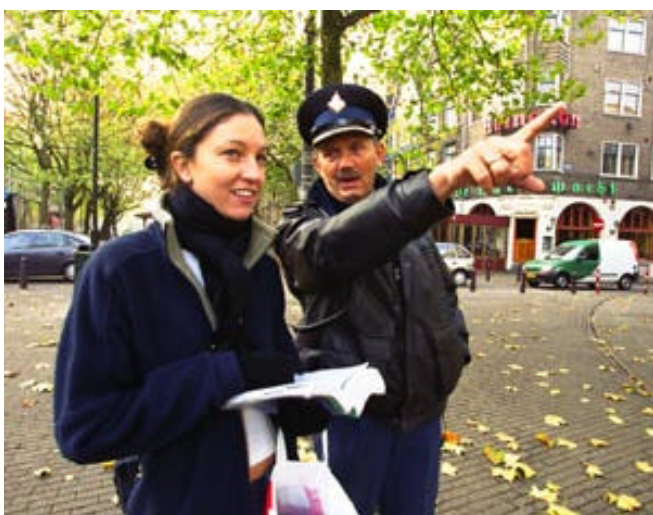


ONDERZOEK TELEWERKEN

# BZK POLITIE

Deelrapport 2:  
Juridische aspecten



Auteur: mr. Y Middelkoop  
Ref: g:../BZK Politie/Stap 2 Juridische aspecten/Juridische aspecten definitief.doc  
Uitgave: 17 juni 2002

# Inhoudsopgave

Inhoudsopgave .....	2
0 Samenvatting.....	4
1 Inleiding.....	5
2 Literatuur en wetgeving .....	6
2.1 Algemeen .....	6
2.2 Specifiek – sector politie .....	6
3 Werkwijze onderzoek .....	7
3.1 Selectie wet- en regelgeving .....	7
3.2 Resultaten onderzoek .....	7
4 Matrix met onderzoeksresultaten .....	8
5 Toelichting op de resultatenmatrix .....	9
5.1 Nederlandse wet- en regelgeving .....	9
Arbeidsrechtelijke en arbeidsvoorwaardelijke aspecten .....	9
5.1.1 Arbeidsomstandighedenwet 1998 (Arbo-wet) .....	9
5.1.2 Arbeidsomstandighedenbesluit (Arbobesluit).....	9
5.1.3 Arbeidstijdenwet.....	9
5.1.4 Besluit Algemene Rechtspositie Politie (Barp).....	10
5.2 Nederlandse wet- en regelgeving, overige juridische aspecten .....	11
5.2.1 Archiefwet 1995.....	11
5.2.2 Besluit wijzigingen i.v.m. het antecedentenonderzoek voor de politie .....	11
5.2.3 Politiewet 1993.....	11
5.2.4 Regeling informatiebeveiliging politie.....	11
5.2.5 Wet bescherming persoonsgegevens.....	12
5.2.6 Wet bescherming staatsgeheimen 1951 .....	12
5.2.7 Voorstel van Wet Computercriminaliteit II .....	12
5.2.8 Wet op de inlichtingen en veiligheidsdiensten.....	12
5.2.9 Wet justitiële gegevens.....	12
5.2.10 Wet op de veiligheidsonderzoeken.....	13
5.2.11 Wet politieregisters.....	13
5.2.12 Besluit politieregisters.....	13
5.2.13 CID regeling 1995.....	13
5.3 Europese regelgeving telewerken, arbeidsrechtelijke en arbeidsvoorwaardelijke aspecten.....	13
5.4 Europese regelgeving telewerken, overige juridische aspecten .....	14
5.4.1 Europol Overeenkomst .....	14
5.4.2 Europol geheime informatie.....	14
5.5 Jurisprudentie.....	15
6 Interviews.....	16
6.1 Inleiding.....	16
6.2 Uitgangsdokument interviews.....	16
6.3 Resultaten interviews.....	17
6.3.1 Hoofdofficier van justitie - Utrecht .....	17
6.3.2 Hoofdofficier van justitie - Groningen.....	18
6.3.3 Hoofd bedrijfsvoering - 's-Hertogenbosch.....	19
6.3.4 Hoofd bedrijfsvoering – Amsterdam.....	20

