou tekort schieten in haar toezichthoudende taak en in de praktijk blijkt juist het protocolleren veel problemen op te leveren, zie: Kielman en Koelewijn, 'Minder registers, meer gegevens', 457.

5. VERZAMELING EN VERWERKING VAN GEGEVENS DOOR INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

In voorgaande hoofdstukken is de verzameling (of vordering) en verwerking van gegevens door opsporingsdiensten behandeld. Verzameling en (verdere) verwerking van gegevens binnen het opsporingsdomein wordt via aparte wetgeving gereguleerd (Wetboek van Strafvordering respectievelijk Wpolg/Wjsg). Binnen het domein van de inlichtingen- en veiligheidsdiensten wordt zowel de verkrijging als de (verdere) verwerking door één wet bestreken, te weten de Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002).

Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002)

De Wet op de inlichtingen- en veiligheidsdiensten 2002 (Wiv 2002)[117] vormt de wettelijke grondslag voor de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) - voorheen de Binnenlandse Veiligheidsdienst (BVD) respectievelijk de Militaire Inlichtingendienst (MID). De Wbp is niet van toepassing op de inlichtingen- en veiligheidsdiensten.

De Wiv 2002 omschrijft de taken van de AIVD/MIVD, de regels omtrent de verwerking van gegevens, de bijzondere bevoegdheden van de diensten, klachtenbehandeling en het recht op kennisneming van betrokkenen en het toezicht op de diensten.[118] Omdat het uitgangspunt bij de taakstelling en de bevoegdheden van de AIVD en de MIVD volgens de Wiv 2002 de gelijkwaardigheid van de beide diensten is, wordt in deze paper alleen over de AIVD gesproken.

Zorgplichten en kwaliteitseisen gegevensverwerking

De AIVD heeft zowel inlichtingentaken (het verrichten van onderzoek -inclusief verzamelen van gegevens) als veiligheidstaken (het bevorderen van beveiligingsmaatregelen)[119]; de ambtenaren van de AIVD hebben géén opsporingsbevoegdheden.

De verwerking van gegevens wordt tot het 'primaire bedrijfsproces' van de AIVD gerekend. De handelingen die tot de verwerking worden gerekend, zijn gelijk aan die

[117] Wet van 7 februari 2002, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 2002), Stb. 2002,148.

[118] Volgend op de in 2006 gerealiseerde uitbreiding van de mogelijkheden voor politie en justitie om gegevens te vorderen (beschreven in paragraaf 3.3.), is momenteel een wetsvoorstel in behandeling dat de opsporingsbevoegdheden van de AIVD aanzienlijk wil verruimen. Het voorstel beoogt de verstrekking van gegevens en zelfs hele bestanden door bestuursorganen en bedrijven in de financiële sector en de transportsector aan de AIVD *verplicht* te stellen, waar deze verstrekking in de huidige situatie (met uitzondering van de telecomsector) nog op vrijwillige basis plaatsvindt (Wiv, artikel 17). Daarnaast geeft het voorstel de AIVD meer armslag om geautomatiseerde data-analyses te maken die 'een ieder' kan betreffen. Omdat deze wet nog niet in werking is getreden, valt de bespreking ervan buiten het domein van deze paper. Zie voor de wijzigingswet Wiv: Wijziging van de Wiv 2002 i.v.m. de verbetering van de mogelijkheden van inlichtingen- en veiligheidsdiensten om onderzoek te doen naar en maatregelen te nemen tegen terroristische en andere gevaren met betrekking tot de nationale veiligheid alsmede andere wijzigingen, Voorstel van Wet, TK 2005-2006, 30 553, nr. 2 en Memorie van Toelichting, TK 2005-2006, 30 553, nr.3. Zie verder over deze wet: CBP, *Advies wetsvoorstel 30 533*, Brief aan voorzitter van de Tweede Kamer (20 december 2007); F. Kuitenbrouwer, 'AIVD mag stofzuigeren naar persoonsgegevens', *Netkwesties*, Digitaal magazine over maatschappij en internet (28 oktober 2008) en 'Onschuldige gegevens', *Computerrecht*, 97 (2006), 192.

[119] De AIVD heeft in het belang van de nationale veiligheid tot taak: a) het verrichten van onderzoek met betrekking tot organisaties en personen die aanleiding geven tot het ernstige vermoeden dat zij een gevaar vormen voor het voortbestaan van de democratische rechtsorde, dan wel voor de veiligheid of voor andere gewichtige belangen van de staat; b) het verrichten van veiligheidsonderzoeken; c) het vorderen van maatregelen ter bescherming van de onder a) genoemde belangen; d) het verrichten van onderzoek betreffende andere landen (Wiv, artikel 6, tweede lid).

van de Wbp, met dit verschil dat de gegevensverwerking niet beperkt is tot de verwerking van alleen *persoons*gegevens, maar ook van andere gegevens. De gegevensverwerking dient aan een aantal algemene (kwaliteits)eisen te voldoen (Wiv, artikel 12 t/m 16). Zo dienen doelbindings- en noodzakelijkheidscriterium aanwezig te zijn, dient de verwerking 'op behoorlijke en zorgvuldige wijze' te geschieden en moeten de gegevens zijn voorzien van 'een aanduiding omtrent de mate van betrouwbaarheid dan wel een verwijzing naar het document of de bron waaraan ze zijn ontleend'. Verwerking van bijzondere persoonsgegeven vindt niet plaats, tenzij dit 'onvermijdelijk' is.[120] De hoofden van de diensten moeten zorg dragen voor de nodige (technische en organisatorische) voorzieningen ter bevordering van de juistheid, volledigheid en beveiliging van de gegevens en de aanwijzing van personen die bevoegd zijn tot de verwerking.

Gegevens die, gelet op het doel waarvoor zij worden verwerkt, hun betekenis hebben verloren, dienen te worden verwijderd. Indien blijkt dat gegevens onjuist zijn of ten onrechte worden verwerkt, worden deze verbeterd onderscheidenlijk verwijderd. Verwijderde gegevens worden vernietigd, tenzij wettelijke regels omtrent bewaring daaraan in de weg staan (Wiv, artikel 43).

Algemene bevoegdheid tot gegevensverzameling

De *algemene* bevoegdheid tot het verzamelen van gegevens is neergelegd in artikel 17, eerste lid van de Wiv, dat bepaalt dat de diensten voor het verzamelen van gegevens bevoegd zijn zich 'te wenden' tot a) bestuursorganen, ambtenaren en voorts een ieder die geacht wordt de benodigde gegevens te kunnen verstrekken en b) de verantwoordelijke[121] voor een gegevensverzameling. De 'verantwoordelijke' is degene die oordeelt over de 'noodzakelijkheid' van een verstrekking waartoe verzocht is en uiteindelijk (al dan niet) tot medewerking aan het *verzoek* besluit; gegevensverstrekking vindt (een enkele uitzondering daargelaten) dus plaats op *vrijwillige* basis.[122] Verzamelingen van persoonsgegevens bij derden worden in de regel voor een ander doel aangelegd, dan voor die waarvoor de AIVD gegevens verzamelt. Indien de verantwoordelijke - in weerwil van de ter zake geldende wettelijke voorschriften - tot medewerking aan het verzoek besluit, dan worden op grond van Wiv, artikel 17, derde lid, de desbetreffende wettelijke voorschriften betreffende de verstrekking buiten toepassing verklaard (zoals de meldplicht richting het CBP of de protocolplicht, d.w.z. de plicht om gedane verstrekkingen vast te leggen, die het mogelijk maakt dat personen via gebruikmaking van het inzagerecht op de hoogte kunnen komen van vestrekkingen).[123]

In enkele specifieke gevallen voorziet de Wiv 2002 dan wel een andere wettelijke regeling wél in een verplichting om aan een verzoek door de AIVD tot gegevensverstrekking te voldoen. Artikel 61 van de Wiv bepaalt dat leden van het Openbaar Ministerie mededeling doen aan de AIVD/MIVD van de te hunner kennis gekomen gegevens die zij voor de diensten van belang achten. Een vergelijkbare verplichting kent artikel 62 voor ambtenaren van de politie, de ambtenaren van de Rijksbelastingdienst bevoegd inzake de douane en de ambtenaar van de Koninklijke marechaussee.[124]

---

[120] De AIVD is echter wel gerechtigd om gegevens te verwerken omtrent een persoon wegens diens politieke gezindheid (Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 19..)[Wiv], Memorie van Toelichting, TK 1997-1998, 25 877, nr. 3, p. 20).

[121] Voor de omschrijving van 'verantwoordelijke' zie noot 11.

[122] Zie hiervoor hoofdstuk 2 over uitzonderingsartikel 43 van de Wbp.

[123] Wiv, MvT, 23. Vgl. noot 49.

[124] De korpschef van een politiekorps, de commandant van de Kmar en de directeur-generaal van de Rijksbelastingdienst verrichten werkzaamheden (die feitelijk worden uitgevoerd door hiertoe aan te wijzen ambtenaren) ten behoeve van de AIVD, onder verantwoordelijkheid van de Minister van BZK en overeenkomstig de aanwijzingen van het hoofd van de AIVD (Wiv, artikel 60). (In een nieuw wetsvoorstel over de uitbreiding van de bevoegdheden van inlichtingen- en veiligheidsdiensten – zie noot 118 - wordt voorgesteld om ook de hoofddirecteur van de IND van het ministerie van Justitie onder de werking van

Naast deze in de Wiv geregelde informatieverplichting, is ook in hoofdstuk 13 van de Telecommunicatiewet een verplichting opgenomen voor aanbieders van openbare telecommunicatiediensten en/of netwerken om gegevens te verstrekken aan de AIVD.[125] Voorts heeft de AIVD op grond van de Wgba recht op gegevensverstrekking uit de Gemeentelijke Basisadministratie Persoonsgegevens.

Bijzondere bevoegdheid tot gegevensverzameling

Naast de algemene bevoegdheden, beschikt de AIVD ook over zogenaamde bijzondere (of geheime) bevoegdheden (of inlichtingenmiddelen) om gegevens en informatie te verkrijgen. Deze bevoegdheden, waaronder het aftappen van telecommunicatie en het vorderen van verkeers- en abonneegegevens, mogen alleen worden ingezet wanneer dat 'strikt noodzakelijk' is voor de taakuitvoering en die evenredig dienen te zijn aan het beoogde doel.[126] Bijzondere bevoegdheden die diep ingrijpen in de privacy van burgers mogen pas worden uitgeoefend na toestemming van de Minister van BZK. Al naar gelang de aard (en de impact op de privacy) van de verschillende soorten bevoegdheden gelden er specifieke toestemmingsvereisten; de verleende toestemming wordt verleend voor een (te verlengen) periode van drie maanden.

Onderscheppen en analyseren van telecommunicatie

De bijzondere bevoegdheden tot het onderscheppen en analyseren van telecommunicatie zijn vergaand. Zo is de AIVD bevoegd tot 'het gericht aftappen, ontvangen, opnemen en afluisteren van elke vorm van gesprek, telecommunicatie of gegevensoverdracht door middel van een geautomatiseerd werk' (Wiv, artikel 25). Deze bepaling maakt zowel het aftappen van telefoonverkeer als van internetverkeer mogelijk.[127] Verder mag de AIVD ongericht 'niet-kabelgebonden telecommunicatie ontvangen en opnemen'[128] (het zogenaamde *'searchen'*, Wiv, artikel 26 en 27). Voorts is de AIVD bevoegd zich te wenden tot de aanbieders van *openbare* telecommunicatienetwerken en -diensten met het verzoek abonneegegevens en zogenaamde 'verkeersgegevens' te verstrekken ten aanzien van een bepaald nummer (dit kunnen telefoonnummers zijn, maar ook IP-adressen); deze aanbieders zijn verplicht deze vervolgens 'terstond' te verstrekken (Wiv, artikel 28 en 29).[129]

Wiv, artikel 60 te brengen). Een speciaal hiertoe aangewezen ondergeschikte ambtenaar zendt de gegevens als bedoeld in artikel 62 aan de AIVD. Inzake gegevensverstrekking door OM en politie aan de AIVD op de voet van artikel 61 onderscheidenlijk 62 van de Wiv 2002 heeft het CBP geen bevoegdheid; omdat dat een gegevensverwerking ten behoeve van de AIVD is, fungeert de CTIVD als toezichthouder. De rechtstreekse verstrekking van politiegegevens aan de AIVD is vastgelegd in Wpolg, artikel 24, zoals in het vorige hoofdstuk is vermeld.

[125] Zie ook paragraaf 3.2. en noot 129.

[126] De in de Wiv neergelegde bijzondere bevoegdheden zijn het observeren en volgen van personen, de inzet van agenten, het doorzoeken van besloten plaatsen, het openen van brieven en het kennisnemen van e-mail, het binnendringen in een geautomatiseerd netwerk (computervredebreuk), het aftappen van telecommunicatie en het vorderen van verkeers- en abonneegegevens.

[127] Onder 'telecommunicatie' wordt in artikel 1.1. onder c van de Telecommunicatiewet immers verstaan 'iedere overdracht, uitzending of ontvangst van signalen van welke aard ook door middel van kabels, radiogolven, optische middelen of andere elektromagnetische middelen', zie: A.H. Ekker, 'Het onderscheppen van telecommunicatie door de inlichtingen- en veiligheidsdiensten', *Computerrecht* 2 (2002), 77-83. Aftappen van telecommunicatie gebeurde overigens ook al door de BVD, maar dan op basis van een aantal *strafuitsluitingsgronden*.

[128] De ongericht ontvangen en opgenomen gegevens mogen één jaar bewaard blijven ten behoeve van een nadere selectie.

[129] De zogenaamde 'medewerkingsverplichting' van aanbieders van openbare telecommunicatienetwerken en -diensten richting AIVD/MIVD en opsporingsdiensten aangaande het aftappen en opnemen van telecommunicatie en het verstrekking van abonnee- en verkeersgegevens is vastgelegd in hoofdstuk 13, 'Bevoegd aftappen', van de Telecommunicatiewet. Hierin is ook bepaald dat aanbieders hun netwerken en diensten uitsluitend aan gebruikers beschikbaar mogen stellen indien deze aftapbaar zijn, zie hiervoor ook noot 37. Met betrekking tot de verwerking van *verkeersgegevens* door telecommunicatie-aanbieders zijn in

Verstrekking van gegevens

De Wiv 2002 kent een gesloten verstrekkingstelsel. Bij de gegevensverstrekking gaat het bij de AIVD om externe verstrekking; het verrichten van onderzoek door de AIVD heeft in de kern tot doel de verantwoordelijke instanties tijdig te kunnen waarschuwen voor mogelijke bedreigingen. Aan deze instanties (onder andere die belast met de opsporing en vervolging van strafbare feiten) kunnen 'mededelingen' worden gedaan omtrent verwerkte gegevens.[130]

Rechtsbescherming belanghebbenden en toezicht

Rechten van belanghebbenden zijn in de Wiv slechts beperkt aanwezig. Een ieder heeft recht op kennisneming of en, zo ja, welke hem betreffende persoonsgegevens zijn verwerkt. Een dergelijke aanvraag kan echter op een groot aantal gronden geweigerd worden. Verder bevat de Wiv de verplichting om een persoon te informeren (notificeren) over het feit dat jegens hem een bepaalde bevoegdheid is gebruikt die inbreuk maakt op in artikel 12 (Huisrecht) en 13 (Brief- en telefoongeheim) van de Grondwet neergelegde grondrechten. Vijf jaar na beëindiging van de uitoefening van de bijzondere bevoegdheid wordt onderzocht of notificatie mogelijk is.

Toezicht (achteraf) op de inlichtingen- en veiligheidsdiensten vindt plaats door een Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten (CTIVD), bestaande uit drie leden die op voordracht van de Tweede Kamer worden benoemd.

---

de Tw, artikel 11.5 regels opgenomen. Hoofdregel is dat verkeersregels bij beëindiging van de oproep moeten worden verwijderd of geanonimiseerd. Verwerking is daarna slechts nog mogelijk voor bepaalde doelen, zoals bijvoorbeeld het opstellen van een nota voor een abonnee; zie: Ekker, 'Het onderscheppen van telecommunicatie', 77-83. De verkeersgegevens die de AIVD mag vorderen zijn vastgelegd in het Besluit ex artikel 28 Wiv 2002 van 19 mei 2005 en omvatten onder meer NAW- en nummergegevens van de verzender en de ontvanger van de communicatie en locatie, duur en tijdstip van het telecommunicatieverkeer (waaronder -mobiele- telefonie en internetverkeer. Het begrip verkeersgegevens omvat dus tevens gebruikersgegevens en is hiermee ruimer dan het begrip zoals dat in de Tw wordt gehanteerd; zie hiervoor ook noot 38 en 43.

[130] In relatie tot een mededeling omtrent een strafbaar feit aan het Openbaar Ministerie, moet op een daartoe strekkend verzoek van het Openbaar Ministerie inzage gegeven worden in alle aan de mededeling ten grondslag liggende gegevens die voor de beoordeling van de juistheid van de mededeling noodzakelijk zijn (Wiv, artikel 38, derde lid).

6. SYSTEMATIEK VAN VORDERING EN UITWISSELING VAN GEGEVENS

Voor de wijze waarop gegevens door opsporings- en veiligheidsdiensten worden verkregen en onderling worden uitgewisseld bestaat geen eenduidige systematiek. Zoals het onlangs gepubliceerde rapport *Data voor daadkracht* hierover vaststelde, is er eerder sprake van een veelheid aan benaderingen, waarbij elke organisatie zijn eigen systematiek en werkwijze kent. Alvorens de bevindingen van dit rapport te bespreken, besteedt dit hoofdstuk aandacht aan twee vormen van verzameling en uitwisseling van gegevens. De eerste betreft een intermediaire dienst die zorg draagt voor de uitvoering van de vordering en verstrekking van telecommunicatiegegevens, verplicht gesteld in het in paragraaf 3.2. behandelde Wet vorderen gegevens telecommunicatie. De tweede vorm behelst een samenwerkingsverband van opsporings- en veiligheidsdiensten om op een centraal punt terrorisme-gerelateerde informatie en gegevens bij elkaar te brengen en te analyseren.

6.1. Uitvoering vordering en verstrekking gebruikersgegevens: CIOT

Door middel van het Centraal Informatiepunt Onderzoek Telecommunicatie (CIOT) worden langs geautomatiseerde weg gevorderde *gebruikers*gegevens van aanbieders van telecommunicatie- en internetdiensten verstrekt aan het OM, (bijzondere) opsporingsdiensten en de AIVD/MIVD. Het CIOT draagt als intermediaire *shared service* zorg voor de opslag en het gebruik van deze gegevens volgens wettelijke kaders.[131]

Werkwijze CIOT

Het CIOT beheert hiertoe een geautomatiseerd informatiesysteem, waarin het vraag- en antwoordverkeer wordt afgehandeld. Aanbieders moeten elk etmaal een actueel digitaal bestand met wettelijk vastgestelde gebruikersgegevens leveren, dat in een aparte, beveiligde omgeving (een zogenaamde *black box*) wordt bewaard dat niet door andere aanbieders kan worden benaderd en dat alleen wordt gebruikt voor rechtmatige verstrekkingen aan bevoegde autoriteiten. De vorderende autoriteiten hebben, hiertoe geautoriseerd door de Minister van Justitie, via een speciale toegangscode continu rechtstreeks toegang tot het informatiesysteem via een eigen *client*. Ingevoerde vorderingen worden door deze *client* naar de CIOT-server doorgestuurd, die de vordering anoniem maakt. Vervolgens gaat de vordering naar alle *black boxen* voor een matching. Het antwoord gaat via de server weer terug naar de *client*. Ten behoeve van de beveiliging wordt onder andere gebruik gemaakt van een gesloten netwerk en versleuteling door *Public Key Infrastructuur* (PKI). De gegevens dienen zodanig te worden verstrekt dat ongeautoriseerde toegang tot het bestand niet mogelijk is en dat de integriteit en onaantastbaarheid van het bestand verzekerd is.[132]

[131] Het CIOT (onderdeel van het Ministerie van Justitie) voert hiermee het Besluit verstrekking gegevens telecommunicatie uit (Besluit van 26 januari 2000, houdende regels voor de verstrekking van gegevens door aanbieders van openbare telecommunicatienetwerken en -diensten met het oog op het onderzoek van telecommunicatie - Besluit verstrekking gegevens telecommunicatie, Stb. 2000, 71 en Besluit van 13 september 2006, houdende wijziging van het Besluit verstrekking gegevens telecommunicatie en het Besluit vergunningen mobiele telefonie, Stb. 2006, 426). Op het CIOT is het regime van de Wbp van toepassing. Het CIOT-systeem regelt alleen de vordering en verstrekking van *gebruikers*gegevens. Met betrekking tot de vordering van andere categorieën gegevens (waaronder verkeersgegevens) stelt dat Nota van Toelichting bij het Besluit vorderen gegevens telecommunicatie, Stb. 2004, 394, p. 5, dat reeds is voorzien in toereikende procedures, afspraken en modellen, waardoor vooralsnog van het stellen van nadere regels op dit punt wordt afgezien.

[132] Besluit en Wijzigingsbesluit verstrekking gegevens telecommunicatie: Besluiten en Nota's van Toelichting.