7	Conclusies en aanbevelingen.....	23
7.1	Deelconclusies .....	23
7.1.1	Algemeen.....	23
7.1.2	Arbeidsrechtelijk / arbeidsvoorwaardelijk.....	23
7.1.3	Overig juridisch .....	23
7.1.4	Interviews .....	24
7.2	Eindconclusie.....	25
7.3	Aanbevelingen .....	25
	BIJLAGE .....	27
	Telewerken politie: relevante wet- en regelgeving.....	27

## 0 Samenvatting

In het juridische deel van het onderzoek is gekeken naar de juridische (on)mogelijkheden van telewerken bij de sector politie. De literatuur op het gebied van de juridische aspecten van telewerken, met uitzondering van het arbeidsrecht, is zeer beperkt. In wet- en/of regelgeving wordt vrijwel nog niet ingegaan op deze specifieke werksituatie. Buiten de juridische aspecten van telewerken in het algemeen is in het kader van dit onderzoek specifiek gekeken naar de telewerkmogelijkheden binnen de sector politie in verband met haar takenpakket en haar positie in de maatschappij.

Voor het onderzoek naar de (on)mogelijkheden van telewerken bij de sector politie is gebruik gemaakt van een lijst met relevante wet- en regelgeving. Deze lijst is na meerdere selecties tot stand gekomen, de wet- en regelgeving is vervolgens gedetailleerd onderzocht. De resultaten zijn in een matrix verwerkt.

Op het gebied van arbeidsrechtelijke en arbeidsvoorwaardelijke aspecten (Nederlandse wetgeving) levert de onderzochte wet- en regelgeving over het algemeen een positieve bijdrage aan de haalbaarheid van de invoering van telewerken bij de sector politie. De Arbeidsomstandighedenwet 1998 brengt knelpunten met zich mee, vanwege het feit dat verplichtingen veelal moeilijker te realiseren zijn in een situatie van telewerken. De overige Nederlandse wet- en regelgeving levert zowel een aantal haalbaarheidsaspecten als een aantal knelpunten op. Een aantal onderzochte wetten levert noch knelpunten, noch haalbaarheidsaspecten op, maar bevat wel bepalingen waar rekening mee gehouden moet worden, het resultaat luidt dan "aandachtspunt". De knelpunten komen met name voort uit wetten betreffende speciale diensten, functies en gegevens (veiligheidsdienst/CID/politieregister).

Op Europees niveau is de relevante wet- en regelgeving beperkt. Op arbeidsrechtelijk en arbeidsvoorwaardelijk gebied zijn er *algemene beginselen voor de vaststelling van een kader voor telewerken*. Wat betreft de overige wet- en regelgeving komen knelpunten voort uit de aard van de te verwerken gegevens en de beveiliging daarvan. Jurisprudentie is niet voorhanden.

De uit de interviews verkregen meningen over de invoering van telewerken bij de sector politie zijn op bepaalde punten gelijklopend en op andere punten divers. De geïnterviewden zijn bijvoorbeeld allen van mening dat telewerken bij de sector politie in deze tijd wenselijk en acceptabel is. Over welke functies in aanmerking moeten komen voor telewerken bestaan uiteenlopende meningen. Regelgeving moet er komen, vinden alle geïnterviewden, maar over de vorm waarin (wet of regeling/richtlijn) zijn de meningen verdeeld. Beveiliging en integriteit zijn items die in alle gesprekken veelvuldig aan de orde kwamen.

De eindconclusie van het onderzoek is dat de invoering van telewerken bij de sector politie in principe haalbaar is. De knelpunten, die voornamelijk worden gevormd door de grotere complexiteit van beveiliging bij telewerken en de verplichtingen in de Arbo-wet, zijn met de nodige inspanning op te lossen.

# 1 Inleiding

In deze rapportage zijn de resultaten van het onderzoek naar de juridische (on)mogelijkheden van telewerken bij de sector politie opgenomen. In hoofdstuk 2 is kort ingegaan op hetgeen op juridisch gebied over telewerken in de literatuur en wetgeving te vinden is. Hoofdstuk 3 bevat een beschrijving van de wijze waarop het onderzoek is verricht en de resultaten zijn verwerkt. In hoofdstuk 4 is een matrix met onderzoeksresultaten opgenomen. De resultaten zijn vervolgens uitgebreid toegelicht in hoofdstuk 5. Hoofdstuk 6 bevat de resultaten van de gehouden interviews. Tot slot zijn in hoofdstuk 7 conclusies en aanbevelingen opgenomen.

## **2 Literatuur en wetgeving**

### **2.1 Algemeen**

Hoewel telewerken de laatste jaren meer en meer een veel besproken en beschreven onderwerp is, blijft de literatuur op het gebied van de juridische aspecten van telewerken ver achter. Eén van de redenen daarvoor is dat nog maar in weinig wet- en/of regelgeving wordt ingegaan op deze specifieke werksituatie. De vraag die daarbij direct gesteld moet worden is, of het wenselijk is om telewerken als bijzondere situatie te beschouwen, waarop aparte wet- en/of regelgeving van toepassing zou moeten zijn. In veel gevallen zal het antwoord “nee” zijn, omdat met name veel procedures, rechten en verplichtingen, die volgen uit wet- en regelgeving, in een telewerksituatie hetzelfde zullen en moeten zijn als in een ‘gewone’ situatie. Wel is het een feit dat voor het nakomen van bepaalde verplichtingen in een telewerksituatie meer inspanning vereist zal zijn.

In tegenstelling tot het gros van wet- en regelgeving is het arbeidsrecht wel een veel besproken item in het kader van telewerken. Met name ter bescherming van de werknemer wordt telewerken als aparte situatie beschouwd, waarvoor ook specifieke regels gelden.

### **2.2 Specifiek – sector politie**

Buiten de juridische aspecten van telewerken in het algemeen is in het kader van dit onderzoek specifiek gekeken naar de telewerkmogelijkheden binnen de sector politie. Want waar er in de meeste bedrijfstakken, branches, beroepen, etc. geen juridische c.q. wettelijke problemen bestaan voor het invoeren van telewerken, zouden er voor de sector politie toch knelpunten kunnen zijn in verband met het takenpakket en de positie in de maatschappij.

## **3 Werkwijze onderzoek**

### **3.1 Selectie wet- en regelgeving**

Voor het onderzoek naar de (on)mogelijkheden van telewerken bij de sector politie is gebruik gemaakt van een lijst met relevante wet- en regelgeving. Deze lijst is als volgt tot stand gekomen:

#### Grove selectie van Nederlandse wetgeving

Lijsten met honderden wetten zijn nagelopen en selectie heeft plaatsgevonden op basis van ervaring, kennis en het gebruiken van zoekopdrachten.

Scannen geselecteerde Nederlandse wetgeving, tweede selectie. Het scannen is gebeurd door middel van het lezen van de wetten of bij omvangrijke wetten onder meer via zoekopdrachten. Bij deze selectie vielen met name wetten af waarin procedures beschreven stonden. De locatie van waaruit werkzaamheden worden verricht is dan niet van belang.

#### Selectie Europese wetgeving

Selectie heeft plaatsgevonden volgens het principe van sub 1 en 2.

Gedetailleerd onderzoek totale selectie Nederlandse en Europese wetgeving. Onderzoek is verricht door middel van het lezen van de geselecteerde wetten. In deze fase zijn nog enkele wetten afgevallen, die na gehele lezing bleken niet van invloed te zullen zijn op de invoering van telewerken bij de sector politie. In deze fase is tevens (relevante) verwante regelgeving bij de geselecteerde wetgeving toegevoegd aan de lijst. Gedacht moet worden aan Besluiten, Regelingen, Wijzigingen, etc.. De definitieve lijst met wet- en regelgeving is als bijlage opgenomen.

### **3.2 Resultaten onderzoek**

De resultaten die verkregen zijn uit het gedetailleerde onderzoek zijn door middel van plus- en mintekens verwerkt in een matrix. Een plusteken geeft aan dat in de betreffende wet bepalingen aanwezig zijn die bijdragen aan de haalbaarheid van telewerken bij de sector politie. Een minteken geeft aan dat in de betreffende wet bepalingen aanwezig zijn die knelpunten (kunnen) vormen voor telewerken bij de sector politie. De resultaten uit de matrix zijn uitgebreid onderbouwd.