Technische voorzieningen en procesinformatie

Het CIOT, de vorderende autoriteit en de aanbieders van gegevensbestanden dienen ieder de technische voorzieningen te treffen die nodig zijn teneinde het geautomatiseerde vraag-antwoord-verkeer uit te kunnen voeren. Deze voorzieningen voldoen aan de voorwaarden en specificaties die in de wet zijn vastgelegd.[133]

Het CIOT slaat procesinformatie op, waarmee het rechtmatige gebruik van het systeem kan worden getoetst. Dit is informatie waaruit blijkt door welke aanbieder, aan welke autoriteit en op welke grondslag informatie is verstrekt. De vastlegging van deze procesinformatie (die drie jaar wordt bewaard) is verplicht ten behoeve van jaarlijkse *audits* (naar functioneren, gebruik en beveiliging van het systeem) en de rapportages aan de Minister van Justitie.[134]

6.2. CT-Infobox

Een jaar na de oprichting in 2004 is in maart 2005 de zogenaamde Contraterrorisme-Infobox (CT-Infobox) officieel van start gegaan. Deze CT-Infobox is een bijzonder samenwerkingsverband - 'op voet van gelijkwaardigheid onder erkenning van ieders bevoegdheden en verantwoordelijkheden'- van AIVD, MIVD, KLPD, FIU-NL, OM, IND en FIOD/ECD.[135] De Infobox ressorteert onder de AIVD en is daardoor onderworpen aan het regime van de Wiv 2002 met als toezichthouder de CTIVD. Verantwoording van de werkzaamheden vindt plaats door rapportages aan de ministers van Justitie en BZK. Periodiek overleg vindt plaats in een coördinerend beraad, waarin naar de deelnemende diensten ook de NCTb vertegenwoordigd is. [136]

Doel en werkwijze

Doel van de CT-Infobox is het leveren van een bijdrage aan de terrorismebestrijding door het op een centraal punt bij elkaar brengen en vergelijken van informatie over netwerken en personen die op de een of andere wijze betrokken zijn bij terrorisme en daaraan te relateren radicalisering. De Infobox beoogt via raadpleging, vergelijking en analyse van de gegevens die door de deelnemers worden ingebracht een snelle, multidisciplinaire analyse en beoordeling van de beschikbare informatie mogelijk te maken, aan de hand waarvan de desbetreffende partners maatregelen kunnen nemen. De CT-Infobox verstrekt in deze gevallen niet zelf informatie naar buiten toe, maar *adviseert* de deelnemende diensten om hiertoe onderling rechtstreeks relevante informatie uit te wisselen binnen het voor ieder van hen geldende wettelijke verstrekkingsregime. Door deelnemers aan het samenwerkingsverband vindt derhalve geen gegevensuitwisseling *via* de CT Infobox plaats.[137]

In het Convenant inzake de samenwerking in de CT-Infobox is bepaald dat de samenwerkende diensten ervoor zorg dragen dat de CT-Infobox toegang krijgt tot alle relevante gegevensbestanden waarover zij beschikken, hetzij door rechtstreekse, *real time* geautomatiseerde raadpleging mogelijk te maken, hetzij op een andere geschikte

[133] Deze voorwaarden en specificaties zijn vastgelegd in de Bijlage bij het Besluit verstrekking gegevens telecommunicatie en onderdeel I van het Wijzigingsbesluit.
[134] Wijzigingsbesluit verstrekking gegevens telecommunicatie, Nota van Toelichting, 13.
[135] De CT-Infobox is in 2004 oorspronkelijk van start gegaan met drie deelnemers, AIVD, KLPD en OM. Begin 2005 werd de Infobox uitgebreid met de MIVD en de IND. In 2006 kwamen de FIOD-DCD en FIU-NL erbij en in 2008 schoof de Kmar aan.
[136] Brief Minister BZK aan de Tweede Kamer over de CT-Infobox (18 maart 2005), TK 2004-2005, 29 754 en 27 925, nr. 21, p. 2.
[137] Ibidem.

wijze.[138] De aan de CT-Infobox verstrekte gegevens worden door de AIVD in een door de AIVD voor de CT-Infobox beschikbaar gesteld informatiesysteem opgenomen, waarbij de herkomst van de desbetreffende gegevens wordt vermeld en de in de Wiv 2002 vastgelegde kwaliteitseisen gelden.[139] Omdat de CT-Infobox onder de AIVD ressorteert, geldt dat al hetgeen in (of ten behoeve van) de Infobox plaatsvindt, dus ook de (verdere) gegevensverwerking, volledig door de Wiv 2002 wordt bestreken. Gegevensverstrekkingen aan de CT-Infobox zijn aan te merken als gegevensverstrekkingen aan de AIVD. In de CT-Infobox ondergebrachte en daarmee aan de AIVD verstrekte gegevens zijn daarmee AIVD-gegevens geworden, waarvan door de aan de CT-Infobox verbonden medewerkers van de deelnemende diensten ten behoeve van de aan hen opgedragen taak kennis genomen kan worden en niet voor andere doelen mag worden gebruikt. Het gaat in dit laatste geval om een *interne* verstrekking van gegevens; dit zelfde geldt voor gegevens die reeds bij de AIVD berusten en voor werkzaamheden in de CT-Infobox beschikbaar komen.[140]

In het Convenant inzake de samenwerking in de CT-Infobox is onder meer een bepaling opgenomen over de aanwijzing van medewerkers van de deelnemende diensten die werkzaamheden in en ten behoeve van de CT-Infobox verrichten. Daar CT-Infobox-werkzaamheden aan te merken zijn als AIVD-werkzaamheden, worden de aan de CT-Infobox verstrekte gegevens door de daarin werkzame medewerkers, die daarin zijn geplaatst vanuit de deelnemende diensten, verwerkt in de hoedanigheid van medewerker van de AIVD.[141]

Toezichtsrapport CTIVD

In 2007 heeft de CTIVD een eerste toezichtsrapport over de CT-Infobox gepubliceerd. De gevreesde ongebreidelde uitwisseling van informatie tussen de deelnemende partijen heeft zich volgens de toezichthouder niet voorgedaan. Volgens de Commissie beantwoordt de gegevensverwerking in de CT-Infobox aan de daarvoor in de Wiv 2002 gestelde vereisten (behoudens de gegevensverwerking van personen die ten onrechte op de lijst staan). Door verwijzing naar de herkomst van gegevens wordt voorkomen dat met betrekking tot opsporing of inlichtingenwerk de verschillende gegevens door elkaar gaan lopen. Ook verder wordt voldaan aan de vereisten van behoorlijkheid en zorgvuldigheid bij de verwerking van persoonsgegevens.[142]

---

[138] In een brief aan de Tweede Kamer stelt de Minister van BZK dat vrijwel alle bestanden van de deelnemende partners inmiddels *real time* raadpleegbaar zijn binnen de CT-Infobox. De handmatige naslag binnen de Infobox wordt volgens verwachting in 2008 vervangen door een zoekschilsysteem, waarmee met één zoekslag geautomatiseerd gezocht kan worden in de relevante systemen, zie: Brief van de Minister van BZK aan de Tweede Kamer, Terrorismebestrijding/AIVD, TK 2007-2008, 29 754 en 30 977, nr. 126, p. 3. In het Toezichtsrapport van de CTIVD is aanbevolen voorrang te geven aan de ontwikkeling van een behoorlijk functionerend zoeksysteem, wat op de achtergrond dreigde te raken ten faveure van de ontwikkeling van nieuwe methodes van geautomatiseerde bestandsanalyse (*datamining*), waarmee aan de hand van vooraf vastgestelde zoekcriteria (profielen) bestanden kunnen worden doorzocht; zie: CTIVD, *Toezichtsrapport inzake het onderzoek van de Commissie van Toezicht naar de Contra Terrorisme Infobox,* CTIVD nr. 12 (10 april 2007) 12.

[139] Convenant inzake de samenwerking in de CT Infobox, dd. 11 maart 2005, Nr. 2325766/01. Bijlage bij de Brief van de Minister BZK aan de Tweede Kamer van 18 maart 2005, TK 2004-2005, 29 754 en 27 925, nr. 21. Voor de zorgplichten en kwaliteitseisen rond gegevensverwerking door de AIVD, zie het voorgaande hoofdstuk.

[140] Brief van de Minster van BZK aan de Tweede Kamer, Terrorismebestrijding, TK 2005-2006, 29 754, nr. 29, p. 2-4.

[141] Ibidem, 4-5. De medewerkers van het KLPD, de Kmar en de FIOD zijn in de CT-Infobox werkzaam in de hoedanigheid van 'artikel 60-ambtenaren' van de Wiv 2002 (binnen de politiekorpsen hebben de medewerkers van de Regionale Inlichtingendiensten - RID - deze art. 60-status, zoals bij de behandeling van de Wpolg is vermeld); zie hiervoor ook noot 124. Hetzelfde geldt voor de medewerkers van de IND, die in afwachting van een wettelijke regeling worden aangemerkt als ware zij artikel 60-ambtenaren. De positie van medewerkers van de MIVD is gerelateerd aan de wettelijke plicht tot samenwerking tussen de AIVD en de MIVD zoals neergelegd in artikel 58 van de Wiv 2002. Het OM heeft een enigszins afwijkende, bijzondere positie ten opzichte van de CT Infobox.

[142] CTIVD, *Toezichtsrapport Contra Terrorisme Infobox*, 27, 31.

Een kritiekpunt is dat de AIVD in de beginfase te zeer een leidende positie ingenomen heeft, wat ten koste is gegaan van een zo goed mogelijke samenwerking tussen de AIVD en de andere organisaties binnen de CT-Infobox.[143] Daarnaast verdient de positie van de NCTb (geen onderdeel van de Infobox, maar wel lid van het coördinerend beraad) meer duidelijkheid.[144]

Ondanks dat de gegevensverwerking beantwoordt aan de Wiv-vereisten, blijken volgens het toezichtrapport de criteria voor opname in de Infobox niet altijd te worden nageleefd en wordt de meerwaarde van het opnemen meestal niet beargumenteerd.[145] Hierdoor zit in de Infobox uiteindelijk een mix van gegevens van verschillende diensten over bepaalde (groepen) personen. Bovendien bevat de Infobox personen die er niet in thuis horen en van de lijst verwijderd dienen te worden. Niet altijd wordt de motivering van opname van (vooral groepen) personen opgegeven en bij aanmelding van groepen personen wordt niet altijd de rol van een bepaalde persoon in een groep beschreven; dit is echter een belangrijk gegeven om te kunnen beoordelen welke personen van de lijst van de Infobox verwijderd kunnen (of zelfs moeten) worden.[146]

In een reactie op het CTIVD-rapport heeft de Minister van BZK te kennen gegeven dat de vereisten voor opname in de CT-Infobox inmiddels stringent worden nageleefd. De Infobox is bovendien opgeschoond en de personen die niet (meer) aan de criteria van de box voldoen zijn daaruit verwijderd. Het bestand wordt volgens de minister thans nauwgezet up to date gehouden.[147]

6.3. *Data voor daadkracht*

In het najaar van 2007 verschenen de resultaten van een onderzoek van de Adviescommissie Informatiestromen Veiligheid naar de systematiek van informatiestromen vanuit geautomatiseerde gegevensbestanden in de publieke en private sector ten behoeve van het veiligheidsdomein.[148] De hoofdconclusie van het onderzoek was dat het totaal aan verschillende systemen om gegevens uit externe gegevensbestanden in te winnen niet voldoen aan de criteria inzake de grondslag, vormvereisten, maatschappelijke zorgvuldigheid, effectiviteit en doelmatigheid. Bovendien zou de overheid te weinig aandacht schenken aan het risico van het ontstaan van een onbalans tussen privacy en veiligheid.

Data, informatie en intelligence[149]

Centraal in het rapport staan gegevensbestanden. Op zichzelf hebben gegevens in bestanden geen waarde voor de veiligheid; pas de combinatie van gegevens (*data*) en de interpretatie daarvan geven waarde: data worden dan *informatie*. Vervolgens leidt

[143] Ibidem, 1, 6, 22-23, 30.
[144] Ibidem, 1, 8-9, 30.
[145] Ibidem, 1, 9-10, 25. Aangezien de CT-Infobox onder het regime van de Wiv 2002 is geplaatst, zal bij aanmelding van personen voldaan moeten worden aan de wettelijke criteria die voor het verwerken van gegevens in de Wiv 2002 zijn opgenomen, d.i. het vereiste dat verwerking slechts mogelijk is waaneer een persoon *aanleiding* geeft tot het *ernstige vermoeden* dat hij of zij een gevaar vormt voor de democratische rechtsorde, dan wel voor de veiligheid of andere gewichtige belangen van de staat. Het CTIVD wijst in dit verband ook op de mogelijke invloed van de Wet verruiming mogelijkheden tot opsporing en vervolging van terroristische misdrijven (zie hoofdstuk 3.4. van deze paper) die het voor de politie immers mogelijk maakt reeds op basis van *aanwijzingen* van een terroristisch misdrijf onderzoekshandelingen te verrichten en hierdoor (eerder) personen aan te melden bij de CT-Infobox.
[146] Ibidem, 25, 31.
[147] Brief van de Minister van BZK aan de Tweede Kamer betreffende het Toezichtsrapport CTIVD inzake CT-Infobox, 10 april 2007.
[148] *Data voor daadkracht. Gegevensbestanden voor veiligheid: observatie en analyse*. Rapport van de Adviescommissie Informatiestromen Veiligheid (30 augustus 2007). Conclusies in managementsamenvatting pagina 8-12.
[149] Deze paragraaf is gebaseerd op hoofdstuk 1 van *Data voor daadkracht*, 14-35.

deze informatie via analyse en onderzoek tot *intelligence*[150], de basis voor besluitvorming over te nemen acties.

De laatste jaren is door de explosieve groei van het aantal geautomatiseerde gegevensbestanden, door de lessen van enkele terroristische aanslagen en door de opkomst van het concept van het informatiegestuurde politiewerk[151] het belang van informatie in het veiligheidsdomein (waaronder vooral de terrorismebestrijding) enorm toegenomen. Voor zowel eigenaren van gegevensbestanden als voor opsporings- en veiligheidsdiensten is het dan ook van het grootste belang dat deze bestanden correct beheerd worden en steeds actueel zijn; een goede *intelligence* is immers alleen mogelijk als de te analyseren onderliggende gegevens correct en eenduidig (en beschikbaar) zijn. Bestuurlijk en politiek is volgens het rapport weliswaar regelmatig aandacht voor verschillende onderdelen van het proces van intelligence, maar wordt nauwelijks aandacht besteed aan het onderdeel van de verzameling van de data en de kwaliteit daarvan. Om de steeds vaker voorkomende criminaliteit met en misbruik van geautomatiseerde gegevensbestanden (zoals het toenemende probleem van de identiteitsfraude) in te dammen, zou ook meer aandacht besteed moeten worden aan de veiligheid en beveiliging van gegevensbestanden.

Systematiek van gegevensverzameling en -uitwisseling[152]

In haar onderzoek naar de systematiek van de gegevensverzameling en -uitwisseling constateert de Adviescommissie dat er weliswaar een woud aan generieke en sectorale wet- en regelgeving bestaat met betrekking tot het verzamelen van gegevens uit externe databanken (de belangrijkste zijn in de voorgaande hoofdstukken behandeld), maar dat een verhelderend totaaloverzicht ontbreekt.

Ditzelfde geldt voor de wijze waarop gegevens worden verkregen; ook voor dit aspect bestaat geen eenduidige systematiek, maar is eerder sprake van een veelheid aan benaderingen, waarbij elke organisatie zijn eigen systematiek en werkwijze kent.[153]

Ook signaleert de Adviescommissie dat er onvoldoende inzicht is in het aantal bevragingen aan externe databases[154], waardoor maatschappelijke verantwoording over dit proces niet mogelijk is. Daarnaast roept de toepassing van *datamining*technieken de nodige vragen op. Niet iedereen is volgens het rapport overtuigd van de waarde ervan en er zijn zorgen over de mate waarin *datamining* de privacy van burgers aan kan tasten.[155]

---

[150] Het rapport presenteert een *cyclische* benadering van het *proces* (dus geen keten met een begin en een eind) '*intelligence'* : 1. behoeftestelling en planning (welke informatie is nodig en hoe deze te verkrijgen?); 2. verzamelen data; 3. bewerking data tot informatie; 3. analyseren informatie, leidend tot intelligence; 4. verspreiding intelligence en voorlegging aan leiding die beslist over vervolg; 5. evaluatie leidend tot eventuele aanpassing behoeftestelling of verbetering proces. Zie: *Data voor daadkracht*, 24-25. Het rapport signaleert overigens in dit verband dat intelligence vooralsnog het domein van de inlichtingen- en veiligheidsdiensten is en dat deze analyse van de informatie bij de politie nog onvoldoende aandacht krijgt.

[151] Zie voor het concept van het informatiegestuurde politiewerk noot 86.

[152] Deze paragraaf is gebaseerd op hoofdstuk 2 van *Data voor daadkracht*, 36-61.

[153] In een aantal gevallen gebeurt de bevraging via een rechtstreekse verbinding van de bevragende partij met het geautomatiseerde gegevensbestand van de verstrekker. Ook komt het voor (bij bijvoorbeeld de politie) dat externe gegevensbestanden worden gekopieerd en vervolgens in eigen huis worden onderzocht en gekoppeld. De AIVD krijgt in het algemeen de beschikking over externe databanken door deze (in kopie) volledig naar 'binnen te halen' (over te hevelen). Zie: *Data voor daadkracht*, 46-47.

[154] Bij de politie wordt dit niet centraal bijgehouden en de AIVD doet om redenen van staatsveiligheid geen mededelingen over het aantal bevragingen.

[155] Het rapport noemt expliciet de zorgen die door het CBP zijn geuit over de toepassing van *datamining* (zie paragraaf 3.4.) en refereert aan een proefschrift van dr. R. Sietsma, waaruit is gebleken dat de Nederlandse wetgeving niet is toegesneden op *datamining*, zowel vanuit het oogpunt van privacy als vanuit het oogpunt van toepassing bij de opsporing. Ook de onderzoeksdienst van het Amerikaanse Congres signaleert zwaarwegende knelpunten rond *datamining*, waaronder de borging van de kwaliteit van de gegevens, problemen met de koppeling van verschillende bestanden, gebruik van gegevens voor een ander doel dan waarvoor zij zijn aangeleverd ('mission creep') en mogelijke inbreuken op de privacy. Enkele Amerikaanse onderzoekers hebben zelfs gesteld dat *datamining* bij de bestrijding van terrorisme

Met betrekking tot de uitwisseling van gegevens binnen de politie en tussen de politie en inlichtingen- en veiligheidsdiensten constateert de Adviescommissie dat deze uitwisseling moeizaam verloopt en ondanks goede bedoelingen 'de praktijk vaak weerbarstiger blijkt te zijn dan gedacht'.[156] Wordt de situatie in het veiligheidsdomein vergeleken met andere maatschappelijke sectoren, dan valt op dat elders samenwerkingsvormen zijn ontstaan, waarbij vanuit een erkenning van eenieders verantwoordelijkheid, door middel van verwijsfuncties gegevens voor andere partners in de keten beschikbaar worden gesteld.

Knelpunten bij gegevensverzameling en -uitwisseling[157]

Een knelpunt aan de vraagkant van het systeem van inwinnen van gegevens is volgens het rapport de versnippering en verkokering van de informatiehuishouding in het veiligheidsdomein. Dit manifesteert zich in het ontbreken van een gemeenschappelijke *strategische* visie op het belang van externe gegevensbanken voor de ontwikkeling van informatie en intelligence en in het onvoldoende (operationeel) met elkaar samenwerken bij het inwinnen, delen en analyseren van gegevens en bij het zoeken naar toepassingsmogelijkheden van nieuwe (*datamining*)technieken.

Een belangrijk knelpunt in het proces van vragen en leveren van gegevens is het dreigende optreden van een onbalans tussen privacy en veiligheid. Waar vroeger inlichtingen- en opsporingsdiensten zich richtten op verdachte personen, richten zij zich nu op hele groepen van personen om vervolgens na te gaan of daar mogelijk verdachte personen onder zouden kunnen zitten. Burgers kunnen ineens ergens van verdacht worden, niet omdat zij iets hebben gedaan, maar omdat zij passen in een bepaald profiel. Tussen de waarden privacy en veiligheid ligt altijd een zekere mate van spanning, aldus de Adviescommissie, maar het is de taak van de overheid om te zorgen dat beide waarden met elkaar in evenwicht zijn.

Verder stelt het rapport vraagtekens bij nut en noodzaak van het fysiek binnenhalen (en vervolgens in eigen beheer koppelen en analyseren) van externe databases door met name de AIVD. Uiteindelijk zal deze praktijk volgens beveiligingsdeskundigen onoverkomelijke beheersproblemen met zich mee gaan brengen.[158]

---

slechts een beperkte rol kan spelen, omdat er *a-priori* onvoldoende patronen (waaronder gegevens over terroristen, hun plannen en hun methoden) zijn om deze techniek toe te passen: 'the statistical likelihood of false positives is so high that predictive data mining will inevitably waste resources and threaten civil liberties', zie: *Data voor daadkracht*, 50-51.

[156] Aangaande de gegevensuitwisseling binnen de politie refereert de Adviescommissie aan rapporten van de Inspectie Openbare Orde en Veiligheid (IOOV), waarin wordt gesteld dat rond de informatiehuishouding bij de politie de nadruk teveel ligt op de informatietechnologie en te weinig op de content. Hoewel de IOOV verbeteringen signaleert op het terrein van de informatiehuishouding bij de politie, blijkt 'de praktijk toch weerbarstiger te zijn dan gedacht' en zijn alle korpsen hier 'ieder te veel op hun eigen wijze mee bezig'. Inzake gegevensuitwisseling tussen politie en inlichtingendiensten wijst het rapport op de blijkens een IOOV-studie soms onwerkbare situatie als gevolg van de dubbele pet van de RID-ambtenaar en op de uit een CTIVD-onderzoek naar voren komende onduidelijkheden rond de positie en het functioneren van de CT-Infobox. Zie: *Data voor daadkracht*, 51-56.

[157] Deze paragraaf is gebaseerd op hoofdstuk 3. van *Data voor daadkracht*, 62-89.

[158] De AIVD haalt databases binnen om de authenticiteit en de geheimhouding van de gegevens(bevraging) te waarborgen. Bevragingen worden immers gelogd en gegevensbeheerders of medewerkers van een bedrijf kunnen hierdoor inzicht krijgen in het zoekproces of in het object van onderzoek. Bevraging op locatie heeft verder als nadeel dat de verbinding tussen de database en de AIVD niet afdoende beveiligd zou kunnen worden. Sommige beveiligingsdeskundigen wijzen erop dat het goed mogelijk is om via procedures en protocollen zoekprocessen in de databases bij de eigenaar zelf uit te voeren op een zodanige wijze dat dit kan worden afgeschermd voor derden of voor gebruikers binnen die organisatie. Andere deskundigen merken weer op dat dergelijke beveiligingsconstructies omzeild kunnen worden. Het zelfde geldt voor de beveiliging van het verzenden van informatie met gebruikmaking van bestaande technologieën. Omdat over beveiligingsconstructies door deskundigen verschillend wordt geoordeeld; verdient dit aspect volgens het rapport nader onderzoek. Zie: *Data voor daadkracht*, 84-85.

Tenslotte wijst het rapport op het feit dat het toezicht op het inwinnen van gegevens niet eenduidig is geregeld; instanties die gegevens vragen of vorderen vallen veelal onder verschillende toezichtregimes.

Conclusies en aanbevelingen[159]

Aangaande het 'totaal aan systematieken' van informatiestromen uit geautomatiseerde gegevensbestanden naar het veiligheidsdomein concludeert de Commissie dat niet voldaan wordt aan de criteria inzake de grondslag, vormvereisten, maatschappelijke zorgvuldigheid, effectiviteit en doelmatigheid. De overheid zou daarnaast te weinig aandacht schenken aan de dreigende verstoring van de balans tussen privacy en veiligheid

De Commissie beveelt tenslotte aan:
- een publieke discussie over de balans tussen privacy voor te bereiden;
- een overzicht van alle wet- en regelgeving te genereren inzake vragen/vorderen van gegevens uit externe databanken;
- de instelling van een onafhankelijk toezichthouder op het inwinnen van gegevens uit externe databanken te verkennen;
- strategische samenwerking binnen het veiligheidsdomein vorm te geven bij het inwinnen, gebruiken en delen van gegevens uit externe databanken;
- *shared services*-vormen in het veiligheidsdomein te onderzoeken, zoals de instelling van een centrale verwijsindex voor ketenpartners[160], de opzet van een betrouwbare, centrale *service provider*[161], de oprichting van zogenaamde *fusion centers* voor samenwerking en uitwisseling van gegevens[162] en van een expertisecentrum voor de ontwikkeling van nieuwe technologieën[163].

Reactie Minister van BZK op het rapport[164]

In een reactie op het rapport heeft de minister van BZK te kennen gegeven de hoofdconclusie níet integraal over te nemen. Volgens de minister is er reeds sprake van een samenhangend wetstelsel (Wiv, Wpolg, Sv) en van gedegen toezicht op de naleving daarvan (CBP, CTIVD). De beoordeling van proportionaliteit en subsidiariteit van informatie-uitwisseling is hiermee voldoende geborgd.[165]

De aanbeveling over het herijken van het evenwicht tussen veiligheid en privacy spreekt de minister wel aan; de ministers van BZK en Justitie zijn voornemens de visie op privacy en veiligheid opnieuw vast te stellen, inclusief de rol van de technologie en internationale aspecten.

De minister verwerpt de aanbeveling van de Adviescommissie voor een systematiek waarin de inwinning en uitwisseling van informatie wordt gecentraliseerd (sic!). Het

---

[159] Deze paragraaf is gebaseerd op hoofdstukken 4 en 5 van *Data voor daadkracht*, 90-113.
[160] Het rapport noemt in dit verband de instelling van een 'Intelligent Verwijsknooppunt' voor ketenpartners in het veiligheidsdomein. Een dergelijke verwijsindex bevat geen inhoudelijke informatie, maar gegevens over personen die in een of ander onderzoek zijn betrokken en gegevens over de dienst die belast is met dit onderzoek.
[161] Een dergelijke betrouwbare, centrale *service provider* moet zorg dragen voor het inwinnen en verspreiden van gegevens ten behoeve van de veiligheids- en opsporingsdiensten. Als voorbeeld hiervan fungeert het eerder besproken CIOT.
[162] Naar Amerikaans voorbeeld zijn *fusion centers* (regionale) samenwerkingsorganen, waarin op basis van onderling vertrouwen tussen de betrokken diensten afspraken zijn gemaakt en waarin pragmatisch wordt samengewerkt, zie: *Data voor daadkracht*, 32-33.
[163] In een expertisecentrum voor de ontwikkeling van nieuwe technologieën (waaronder *datamining*, *profiling* en patroonherkenning) kan volgens het rapport verdere professionalisering plaatsvinden van de wijze waarop gegevens worden ingewonnen en verwerkt.
[164] Brief van de minister van BZK aan de Tweede Kamer ter aanbieding rapport *Data voor daadkracht*, 30 augustus 2007 (www.minbzk.nl/108221/brief-aan-de-tweede).
[165] Zie hiervoor ook de opmerkingen over de EVRM, artikel 8-toets in *Bijlage II.*

bestaande stelsel is niet gecentraliseerd, maar gesegmenteerd. Hierbij is volgens de minister bewust gekozen voor een ketenbenadering, waarbij elk van de diensten, naar gelang van het proces waarin zij werkzaam zijn, onderscheiden taken, bevoegdheden en verantwoordelijkheden hebben en elk vanuit hun eigen verantwoordelijkheden informatie inwinnen en uitwisselen. De minister gaat hierbij echter voorbij aan het feit dat de door het rapport beoogde instelling van een 'Intelligent Verwijsknooppunt' als *shared service* nu juist betrekking heeft op de ketenbenadering in het veiligheidsdomein...[166]

[166] Overigens ziet iemand als Buruma wel voordelen in een hiërarchisch informatiesysteem boven een netwerksysteem. Een netwerksysteem (waarin databestanden van inlichtingen- en opsporingsdiensten met elkaar verknoopt zijn) is dan wel flexibel, maar ook oncontroleerbaar. Een hiërarchisch systeem geeft de mensen achter de knoppen weliswaar een enorme machtspositie, maar is daarentegen wel beter democratisch en rechterlijk te controleren. Zie: J. v. Buuren en W. v.d. Schans, 'Strijd om de databanken: de informatiehuishouding van de politie in Europa', *Privacy & informatie*, 6 (2003) 247-252, aldaar 252.

7. SPANNINGSVELD VEILIGHEID - PRIVACY

Bij de bespreking van de wetgeving met betrekking tot het verzamelen en (verder) verwerken van gegevens door opsporings- en veiligheidsdiensten is steeds weer het spanningsveld tussen veiligheid en privacy naar voren getreden. De vraag dringt zich hierbij op of het fragiele evenwicht tussen beide polen niet te veel verstoord dreigt te raken ten nadele van de informationele privacy. Na een beschouwing over de privacywaarborgen die de besproken wetgeving kent, besteedt dit hoofdstuk vervolgens aandacht aan de bedreigingen voor de informationele privacy.

7.1. Veiligheid versus privacy: de ene kant

Door degenen die de in deze paper besproken maatregelen en wetgeving noodzakelijk achten wordt niet ontkend dat deze een nadelige invloed (kunnen) hebben op de informationele privacy van de burger. Het inleveren van een stukje privacy zou echter nodig zijn om (de dreiging van) het terrorisme effectief te kunnen bestrijden. Daarbij voldoen volgens de regering de wettelijke regelingen aan de beginselen van noodzakelijkheid, proportionaliteit en subsidiariteit, zoals voorgeschreven in EVRM, artikel 8. Bovendien bevatten de regelingen allerlei voorwaarden en waarborgen, die een onevenredige inbreuk op de privacy moeten voorkomen.

Privacywaarborgen

Bij de voorwaarden en waarborgen ter voorkoming van een ongerechtvaardigde inbreuk op de informationele privacy geldt dat deze zwaarder zijn naarmate de dreigende inbreuk op de privacy groter is.

Deze waarborgen liggen onder meer in de sfeer van noodzakelijks-, rechtmatigheids- en doelbindingscriteria van gegevensverwerking, evenals in vereisten inzake kwaliteit (waaronder juistheid, volledigheid, vermelding herkomst en mate van betrouwbaarheid), beveiliging en (gedifferentieerde) bewaar-/vernietigingstermijnen van gegevens. Daarnaast zijn er strikte procedures en procesverbalen voorgeschreven voor bepaalde vorderingen en verwerkingen, is een stelsel van machtigingen, getrapte toegankelijkheid en autorisaties gedefinieerd en is het nemen van passende technische en organisatorische maatregelen verplicht gesteld ter voorkoming van diefstaf of onrechtmatige verzameling/vordering, uitwisseling en verwerking van gegevens.

Daarnaast zijn waarborgen gelegen in de rechten die personen hebben over wie gegevens zijn verwerkt. Zo bestaat er een notificatieverplichting jegens betrokkenen, hebben betrokken een recht op kennisneming, correctie en het indienen van een klacht. Wel dienen deze rechten afgezet te worden tegen het belang van het onderzoek en zijn ze in het geval van de Wiv 2002 slechts beperkt aanwezig.

Tenslotte zijn in de wet- en regelgeving waarborgen opgenomen middels diverse vormen van controle, *privacy-auditing*, protocolplicht, rapportageverplichting en toezicht. Deze hebben een extra gewicht daar de rechten van betrokkenen relatief minder reiken dan daar waar gegevensverwerking plaatsvindt onder het regime van de Wbp.

7.2. Veiligheid versus privacy: de andere kant

Door degenen die kritische kanttekeningen plaatsen bij de besproken wetgeving en maatregelen wordt niet de noodzakelijkheid van antiterreurwetgeving ontkend, noch wordt bestreden dat de afweging tussen privacybelangen en het belang van opsporing of veiligheid gepaard zou kunnen (of moeten) gaan met het inleveren van een stukje

privacy. Juist omdat het recht op privacy geen absolute waarde is en er altijd sprake is van een afweging tussen verschillende belangen, behoeven inbreuken op de privacy echter wel een zorgvuldige argumentatie.[167] Bij de noodzakelijkheid, proportionaliteit, subsidiariteit en effectiviteit van de besproken wetgeving worden door critici echter grote vraagtekens gezet. Ook zijn volgens hen de waarborgen voor een zorgvuldige omgang met gegevens niet of slecht uitgewerkt en worden ze, voorzover ze al bestaan, amper nageleefd.[168]

Trends in terreurbestrijding

Op grond van een studie naar de ontwikkeling in de bevoegdheden van politie, justitie en inlichtingen- en veiligheidsdiensten met betrekking tot terrorismebestrijding, signaleert een rapport van het Rathenau Instituut een aantal trends, die elk afzonderlijk, maar bovenal *cumulatief* en *in samenhang* een groot effect hebben op de privacy van burgers. Deze trends zijn onder meer:[169]

1. Het onderzoek breidt zich steeds vaker uit tot personen op wie zelf geen verdenking rust, in de omgeving van verdachten;
2. Het onderzoek is steeds vaker verkennend van karakter, waarbij op basis van risicoprofielen potentieel verdachte groepen worden gevolgd;
3. Wettelijke beperkingen op het gebruik van bepaalde opsporingsmethoden worden verlicht of weggenomen;
4. Opsporings- en veiligheidsdiensten krijgen, zowel juridisch als technologisch, steeds meer mogelijkheden om (zelfstandig) onderzoek te verrichten;
5. Opsporings- en veiligheidsdiensten kunnen in toenemende mate beschikken over persoonsgegevens afkomstig van 'derden', die voor andere doeleinden zijn verzameld; door vorderingsbevoegdheden zijn deze 'derden' verplicht tot medewerking.

De besproken wetgeving met betrekking tot het vorderen en verwerken van persoonsgegevens in het kader van de terrorismebestrijding brengt risico's met zich mee voor de privacy van burgers.

Verstoring vrijheid en individualiteit door Big Brother-gevoel

Door het in toenemende mate proactieve en verkennende karakter van onderzoeken, die bovendien steeds meer uitgebreid worden naar niet-verdachte, 'gewone' burgers kan een ieder steeds makkelijker object van onderzoek worden. Onderzoekssubjecten zullen vaak niet (kunnen) weten dat zij onderwerp van onderzoek zijn. Ogenschijnlijk irrelevante persoonsgegevens kunnen door verwerking op geaggregeerd niveau en groepsprofilering iemand ineens tot lid van een verdachte groep maken. Bij deze risicoprofilering lopen sommige maatschappelijke groepen grotere risico's dan andere. Deze wetenschap verkleint de mogelijkheden van mensen om ongestoord zichzelf te zijn en te doen waar ze zin in hebben, waardoor waarden als vrijheid en individualiteit in het geding komen.[170]

---

[167] In een rapport van het Rathenau Instituut staat beschreven dat in de hedendaagse literatuur brede overeenstemming bestaat over de status die aan privacy moet worden toegekend. De beschermwaardigheid hiervan is weliswaar van principiële aard, maar heeft geen absolute gelding. Er kunnen dus goede redenen bestaan die een inbreuk op de privacy rechtvaardigen. Reikwijdte en betekenis van het begrip privacy zijn contextueel bepaald: 'privacy is een knecht van vele meesters'. Zie: A. Vedder, e.a. *Van privacyparadijs tot controlestaat?* 62-63.
[168] Ibidem, 65.
[169] Ibidem, 36-37, 66.
[170] Ibidem, 68; Vedder, e.a., 'Big Brother's bevoegdheden zijn er - nu hij zelf nog?' 2359-2360.

Kwaliteit gegevens

Door de steeds toenemende omvang, de steeds gedifferentieerdere herkomst en de steeds langere bewaartermijnen van gegevensbestanden neemt de kans toe dat de juistheid en volledigheid van gegevens steeds moeilijker te waarborgen zijn en dat de kwaliteit van de gegevens hierdoor steeds meer te wensen over laat. Dit probleem wordt nog verergerd door het feit dat veel mensen niet weten dat ze in bestanden voorkomen en ze derhalve ook niet hun recht op inzage en correctie kunnen uitoefenen. Bovendien worden gegevens die in een bepaalde context en voor een bepaald doel zijn verzameld en verwerkt door (verplichte) verstrekking in een andere context geplaatst, waardoor ze ineens een heel andere -onbedoelde of foute- betekenis kunnen krijgen.[171]

Select before you collect

Deze vervuilde en/of uit hun oorspronkelijke context gerukte gegevens vormen echter wel de basis voor steeds verdere verwerking, waaronder de toepassing van allerlei, soms hevig bekritiseerde, onderzoekstechnieken als *datamining* en risicoprofilering. Behalve dat dit nadelig kan uitwerken voor de effectiveit van opsporings- en veiligheidsactiviteiten (*'false negatives'*), kan het ook erg vervelende (onbedoelde) gevolgen hebben voor de privacy van onderzoekssubjecten (*'false positives'*).

Daarnaast leidt het verzamelen van steeds meer gegevens ten behoeve van analyse alleen maar tot een steeds verder afnemende *'actionable intelligence*' in verhouding tot de '*noise*' en tot een steeds grotere hooiberg waarin de speld gevonden moet worden. Uit effectiviteits- én privacyoverwegingen gaan in dit kader dan ook stemmen op om af te stappen van het idee dat 'meer informatie beter is' (integendeel, wordt betoogd, vaak is minder informatie zelfs beter, mits het maar de *juiste* informatie betreft: *'erst in der Begrenzung zeigt sich der Meister*) en weer terug te keren naar het traditionele principe van *'select before you collect'.* [172]

De door de informatietechnologische ontwikkelingen mogelijk geworden omdraaiing van selecteren en verzamelen heeft, los van de vraag naar de effectiviteit en doelmatigheid ervan, ook tot gevolg dat daarmee in principe iedereen als potentiële verdachte wordt gezien, waarmee een fundamenteel aspect van de rechtstaat wordt geraakt.[173]

Misbruik van gegevens

Een gevaar bij grootschalige opslag en verwerking van gegevens is verder dat zelfs de meest stringente organisatorische en technische maatregelen niet zullen kunnnen voorkomen dat door slechte beveiliging persoonlijke gegevens op straat komen te liggen of (vrijwillig of onvrijwillig onder druk van criminele organisaties) misbruikt worden. Dit risico is groter naarmate de toegang laagdrempeliger is. Vooral digitale identiteitsroof- of fraude is een snel groeiende vorm van misdaad met ingrijpende gevolgen voor de slachtoffers.[174]

---

[171] Ibidem. Zie ook paragraaf 3.4. Dezelfde gegevens die een derde op grond van het Wbp-vrijstellingsbesluit na enkele maanden dient te vernietigen, kunnen na verplichte verstrekking nog vele jaren rond blijven zwerven binnen het opsporings- en veiligheidsdomein.

[172] B. Jacobs, 'Select before you collect', *Ars Aequi*, 54 (2005) 1006-1009; B. Custers, 'Privacy en risicoprofilering bij keteninformatisering' in: J.A.H.M. Grijpink (red.), *Geboeid door ketens. Samen werken aan keteninformatisering* (Voorburg 2007) 181-190, aldaar 186-189.

[173] Custers wijst in dit verband op de omkering van bewijslast bij het optreden van '*false negative's* en '*false positives'* en de hiermee samenhangende *privacy paradox*: het aantonen van onschuld als gevolg van een verkeerd uitgepakte inbreuk op de privacy kan alleen maar rechtgezet worden door nog meer privacy af te staan. Zie: Custers, 'Privacy en risicoprofilering', 187-188.

[174] Jacobs, 'Select before you collect', 1007-1008.

Function creep

De wetgeving met betrekking tot het vorderen en verwerken van gegevens brengt ook een risico van *function creep* met zich mee, het geleidelijk aan veranderen van doelstellingen waarvoor informatie wordt verzameld. Op dezelfde wijze als door de vorderingwetgeving nu gegevens van derden door opsporings- en veiligheidsdiensten kan worden gebruikt voor andere doeleinden dan waarvoor ze oorspronkelijk is verzameld, kan diezelfde informatie omdat ze 'toch al' bij de genoemde diensten aanwezig is, worden gebruikt voor nog weer andere doeleinden. Deze *function creep* heeft zowel betrekking op personen/onderzoeksubjecten als op de doelbinding: enerzijds worden verzamelde gegevens voor een bepaald doel ten behoeve van een ander doel (verplicht) verstrekt en verwerkt, terwijl anderzijds technologieën die aanvankelijk gericht zijn op bepaalde groepen gaandeweg worden toegepast op (bijna) iedereen (ook op onverdachte personen).[175]

Rechten betrokken wassen neus

Rechten van onderzoekssubjecten blijken in de praktijk vaak weinig op te leveren; in de Wiv 2002 zijn deze rechten sowieso erg beperkt. Van het kennisnemingsrecht wordt zelden gebruik gemaakt. Vaak weten burgers zelfs helemaal niet dat er gegevens over hen worden verzameld en verwerkt. Volgens het CBP leert de ervaring dat ook de vereisten van schriftelijkheid bij vordering, de verbaliseringsplicht en de notificatieplicht slechts papieren garanties zijn.[176]

Toezicht en controle

Inzake de waarborgen rond toezicht en controle heeft het CBP naar eigen zeggen onvoldoende middelen om dit toezicht effectief uit te voeren[177]. Bovendien signaleert het CBP dat de groei in het aantal en de omvang van afgeschermde verwerkingen door opsporings- en inlichtingendiensten niet vergezeld gaat van een evenredige toename van controle en toezicht op dergelijke verwerkingen.[178]

---

[175] Zie paragraaf 3.4. en Vedder, e.a., *Van privacyparadijs tot controlestaat?* 68 en ibidem, 'Big Brother's bevoegdheden', 2360. Er bestaan weliswaar allerlei regels voor het gebruik van politie-informatie, maar of daar in de informele kanalen strak de hand aan wordt gehouden is onduidelijk. In dit verband wordt uit bijvoorbeeld politiekringen keer op keer vernomen dat de officiële lijnen rond doelbinding en verwerking vaak omzeild worden. Uiteindelijk gaat het om de creativiteit en dan blijken er duizend en één mogelijkheden te zijn. In politiekringen noemde men dit vroeger altijd: "Tom Poes, verzin een list", zie: J. v. Buuren en W. v.d. Schans, 'Strijd om de databanken: de informatiehuishouding van de politie in Europa', 250-251.

[176] Zie paragraaf 3.3. en noot 115.

[177] Zie noot 78.

[178] CBP, *Advies conceptwetsvoorstel bijzondere bevoegdheden tot opsporing van terroristische misdrijven*, 12.

8. PRIVACYBESCHERMING EN ARCHIVERINGSSYSTEEM: KADERSTELLING

In de voorgaande hoofdstukken is de antiterrorismewetgeving met betrekking tot de gegevensverwerking (verzameling/vordering, verwerking en verstrekking) door of ten behoeve van opsporings- en veiligheidsdiensten als juridisch-maatschappelijke context geconstrueerd. Vervolgens is het hieruit voortvloeiende spanningsveld tussen veiligheid en privacy geschetst. Ook is de systematiek van vordering en uitwisseling van gegevens aan bod gekomen, waarbij gesignaleerd is dat hierbij geen sprake is van eenduidigheid, maar veeleer van een veelheid aan benaderingen, waarbij elke organisatie zijn eigen systematiek en werkwijze kent.

De komende hoofdstukken gaan in op de vraag hoe het archiveringssysteem van opsporings- en veiligheidsdiensten ervoor kan zorgen dat de informationele privacy van degenen op wie de gegevens betrekking hebben, worden beschermd. Zoals in de inleiding al is aangegeven, hanteert dit onderzoek hierbij een ideaaltypische benadering van een archiveringssysteem binnen (samenwerkingsverbanden van) diensten die onder de werking van de Wpolg en de Wiv 2002 vallen. Kant-en-klare praktische oplossingen worden dan ook niet aangedragen; het accent ligt op het signaleren van aandachtspunten en nieuwe dimensies waar een archiveringssysteem mee geconfronteerd wordt of kan worden in zijn reactie of aanpassing op de gewijzigde juridisch-maatschappelijke context.

Archivistische vertaling privacywaarborgen

De opsporings- en veiligheidsdiensten vallend onder de Wpolg en de Wiv 2002 zijn overheidsorganen en vallen derhalve onder de werking van de Archiefwet 1995; bijgevolg zijn deze organen verplicht de onder hen berustende archiefbescheiden in goede, geordende en toegankelijke staat te brengen en te bewaren, alsmede zorg te dragen voor de vernietiging van daarvoor in aanmerking komende archiefbescheiden.