## 4 Matrix met onderzoeksresultaten

De resultaten die in onderstaande matrix zijn opgenomen, geven weer dat in de betreffende wetten of-  
 tewel mogelijke knelpunten oftewel haalbaarheidsaspecten voor het invoeren van telewerken bij de sec-  
 tor politie voorkomen. Het aantal tekens geeft de mate/omvang van knelpunten of haalbaarheid aan.  
 Indien een wet aspecten bevat die geen knelpunt of haalbaarheidsaspect vormen, maar wel van belang  
 zijn, wordt als resultaat "aandachtspunt" vermeld.

Wet- en regelgeving	Haalbaarheid	Knelpunt
Arbeidsomstandighedenwet 1998 (Arbowet)	+	-/- -/- -/-
Arbeidsomstandighedenbesluit (Arbobesluit)	+++	
Arbeidstijdenwet	+	-/-
Besluit Algemene Rechtspositie Politie (Barp)	+++	
Archiefwet 1995	aandachtspunt	
Besluit wijzigingen i.v.m. het antecedentenonderzoek voor de politie	aandachtspunt	
Politiewet 1993	++	
Regeling informatiebeveiliging politie	++	-/-
Wet bescherming persoonsgegevens	aandachtspunt	
Wet bescherming Staatgeheimen 1951	aandachtspunt	
Voorstel Wet Computercriminaliteit II	+	
Wet op de inlichtingen en veiligheidsdiensten		-/- -/-
Wet justitiële gegevens	+	-/-
Wet veiligheidsonderzoeken	aandachtspunt	-/-
Wet politieregisters		-/-
Besluit politieregisters	+	-/- -/-
CID regeling 1995		-/- -/-
Europol overeenkomst	+	-/-
Europol geheime informatie		-/- -/-

## 5 Toelichting op de resultatenmatrix

### 5.1 Nederlandse wet- en regelgeving Arbeidsrechtelijke en arbeidsvoorwaardelijke aspecten

#### 5.1.1 Arbeidsomstandighedenwet 1998 (Arbo-wet)

De Arbeidsomstandighedenwet 1998 bevat dwingend rechtelijke bepalingen oftewel dwingende verplichtingen, hetgeen betekent dat een werkgever en een werknemer zich niet aan die bepalingen/verplichtingen kunnen onttrekken. Het feit dat een werknemer vrijwillig gaat telewerken doet aan de wettelijke verplichtingen niet af.

Op grond van de Arbo-wet moet de werkgever door middel van een arbeidsomstandighedenbeleid zorg dragen voor de arbeidsomstandigheden op de telewerkplek. Daarbij dient aangetekend te worden dat de telewerkplek zich doorgaans in de woning van de telewerker bevindt, aldus buiten de invloedssfeer van de werkgever.

Bij de politie zal een telewerkplek niet per definitie in de woning van de betreffende politiemedewerker gesitueerd zijn. Telewerkplekken zullen zich op diverse locaties bevinden. Het is goed denkbaar dat een telewerkplek mobiel is. De vraag die in dit kader rijst, is of de werkgever bij een mobiele telewerkplek (nog) kan voldoen aan de verplichtingen uit de Arbo-wet. Dit aspect levert een knelpunt op.

Artikel 1 lid 3 sub g Arbo-wet bevat een definitie van "arbeidsplaats": *iedere plaats die in verband met het verrichten van arbeid wordt of pleegt te worden gebruikt.*

De definitie lijkt mobiele telewerkplekken niet uit te sluiten.

In artikel 2 Arbo-wet zijn enkele specifieke arbeidssituaties benoemd die eveneens onder het toepassingsgebied van de wet vallen. In het kader van telewerken bij de politie is sub a relevant. Het betreft "arbeid verricht bij een verkenning- of opsporingsonderzoek....".

Verondersteld mag worden dat verkenning- en opsporingsonderzoek zowel vanaf vaste locaties, maar met name mobiel wordt verricht. Mobiele telewerkplekken doen daarmee hun intrede en vallen onder de werking van de Arbo-wet. Dit aspect draagt bij aan de haalbaarheid.