Daarnaast zijn vanuit de wettelijke en regelgevende verplichtingen zoals geformuleerd in de behandelde wetgeving inzake vordering en verwerking van persoonsgegevens, specifieke eisen te identificeren ten aanzien van het maken, ontvangen en beheren van archiefbescheiden en aangaande de inrichting van het archiveringssysteem. Hiertoe dienen de privacywaarborgen vertaald te worden naar eisen ten aanzien van de kwaliteit van de archiefbescheiden (de gegevens) en hiermee naar eisen ten aanzien van de inrichting (of aanpassing) van het archiveringssysteem. Deze privacy-gerelateerde eisen komen niet in de plaats van de eisen voortvloeiend uit de verplichting de gegevens in goede, geordende en toegankelijke staat te brengen en te bewaren, maar betreffen een specifieke invulling hiervan.

Als normeringskaders voor de invulling van deze eisen fungeren *NEN-ISO 15489: Informatie- en Archiefmanagement, ISO 23081: Metadata for Records, NEN 2082: Eisen voor functionaliteit van informatie- en archiefmanagement in programmatuur,* de door Horsman geformuleerde (in eisen aan archiveringssystemen te vertalen) kwaliteitsattributen van archiefdocumenten en de Nederlandse Overheid Referentie Architectuur (NORA).[179]

De archivistisch te vertalen privacywaarborgen betreffen onder meer de noodzakelijkheids-, rechtmatigheids-, zorgvuldigheids- en doelbindingscriteria van gegevensverwerking, de kwaliteit van de gegevens (juistheid, volledigheid, nauwkeurigheid, beveiliging), de bewaartermijnen van gegevens en de te nemen

[179] *NEN-ISO 15489-1 (nl) Informatie- en archiefmanagement. Deel 1: Algemeen* (november 2001); *NEN-ISO/TR 15489-2 (nl). Archiefbeheer. Deel 2: Richtlijnen* (november 2001); *ISO 23081-1. Metadata for records. Part 1: Principles* (2004); *NEN 2082, eisen voor functionaliteit van informatie- en archiefmanagement in programmatuur* (ontwerp) (Delft, juni 2007); P. Horsman, *Kwaliteit van documenten*. Discussiestuk Archiefschool. Versie 2.1. (2005). *NORA, Nederlandse Overheid Referentie Architectuur. Samenhang en samenwerking binnen de elektronische overheid*. ICTU, versie 1 (27 september 2006)

technische en organisatorische maatregelen ter voorkoming van een onrechtmatige verwerking (waaronder de afscherming van gegevens via een systeem van getrapte toegankelijkheid en autorisaties). In de volgende hoofdstukken wordt de archivistische omzetting van deze waarborgen besproken, maar niet nadat in dit verband eerst enkele algemene opmerkingen zijn geplaatst.

Informatie op orde

Een archiveringssysteem kan niet zorgen voor het voorkómen van onrechtmatige gegevensverwerkingen en hiermee voor de borging van de informationele privacy als het er niet in slaagt in algemene zin de archiefbescheiden in goede, geordende en toegankelijke staat te beheren en te bewaren. Bescherming van de informationele privacy is in dit opzicht 'slechts' een aspect of afgeleide van de (kwaliteit van de) interne informatiehuishouding, of anders geformuleerd: het op orde hebben van de informatiehuishouding is een c*onditio sine qua non* voor privacybescherming.

In dit verband kan het volgende voorbeeld genoemd worden. Ter bescherming van de informationele privacy moet een organisatie in kaart hebben op welke plaatsen zij welke persoonsgegevens voor welk doel verwerkt en moet ze dit op de juiste plaatsen en de juiste wijze hebben geregistreerd. Het is dus raadzaam dat de organisatie óók met betrekking tot de veelal op termijn te vernietigen persoonsgegevens beschikt over een actueel, compleet en logisch samenhangend (bestands)overzicht, zoals dat in de *Regeling geordende en toegankelijke staat archiefbescheiden* (artikel 3 en 9) wettelijk is voorgeschreven voor de permanent te bewaren bescheiden. Hoewel de *Regeling* formeel alleen betrekking heeft op blijvend te bewaren archiefstukken, kan de vergroting van de reikwijdte vastgelegd worden in de beheersregels (Besluit Informatiebeheer).

Risicomanagement

NEN-ISO 15489 spreekt ten aanzien van de invulling van het informatie- en archiefmanagement van een organisatie expliciet van 'risicomanagementbeslissingen'.[180] Ook met betrekking tot de privacybescherming zullen organisaties risico-analyses maken. Dit kan betekenen dat (gepercipieerde!) risico's van invloed kunnen zijn op de mate waarin aan wet- of regelgeving tegemoet gekomen zal worden. Ontbreken bijvoorbeeld toezicht of sancties bij niet-naleving van wettelijke bepalingen, dan kan dit resulteren in de verschuiving *van de mate waarin* regelgeving wordt nageleefd. Dat iets volgens de wet verplicht is en zonder problemen kán worden uitgevoerd, wil dus niet in alle gevallen zeggen dat dit in de praktijk ook volgens de regels zál plaatsvinden…

Stofzuigeren of eerst selecteren?

Bescherming van de informationele privacy is natuurlijk maximaal als er helemaal geen verwerking van persoonsgegevens plaatsvindt. Hoe minder gegevensverwerking, hoe kleiner de kans op onrechtmatige verwerkingen en dus op privacy-aantastingen. Per slot van rekening kan geen misbruik worden gemaakt van gegevens die niet worden verzameld, is er minder kans op vervuiling van persoonsgegevens en is er minder inspanning nodig voor het beheer en de beveiliging van de persoonsgegevens.

De beslissing over doel en noodzaak van het verwerken van een bepaalde hoeveelheid gegevens (rakende de beginselen van noodzakelijkheid, subsidiariteit en proportionaliteit) wordt, vanuit organisatieperspectief beschouwd, genomen in het primaire proces. Het archiveringssysteem is vanuit dit perspectief het secundaire proces ter facilitering van dit primaire proces (waarvan het de documentaire

[180] *NEN-ISO 25489-2*, p. 9-10, 19.

afspiegeling vormt); het zorgt voor het verwerven, beheren en beschikbaar stellen van archiefdocumenten, waartoe in deze paper ook persoonsgegevens worden gerekend, die de organisatie nodig heeft (of *meent* te hebben!) voor de uitvoering van het primaire proces, waarbij het systeem de kwaliteit van deze gegevens dient te waarborgen.

Het is in het primaire proces dat de keus wordt gemaakt voor de 'stofzuigermethode' van het massaal verzamelen van gegevens om er vervolgens een 'elektronisch sleepnet' door te halen ten behoeve van *datamining*, dan wel voor toepassing van het minder privacy-belastende concept van '*select before you collect'.* Het archiveringssysteem reflecteert de gemaakte keuzes voor of binnen bepaalde werkprocessen (de vanuit deze keuzes vastgelegde procedures en definities inzake al dan niet in het systeem op te nemen gegevens vormen een component van het archiveringssysteem) … en ondervindt de gevolgen ervan.[181]

[181] F. Kuitenbrouwer, 'AIVD mag stofzuigeren naar persoonsgegevens', *Netkwesties*, Digitaal magazine over maatschappij en internet (28 oktober 2008). Kuitenbrouwer gebruikt de stofzuigermetafoor ter illustratie van de door de AIVD voorgestane methode van 'gegevensverzameling voor je weet maar nooit ', als er uiteindelijk maar genoeg materiaal beschikbaar is om er ten behoeve van *datamining* een 'elektronisch sleepnet' door te halen. Opvallende kwinkslag: Geheime diensten en stofzuigers hebben kennelijk iets met elkaar. Want wat verkocht Graham Greene's 'Our Man in Havana' als dekmantel voor zijn activiteiten ... ?

9. KWALITEIT, METADATA EN CONTEXT

Bij de vormgeving van de archiveringsfunctie dient het archiveringssysteem ervoor te zorgen dat de archiefbescheiden, waaronder de persoonsgegevens, de vereiste kwaliteit behouden, d.w.z. zich in 'goede, geordende en toegankelijke staat' bevinden; de data dienen daartoe volgens NEN-ISO 15489 *authentiek*, *integer*, *bruikbaar* en *betrouwbaar* te zijn.[182] In de woorden van Horsman betekent dit dat de archiefgegevens *integer* (dat wil zeggen naar inhoud betrouwbaar - volledig, nauwkeurig, juist en controleerbaar - en naar vorm authentiek*), toegankelijk/bruikbaar* (vindbaar, raadpleegbaar, leesbaar en interpreteerbaar) en *duurzaam beheerbaar* moeten zijn.[183] Door de kwaliteit van de data te waarborgen geeft het archiveringssysteem invulling aan de in de privacywetgeving opgenomen vereisten van juistheid, nauwkeurigheid, volledigheid en beveiliging van gegevens. En deze kwaliteitsborging is een noodzakelijke voorwaarde om inbreuken op de informationele privacy te voorkomen.

Kwaliteit en metadata

Kwaliteit van digitale gegevens wordt in hoge mate bepaald door zogenaamde 'metadata'[184] die expliciet toegekend zijn aan de gegevens gedurende hun gehele levensloop. Deze zijn essentieel voor het betrouwbaar kunnen herleiden van de status, de structuur en de integriteit van de archiefgegevens op elk willekeurig moment en om hun relaties met andere archiefgegevens aan te tonen.

Archiveringssystemen behoren volgens NEN-ISO 15489 aan archiefstukken verbonden metadata (over de aspecten *context*, *inhoud* en *structuur*) vast te leggen op een manier die:

a) het archiefstuk beschrijft zowel wat de inhoud als de ontstaanscontext betreft;
b) het mogelijk maakt dat het archiefstuk een gefixeerde weergave van de handeling is;
c) terugvinden en zinvolle weergave mogelijk maakt.[185]

Metadata zijn er in vele soorten en maten. Ditzelfde geldt voor typeringen en indelingen die van metadata zijn gemaakt.[186] Een globale driedeling is de categorisering in:[187]

---

[182] *NEN-ISO 15489-1,* 7.2, p. 10-11.
[183] P. Horsman, *Kwaliteit van documenten*, passim.
[184] In *NEN-ISO 15489-1,* 3.12. (p. 6) worden metagegevens omschreven als 'gegevens die context, inhoud en structuur van archiefbescheiden en hun beheer door de tijd heen beschrijven'. *ISO 23081* (p. 1) borduurt hierop voort en definieert metadata als 'structured or semi-structured information that enables the creation, registration, classification, access, preservation and disposition or records through time and within and across domains'.
[185] *NEN-ISO 15489-1*, 9.3., p. 18; *NEN-ISO 15489-2,* 4.3.2., p. 23.
[186] De ISO-norm voor metadata onderscheidt twee organisatorische categorieën, een vijftal categorieën naar gelang doel van de metadata en vijf categorieën gebaseerd op de inhoud van de metadata. Organisatorisch onderscheidt *NEN 23081* (hoofdstuk 5.3., p. 3-4) de ontstaansmetadata (*'metadata at the point of capture*'), die tot stand komen bij de opname van het archiefstuk in het systeem, en de procesmetadata (*'metadata after record capture'*), die tijdens de levensloop van het archiefstuk worden toegevoegd of gewijzigd. De indeling naar doel van de metadata zijn (hoofdstuk 7, p. 5-6): metadata voor e-business, metadata voor -duurzame- bewaring (*'preservation'*), metadata voor identificatie van archiefstukken (*'resource description'* - 'resources' kunnen volgens *NEN 23081*, 7.3., p. 5 behalve *'records'* ook *'books, journals, videos, documents, images and artefacts'* zijn), metadata voor terugvindbaarheid en information retrieval (*'resource discovery'*) en metadata voor rechtenbeheer (*'rights management'*). Een indeling naar inhoud (hoofdstuk 9, p. 10-18) levert een categorisering op van metadata over het archiefstuk zelf ('metadata about records'), metadata over de bedrijfsregels, -politiek en -mandaten (*'metadata about the business rules, policies and mandates'*), metadata over actoren (*'agent metadata'*) , metadata over bedrijfsprocessen (*'business process metadata'*) en metadata met betrekking tot archiefbeheer (*'metadata about record management processes'*). Voor een korte beschrijving van de NEN-norm voor metadata, zie J. Poppe, 'Metadata: ISO 23081 en andere standaarden (1) en (2)', *Od* 9 (2006) 20-21 en *Od* 10 (2006) 18-20. Horsman somt in het *Jaarboek Paradigma* en in een concept-metadatamodel drie soorten metadata op (beschrijvende, contextuele metadata, technische metadata en

1) *Beschrijvende metadata*, hoofdzakelijk bestaande uit gegevens over de *context* van documenten, die documenten identificeren, de juiste interpretatie van documenten mogelijk maken, de authenticiteit van documenten aantonen en het vinden van documenten vergemakkelijken;
2) *Administratieve metadata of beheersmetadata* die beheershandelingen mogelijk maken of aansturen en uitgevoerde beheershandelingen vastleggen;
3) *Technische metadata* die correcte (re)presentatie mogelijk maken.

Vastlegging van metadata kan op verschillende niveaus van detaillering. De mate van vereiste detaillering hangt af van de bedrijfsbehoefte en de gebruiksmogelijkheden van het archiefstuk. Hoe breder of langer het archiefstuk beschikbaar of toegankelijk moet zijn, hoe breder het scala aan noodzakelijke contextinformatie.[188]

Contextualisering, decontextualisering en recontextualisering

Het opnemen van archiefdocumenten, waaronder digitale persoonsgegevens, in een archiveringssysteem en de ermee gepaard gaande vastlegging of fixering van de relevante context in metadata betekent anders geformuleerd dat de archiefdocumenten of persoonsgegevens worden *'gecontextualiseerd'*. Worden de gegevens uit de oorspronkelijke context gehaald en naar een andere omgeving geëxporteerd of overgebracht (als gevolg van al dan niet verplichte verstrekking of overbrenging naar een bewaarplaats), dan vindt *'decontextualisering'* plaats. In de nieuwe context moeten de gedecontextueliseerde gegevens vervolgens weer worden *gerecontextualiseerd*; ze moeten bijvoorbeeld weer geschikt gemaakt worden voor andere dan de oorspronkelijke gebruikers die de gegevens verwerken voor andere doelen dan waarvoor ze aanvankelijk zijn verzameld. Bij elke re- en decontextualisering gaan betekenissen (en daarmee kwaliteit) van gegevens verloren.[189]

9.1. Kwaliteitsnormen vertaald naar het ideaaltypische archiveringssysteem

Door de borging van de kwaliteit van de persoonsgegevens geeft het archiveringssysteem van organisaties vallend onder de Wpolg en de Wiv invulling aan de in de betreffende wetgeving genoemde vereisten van juistheid, nauwkeurigheid en volledigheid van gegevens. Deze kwaliteitsborging is een noodzakelijk element in het voorkómen van inbreuken op de informationele privacy. Het archiveringssysteem moet deze kwaliteit overigens veelal garanderen zonder gebruik te kunnen maken van de corrigerende invloeden van onderzoeksubjecten, door de relatief beperkte rechten die deze hebben in vergelijking met gegevensverwerkingen die plaatsvinden onder het regime van de Wbp.

De in de paper besproken wetgeving met betrekking tot de gegevensverwerking stelt specifieke uitdagingen aan het archiveringssysteem ter borging van de kwaliteit van de gegevens. De belangrijkste hiervan worden in dit hoofdstuk belicht, met uitzondering van die aangaande gegevensbeveiliging en toegangregulering. De in dat kader te

---

administratieve data of beheersdata) en elders onderscheidt hij vijf groepen, zie P. Horsman, 'Archiefsystemen en kwaliteit' in: P. Horsman, F.C.J. Ketelaar en T.H.P.M. Thomassen, *Naar een nieuw paradigma in de archivistiek* ('s Gravenhage 1999) 85-105, aldaar 92-93, P. Horsman, H. Waalwijk en G-J. v. Bussel, *Metadatamodel. Beschrijving van entiteiten en attributen*. Versie 3.1. (Archiefschool, 6 juni 2002), 2, respectievelijk P.J. Horsman, *Archiveren. Een inleiding* ('s Gravenhage 2004) 98.

[187] P. Horsman, H. Waalwijk en G.-J. v. Bussel, *Metadatamodel. Beschrijving van entiteiten en attributen*. Versie 3.1. (Archiefschool, 6 juni 2002), 2.

[188] *NEN-ISO 15489-2*, p. 23; *ISO 23081*, 5.1., p. 2.

[189] T. Thomassen, 'De veelvormigheid van de archiefontsluiting en de illusie van de toegankelijkheid' in: T. Thomassen, B. Looper en J. Kloosterman (red.), *Toegang. Ontwikkelingen in de ontsluiting van archieven* ('s Gravenhage 2001) 13-43, aldaar 33-34.

nemen organisatorische en technische maatregelen komen in het volgende hoofdstuk aan de orde.

Toename beschikbare gegevens

Allereerst zorgt de simpele toename van te (re)contextualiseren gegevens ervoor dat de kwaliteit van de gegevens middels het correct vastleggen van relevante metadata aan belang wint. Bijvoorbeeld om nog iets in de grote berg terug te kunnen vinden (via metadata voor terugvindbaarheid), om het kaf van het koren te kunnen scheiden (via metadata voor herkomst, verwerkingsdoel, betrouwbaarheid, vertrouwelijkheid of rol van personen in een groep) of gegevens op langere termijn verder te kunnen blijven verwerken (technische metadata en beheersmetadata).

Deze gegevenstoename vloeit enerzijds voort uit de nieuwe bevoegdheden gegevens te kunnen vorderen, uit te wisselen of te verstrekken, *aanvullend* op de al langer bestaande mogelijkheden gegevens uit (steeds algemener beschikbare) openbare bronnen of eigen onderzoek en inlichtingen te verkrijgen. Anderzijds groeit de hoeveelheid data door de verruiming van de mogelijkheden gegevens verder te bewerken via koppeling en onderlinge vergelijking waardoor *nieuwe* gegevens ontstaan, die op hun beurt ook weer verder bewerkt kunnen worden.

Verlenging bewaartermijnen

Niet alleen groeit het aantal gegevens waarover opsporings- en veiligheidsdiensten de beschikking krijgen, deze gegevens mogen ook nog eens langer ter beschikking staan van de diensten door de verlenging van de bewaartermijnen. Het totale volume van duurzaam te beheren gegevens neemt hierdoor sterk toe. Vanuit privacy-oogpunt beschouwd betekent een langere bewaartermijn een vergroting van het risico op onrechtmatige verwerkingen. Om de kwaliteit van de gegevens (en hiermee de bescherming van de informationele privacy) over een langere periode te kunnen garanderen is vastlegging en onderhoud van een grotere variëteit aan metadata met een hogere detailleringsgraad vereist. Denk in dit verband aan beheersmetadata over autorisaties of vernietigingstermijnen (waarbij bovendien nog eens rekening moet worden gehouden met het in de Wpolg geïntroduceerde onderscheid tussen te 'verwijderen' en te 'vernietigen' gegevens) en aan technische metadata ten behoeve van duurzame (re)presentatie van de digitale bescheiden. Dit vergt extra (kostenverhogende) inspanningen van het archiveringssysteem.

Gedifferentieerde herkomst en kwaliteit: garbage in, garbage out

Analoog aan de groei in gegevensomvang, zorgt de nieuwe wetgeving voor een steeds gedifferentieerdere herkomst van gegevens. De kwaliteit van deze gegevens kan heel wisselend zijn en wordt mede bepaald door de eisen die vanuit de bedrijfsvoering van de verstrekkende partij worden gesteld. Het is derhalve van groot belang dat bij de recontextualisering van deze diversiteit aan gegevens metadata worden vastgelegd met betrekking tot de herkomst, wijze van verkrijging en de betrouwbaarheid van de verkregen gegevens.

Het archiveringssysteem moet verhinderen dat *'garbage'* ongeoormerkt het systeem binnenkomt en verder wordt verwerkt ('*garbage in, garbage out')*. Bij opeenvolgende verwerkingen en uitwisseling van gegevens kan dit (vroeg of laat) vervelende consequenties hebben voor zowel de activiteiten van opsporings- en veiligheidsdiensten als uiteraard voor de degenen op wie de gegevens betrekking hebben.

De- en recontexualisering: damage control

Bij gegevensvordering kan niet genoeg benadrukt worden dat de gegevens door de verstrekkende partij oorspronkelijk verwerkt (*gecontextualiseerd*) zijn voor een ander doel dan waarvoor opsporings- en veiligheidsdiensten ze willen gebruiken. Omdat de mate van vereiste detaillering van metadata (en hiermee de invulling van het concept 'kwaliteit') afhangt van de bedrijfsbehoefte van de contexualiseerder, kan het doorbreken van het doelbindingsprincipe als gevolg van de vordering ertoe leiden dat kwalititatief goede gegevens in de ene (ontstaans)context van onvoldoende kwaliteit zijn in een andere context, waar immers andere bedrijfsbehoeften zullen bestaan en ook andere eisen worden gesteld aan de gebruiksmogelijkheden van de gegevens.

Al naar gelang de methode van verkrijging (variërend van *shared services* als CIOT, gegevensexport tot *online* raadplegen van geïsoleerde gegevens dan wel complete databanken) worden gevorderde gegevens in meer of mindere mate gedecontextualiseerd en vervolgens in meer of mindere mate weer ge(re)contextualiseerd. Bij deze (re)contextualisering moeten metadata worden vastgelegd die de kwaliteit van de gegevens dusdanig maakt dat tegemoetgekomen wordt aan zowel de nieuwe bedrijfsbehoeften en de verregaande gebruiksmogelijkheden van data van de diensten vallend onder de Wpolg en de Wiv, als aan de vereisten die een onevenredige inbreuk op de informationele privacy voorkómen.