Ten aanzien van het genoemde knelpunt is de verwachting dat de verplichtingen van de werkgever goed te realiseren zijn bij vaste telewerkplekken, zoals bijvoorbeeld in een woning. Bij mobiele telewerkplekken zal er echter meer vooronderzoek verricht moeten worden en zullen procedures, rechten en verplichtingen eenduidig vastgelegd moeten worden. Indien dit gebeurt in een arbeidsomstandighedenbeleidsplan, wordt daarmee een goede basis voor de uitvoering gelegd.

#### 5.1.2 Arbeidsomstandighedenbesluit (Arbobesluit)

In artikel 1.1 van het Arbobesluit -de lijst met definities- staan onder andere de begrippen 'thuiswerkgever', 'thuiswerker' en 'thuiswerk'. Het besluit erkent telewerken in een woning.

Artikel 1.17 Arbobesluit geeft de politie en brandweer een uitzonderingspositie. Het artikel vermeldt een aantal artikelen van de Arbo-wet die van toepassing zijn, voor zover door de toepassing een goede taakuitoefening door politie en brandweer niet wordt belemmerd.

Afdeling 2 van het Arbobesluit betreft het beeldschermwerk. De bepalingen betreffende beeldschermwerk zijn echter niet van toepassing op zogenoemde draagbare systemen die niet aanhoudend worden gebruikt op een werkplek (artikel 5.8 lid 1 sub c). Dit artikel heeft een positieve werking in het kader van de inrichting van mobiele telewerkplekken.

Het Arbobesluit draagt bij aan de haalbaarheid van telewerken bij de sector politie.

#### 5.1.3 Arbeidstijdenwet

De Arbeidstijdenwet voorziet in flexibele arbeidspatronen en zal derhalve in directe zin geen knelpunt vormen voor telewerken.

Aangezien telewerken buiten de invloedssfeer van de werkgever geschiedt, zal deze geen directe controle op de naleving van arbeids- en rusttijden kunnen uitoefenen. De verantwoordelijkheid voor de naleving komt in eerste instantie op de telewerker zelf te rusten. De werkgever heeft wel de mogelijkheid enige controle uit te oefenen door gebruik te maken van geautomatiseerde toezichtsystemen. Hierbij dient rekening te worden gehouden met de privacy van medewerkers. Telewerken en de daarbij behorende flexibiliteit kan immers leiden tot verstengeling van werksfeer en privé-sfeer. Bij langdurige observatie zouden tevens gegevens uit de privé-sfeer verzameld kunnen worden. Een dergelijke inbreuk is niet acceptabel. Ten aanzien van de mate van toezicht moeten derhalve de noodzaak en de doeleinden aangegeven kunnen worden.

Om het knelpunt van controle op de naleving van arbeids- en rusttijden te beperken, dient onderzocht te worden op welke wijze (geautomatiseerde) controle plaats kan vinden, daarbij rekening houdend met het privacyaspect.<sup>1</sup>

#### 5.1.4 Besluit Algemene Rechtspositie Politie (Barp)

Bij een arbeidsovereenkomst gesloten op grond van het klassieke arbeidsrecht (Boek 7 Burgerlijk Wetboek) is de vraag naar het karakter van de arbeidsverhouding aan de orde. Dit zou een knelpunt kunnen vormen bij de invoering van telewerken.

Met betrekking tot ambtenaren, aangesteld voor de uitvoering van de politietaken, speelt dit probleem niet, omdat in artikel 1 lid 1 sub c van het Barp in een definitie is vastgelegd welke personen de ambtenarenstatus bezitten. Dit artikel voorkomt derhalve discussies over het karakter van de arbeidsverhouding bij (politie)ambtenaren. Dit aspect levert een bijdrage aan de haalbaarheid.

In artikel 1 lid 1 sub t en u zijn de definities opgenomen van: "plaats van tewerkstelling" en "hoofdplaats van tewerkstelling".

*Plaats van tewerkstelling:*

1. *het gebouw, gebouwencomplex of terrein dat de ambtenaar voor de normale uitoefening van zijn ambt is aangewezen;*
2. *de aangewezen aanleplaats van het vaartuig...;*
3. *bij gebrek aan een aanwijzing, bedoeld in het eerste en tweede onderdeel, het gebouw, gebouwencomplex, of terrein, waar de ambtenaar gewoonlijk zijn werkzaamheden verricht, het gebouwencomplex waar hij kantoor houdt, dan wel de aanleplaats waar hij gewoonlijk het vaartuig aanlegt.*

Bij meerdere aangewezen plaatsen van tewerkstelling, wordt een hoofdplaats van tewerkstelling benoemd.