Het doelbindingsprincipe in de privacywetgeving is één van de belangrijkste bepalingen ter voorkoming van onrechtmatige verwerking van persoonsgegevens. Via het creëren van de in de paper besproken wettelijke verplichtingen heeft de wetgever ervoor gezorgd dat vordering en hiermee het omzeilen van dit principe juridisch toegestaan is. Hiermee is de weg geplaveid om op grote schaal gegevens te verwerken voor andere doelen dan waarvoor ze oorspronkelijk verwerkt en 'gecontextualiseerd' zijn, waardoor de risico’s op onrechtmatige verwerkingen en hiermee op privacy-inbreuken aanzienlijk toenemen. Elk proces van decontextualisering en recontextualisering brengt een risico van betekenisverlies met zich mee. Hoe verder de doelen waarvoor de gegevens verwerkt worden van elkaar verwijderd liggen, hoe groter dit risico is. Dit geldt in sterke mate voor de- en recontextualisering voortvloeiend uit gegevensvordering, maar ook voor die voortvloeiend uit onderlinge uitwisseling en verdere bewerking (*datamining*) van gegevens binnen het opsporings- en veiligheidsdomein.

Voor het archiveringssysteem is het vanuit het oogpunt van de bescherming van de informationele privacy dan ook zaak om processen van re- en decontextualisering zoveel mogelijk te beperken en, indien deze onvermijdelijk zijn, bij de recontextualisering het betekenisverlies van decontextualisering zoveel mogelijk te compenseren. Deze *damage control* kan het systeem onder meer uitvoeren door oog te hebben voor (en met de verstrekker in overleg te treden over) de import van relevante oorspronkelijke contextuele metadata en voor de aanpassing en creatie van (beschrijvende) metadata die contextverlies minimaliseren.

9.2. Het hellende vlak van het expanderende archiveringssysteem

De uitbreiding van de bevoegdheden om gegevens bij derden te vorderen en ze voor een ander doel te verwerken dan waarvoor ze oorspronkelijk verzameld zijn, zorgt ervoor dat het archiveringssysteem van de vorderende partij extra inspanningen moet verrichten om de kwaliteit van de gegevens te waarborgen en daarmee de informationele privacy van onderzoekssubjecten te beschermen. Er is een onzekere factor in de wisselende en soms onbekende kwaliteit van de verstrekte gegevens, wat volgens het *garbage in, garbage out*-principe vroeg of laat vervelende gevolgen kan hebben. Daarbij gaat elk proces van de- en recontextualisering gepaard met (risico's op) context- en hierdoor betekenisverlies.

Deze aan de vordering inherente complicaties kan het archiveringssysteem eigenlijk alleen maar minimaliseren als het zijn tentakels uitslaat naar het archiveringssysteem van de verstrekkende (in eerste instantie contextualiserende) partij. Het vorderende systeem zou zijn kwaliteitseisen samenhangend met een (van de verzamelaar afwijkend) bepaald gebruik (denk aan ordening, toegankelijkheid, maar ook aan duurzame digitale representatie) moeten opleggen (en controleren!) aan de verzamelende partij. In een digitale omgeving is de vastlegging van metadata direct bij de creatie van de gegevens van groot belang; het in een later stadium toevoegen of wijzigen van metadata voor een ander en bovendien langduriger gebruik is immers (zo al mogelijk) geen eenvoudige, en in ieder geval tijdrovende en kostbare aangelegenheid.

Expansie en function creep

Dit impliceert dat er een (op termijn wellicht wettelijk afgedwongen) praktijk zou kunnen gaan ontstaan dat gegevensverzamelende instanties bij de inrichting van hun archiveringssysteem rekening (moeten) gaan houden met mogelijke verplichte verstrekkingen. Deze praktijk is niet denkbeeldig. Zo wordt binnenkort een wet van kracht die met het oog op de vordering van verkeersgegevens bedrijven verplicht deze gegevens veel langer te bewaren dan voor de eigen bedrijfsvoering noodzakelijk is. Ook het bewerken en verwerven van gegevens door derden ten behoeve van (vordering door) opsporings- en veiligheidsdiensten is al eens (door de Commissie Mevis) geopperd.

Het archiveringssysteem van derde partijen dreigt hierdoor slachtoffer van een *function creep* te worden. Dit systeem behoort procesgebonden informatie te beheren en beschikbaar te stellen die de organisatie nodig heeft voor de uitvoering van taken of het afleggen van verantwoording. De kwaliteit (en contextualisering) van de gegevens is afgestemd op de eisen van de bedrijfsvoering. Door de in gang gezette interventie van vorderende partijen krijgt het archiveringssysteem ook steeds meer de functie om de buiten de eigen bedrijfsvoering gelegen taken van opsporings- en veiligheidsdiensten te ondersteunen; het archiveringssysteem van de derde partij dreigt hierdoor steeds meer een verlengstuk (of onderdeel?) van het archiveringssysteem van opsporings- en veiligheidsdiensten te worden. Vanuit de privacywetgeving roept dit de vraag op naar de verhouding tussen 'verantwoordelijke' en 'verwerker'; archivistisch beschouwd kunnen aspecten als eigendom van gegevens (die naar hun aard bestemd zijn waaronder te berusten?) en zorgdragerschap in een ander daglicht komen te staan.

Vanuit het perspectief van de bescherming van de informationele privacy beschouwd, doet zich met betrekking tot de expansie van het archiveringssysteem van opsporings- en veiligheidsdiensten in de interne aangelegenheden van verstrekkende derde partijen een merkwaardige paradox voor. Dezelfde ontwikkelingen die in dit geval (controle over) kwaliteit en privacybescherming doen toenemen, vergroten namelijk ook weer exponentieel de risico's op inbreuk op de informationele privacy.

10. TOEGANGSBEVEILIGING: TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

In de besproken wetgeving wordt veelvuldig gerefereerd aan te nemen *'technische en organisatorische maatregelen'* teneinde onrechtmatige gegevensverwerking en de hieraan inherente aantasting van de informationele privacy te voorkomen. Een meer enge interpretatie spitst zich in dit verband toe op het reguleren van het gebruik van de gegevens. In het archivistische discours betekent dit dat het archiveringssysteem ervoor moet zorgen dat formele richtlijnen opgesteld behoren te zijn die regelen aan wie het geoorloofd is onder welke condities toegang te hebben tot welke (categorie van) gegevens en dat de gegevens beveiligbaar moeten zijn tegen ongeoorloofde wijzigingen en/of raadplegingen. Dit draagt op zijn beurt bij aan de borging van de integriteit en daarmee de kwaliteit van de gegevens.

De componenten van het archiveringssysteem moeten in onderlinge samenhang ieder op hun wijze bijdragen aan het uitvoeren van deze taak. Organisatorische maatregelen om het gebruik van gegevens te reguleren liggen in de sfeer van het opstellen van procedures en bepalingen omtrent (de verantwoordelijkheden voor het toekennen van) toegangsrechten, -condities en -beperkingen, alsmede in het creëren van voorzieningen om toezicht op de naleving van deze procedures mogelijk te maken. Technische maatregelen zijn in dit verband veelal de omzetting van organisatorische procedures en autorisaties naar (schillen rond) computerprogramma's of architectuur.

10.1. Toegangsbepalingen NEN-ISO 15489 en NEN 2082 vertaald naar het ideaaltypische archiveringssysteem

NEN-ISO 15489 schrijft voor dat organisaties formele richtlijnen behoren te hebben die regelen aan wie het geoorloofd is toegang tot de archiefbescheiden te hebben en onder welke condities; deze rechten en condities behoren in het archiveringssysteem te zijn geïntegreerd.[190] NEN 2082 definieert in dit verband het archiveringsproces 'beschikbaar stellen' als het op basis van toegangscontrole en informatiebeveiliging ondersteunen van het zoeken naar, beschikbaar stellen en (re)presenteren van archiefbestanddelen en informatieobjecten op elk aggregatieniveau.[191] Het bewerkstelligen van passende toegangscontrole kan worden bereikt door het ontwikkelen en permanent bijhouden van (en toezicht houden op de naleving van!) autorisatietabellen of classificatieschema's voor beveiliging en toegang, waarin - door vastlegging van metadata - een toegangsstatus is toegekend aan zowel (categorieën) archiefbescheiden als individuen (gebruikers). Wijzigt de maatschappelijk-juridische context, dan dient het toegangs- en beveiligingsregime hieraan aangepast te worden.[192]

Het beheer van dit proces van toegangscontrole betekent volgens NEN-ISO 15489 dat een archiveringssysteem ervoor moet zorgen dat:[193]

a. archiefbescheiden in categorieën worden ingedeeld in overeenstemming met hun toegangsstatus op een bepaald moment;
b. archiefbescheiden alleen worden vrijgegeven aan personen die geautoriseerd zijn om ze te zien;

---

[190] *NEN-ISO 15489-1*, 9.7 en 9.8, p. 20-21; *NEN-ISO 15489-2,* 4.2.5., p. 20-22.
[191] *NEN 2082*, 11.
[192] *NEN-ISO 15489-1*, 9.7 en 9.8, p. 20-21; *NEN-ISO 15489-2,* 4.2.5., p. 20-22; *NEN 2082*, 6.7.2. en 6.8.3., p. 24, 29-30. Waar in NEN-ISO 15489 de term 'toegangsclassificatieschema' wordt gebruikt, hanteert NEN 2082 het begrip 'autorisatietabel'. Deze tabel bepaalt welke handelingen, activiteiten of taken tot een rol binnen een gebruikersprofiel behoren en welke rollen toegangsrechten geven tot archiefstukken die bepaalde beveiligingsniveaus hebben. De categorie metadata die gegevens bevat over wie waarop welke rechten heeft, wordt in ISO 23081 (hoofdstuk 7.5, p. 6) de categorie metadata voor rechtenbeheer (*'metadata for rights management'*) genoemd.
[193] *NEN-ISO 15489-1*, 9.7., p. 21.

c. mutaties, processen en transacties met betrekking tot archiefbescheiden alleen kunnen worden uitgevoerd door personen die hiertoe geautoriseerd zijn;
d. onderdelen van de organisatie met verantwoordelijkheid voor bepaalde bedrijfs*functies* toegangsregels specificeren voor archiefbescheiden die betrekking hebben op hun verantwoordelijkheidsgebied.

NEN-ISO 15489 en NEN 2082 bepalen verder dat het archiveringssysteem gebruikersautorisaties binnen de organisatie dient te identificeren, evenals toegangsrechten voor personen van *buiten* de organisatie. Dit om te kunnen garanderen dat alleen gebruikers met de juiste bevoegdheden gegevens kunnen verwerken waarvoor zij zijn geautoriseerd. Hiertoe moet het systeem het gebruik van de gegevens volgen; het dient elke (poging tot) verwerking of gebruik van gegevens te documenteren (te loggen) met het vereiste detailniveau. Deze log-gegevens behoren tot de metadata en moeten op hun beurt worden beheerd. Behalve dat de door logging ontstane controleerbare *audit-trail* bijdraagt aan het voorkomen van onrechtmatige verwerkingen, vergemakkelijkt dit bovendien *privacy-audits* en het nakomen van de informatieplicht richting betrokkenen.[194]

Toegangsstatus gegevens

Een gevolg van de wijziging in de juridische context van gegevenswerking is dat het archiveringssysteem van organisaties vallend onder de Wpolg of de Wiv 2002 de categorie-indeling van gegevens moet aanpassen. Nu kunnen gegevens door toekenning van metadata uiteraard in vele categorieën ingedeeld worden die een toegangsstatus met een daarbij passend beveiligingsniveau vertegenwoordigen. Het opsommen van deze veelheid aan categorieën is in het kader van deze paper niet doenlijk en zal bovendien nooit volledig kunnen zijn. Enkele nieuwe of aan te passen categorieën mogen echter niet onvermeld blijven.

Voor de hand liggende categorieën zijn de in de paper genoemde ‘oormerking’ naar herkomst, wijze van verkrijging en de (hiermee samenhangende) mate van vertrouwelijkheid en/of betrouwbaarheid van (identificerende, ook andere dan identificerende of gevoelige) gegevens. Een belangrijke aanpassing vloeit voort uit de vervanging van het registerbegrip door het doelbindingsprincipe in de nieuwe Wpolg, wat betekent dat gegevens ingedeeld zullen moeten worden naar het doel waarvoor ze verwerkt mogen worden door daartoe geautoriseerde personen. Deze (indeling naar) doelbinding is een belangrijke waarborg om onrechtmatige verwerking en *function creep* te voorkomen. Omdat de Wpolg de mogelijkheid biedt gegevens verder te verwerken voor een ander doel binnen de politietaak, kent deze indeling een dynamisch karakter en is het up-to-date houden van de status 'op een bepaald moment' van groot belang. Een nieuwe uit de Wpolg voortvloeiende (eveneens dynamische) categorie betreft daarnaast de groep 'achter het schot-'geplaatste (verwijderde, maar nog niet te vernietigen) gegevens.

Toegangsstatus gebruikers

Naast het vastleggen van de toegangsstatus van *gegevens*, moet het archiveringssysteem ervoor zorgen dat via autorisaties ook aan *gebruikers* een 'toegangsstatus' wordt toegekend. Organisatieonderdelen verantwoordelijk voor bepaalde bedrijfsfuncties specificeren hiertoe toegangsregels die *rol-gebaseerd* en dynamisch zijn: de mate van toegang is afhankelijk van welke rol een persoon op het moment van toegang zoeken heeft in relatie tot de (gegevens over een) onderzoekssubject. Een persoon in een bepaalde functie kan meerdere rollen vervullen, zoals de Wiv-artikel 60-ambtenaren, waaronder de RID-medewerkers.

[194] *NEN-ISO 15489-1*, 8.3.2., p. 14; *NEN-ISO 15489-2,* 4.3.8., p. 29, *NEN 2082*, 6.6., p. 21-22.

In de Wiv is bepaald dat de hoofden van diensten verantwoordelijk zijn voor de aanwijzing van personen die bevoegd zijn tot de verwerking van gegevens; het archiveringssysteem moet deze autorisaties vastleggen. De Wpolg schrijft een door de verantwoordelijke te onderhouden getrapt systeem van autorisaties voor, waarbij gegevens slechts mogen worden verwerkt door ambtenaren die daartoe door de verantwoordelijke zijn geautoriseerd en voor zover de autorisatie strekt. Dit autorisatiesysteem dient aangepast te worden aan de nieuwe doelbindingscriteria.

Gekoppeld aan een autorisatiesysteem dient het archiveringssysteem methoden van authenticatie te ontwikkelen en te beheren, opdat identificatie kan plaatsvinden van gebruikers die geautoriseerd zijn tot het uitvoeren van bepaalde verwerkingen.

Nieuwe dimensies toegangsbeveiliging

Methoden van toegangsbeveiliging, autorisatie en authenticatie van gebruikers zijn belangrijke componenten van het archiveringssysteem ter voorkoming van onrechtmatige gegevensverwerking. Hoewel deze aspecten van het archiveringssysteem op zich natuurlijk niet nieuw zijn, zijn er tegen de achtergrond van de gewijzigde juridische context van gegevensverwerking toch enkele factoren aan te wijzen die maken dat ze als het ware een andere dimensie krijgen.

Allereerst maakt het simpele feit dat de opsporings- en veiligheidsdiensten op een veel grotere schaal dan voorheen de beschikking krijgen over een breed scala aan gegevens dat het risico op onrechtmatige verwerkingen aanmerkelijk groter wordt. Alleen dit *volume*-aspect al maakt dat het vraagstuk van de toegangsbeveiliging meer gewicht krijgt.

Daarnaast zorgen de uitbreiding van de mogelijkheden om (gevorderde of anderszins verkregen) gegevens *verder te verwerken* (zoals *datamining*) en de *verlenging van de bewaartermijnen* voor een toename van de kans op onrechtmatige verwerkingen. Ook hierdoor wint het aspect toegangsbeveiliging aan belang.

Een belangrijke extra dimensie krijgt het toegangselement vooral ook door de *uitbreiding van verstrekkingsregimes* en (steeds meer in ketenverband plaatsvindende) *gegevensuitwisseling*. Verstrekking van gegevens kan op verschillende manieren plaatsvinden. Net als bij de vordering (verkrijging) van gegevens geldt hier dat uniformiteit in methodiek ontbreekt. In geval van externe verstrekking van politiegegevens dient de verantwoordelijke voorwaarden te stellen die opslag en onrechtmatige verdere verwerking bij de ontvangende derde voorkomt; bovendien zal voorzien moeten zijn in methoden van toezicht op naleving hiervan. Ook rechtstreekse verstrekking langs geautomatiseerde weg (*online* en *real time*) behoort tot de mogelijkheden. Op een dergelijke wijze kunnen politiegegevens in enkele gevallen extern worden verstrekt en hebben medewerkers van de CT-Infobox bijvoorbeeld toegang tot politiegegevens.

Het toenemende gebruik van privacygevoelige gegevens door externe partijen, als gevolg van verstrekking aan derden of gegevensuitwisseling in ketenverband, betekent dat het archiveringssysteem de methoden van toegangsbeveiliging, autorisatie en authenticatie (en toezicht op de naleving ervan) ook steeds meer zal moeten externaliseren, in de zin dat deze methoden zich steeds meer zullen moeten uitstrekken *buiten* het domein van de eigen organisatie. *Mutatis mutandis* geldt dit natuurlijk ook voor de verstrekkende derde in geval van vordering door opsporings- en veiligheidsdiensten. Dit betekent dat diensten en organisaties die gegevens vorderen, verstrekken of uitwisselen afspraken moeten maken, die erop gericht zijn informatiebeveiliging- en privacystelsels op elkaar af te stemmen en afgestemd te houden. In geval van bilaterale verstrekkingen zullen dit veelal bilaterale afspraken zijn; is er sprake van een uitgebreid samenwerkingsverband of keten (zoals bij de CT Infobox) dan zullen de samenwerkende partijen gezamenlijk de *governance* voor hun

informatiebeveiliging en privacy moeten inrichten, waartoe zij ter coördinatie een eenduidige ketenverantwoordelijke (moeten) aanstellen.[195]

De verstrekker van gegevens past natuurlijk ook toegangsbeveiliging toe. Een bijzondere eis die de vorderende of verzoekende partij aan de verstrekkende derde zal moeten stellen, is dat eventuele beveiliging (bijvoorbeeld encryptie of versleuteling) van een informatieobject verwijderd moet kunnen worden bij verstrekking, waarna de ontvanger een nieuw beveiligingsregime kan instellen. Deze nieuwe dimensie geldt ook in geval van gegevensuitwisseling tussen opsporings- en veiligheidsdiensten. Met betrekking tot die (aggregaten van) informatieobjecten of gegevens die ingevolge Wiv 2002, artikel 43 en 44 of Wpolg, artikel 14 (vierde lid) in aanmerking komen voor overbrenging naar een (digitale) archiefbewaarplaats, vormt dit eveneens een belangrijk aandachtspunt; het archiveringssysteem moet ervoor waken niet de sleutels kwijt te raken van uit privacy-overwegingen afgesloten gegevensaggregaten, opdat eventueel toekomstig historisch onderzoek niet het kind van de rekening wordt.

10.2. PET of PEM?

Bij het nemen van 'technische en organisatorische maatregelen' ter voorkoming van onrechtmatige gegevensverwerking (en hiermee ter bescherming van de informationele privacy) kan de vraag gesteld worden naar de verhouding die er moet zijn tussen de technische respectievelijk organisatorische component van het archiveringssysteem. Gekoppeld hieraan is de vraag hoe *diep* de technologie in systemen of architectuur verankerd moet zijn. Enkele facetten van dit voor de inrichting van het archiveringssysteem interessante vraagstuk worden behandeld aan de hand van een bespreking van het systeem van *Private Enhancing Technologies* of *PET*.

To PET...?

De technische ontwikkelingen die in veel gevallen de kans op inbreuken op de informationele privacy vergroten (zoals het op het grote schaal vastleggen en koppelen van gegevens), kunnen ook worden ingezet om deze privacy juist weer te waarborgen. Dit is althans de overtuiging van voorvechters van het systeem van *'Privacy Enhancing Technology'* (PET), wat staat voor een verzameling van informatie- en communicatietechnologieën die de bescherming van de persoonlijke levenssfeer van individuen binnen een informatiesysteem versterken door het voorkomen van onnodige dan wel ongewenste verwerking van persoonsgegevens, zonder dat de functionaliteit van een informatiesysteem hiervoor moet boeten. Vanuit een strikte doelbinding redenerend is het uitgangspunt bij PET het streven naar gegevensminimalisatie: 'hoe minder persoonsgegevens we verwerken, hoe beter'.[196]

Het toepassen van PET is een van de manieren waarop het archiveringssysteem de kwaliteit van gegevens zou kunnen waarborgen en tegelijkertijd tegemoet zou kunnen komen aan de vanuit de maatschappelijk-juridische context gestelde eisen aangaande de bescherming van de informationele privacy van onderzoekssubjecten. Volgens het Ministerie van BZK zou PET zonder problemen toegepast kunnen worden; indien vroegtijdig over gegevensbescherming wordt nagedacht en dit wordt meegenomen in de systeemontwikkeling, zouden bescherming van persoonsgegevens en functionaliteit

[195] *NORA*, 133-134.
[196] *Privacy Enhancing Technologies. Witboek voor beslissers*. KPMG rapport i.o.v. Ministerie van BZK (december 2004), 14, 69-70, 89. Het *Witboek* citeert professor Boasson van de UvA die in dit verband opmerkt dat voor dit uitgangspunt wel een rechte rug nodig is: er is nog steeds een weerstand om bepaalde gegevens niet te verzamelen of niet op te slaan met de gedachte dat je maar beter de gegevens beschikbaar kunt hebben voor het geval dat het eens handig kan blijken. Zie ook: R.J. Gerding, 'De meekijkende maatschappij', *Privacy & informatie*, 2 (2007), 57-63, aldaar 62.

van het informatiesysteem hand in hand kunnen gaan.[197] Ook NORA stelt dat privacy zoveel mogelijk middels PET in het ontwerp van geautomatiseerde systemen geborgd moet worden.[198]

Tot de algemene PET-maatregelen behoren de *versleuteling van gegevens* (encryptie) en de *logische toegangsbeveiliging*. Bij deze logische toegangsbeveiliging zijn vooral het goede beheer van uniek identificerende persoonsgegevens (authenticatie) en bijbehorende (dynamische, rol-gebaseerde) autorisatiegegevens van belang. Hoewel het gebruik van logische toegangsbeveiliging belangrijk is om ongeautoriseerde toegang tot persoonsgegevens te voorkomen, is een beperking van deze beveiliging dat de gegevens nog steeds identificeerbaar en bij elkaar worden opgeslagen.[199]

Een belangrijke PET-vorm betreft de *ontkoppeling* of *scheiding van gegeven*s in meerdere domeinen. Het ene domein bevat de *identificerende* persoonsgegevens, het andere de overige (bijvoorbeeld justitiële, financiële, lidmaatschap-, opsporings- of telecommunicatie-) gegevens. De gegevens in ieder afzonderlijk domein zijn niet privacygevoelig, omdat ze zo zijn opgeslagen dat ze niet herleidbaar zijn naar een natuurlijke persoon. De scheiding tussen beide domeinen wordt aangebracht en beheerd door een identiteitsbeschermer (*'identity protector'*) Alleen met behulp van deze identiteitsbeschermer kan een hiertoe geautoriseerde systeemgebruiker toegang verkrijgen tot de beide domeinen en de relatie tussen de gegevensdomeinen zien. De autorisatie en authenticatie van personen die de identiteitsbeschermer mogen gebruiken is hierbij vanzelfsprekend van essentieel belang. [200]

Met PET worden privacybepalingen direct in de applicatie of ICT-infrastructuur verankerd, waardoor in mindere mate gesteund hoeft te worden op het naleven van organisatorische en procedurele maatregelen, waarbij de gegevensbescherming vaak zo sterk is als de zwakste schakel. Dit zou de beheersing van en het toezicht op de gegevensverwerking optimaliseren. Belangrijke rol hierbij speelt tevens het loggen van elke verwerkingshandeling, waardoor een controleerbare *audit-trail* ontstaat.[201]

Or not to PET..?

Toch kent PET ook de nodige haken en ogen. Zo is PET een element in de informatie*architectuur* dat voor informatiesystemen wordt ontwikkeld. Toepassing op bestaande systemen blijkt in de praktijk een lastige opgave. PET profiteert pas optimaal als het is meegenomen in het *ontwerp*proces van deze architectuur (*'privacy by design'*). Vooral bij meervoudig gebruik en uitwisseling van gegevens levert PET nogal wat barrières op; deze vragen hierdoor een op voorhand zorgvuldig overdachte informatiearchitectuur.[202]

Daarbij komt nog dat het in de informatiearchitectuur verankeren van een strikte doelbinding-indeling en regulering van gebruik deze architectuur behalve meer complex ook meer rigide maakt, terwijl de (onder meer in deze paper besproken) veranderende wetgeving niet bepaald aanleiding geeft om het gebruik van gegevens voor altijd in te perken.

Daarnaast kunnen vraagtekens worden gezet bij de noodzaak van PET in relatie tot informatiebeveiliging. De huidige beveiligingspraktijk voldoet en is flexibeler door vanuit

[197] Ibidem, 10.
[198] *NORA*, 142.
[199] Ibidem, 28-32.
[200] Ibidem, 33-35.
[201] Ibidem, 15, 44-45. Uiteraard dienen de logbestanden niet gemanipuleerd te kunnen worden en moeten ze zelf ook *PET-proof* zijn; logbestanden mogen geen persoonsgegevens bevatten, waarvan juist PET geprobeerd wordt de verwerking te voorkomen.
[202] *PET. Witboek*, 66, 72. M.J. v. Lieshout, 'Privacy Enhancing Technologies: een zaak van lange adem', *Privacy & informatie*, 5 (2002) 203-209, aldaar 208.

een rond de gegevens gelegde ‘schil’ de gegevens (geautoriseerd) benaderbaar te maken. In tegenstelling tot PET grijpt deze 'schil' niet in op de architectuur.[203]

Tenslotte dreigt door PET het geheel van beheersmaatregelen op het gebied van de organisatie en het personeel en fysieke en procedurele maatregelen (de zogenaamde *Privacy Enhancing Measures* of PEM) onderbelicht te raken; PET beoogt deze 'zwakste schakel' immers zoveel mogelijk te omzeilen. De heiligverklaring van de techniek, mag er niet toe leiden dat de noodzakelijke organisatie (PEM) rond die techniek verwaarloosd wordt: een slechte techniek kan weliswaar moeilijk door de organisatie gecompenseerd worden, een uitstekende techniek kan daarentegen eenvoudig door een niet-functionerende organisatie om zeep worden geholpen.[204]

10.3. Keteninformatisering

In de paper is in relatie tot het vorderen, verstrekken en uitwisselen van gegevens diverse keren het verschijnsel ‘keteninformatisering’ ter sprake gekomen. De verwerking en koppeling van gegevens in ketenverband kan de kans op inbreuken op de informationele privacy aanmerkelijk vergroten. Toch dringt zich de vraag op of het archiveringssysteem door een slimme invulling van de technisch-organisatorische component ‘keteninformatisering’ bij zou kunnen dragen aan de bescherming van de informationele privacy in plaats van deze verder aan te tasten.

Een begrip als keteninformatisering is erg in de mode en kent diverse varianten. Een algemene omschrijving van keteninformatisering luidt dat het een manier is om geautomatiseerde informatie-uitwisseling mogelijk te maken tussen samenwerkende, zelfstandige organisaties die als ketenpartner ieder een specifieke rol binnen samenhangende werkprocessen spelen. De ketenpartners delen informatie met elkaar, in beginsel zonder dat zij een gemeenschappelijke informatiestructuur hebben, met als doel om te komen tot *eenmalige opslag* en *meervoudig gebruik*. Aangezien niet langer sprake is van een duidelijke archiefvormer die verantwoordelijk is voor het gehele proces van archiefvorming, dient een ketenverantwoordelijke aangewezen te worden.[205] Toch is keteninformatisering niet nieuw en wordt het begrip al langere tijd gebruikt in de literatuur over interorganisationele informatiesystemen (IOS).

Interorganisationele informatiesystemen (IOS)

Een veel gehanteerde typologie van IOS-systemen, gebaseerd op processtructuren, coördinatievormen en informatie-infrastructuren, levert drie soorten ketensystemen op, waarbij elk type ketenproces een bijbehorende informatie-infrastructuur heeft waarmee invulling wordt gegeven aan de voor de processtructuur vereiste coördinatievorm:[206]

1. de *pooled information resource IOS, met een ondersteunende* (*mediating*) informatiestructuur, gericht op het in contact brengen van (informatie)vraag en aanbod, horend bij *parallelle* processen die afhankelijk zijn van een *gemeenschappelijke bron*;
2. de *value/supply-chain IOS*, met een *estafette* (*long-linked*) informatiestructuur, gericht op het ondersteunen van (volgorderlijke) *serie-afhankelijkheid* over meerdere schakels, horend bij *ketenprocessen* met *lineaire* afhankelijkheden;

[203] R.J.M. v.d. Horst, 'To PET or not to PET...', *Privacy & informatie*, 4 (2003) 160-164, aldaar 162-163.
[204] Ibidem, 163.
[205] *Gewaardeerd verleden. Bouwstenen voor een nieuwe waarderingsmethodiek voor archieven*. Rapport van de Commissie Waardering en Selectie (september 2007) 17.
[206] D. v. Bremen, 'Keteninformatisering in het perspectief van de vakliteratuur' in: Grijpink, *Geboeid door ketens,* 29-37, aldaar 30-31 en 'Keteninformatisering, breder toepasbaar dan je zou denken' in: ibidem, 153-167, aldaar 155-156. Ook de NORA onderscheidt samenwerking in ketens en in netwerken en, hiermee samenhangend, drie principes van ketenbesturing, zie: *NORA, Nederlandse Overheid Referentie Architectuur. Samenhang en samenwerking binnen de elektronische overheid*. ICTU, versie 1 (27 september 2006) 81, 86.

3. de *networked IOS*, met een *intensieve* (*intensive*) informatiestructuur ten behoeve van *intensieve* afstemming in *ketenprocessen* met *wederkerige* afhankelijkheden.

Het principe van de eenmalige opslag en het meervoudige gebruik geldt overigens voor alle drie de procesafhankelijke typologieën, maar dan welk steeds op een andere wijze.[207]

Keteninformatisering volgens Grijpink[208]

Grijpink ziet keteninformatisering als 'het structuren en automatiseren van de communicatie die nodig is om gegevens aan elkaar beschikbaar te stellen waarover deelnemers in de keten moeten kunnen beschikken'. Grijpinks concept van keteninformatisering concentreert zich voornamelijk op toepassing van ketenbrede informatiesystemen ten behoeve van de coördinatie van ketenprocessen met wederkerige afhankelijkheden (de *networked IOS*). Hierbij richt keteninformatisering zich op de *communicatie* van slechts enkele voor de keten kritische (gemeenschappelijke) gegevens; de keteninformatiestructuur dient zo 'kaal' mogelijk te zijn. Centraal staat de vraag waar het benodigde gegeven op het juiste moment uit de keten vandaan kan worden gehaald om op de juiste plaats een foute beslissing te voorkomen. Informatie en gegevens dienen (vanuit het non-interventiebeginsel) bij de eigenaar (de ketenpartner) te blijven en daar beheerd te worden; essentieel is een centraal toegangsstelsel, inclusief een methode voor geautomatiseerde signaleringen en waarschuwingen. Bij keteninformatisering draait het in Grijpinks visie dus vooral om toegangsmechanismen.

Grondvlak- en ketenniveau[209]

Belangrijk element in Grijpinks visie is het onderscheid tussen het zogenaamde *grondvlak*- en het *ketenniveau*. Met het grondvlakniveau bedoelt Grijpink de eigen (inhoudelijke) brongegevens van de ketenpartners, waar de ketenpartners zelf verantwoordelijk voor zijn. Directe bilaterale uitwisseling tussen gegevens vindt vanuit dit grondvlak plaats. Keteninformatiesystemen zijn aan deze brongegevens gekoppeld en ontsluiten (delen van) het grondvlak. Hiertoe bevatten deze alleen de *metagegevens* die voor alle ketenpartners van belang zijn, zoals verwijsindexen, verificatieregisters en anonimiserende nummerstelsels, die een ketenbrede deling van identificerende gegevens garanderen en inzicht bieden in de plaats waar iemand uit de doelgroep zich in het ketenproces zich bevindt. Deze metagegevens vormen het ketenniveau en worden op ketenniveau gezamenlijk beheerd.

---

[207] In de *pooled information resource IOS* vindt de éénmalige opslag plaats in een gemeenschappelijke informatiebron, waar gebruikers uit kunnen putten (centraal opgeslagen en decentraal te raadplegen basisregistraties zijn hier een voorbeeld van); in de *value/supply chain IOS* vindt bilateraal uitwisseling van gegevens plaats, waarbij eenmalig opgeslagen gegevens als output van de ene partij dienst doen als input voor een andere partij in een serie; in een *networked IOS* dient de vastgelegde output van de ene partij als de input voor meerdere andere partijen en kan de input van een partij bestaan uit de output van meerdere andere partijen.

[208] Deze paragraaf is gebaseerd op de volgende bronnen: J.A.H.M. Grijpink, 'Onze informatiesamenleving in wording. De uitdaging van grootschalige informatie-uitwisseling in de rechtstaat', Rede uitgesproken bij de aanvaarding van het ambt van bijzonder hoogleraar Keteninformatisering in de rechtstaat (Voorburg/Den Haag 2005), passim; J.A.H.M. Grijpink, 'ICT, Spelbederver of Dwarsligger?' in: A. Valstar en M. v. Genuchten, (red.), *Liber Amicorum T.M. Bemelmans* (Eindhoven 2004*)* passim; J.A.H.M. Grijpink, 'Het leerstuk Keteninformatisering in vogelvlucht' in: Grijpink, *Geboeid door ketens,* 9-17.

[209] Ibidem.

Keteninformatisering als PET?[210]

Waarschuwingen uit het ketenniveau leiden ertoe dat alleen díe (via de metagegevens toegankelijk gemaakte) gegevens via het grondvlak worden uitgewisseld die aan de signalering voldoen. Hiertoe wordt het voor dat specifieke geval vereiste gegeven (of inhoudelijke informatie) voor eenmalig gebruik opgehaald waar het zich op dat moment bevindt en geautomatiseerd gepresenteerd (gebracht) waar het op dat moment nodig is. Keteninformatisering maakt zodoende het, voor de privacy van onderzoekssubjecten vaak nadelige, rechtstreeks koppelen van complete databanken overbodig.[211] Hiermee kan het eraan bijdragen dat aan de cumulatieve effecten van afbreuk aan privacy een halt toe wordt geroepen. In deze zin zou de keteninformatisering á la Grijpink beschouwd kunnen worden als een PET - *Privacy Enhancing Technology* (privacybeschermende technologie).

[210] Ibidem, alsmede B. Custers, 'Privacy en risicoprofilering bij keteninformatisering', passim.
[211] Bovendien is volgens Custers het koppelen van gegevens in de praktijk vaak irreversibel: het 'ontkoppelen' kost gewoonlijk veel meer moeite dan het koppelen, of kan zelfs onmogelijk blijken; zie: Custers, 'Privacy en risicoprofilering', 190.

11. CONCLUSIE

De probleemstelling in herinnering roepend:

Wat betekenen de in Nederland in het kader van de terreurbestrijding van kracht geworden wettelijke bevoegdheden van opsporings- en veiligheidsdiensten inzake verwerking van persoonsgegevens voor de informationele privacy van onderzoekssubjecten en hoe kan het archiveringssysteem van opsporings- en veiligheidsdiensten ervoor zorgen dat deze privacy wordt beschermd?

kunnen de volgende conclusies getrokken worden.

Doelbinding, uitzonderingsartikel Wbp en wettelijke verplichting.

Om opsporings- en veiligheidsdiensten van de benodigde grondstof voor terrorismebestrijding te voorzien heeft de Nederlandse regering wetgeving ontwikkeld die deze diensten de mogelijkheid biedt te kunnen beschikken over bij derden berustende gegevens. Daar deze derden hun gegevens verwerken onder het Wbp-regime is verstrekking onrechtmatig als deze onverenigbaar is met de doeleinden waarvoor de gegevens zijn verzameld. Dit doelbindingsbeginsel is echter niet van toepassing indien op verzoek, na een 'noodzakelijkheidsafweging' door de verantwoordelijke, vrijwillige verstrekking plaatsvindt aan opsporings- en veiligheidsdiensten op grond van uitzonderingsartikel 43 of indien aan een wettelijke verplichting voldaan moet worden. In essentie komt de ontwikkelde antiterreurwetgeving inzake gegevensverwerking er dan ook op neer de vrijwillige verstrekking op grond van artikel 43 te omzeilen door een verzoek de status te geven van een wettelijke verplichting waaraan voldaan moet worden, waarbij de vorderende partij beslist over de noodzakelijkheid van de verstrekking.

Uitbreiding wettelijke bevoegdheden

Ten behoeve van politie en justitie is door wetgeving op het gebied van gegevensvordering verplichte verstrekking van telecommunicatiegegevens, financiële gegevens en uiteindelijk zelfs van in principe *alle* soorten gegevens(bestanden) van maatschappelijke instellingen en bedrijven over zowel verdachten als 'anderen dan de verdachte' mogelijk gemaakt. In geval van 'aanwijzingen' voor de voorbereiding van een terroristisch misdrijf mogen opsporingsdiensten in een verkennend onderzoek over 'een ieder' gegevens vorderen.

Het vorderen van telecommunicatiegegevens is ook een bevoegdheid van de inlichtingen- en veiligheidsdiensten. De algemene bevoegdheid tot gegevensverzameling heeft vooralsnog echter het karakter van een verzoek, waarop overeenkomstig Wbp, artikel 43 een vrijwillige verstrekking kan volgen.

Naast de vordering van gegevens, zijn in de wetgeving ook de verdere verwerkingsmogelijkheden van de verkregen gegevens aanzienlijk uitgebreid. De nieuwe Wet politiegegevens verruimt de mogelijkheid van de politie om gegevens te verwerken over onverdachte personen, deze gegevens langer te bewaren en bovendien opnieuw te gebruiken voor andere onderzoeken. Onder meer biedt de wet de mogelijkheid tot permanente gegevensverwerking ter verkrijging van inzicht in terroristische activiteiten. Verder is het gebruik van zoekmogelijkheden en *datamining*technieken verruimd en is het verstrekkingsregime uitgebreid. Voorts is de politie verplicht rechtstreeks gegevens te verstrekken aan de AIVD. De verwerking door de AIVD is gereguleerd in de Wiv 2002.

Hoewel opsporings- en veiligheidsdiensten wettelijk meer armslag hebben gekregen gegevens te vorderen en uit te wisselen, bestaat in de uitvoeringspraktijk hierin (nog) geen eenduidige systematiek. Eerder is sprake van een veelheid aan benaderingen, waarbij elke organisatie zijn eigen systematiek en werkwijze kent.

Risico's voor informationele privacy

De maatregelen ter verruiming van de mogelijkheden om gegevens te verwerken hebben cumulatief en in samenhang een groot effect op de privacy van burgers. Onderzoeken hebben steeds vaker een verkennend karakter en richten zich ook op niet-verdachte personen. Door de toenemende omvang, de gedifferentieerde herkomst en de langere bewaartermijn van gegevens, die bovendien voor een ander doel worden gevorderd dan waarvoor ze zijn verzameld, neemt de kans toe dat de juistheid, volledigheid, (toegangs)beveiliging en interpreteerbaarheid - en daarmee de kwaliteit - van gegevens moeilijker te waarborgen zijn. Door de verdere verwerking van deze gegevens middels *datamining* en risicoprofilering vergroot dit de kans op *'false positives'* en *'false negatives'*, met mogelijk grote nadelige gevolgen voor de privacy van onschuldige burgers die meenden niets te verbergen te hebben.

Privacywaarborgen en archiveringssysteem

Geplaatst tegen de gewijzigde juridisch-maatschappelijke context dient het archiveringssysteem van de opsporings- en veiligheidsdiensten ter bescherming van de informationele privacy de privacywaarborgen te vertalen naar eisen ten aanzien van de kwaliteit van de persoonsgegevens (zijnde archiefbescheiden) en hiermee naar eisen ten aanzien van de inrichting van het archiveringssysteem. Een *conditio sine qua non* voor elke privacybescherming is echter dat de informatiehuishouding op orde is.

Het nemen van technische en organisatorische maatregelen ter voorkoming van onrechtmatige gegevensverwerking als privacywaarborg betekent in het archivistische discours dat het archiveringssysteem autorisatietabellen met authenticatiemethoden moet ontwikkelen en bijhouden (en door logging toezien op de naleving ervan), waarin een toegangsstatus is toegekend aan zowel (categorieën) archiefbescheiden als aan gebruikers. Deze toegangsbeveiliging wint aan belang door de toename van het aantal beschikbare gegevens en krijgt een extra, externaliserende, dimensie door de uitbreiding van verstrekkingsregimes en de steeds meer in interdependent ketenverband plaatsvindende gegevensuitwisseling. Hierdoor moeten diensten die gegevens vorderen, verstrekken of uitwisselen bilateraal of in ketenverband afspraken maken die erop gericht zijn toegangs-, informatiebeveiliging- en privacystelsels op elkaar af te stemmen en afgestemd te houden. Het archiveringssysteem dient zich in dit verband ook af te vragen welke PET-maatregelen zij wil toepassen en hoe diep zij deze in de programmatuur of architectuur wil verankeren. Als specifieke *Privacy Enhancing Technology* geldt in dit verband de keteninformatisering à la Grijpink met haar onderscheid tussen grondvlak- en ketenniveau.

De vereiste juistheid, nauwkeurigheid, volledigheid en beveiliging van persoonsgegevens als privacywaarborg garandeert het archiveringssysteem door de kwaliteit van de gegevens (zijnde archiefbescheiden) in archivistische zin te borgen door het toekennen van de juiste beschrijvende/contextuele, administratieve/beheersmatige en technische metadata. De toename van beschikbare gegevens vergroot het belang van metadata voor terugvindbaarheid en de verlenging van bewaartermijnen noodzaakt tot bijzondere aandacht voor specifieke beheersmetadata. De gedifferentieerde herkomst en de wisselende kwaliteit van de verstrekte gegevens nopen tot het vastleggen van metadata over herkomst, wijze van verkrijging en betrouwbaarheid van de verkregen gegevens; *'garbage'* mag niet

onge(oor)merkt het systeem binnenkomen en verder worden verwerkt (*'garbage in, garbage out'*).

De wettelijk verplichte verstrekking van gegevens die oorspronkelijk voor een ander doel zijn gecontextualiseerd, vergroot de risico's op onrechtmatige verwerkingen. Daar elk proces van de- en recontextualisering kwaliteitsverlies met zich mee kan brengen (dit geldt zowel voor gegevensvordering, als voor verdere verwerking en uitwisseling binnen het opsporings- en veiligheidsdomein), dient het archiveringssysteem ten behoeve van de privacybescherming bij de recontextualisering het betekenisverlies van decontextualisering zoveel mogelijk te compenseren. Bij deze *damage control* spelen beschrijvende, contextuele metadata een sleutelrol.

Expansie als privacywaarborg?

Daar vastlegging van de voor contextbehoud, terugvindbaarheid en kwaliteit vereiste metadata in een digitale omgeving veelal direct bij de creatie van persoonsgegevens plaatsvindt, zou ter bescherming van de informationele privacy het archiveringssysteem van de vorderende partij uiteindelijk haar eisen op moeten leggen (en controleren) aan de verzamelende partij en het archiveringssysteem van de contextualiseerder tot haar verlengstuk (of onderdeel?!) moeten maken. De vrees is niet ongegrond dat een dergelijke inmenging weer tot gevolg heeft dat er ontwikkelingen optreden die de risico's op een inbreuk op de informationele privacy exponentieel vergroten.

GERAADPLEEGDE BRONNEN

De geraadpleegde bronnen zijn per hoofdstuk geclusterd. Binnen elk cluster zijn eerst steeds in chronologische volgorde de wetteksten vermeld (indien van toepassing), gevolgd door een alfabetisch gerangschikt overzicht van de overige geraadpleegde bronnen (literatuur, rapporten, tijdschriftartikelen en internetsites).