De begrippen *gebouw*, *gebouwencomplex* en *terrein* kunnen ruim uitgelegd worden en zullen geen belemmering vormen voor telewerken. Onderdeel 3 geeft eveneens ruimte voor telewerken door de zinsede *'waar de ambtenaar gewoonlijk zijn werkzaamheden verricht'*. Het probleem dat laatstgenoemde duidt op één locatie kan verholpen worden door meerdere plaatsen van tewerkstelling aan te wijzen.

Hoofdstuk III van het Barp bevat bepalingen over Arbeids- en Rusttijden. Het feit dat het Barp deze bepalingen bevat, zegt iets over de wil om een en ander goed te regelen, hetgeen bij de invoering van telewerken knelpunten op dit gebied zou kunnen beperken c.q. voorkomen.

In artikel 64 Barp is bepaald dat *'indien het belang van de dienst dit in bijzondere gevallen vordert, de ambtenaar verplicht is zijn functie op een andere dan de hem aangewezen plaats van tewerkstelling of binnen een ander dan het hem aangewezen werkgebied uit te oefenen....'*. Deze bepaling kan invloed hebben op een individuele bevoegdheid tot telewerken. Gezien het individuele karakter zal de bepaling geen knelpunt vormen voor de invoering van telewerken bij de politie in het algemeen.

---

<sup>1</sup> Hierbij kunnen rapporten en uitspraken van de Registratiekamer/het College Bescherming Persoonsgegevens van pas komen. Rapporten Registratiekamer: *Als de telefoon wordt opgenomen*, november 1996; *Goed werken in netwerken, regels voor controle op e-mails en internetgebruik van werknemers*, 2000.

## 5.2 Nederlandse wet- en regelgeving, overige juridische aspecten

### 5.2.1 Archiefwet 1995

In artikel 45 lid 5 Politiewet worden de artikelen 32, tweede lid, 33, eerste en derde lid, en 34 van de Archiefwet 1995 van overeenkomstige toepassing verklaard. De genoemde artikelen betreffen de zorg voor en het beheer van archiefbescheiden.

Er dient voor gewaakt te worden dat telewerken het beheer van archiefbescheiden niet bemoeilijkt. Het is raadzaam de zogeheten "zorgdrager"<sup>2</sup> te informeren over de invoering van telewerken. De zorgdrager kan vervolgens aangeven of er specifieke zaken geregeld moeten worden of dat er richtlijnen opgesteld moeten worden.

De archiefwet bevat noch knelpunten, noch haalbaarheidsaspecten met betrekking tot invoering van telewerken bij de sector politie.

### 5.2.2 Besluit wijzigingen i.v.m. het antecedentenonderzoek voor de politie

Dit wijzigingsbesluit bevat wijzigingen voor diverse besluiten, waaronder het Barp. Een relevante wijziging betreft het opnieuw mogen uitvoeren van een antecedentenonderzoek. Eén van de gronden is: *bij wijziging van werkzaamheden*. De vraag waarbij stilgestaan moet worden, is of telewerken gezien kan worden als wijziging van werkzaamheden en derhalve aanleiding kan zijn voor het opnieuw uitvoeren van een antecedentenonderzoek. Wij menen van niet: bij telewerken wijzigt wel de wijze van werken, maar niet de werkzaamheden zelf.

Dit aandachtspunt lijkt onbelangrijk en niet relevant, echter een duidelijk standpunt in deze kan in de toekomst misbruik van deze regelgeving voorkómen.<sup>3</sup>

### 5.2.3 Politiewet 1993

In artikel 3 lid 1 Politiewet is de ambtenarenstatus van de politie vastgelegd. In het reeds besproken Besluit Algemene Rechtspositie Politie (Barp) zijn nadere regels opgenomen omtrent de positie van een politieambtenaar. Mede door artikel 3 Politiewet en het Barp is er geen discussie mogelijk over de rechtspositie van een politieambtenaar, hetgeen de haalbaarheid van telewerken positief beïnvloedt.