1. Inleiding

- Brief van de Ministers van Justitie en van BZK aan de Voorzitter van de Tweede Kamer der Staten-Generaal over Terrorismebestrijding (10 september 2004), TK 2003-2004, 29 754, nr.1.

- Horsman, P., *Archiveren. Een inleiding* ('s Gravenhage 2004).
- Shepherd E. en Yeo, G., *Managing records. A handbook of principles and practice* (Londen 2003).
- www.overheid.nl – wet- en regelgeving.
- www.recht.nl – wet- en regelgeving.

2. Generieke informationele privacywetgeving: Wbp

- Regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), Memorie van Toelichting, TK 1997-1998, 25 892, nr. 3.
- Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), Stb. 2000, 302.

- Cook, T., 'Archives and privacy in a wired world: the impact of the *Personal Information Act* on archives', *Archivaria* 53 (2002) 94-114.
- Ketelaar, F.C.J., 'Elke handeling telt. Archiefdiensten en de Wet bescherming persoonsgegevens' (geactualiseerde versie van 6 augustus 2001 van een artikel, verschenen in het Archievenblad 104/3 (mei 2000) 18-23 en 104/4 (juni 2000) 26-29).
- Ketelaar, F.C.J. en Noordam, C.G.M., Archiefrecht, een inleiding (Amsterdam: Archiefschool, 2005).
- Klep, P.M.M. 'Verschuivende visies en praktijken. Archieven bewaren voor onderzoek en cultuur' in: P. Brood, e.a. (red*), Selectie. Waardering, selectie en acquisitie van archieven* ('s Gravenhage 2004) 84-105.
- Meij, A.C.M. de, 'Het WBP-vrijstellingsbesluit', *Privacy & Informatie*, 2 (april 2001) 59-63.
- *Persoonsdossiers: een geval apart* (Den Haag: Nationaal Archief, 2006).
- *Wet bescherming persoonsgegevens. Handleiding voor verwerkers van persoonsgegevens* (Den Haag: Ministerie van Justitie, april 2002).
- www.cbpweb.nl - site van het College Bescherming Persoonsgegevens.

3. Gegevensverzameling door opsporingsdiensten

3.1. Wet BOB

- Wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), TK 1996-1997, 25 403, nr. 1-2.
- Wijziging van het Wetboek van Strafvordering in verband met de regeling van enige bijzondere bevoegdheden en wijziging van enige andere bepalingen (bijzondere opsporingsbevoegdheden), Memorie van Toelichting, TK 1996-1997, 25 403, nr. 3.

- *Factsheet Wet bijzondere opsporingsbevoegdheden (BOB)* ('s Gravenhage: Ministerie van Justitie, z.j.).

3.2. De slag om de telecommunicatiegegevens

- Telecommunicatiewet (1998), hoofdstuk 13, Bevoegd aftappen.
- Besluit aftappen openbare telecommunicatienetwerken -en diensten, Stb. 2001, 262.
- Regeling aftappen openbare telecommunicatienetwerken en -diensten (ingang 15 juni 2001).
- Besluit bijzondere vergaring nummergegevens telecommunicatie 18 december 2001, Stb. 2002, 31.
- Wijziging van het Wetboek van Strafvordering en andere wetten in verband met de aanpassing van de bevoegdheden tot het vorderen van gegevens terzake van telecommunicatie (vorderen gegevens telecommunicatie), Voorstel van Wet, TK 2001-2002, 28 059, nr. 2.
- Wijziging van het Wetboek van Strafvordering en andere wetten in verband met de aanpassing van de bevoegdheden tot het vorderen van gegevens terzake van telecommunicatie (vorderen gegevens telecommunicatie), Memorie van Toelichting, TK 2001-2002, 28 059, nr. 3.
- Wet van 18 maart 2004 tot wijziging van het Wetboek van Strafvordering en andere wetten in verband met de aanpassing van de bevoegdheden tot het vorderen van gegevens terzake van telecommunicatie (vorderen gegevens telecommunicatie), Stb. 2004, 105.
- Besluit vorderen gegevens telecommunicatie van 3 augustus 2004, Stb. 2004, 394.
- Richtlijn 2006/24/EG van het Europees Parlement en de Raad van 15 maart 2006.
- Wet bewaarplicht telecommunicatiegegevens, Voorstel van Wet, TK 2006-2007, 31 145, nr. 2.
- Wet bewaarplicht telecommunicatiegegevens, Memorie van Toelichting, TK 2006-2007, 31 145, nr. 3.

- Bits of Freedom, Dossier verkeersgegevens (www.bof.nl/verkeersgegevens.html) (2005).
- CBP, *Advies Wetsontwerp implementatie Europese Richtlijn Dataretentie* (22 januari 2007).
- Erasmus Universiteit Rotterdam, *Wie wat bewaart, heeft wat* (Rotterdam 2005).
- Koops, B.-J., *Strafvorderlijk onderzoek van (tele)communicatie 1838-2002. Het grensvlak tussen opsporing en privacy* (Deventer 2002).
- Prins, J.E.J., 'Wapenwedloop in cyberspace. Gegevensmunitie ten koste van privacy?' *Ars Aequi,* 51 (2002) 315-323.
- Steenbruggen, W., 'I know what you did last summer! Over grenzeloze en ongegeneerde verwerking van verkeersgegevens in de informatiemaatschappij', JAVI, 3 (december 2002) 89-97.
- Stratix Consulting Group B.V., *Onderzoek "Bewaren verkeersgegevens door telecommunicatie-aanbieders".* Eindrapport uitgebracht aan het WODC (Schiphol, augustus 2003).

3.3. Algemene vorderingswet: Wet bevoegdheden vorderen gegevens (Wbvg)

- Wijziging van het Wetboek van Strafvordering en enkele andere wetten i.v.m. de regeling van bevoegdheden tot het vorderen van gegevens (bevoegdheden vorderen gegevens), Voorstel van wet, TK 2003-2004, 29 441, nr. 2.
- Wijziging van het Wetboek van Strafvordering en enkele andere wetten i.v.m. de regeling van bevoegdheden tot het vorderen van gegevens (bevoegdheden vorderen gegevens), Memorie van Toelichting, TK 2003-2004, 29 441, nr. 3.

- Wet van 16 juli 2005 tot wijziging van het Wetboek van Strafvordering en enkele andere wetten i.v.m. de regeling van bevoegdheden tot het vorderen van gegevens (bevoegdheden vorderen gegevens), Stb. 2005, 380.

- Dijk, J. v., 'Kloof tussen idealen en veiligheidsdenken', *InformatieProfessional* (juni 2006) 12-13.
- Jeloschek, C. en Vries, H.H. de, 'Het spanningsveld tussen het vorderen en het beschermen van persoonsgegevens', *NJB*, 2 (12 januari 2007) 86-91.
- Jongeneel-van Amerongen, M., 'Geen spanningsveld tussen het vorderen van gegevens en de Wet bescherming persoonsgegevens', *NJB*, 28 (3 augustus 2007) 1755.
- Jongeneel-van Amerongen, M., 'Wet bevoegdheden vorderen gegevens', *Ars Aequi*, 54 (2005) 954-961.
- Koren, M., 'Reflexie en debat', *InformatieProfessional* (januari 2005) 30-32.
- Stevens, L., Koops, B.-J. en Wiemans, P., 'Een strafvorderlijke gegevensgaring nieuwe stijl', *NJB*, 32 (10 september 2004) 1680-1686.
- Verstappen, M., 'Survivalpakket voor privacyfreaks', *InformatieProfessional* (januari 2005) 6.
- 'Vorderen bibliotheekgegevens', *NJB*, 25 (24 juni 2005) 1321.
- Wesseling, M., 'Los Alamos', *InformatieProfessional* (mei 2005) 30-31.
- Wiemans, P., 'Bescherming privacy op de tocht', *InformatieProfessional* (april 2006) 14-19.

3.4. Wet verruiming mogelijkheden tot opsporing en vervolging van terroristische misdrijven (Wvm)

- Wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven, Voorstel van Wet, TK 2004-2005, 30 164, nr. 2.
- Wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven, Memorie van Toelichting, TK 2004-2005, 30 164, nr. 3.
- Wet van 20 november 2006 tot wijziging van het Wetboek van Strafvordering, het Wetboek van Strafrecht en enige andere wetten ter verruiming van de mogelijkheden tot opsporing en vervolging van terroristische misdrijven, Stb. 2006, 580.

- CPB, *Advies conceptwetsvoorstel bijzondere bevoegdheden tot opsporing van terroristische misdrijven*, Brief van de Minister van Justitie (22 december 2004).
- CBP, *Wetsvoorstel tot verruiming van de mogelijkheden ter opsporing en vervolging van terroristische misdrijven*. Brief aan de Vaste commissie voor Justitie van de Eerste Kamer (2 november 2006).
- Kempen, P.H.P.H.M.C. van, 'Terrorismebestrijding door marginalisering strafvorderlijke waarborgen', *NJB*, 8 (25 februari 2005) 397-400.

4. Sectorale wetgeving gegevensverwerking opsporingsdiensten: Wpolg

- Wet van 21 juni 1990, houdende regels ter bescherming van de persoonlijke levenssfeer in verband met politieregisters (Wet politieregisters), Stb, 1990, 414.
- Besluit van 14 februari 1991, houdende bepalingen ter uitvoering van de Wet politieregisters (Besluit politieregisters), Stb, 1991, 56.
- Brief van de Minister van Justitie, Bestrijding internationaal terrorisme, TK, 2002-2003, 27 925, nr. 82.
- Regels inzake de verwerking van politiegegevens (Wet politiegegevens), Memorie van Toelichting, TK 2005-2006, 30 327, nr. 3.

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

- Algemene Rekenkamer, *Terugblik 2005*. *Elf onderzoeken nader beschouwd* (Den Haag, 24 maart 2005).
- Buuren, J. v. en Schans, W. v.d., 'Strijd om de databanken: de informatiehuishouding van de politie in Europa', *Privacy & informatie*, 6 (2003) 247-252.
- CBP, *Advies conceptwetsvoorstel inzake de verwerking van politiegegevens (Wet politiegegevens),* Brief aan de Minister van Justitie (3 augustus 2004).
- *Gegevensuitwisseling en Terrorismebestrijding*, Werkgroep Gegevensuitwisseling en Terrorismebestrijding (6 januari 2003).
- Kielman, H.H. en Koelewijn, W.I., 'Minder registers, meer gegevens. Over gegevensverwerking betreffende zware criminaliteit', *Ars Aequi* (juni 2005) 451- 457.
- Kielman, H.H. en Koelewijn, W.I., 'Privacy als tunnelvisie: over de strafprocessuele waarde van politiële informatieverwerking', *Privacy & Informatie*, 3 (juni 2006) 106-109.
- Mac Gillavry, E.C., 'Heeft u even voor de nieuwe Wet politiegegevens?' in: Harteveld, A., Jong, D.H. de, en Stamhuis, E. (red.) in: *Systeem in ontwikkeling, Liber amicorum G. Knigge* (Nijmegen 2005; http://irs.ub.rug.nl/ppn/296127892) 385-416.
- Prins, C., 'Politiegegevens: laveren tussen wet en praktijk' in: *NJB*, 14 (8 april 2005) 725.
- *Uitwisseling van opsporings- en terrorisme-informatie*, Rapport Algemene Rekenkamer, TK 2002-2003, 28 845, nr. 2.
- *Vaststelling Selectielijst archiefbescheiden regionale politieorganisaties vanaf 1 april 1994 voor neerslag handelingen Korps Landelijke Politiediensten. Basisselectielijst 2004* (2 februari 2006).

5. Verzameling en verwerking van gegevens door inlichtingen- en veiligheidsdiensten

- Regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 19..), *Memorie van Toelichting*, TK 1997-1998, 25877, nr. 3.
- Wet van 7 februari 2002, houdende regels met betrekking tot de inlichtingen- en veiligheidsdiensten alsmede wijziging van enkele wetten (Wet op de inlichtingen- en veiligheidsdiensten 2002), *Stb*, 148.
- Wijziging van de Wiv 2002 i.v.m. de verbetering van de mogelijkheden van inlichtingen- en veiligheidsdiensten om onderzoek te doen naar en maatregelen te nemen tegen terroristische en andere gevaren met betrekking tot de nationale veiligheid alsmede andere wijzigingen, Voorstel van Wet, TK 2005-2006, 30 553, nr. 2.
- Wijziging van de Wiv 2002 i.v.m. de verbetering van de mogelijkheden van inlichtingen- en veiligheidsdiensten om onderzoek te doen naar en maatregelen te nemen tegen terroristische en andere gevaren met betrekking tot de nationale veiligheid alsmede andere wijzigingen, Memorie van Toelichting, TK 2005-2006, 30 553, nr.3.

- Ekker, A.H., 'Het onderscheppen van telecommunicatie door de inlichtingen- en veiligheidsdiensten' in: *Computerrecht* 2002-2, 77-83.
- Kuitenbrouwer, F., 'Onschuldige gegevens', *Computerrecht*, 97 (2006), 192.

6. Systematiek van vordering en uitwisseling van gegevens

6.1. Uitvoering vordering en verstrekking gebruikersgegevens: CIOT

- Besluit verstrekking gegevens telecommunicatie van 26 januari 2000, Stb. 2000, 71.

- Besluit tot wijziging van het Besluit verstrekking gegevens telecommunicatie van 13 september 2006, Stb. 2006, 426.

6.2. CT-Infobox

-Brief Minister BZK aan de Tweede Kamer over de CT-Infobox (18 maart 2005) TK 2004-2005, 29 754 en 27 925, nr. 21.
- Convenant inzake de samenwerking in de CT Infobox, dd. 11 maart 2005, Nr. 2325766/01. Bijlage bij de Brief van de Minister BZK aan de Tweede Kamer van 18 maart 2005, TK 2004-2005, 29 754 en 27 925, nr. 21.
- Brief van MZK aan de Tweede Kamer, Terrorismebestrijding (reactie op CBP-advies), TK 2005-2006, 29 754, nr. 29.
- Brief van de Minister van BZK aan de Tweede Kamer betreffende het Toezichtsrapport CTIVD inzake CT-Infobox (10 april 2007).
- Brief van de Minister van BZK aan de Tweede Kamer, Terrorismebestrijding/AIVD, TK 2007-2008, 29 754 en 30 977, nr. 126.

- CBP, Brief aan de Minister van Justitie, Controle op informatieverzameling over onverdachte burgers ontbreekt (22 september 2004).
- CBP, Brief aan de vaste commissie voor BZK en Justitie, CT Infobox (29 september 2005).
- CTIVD, *Toezichtsrapport inzake het onderzoek van de Commissie van Toezicht naar de Contra Terrorisme Infobox*, CTIVD nr. 12 (10 april 2007).

6.3. Data voor daadkracht

- Brief van de minister van BZK aan de Tweede Kamer ter aanbieding rapport 'Data voor daadkracht', 30 augustus 2007 (www.minbzk.nl/108221/brief-aan-de-tweede).

- *Data voor daadkracht. Gegevensbestanden voor veiligheid: observatie en analyse*. Rapport van de Adviescommissie Informatiestromen Veiligheid (30 augustus 2007).
- Cuijpers, C., 'Privacybescherming: data voor daadkracht', *Computerrecht* 27 (2008).

7. Spanningsveld veiligheid - privacy

- Custers, B., 'Privacy en risicoprofilering bij keteninformatisering' in: Grijpink, J.A.H.M. (red.), *Geboeid door ketens. Samen werken aan keteninformatisering* (Voorburg 2007) 181-190.
- Gerding, R.J., 'De meekijkende maatschappij', *Privacy & informatie*, 2 (2007) 57-63.
- Harten, D.W. v., 'Privacy en veiligheid in een informatiesamenleving', *Privacy & informatie*, 1 (2003), 11-14.
- Holvast, J., Merkus, S. en Michels, G., 'De staat van de privacybescherming van de burger', *Privacy & informatie*, 6 (2006) 262-269.
- Holvast, J., Michels, G. e Schoonhoven, J.P. v., 'De staat van de privacybescherming van de burger 2005-2006', *Privacy & informatie*, 6 (2004) 242-249.
- Jacobs, B., 'Select before you collect', *Ars Aequi,* 54 (2005) 1006-1009.
- Koning, B. de, *Alles onder controle. De overheid houdt u in de gaten* (Amsterdam 2008).
- Vedder, A., Wees, L. v.d. en Koops, B-J., 'Big Brother's bevoegdheden zijn er - nu hij zelf nog?' *NJB*, 41 (17 november 2006) 2356-2360.
- Vedder, A., Wees, L. v.d., Koops, B.-J. en Hert, P. de, *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw* (Den Haag: Rathenau Instituut, 2007).
- www.bof.nl – site van Bits for Freedom.
- www.burojansen.nl – site van Buro Jansen.

8. Privacybescherming en archiveringssysteem, 9. Kwaliteit, metadata en context en 10. Toegangsbeveiliging: technische en organisatorische maatregelen

- Boven, M.W. v., Kramer, R. en Noordam, C.G.M.,*'De Archiefwet 1995 in 100 trefwoorden* (Den Haag. 2003).
- Horsman, P., 'Archiefsystemen en kwaliteit' in: Horsman, P., Ketelaar F.C.J. en Thomassen, T.H.P.M., *Naar een nieuw paradigma in de archivistiek* ('s Gravenhage 1999) 85-105.
- Horsman, P., *Kwaliteit van documenten*. Discussiestuk Archiefschool. Versie 2.1. (2005).
- Horsman, P., Waalwijk, H. en Bussel, G-J. v., *Metadatamodel. Beschrijving van entiteiten en attributen*. Versie 3.1. (Archiefschool, 6 juni 2002).
- *ISO 23081-1. Metadata for records. Part 1: Principles* (2004).
- Kuitenbrouwer, F., 'AIVD mag stofzuigeren naar persoonsgegevens', *Netkwesties*, Digitaal magazine over maatschappij en internet (28 oktober 2008) .
- *NEN 2082, eisen voor functionaliteit van informatie- en archiefmanagement in programmatuur* (ontwerp) (Delft, juni 2007).
- *NEN-ISO 15489-1 (nl) Informatie- en archiefmanagement. Deel 1: Algemeen* (november 2001).
- *NEN-ISO/TR 15489-2 (nl). Archiefbeheer. Deel 2: Richtlijnen* (november 2001).
- Poppe, J., 'Metadata: ISO 23081 en andere standaarden (1) en (2)', *Od* 9 (2006) 20-21 en *Od* 10 (2006) 18-20.
- Thomassen, T. 'De veelvormigheid van de archiefontsluiting en de illusie van de toegankelijkheid' in: Thomassen, T., Looper, B. en Kloosterman, J. (red.), *Toegang. Ontwikkelingen in de ontsluiting van archieven* ('s Gravenhage 2001) 13-43.

10.2. PET of PEM?

- Borking, J.J., 'Privacy Enhancing Technologies: het Derde Spoor. Een terugblik', *Privacy & informatie*, 5 (2002) 196-202.
- Borking, J.J. en Koorn, R.F., 'Witboek 'Privacy Enhancing Technologies voor beslissers'', *Privacy & informatie*, 5 (2005) 202-207.
- Gerding, R.J., 'De meekijkende maatschappij', *Privacy & informatie*, 2 (2007), 57-63.
- Horst, R.J.M. v.d.,'To PET or not to PET...', *Privacy & informatie*, 4 (2003) 160-164.
- Lieshout, M. v., 'Privacy Enhancing Technologies: een zaak van lange adem', *Privacy & informatie*, 5 (2002) 203-209.
- *Privacy Enhancing Technologies. Witboek voor beslissers*. KPMG rapport i.o.v. Ministerie van BZK (december 2004).

10.3. Keteninformatisering

- As, A. v., *Praktische keteninformatisering* (maart 2006).
- *Gewaardeerd verleden. Bouwstenen voor een nieuwe waarderingsmethodiek voor archieven*. Rapport van de Commissie Waardering en Selectie (september 2007).
- Grijpink, J.A.H.M. (red.), *Geboeid door ketens. Samen werken aan keteninformatisering* (Voorburg 2007). Hierin met name de volgende bijdragen:
    - Grijpink, J. 'Het leerstuk Keteninformatisering in vogelvlucht', 9-27;
    - Breemen, D. v., 'Keteninformatisering in het perspectief van de vakliteratuur', 29-37;
    - Dommisse, B., 'Samenwerken in ketens in de publieke sector', 51-58;
    - Kouwenhoven, R. en Stuive, K., 'Keteninformatisering rond terrorismebestrijding', 71-90;
    - Berkelaar, T., 'Strategieën voor de ontwikkeling van een ICT-infrastructuur voor de overheid', 141-151;

- Breemen, D. v., 'Keteninformatisering, breder toepasbaar dan je zou denken', 153-167.
- Grijpink, J.A.H.M., 'ICT, Spelbederver of Dwarsligger?' in: Valstar A. en Genuchten, M. v., (red.), *Liber Amicorum T.M. Bemelmans* (Eindhoven 2004*).*
- Grijpink, J.A.H.M., 'Persoonsnummers en privacy (1)', *Privacy & informatie*, 2 (2002) 52-56.
- Grijpink, J.A.H.M., 'Persoonsnummers en privacy (2), *Privacy & informatie*, 3 (2002) 100-105.
- Grijpink, J.A.H.M., 'Onze informatiesamenleving in wording. De uitdaging van grootschalige informatie-uitwisseling in de rechtstaat', Rede uitgesproken bij de aanvaarding van het ambt van bijzonder hoogleraar Keteninformatisering in de rechtstaat (Voorburg/Den Haag 2005).
- *NORA, Nederlandse Overheid Referentie Architectuur. Samenhang en samenwerking binnen de elektronische overheid*. ICTU, versie 1 (27 september 2006).
- *Ruimte voor regie. Handreiking voor ketenregie in het openbaar bestuur* (Den Haag: Ministerie van BZK, 2003).
- www.keteninformatiserng.nl.
- www.ketens-netwerken.nl.

Bijlage I: Organisatie terrorismebestrijding

- Instellingsregeling NCTb/Regeling van de Ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties van 29 juni 2005, nr. DDS5357209, houdende instelling van de Nationaal Coördinator Terrorismebestrijding.
- Instellingsbesluit Gezamenlijk Comité Terrorismebestrijding (GCT), nr. 5272172/504/PW, 15 juli 2004.

Bekke, A.J.G.M. en Vries, J. de, *U bent herkend. Aantreden en optreden van de Nationaal Coördinator Terrorismebestrijding*. Rapport evaluatie NCTb (Apeldoorn/Leiden 2007).
- www.nctb.nl – site van de Nationaal Coördinator Terrorismebestrijding.

Bijlage III: Rapport Commissie Mevis

- CBP, *Advies Rapport Commissie Strafvorderlijke gegevensvergaring*, Brief aan de Minister van Justitie (18 oktober 2001).
- Gegevensgaring in stafvordering. Brief van de Minister van Justitie met kabinetsstandpunt over rapport Mevis, TK 2001-2002, 28 366, nr. 1.
- *Gegevensgaring in strafvordering. Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek*. Rapport van de Commissie Strafvorderlijke gegevensgaring in de informatiemaatschappij (Commissie Mevis) (mei 2001).

Bijlage IV: Wet Justitiële en strafvorderlijke gegevens - Wjsg

- 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 en strafvorderlijke gegevens), Stb, 7 november 2002, 552.
- Wijziging van de Wet justitiële gegevens in verband met het verwerken van strafvorderlijke gegevens, Memorie van Toelichting, TK, 2002-2003, 28886, nr. 3.

-CBP, Wet justitiële strafrechtelijke gegevens. Brief aan de Vaste commissie voor Justitie van de Tweede Kamer, 13 oktober 2003.

BIJLAGE I: ORGANISATIE TERRORISMEBESTRIJDING

In Nederland is een twintigtal instanties betrokken bij terrorismebestrijding. Deze bijlage geeft een overzicht van de belangrijkste actoren in deze strijd.

Nationaal Coördinator Terrorismebestrijding (NCTb)

Om de samenwerking tussen de bij terrorismebestrijding betrokken instanties te verbeteren, is op 23 april 2004 de Nationaal Coördinator Terrorismebestrijding (NCTb) aangesteld. De NCTb is onder gezamenlijke verantwoordelijkheid van de Ministers van Justitie (tevens coördinerend minister voor terrorismebestrijding**)** en van Binnenlandse Zaken en Koninkrijksrelaties (BZK) belast met de voorbereiding en uitvoering van het beleid inzake terrorismebestrijding en met bewakings- en beveiligingstaken ter voorkoming van onder meer terroristische aanslagen. Organisatorisch en beheersmatig is de NCTb ondergebracht bij het ministerie van Justitie.[212]

De NCTb bestaat uit een aantal afdelingen of directies. Zo verzamelt, combineert en veredelt de Directie Kennis en Analyse informatie over radicalisering en terrorisme, afkomstig van bestuurlijke en wetenschappelijke bronnen en van inlichtingenverschaffende diensten, ten behoeve van integrale analyses en dreigingsbeelden met betrekking tot terrorisme. Op basis hiervan ontwikkelt de Directie Beleid en Strategie beleid op het vlak van terrorismebestrijding, waaronder strategische en internationale beleidsontwikkeling en communicatiestrategie.

Politieke en beleidsmatige afstemming

Politieke afstemming rond veiligheidskwesties en terrorismebestrijding vindt plaats in de Raad voor de Nationale Veiligheid (RNV)[213], onder leiding van de minister-president. Hierin overleggen de meest betrokken bewindspersonen op het terrein van terrorismebestrijding en inlichtingen- en veiligheidsdiensten met elkaar.

Het overleg in de RNV wordt voorbereid door het Gezamenlijk Comité Terrorismebestrijding (GCT). Het GCT is in juni 2004 ingesteld ter ondersteuning van de Minister van Justitie in de invulling van zijn coördinerende taak inzake terrorismebestrijding en vormt op hoog ambtelijk niveau de schakel tussen regeringsbeleid en uitvoering. In het GCT zijn de bij terrorismebestrijding betrokken ministeries en overheids-/inlichtingendiensten vertegenwoordigd.[214] Als voorzitter fungeert de Nationaal Coördinator Terrorismebestrijding (NCTb), die in deze hoedanigheid rapporteert aan de minister van Justitie en de minister van BZK. De staf van het NCTb verzorgt tevens het secretariaat van het GCT.

---

[212] Instellingsregeling NCTb/Regeling van de Ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties van 29 juni 2005, nr. DDS5357209, houdende instelling van de Nationaal Coördinator Terrorismebestrijding.

[213] De Raad voor de Nationale Veiligheid (RNV) is de opvolger van de Raad voor de Inlichtingen- en Veiligheidsdiensten

[214] Het GCT is samengesteld uit de NCTb (voorzitter), directeur-generaal Rechtshandhaving van het ministerie van Justitie, directeur-generaal Openbare Orde en Veiligheid van het ministerie van BZK, de voorzitter van het College van Procureurs-generaal, de korpschef van het KLPD, het plaatsvervangend hoofd van de AIVD - ministerie van BZK, de plaatsvervangend directeur van de MIVD - ministerie van Defensie, de bevelhebber van de Koninklijke Marechaussee, de raadsadviseur (plaatsvervangend coördinator van de inlichtingen- en veiligheidsdiensten van het ministerie van Algemene Zaken, de plaatsvervangend thesaurier-generaal van het ministerie van Financiën, het MT-lid Belastingdienst, de directeur-generaal Politieke Zaken van het ministerie van Buitenlandse Zaken, de directeur-generaal Internationale Aangelegenheden en Vreemdelingenzaken van het ministerie van Justitie, de directeur Juridische Zaken van het ministerie van Defensie en de directeur van de directie Wetgeving van het ministerie van Justitie (Instellingsbesluit Gezamenlijk Comité Terrorismebestrijding (GCT), nr. 5272172/504/PW, 15 juni 2004, artikel 3).

Uitvoerende organisaties

Om de schakelfunctie tussen beleid en uitvoering goed te kunnen uitvoeren, wordt het op strategie en beleid gerichte GCT ondersteund door het meer operationeel getinte Coördinerend Overleg Terrorismebestrijding (COTB), waarin de *uitvoerende* organisaties op het terrein van de terrorismebestrijding zijn vertegenwoordigd.[215] De voorzitter van de COTB is de directeur Opsporingsbeleid van het Ministerie van Justitie; het secretariaat wordt gevoerd door de AIVD. De secretaris van het CGT neemt deel in het COTB. De taken van het COTB zijn onder meer het verstrekken van informatie aan het GCT over ontwikkelingen, aandachtspunten en probleemgebieden uit de dagelijkse praktijk, het opstellen van een gemeenschappelijke analyse van de terroristische dreiging en de verantwoordelijkheden van de verschillende COTB-leden hierbij, en het zorgdragen voor uitvoering van besluiten van het GCT.

De uitvoerende, operationele taken in de bestrijding van terrorisme worden in hoofdzaak uitgevoerd door opsporingsdiensten van politie en justitie (waaronder de politieorganisaties, het OM en de FIOD) en de inlichtingen- en veiligheidsdiensten (waaronder de AIVD).

[215] In het COTB zijn de volgende organisaties vertegenwoordigd: AIVD, MIVD, KLPD, OM, FIOD/ECD, Douane, Kmar, IND en de Nationaal Coördinator Bewaking en Beveiliging (Instellingsbesluit GCT, artikel 9).

BIJLAGE II: ARTIKEL 8 EVRM

De belangrijkste Europese verdragsbepaling op het gebied van de informationele privacy bestaat uit artikel 8 van het Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM).

Dit artikel 8 EVRM luidt:
Lid 1: Een ieder heeft recht op respect voor zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie;
Lid 2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of voor de bescherming van de rechten en vrijheden van anderen.

Deze verdragsbepaling heeft voorrang boven nationale voorschriften; indien privacybepalingen in de Grondwet, de Wbp of de sectorale privacywetten niet verenigbaar zijn met het verdrag, dan gelden de bepalingen van de EVRM. Een regeling van een bevoegdheid die een inbreuk kan maken op het recht op bescherming van de persoonlijke levenssfeer dient getoetst te worden aan EVRM, artikel 8, tweede lid, waarin het noodzakelijkheids-, proportionaliteits- en subsidiariteitsbeginsel een belangrijke rol spelen. Artikel 8 EVRM en de daarop gebaseerde jurisprudentie stellen ook eisen aan de kwaliteit van wettelijke regelingen die een inmenging in het privacyrecht met zich meebrengen. Deze houden in dat de regeling voor de burger voldoende toegankelijk en voorzienbaar moet zijn en dat de regeling waarborgen moet bieden tegen willekeurige inmenging van de overheid.[216]

Opvallend bij de in de volgende hoofdstukken te bespreken antiterrorismewetgeving met betrekking tot gegevensverwerking is dat de maatregelen volgens de regering allemaal de 'EVRM-artikel 8-toets' kunnen doorstaan, terwijl bij de bedenkingen die - onder andere door het CBP- tegen de maatregelen worden geuit juist hetzelfde artikel wordt aangevoerd.[217] Het artikel laat derhalve veel ruimte voor uiteenlopende interpretaties...

[216] Wbp, MvT, 7-8; Ketelaar en Noordam, *Archiefrecht*, 75.
[217] Raadplege hiervoor de verschillende MvT's van de in de besproken wetten en de erop betrekking hebbende CBP-adviezen.

BIJLAGE III: RAPPORT COMMISSIE MEVIS

Veel van de wetgeving inzake het verkrijgen van bij derden berustende gegevens die na de millenniumwisseling is doorgevoerd, waaronder de in de paper besproken Wet vorderen gegevens telecommunicatie en Wet bevoegdheden vorderen gegevens, is terug te voeren op een in 2001uitgebracht rapport van de Commissie Strafvorderlijke gegevensgaring in de informatiemaatschappij (de zogenaamde Commissie Mevis).[218]

Bevindingen rapport Commissie Mevis

In het rapport concludeerde de commissie dat het Wetboek van Strafvordering, gelet op de ontwikkelingen op het gebied van de ICT, niet meer voorzag in een toereikend wettelijk kader voor die vormen van gegevensvergaring die voor de strafvordering noodzakelijk zouden zijn.[219] Het was volgens de commissie ongewenst dat de praktijk van strafvorderlijke gegevensgaring ten dele gebaseerd was op de *vrijwillige* medewerking van diegenen die toegang hadden tot voor de strafvordering relevante gegevens. De commissie stelde voor de bevoegdheden binnen het Wetboek van Strafvordering zodanig aan te passen, dat de strafvorderlijke autoriteit geautomatiseerde gegevens van zowel verdachte als onverdachte personen zou kunnen *vorderen* en dat degene tot wie de vordering zich richtte (in potentie alle maatschappelijke sectoren), *verplicht* zou zijn deze te verstrekken. Bij deze informatieverplichting was het de strafvorderlijke autoriteit die de afweging moest maken of de gegevensverstrekking noodzakelijk was ten behoeve van het onderzoek.[220]

Bij deze vordering zouden van de houder van de gegevens handelingen kunnen worden gevraagd met betrekking tot zowel *historische* als *toekomstige* gegevens. Met toekomstige gegevens bedoelt de commissie 'gegevens die op het moment van de vordering nog niet bestaan en pas na het tijdstip van vordering zullen ontstaan en voor het eerst worden bewerkt'. Historische gegevens zijn op het moment van vordering al wel aanwezig bij de houder.[221] De gevraagde handelingen zouden kunnen variëren van het enkele verstrekken tot het *bewerken, bewaren of verwerven.*[222]

Met betrekking tot de gegevens onderscheidde de commissie een drietal categorieën ('identificerende gegevens', 'andere gegevens' en 'gevoelige -bijzondere- gegevens'), die bepalend waren voor de mate van inbreuk op de persoonlijke levenssfeer en de mate van belasting van een vordering voor de houder/verantwoordelijke van de gegevens.[223]

Reactie CBP

Het CBP reageerde erg kritisch op het rapport. De gegevensverwerking zou veelal buiten de betrokkenen om plaatsvinden. Het opsporingsbelang zou te zeer benadrukt worden ten koste van het belang van de bescherming van de persoonlijke levenssfeer, vooral waar het ging om gegevensverwerking van onverdachte personen. De toekenning van de bevoegdheid tot het bevelen van een bewerking van gegevens door

---

[218] *Gegevensgaring in strafvordering. Nieuwe bevoegdheden tot het vorderen van gegevens ten behoeve van strafvorderlijk onderzoek*. Rapport van de Commissie Strafvorderlijke gegevensgaring in de informatiemaatschappij (Commissie Mevis) (mei 2001). Voor een samenvatting van de voorstellen, zie: ibidem, 1-12.

[219] Ibidem, 6.

[220] De Wbp schrijft in artikel 8 voor dat gegevensverwerking onder meer toelaatbaar is als de verwerking noodzakelijk is om aan een *wettelijke verplichting* te voldoen (zie hoofdstuk 2). Indien er geen sprake is van een wettelijke verplichting tot verstrekking (en verstrekking *vrijwillig* plaatsvindt op verzoek), dient de houder/verantwoordelijke te beslissen over de noodzakelijkheid van de verstrekking en een belangenafweging in deze te maken. De houder/verantwoordelijke is dan jegens de betrokkene tevens aansprakelijk, indien deze door een eventuele onrechtmatige verstrekking schade ondervindt.

[221] *Gegevensgaring in strafvordering*, 64.

[222] Ibidem, 8. Vgl. noot 55.

[223] Ibidem.

de verantwoordelijke leidde volgens het CBP tot 'een ongerechtvaardigde aantasting' van het recht op eerbiediging van de persoonlijke levenssfeer. Deze bevoegdheid zou impliceren dat aan welk(e) bedrijf of overheidsinstelling dan ook de verplichting zou kunnen worden opgelegd als verlengde arm van justitie of politie te fungeren, door zelf opsporingshandelingen te verrichten. Elke onderbouwing van de legitimatie hiervoor zou ontbreken.[224]

[224] CBP, *Advies Rapport Commissie Strafvorderlijke gegevensvergaring*, Brief aan de Minister van Justitie, (18 oktober 2001) 1, 2, 10.

BIJLAGE IV: WET JUSTITIËLE EN STRAFVORDERLIJKE GEGEVENS - WJSG

De in september 2004 in werking getreden Wet justitiële en strafvorderlijke gegevens (Wjsg)[225] bevat onder meer bepalingen omtrent de bewerkingstermijnen en verstrekkingsregime van justitiële en strafvorderlijke gegevens en omschrijft de rechten van de betrokkenen op kennisneming en verbetering. Daarnaast regelt de wet de afgiften van verklaringen omtrent het gedrag. De Wjsg is aanvullend op de Wbp. Toezichthoudend orgaan is het CBP.

De wet regelt het in justitiële documentatie verwerken van justitiële gegevens in verband met de strafrechtpleging. Het bepaalt welke justitiële gegevens mogen worden verwerkt, welke normen daarbij gelden, wanneer de gegevens uit de documentatie moeten worden verwijderd, aan wie gegevens mogen worden verstrekt en wat de rechten van betrokkenen zijn.

Behalve de verwerking van justitiële gegevens regelt de wet ook de verwerking van strafvorderlijke gegevens door het OM. Het College van procureurs-generaal is verantwoordelijk voor de verwerking van strafvorderlijke gegevens en ziet erop toe dat de gegevens rechtmatig zijn verkregen en binnen de daarvoor geldende termijnen worden verwijderd. Door het periodiek laten uitvoeren van een *audit* kan het College toezicht houden op de kwaliteit van de gegevens.[226]

Strafvorderlijke gegevens mogen worden verwerkt indien dit noodzakelijk is voor een goede invulling van de taak van het OM (doelbinding) of voor het nakomen van een wettelijke verplichting. Verstrekking van de gegevens voor zowel binnen als buiten de strafrechtspleging gelegen doeleinden is mogelijk indien dit 'noodzakelijk' is met het oog op 'een zwaarwegend algemeen belang'. De gegevens mogen niet langer worden bewaard dan noodzakelijk is voor het opsporen en vervolgen van strafbare feiten; de termijnen voor het bewaren, verwijderen en vernietigen zijn gedifferentieerd.[227]

[225] Wet van 7 november 2002 tot wijziging van de regels betreffende de verwerking van justitiële gegevens (Wet justitiële en strafvorderlijke gegevens), Stb. 2002, 552.
[226] Wijziging van de Wet justitiële gegevens in verband met het verwerken van strafvorderlijke gegevens, Memorie van Toelichting, TK 2002-2003, 28886, nr. 3, p. 13.
[227] Ibidem, 3-13. Verwijdering betekent in de Wjsg niet dat de strafvorderlijke gegevens direct vernietigd moeten worden, maar dat de gegevens niet meer voor operationele doeleinden mogen worden gebruikt; ze kunnen na verwijdering wel worden gearchiveerd.

BIJLAGE V: OVERZICHT WETGEVING BEVOEGDHEDEN GEGEVENSVERZAMELING EN –BEWERKING OPSPORINGS- EN VEILIGHEIDSDIENSTEN

Gebaseerd op: Vedder, A., Wees, L. v.d. en Koops, B-J., 'Big Brother's bevoegdheden zijn er - nu hij zelf nog?' *NJB*, 41 (17 november 2006) 2356-2360.

- *Wet computercriminaliteit* (1993): aftappen faxen en computernetwerken;
- *DNA-onderzoek bij misdrijven* (1994, 2001, 2003, 2004): geleidelijke en gefaseerde uitbreiding toepassingsmogelijkheden DNA-onderzoek, aanleggen en vullen DNA-databank;
- *Wet mobiele telecommunicatie* (1994), *Wet aftappen van GSM* (1995), *Telecommunicatiewet* (1998): gefaseerd doorgevoerde verplichtingen tot aftapbaarheid van telecommunicatie en meewerkplichten voor telecom-aanbieders;
- *Wet Bijzondere Opsporingsbevoegdheden (BOB)* (2000): stelselmatige observatie, infiltratie, pseudo-koop, inkijken, gebruik van infiltranten, direct afluisteren, tappen en verkennend onderzoek;
- *Wet op de inlichtingen- en veiligheidsdiensten* (2002): hacken, aftappen van elke vorm van communicatie, ongericht opnemen van draadloze communicatie, opvragen verkeersgegevens, kraken van versleuteling, opvragen van gegevens, observatie, inkijken, inbreken;
- *Wet EU-rechtshulp* (2004): grensoverschrijdend aftappen;
- *Wet justitiële en strafvorderlijke gegevens* (2004);
- *Wetten vorderen gegevens*: *financiële sector* (2004), *telecommunicatie* (2004) en *algemeen* (2005): uitbreiding bevoegdheden om alle soorten opgeslagen en toekomstige gegevens te vorderen, bevriezing van gegevens, bewaarplicht verkeersgegevens mobiele telecommunicatie;
- *Verruiming mogelijkheden tot opsporing en vervolging van terroristische misdrijven* (2006)
- *Biometrisch paspoort* (2006): (vanaf 1999 voorbereid) paspoort met chip met biometrische gegevens;
- *Wet computercriminaliteit II* (2006): aftappen besloten netwerken, ontoegankelijk maken van gegevens;
- *Wet politiegegevens* (2007);
- *Wet op BurgerServiceNummer* (2007);
- *Wet bewaarplicht telecommunicatiegegevens* (in voorbereiding, in mei 2008 door Tweede Kamer aangenomen)
- *Bevoegdheden veiligheidsdiensten* tot vorderen gegevens bij derden en koppelen gegevens (in voorbereiding);
- *Centrale databank biometrische gegevens* (in voorbereiding)

BIJLAGE VI: GEBRUIKTE AFKORTINGEN

Organisaties

AIVD	Algemene Inlichtingen- en Veiligheidsdienst (voorheen: BVD - Binnenlandse Veiligheidsdienst) van het Ministerie van BZK
BVD	Binnenlandse Veiligheidsdienst (tegenwoordig: AIVD)
CBP	College Bescherming Persoonsgegevens
CIOT	Centraal Informatiepunt Onderzoek Telecommunicatie
COTB	Coördinerend Overleg Terrorismebestrijding
CT-Infobox	Contra Terrorisme Infobox
CTIVD	Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten
ECD	Economische Controledienst
FIOD	Fiscale Inlichtingen en Opsporingsdienst
FIU-NL	Financial Intelligence Unit Nederland (onderdeel van het KLPD)
GCT	Gezamenlijk Comité Terrorismebestrijding
IND	Immigratie- en Naturalisatiedienst
KLPD	Korps Landelijke Politiediensten
Kmar	Koninklijke Marechaussee
MID	Militaire Inlichtingendienst (tegenwoordig: MIVD)
Ministerie van BZK	Ministerie van Binnenlandse Zaken en Koninkrijkrelaties
MIVD	Militaire Inlichting- en Veiligheidsdienst (voorheen: MID) van het Ministerie van Defensie
NCTb	Nationaal Coördinator Terrorismebestrijding
OM	Openbaar Ministerie
RID	Regionale Inlichtingen Dienst - Wiv art. 60-ambtenaren
RNV	Raad voor de Nationale Veiligheid

Wetgeving

SV	Wetboek van Strafvordering
Tw	Telecommunicatiewet
Wbp	Wet bescherming persoonsgegevens
Wbvg	Wet bevoegdheden vorderen gegevens
Wet BOB	Wet bijzondere opsporingsbevoegdheden
Wgba	Wet gemeenschappelijke basisadministratie persoonsgegevens
WGBO	Wet geneeskundige behandelingsovereenkomst
Wiv 2002	Wet inlichtingen- en veiligheidsdiensten 2002
Wjsv	Wet justitiële en strafvorderlijke gegevens
Wpolg	Wet politiegegevens
Wpolr	Wet politieregisters
Wvgt	Wet vorderen gegevens telecommunicatie
Wvm	Wet verruiming mogelijkheden tot opsporing en vervolging van terroristische misdrijven