In artikel 7 Politiewet is vermeld dat een ambtenaar van politie bevoegd is zijn taak in het gehele land uit te oefenen. Deze bevoegdheid wordt vervolgens beperkt door de regel dat de ambtenaar van politie zich dient te onthouden van optreden buiten zijn gebied van aanstelling. Ondanks de beperking biedt deze bepaling de politieambtenaar vrijheid, waardoor dit artikel de invoering van telewerken niet in de weg zal staan.

### 5.2.4 Regeling informatiebeveiliging politie

Op grond van deze regeling moet een korpsbeheerder<sup>4</sup> een informatie-beveiligingsbeleid vaststellen. Het beleid dient ertoe te leiden c.q. ervoor te zorgen dat de omvangrijke gegevensverzamelingen die de politie heeft over natuurlijke personen, beveiligd is, zodat gemeenschappelijke betrouwbaarheidseisen gelden en per informatiesysteem of IT-dienst afhankelijkheids- en kwetsbaarheidsanalyses worden toegepast, die tot maatregelen leiden die in beveiligingsplannen worden vastgelegd.

In de toelichting op de regeling is onder andere de volgende alinea opgenomen:

*"De complexiteit van het beveiligingsvraagstuk zal nog toenemen naarmate de technologie meer mogelijkheden biedt tot directe communicatie op elk gewenst moment en elke gewenste plaats. In de praktijk zal van deze mogelijkheden gebruik worden gemaakt. Het is daarom noodzakelijk voor de politie aandacht te besteden aan de beveiliging van de informatievoorziening en om de informatiebeveiliging aan te pakken op een gemeenschappelijke basis."*

<sup>2</sup> Zorgdrager: degene die bij of krachtens de wet belast is met de zorg voor de archiefbescheiden.

<sup>3</sup> In de klassieke arbeidsverhoudingen zijn er tal van voorbeelden waarbij telewerken is aangegrepen om werknemers buiten spel te zetten.

<sup>4</sup> ....en voor zover het betreft het KLPD en de ITO de Minister van Binnenlandse Zaken en Koninkrijksrelaties.

Met deze laatste alinea is de deur voor invoering van telewerken bij de sector politie open gezet. Dit levert een grote bijdrage aan de haalbaarheid. Gezien de toenemende complexiteit van het beveiligingsvraagstuk bij telewerken, wordt hiervoor een knelpunt genoteerd. Met extra inspanning en extra tijd zal dit knelpunt overwonnen kunnen worden.

### 5.2.5 Wet bescherming persoonsgegevens

Artikel 2, lid 2 van deze wet bevat een opsomming van situaties van verwerking van persoonsgegevens waarop de wet **niet** van toepassing is.

Sub b betreft: *verwerking van persoonsgegevens ten behoeve van de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen en veiligheidsdiensten.*

Sub c betreft: *verwerking van persoonsgegevens ten behoeve van de uitvoering van de politietaak, omschreven in artikel 2 van de Politiewet 1993.*

De niet toepasselijkheid van de wet geldt tevens voor het verbod om strafrechtelijke persoonsgegevens te verwerken (artikel 22).

De knelpunten die de Wet bescherming persoonsgegevens met betrekking tot telewerken zou kunnen opwerpen, zijn op grond van bovenstaande niet relevant. Ter 'vervanging' van de Wet bescherming persoonsgegevens kent de sector politie de Wet politieregisters, waarin regels met betrekking tot de omgang met persoonsgegevens zijn opgenomen.

### 5.2.6 Wet bescherming staatsgeheimen 1951

Artikel I van de wet luidt: *Elke plaats in gebruik bij de staat of een staatsbedrijf kan ter bescherming van gegevens, waarvan de geheimhouding door het belang van de veiligheid van de staat wordt geboden, door Ons als verboden plaats worden aangewezen.*

Op grond van deze wet zou het mogelijk kunnen zijn dat een bepaalde (toekomstige) telewerklocatie niet gebruikt mag worden, omdat de locatie als een 'verboden plaats' is aangewezen.

Voor de invoering van telewerken bij de sector politie zal deze wet geen knelpunten opleveren.

### 5.2.7 Voorstel van Wet Computercriminaliteit II

Artikel I sub G bevat een wijziging van artikel 139b Wetboek van Strafrecht. De tekst luidt als volgt: *"Met dezelfde straf wordt gestraft hij die met een technisch hulpmiddel opzettelijk en zonder daartoe gerechtigd te zijn heimelijk gegevensoverdracht aftapt of opneemt die, elders dan in een woning, besloten lokaal of erf, plaatsvindt door middel van een geautomatiseerd werk of door middel van telecommunicatie."*

De wijziging is met name gericht op bescherming van telecommunicatie via bedrijfsnetwerken. In verband met de invoering van telewerken en daarmee de toename van telecommunicatie via een bedrijfsnetwerk levert deze wijziging een positieve bijdrage.

### 5.2.8 Wet op de inlichtingen en veiligheidsdiensten

Artikel 16 van deze wet draagt aan de hoofden van de diensten op zorg te dragen voor onder andere:

- de nodige voorzieningen van technische en organisatorische aard ter beveiliging van de gegevensverwerking tegen verlies of aantasting van gegevens alsmede tegen onbevoegde gegevensverwerking;
- de aanwijzing van personen die bij uitsluiting van anderen bevoegd zijn tot de bij de aanwijzing vermelde werkzaamheden in het kader van de verwerking van gegevens.

Ten opzichte van andere wet- en regelgeving is de beveiligingseis in artikel 16 strikter, oftewel heeft deze eis een minder 'open' karakter. Dit betekent dat voor de invoering van telewerken, voor de ambtenaren van de inlichtingen en veiligheidsdiensten, op beveiligingsgebied een grotere inspanning vereist is, vanwege de grotere mate van complexiteit.

### 5.2.9 Wet justitiële gegevens

De Wet justitiële gegevens noemt de mogelijkheid van het door middel van telecommunicatie verstrekken van justitiële gegevens. Hierbij is voorts de beperking gesteld dat de ontvanger van de gegevens, die verstrekt zijn via telecommunicatie, deze niet op geautomatiseerde wijze vastlegt of vermenigvuldigt, tenzij dit noodzakelijk is voor de uitvoering van een bepaalde taak. In het laatste geval moeten passende technische en organisatorische maatregelen ten uitvoer gelegd worden. De Minister van Justitie is hiervoor verantwoordelijk.

Door de genoemde mogelijkheid van gegevensverstrekking via telecommunicatie wordt telewerken erkent. Hoewel dit een bijdrage levert aan de haalbaarheid van telewerken dient wel rekening te worden gehouden met de genoemde beperking, waartoe in bijvoorbeeld een beveiligingsplan maatregelen getroffen dienen te worden.

#### **5.2.10 Wet op de veiligheidsonderzoeken**

Vertrouwensfuncties zijn functies die de mogelijkheid bieden de veiligheid of andere gewichtige belangen van de staat te schaden.

Gezien het feit dat vertrouwensfuncties schade kunnen toebrengen, is de vraag of telewerken bij dergelijke functies gewenst respectievelijk acceptabel is, zeer relevant. De wet zelf geeft hierover geen duidelijkheid.

#### **5.2.11 Wet politieregisters**

De beheerder van een politieregister is verantwoordelijk voor het treffen van de nodige voorzieningen van technische en organisatorische aard ter beveiliging van het register. Zoals reeds eerder bij andere wet- en regelgeving is opgemerkt, is de beveiligingseis een 'open' eis. Iedere beheerder kan deze eis naar eigen inzicht invullen. Met de invoering van telewerken zal de beveiliging naar verwachting verzwakt moeten worden en zullen de te treffen voorzieningen complexer worden.

In deze wet is onder andere de rol van een beheerder beschreven. Over de eigenaar van een bepaald systeem of de door hem/haar te verlenen toestemming voor het tijdens telewerken gebruikmaken van zijn/haar systeem is niets vermeld. Ook in andere wet- en regelgeving waarin de rol van een beheerder wordt belicht, wordt de positie van een eigenaar van een systeem niet genoemd.

#### **5.2.12 Besluit politieregisters**

In het besluit zijn beperkingen opgenomen ten aanzien van gegevensverstrekking langs geautomatiseerde weg. Slechts personen die van de beheerder een schriftelijke autorisatie voor een daarbij bepaald omschreven doel hebben gekregen, kunnen gegevens langs geautomatiseerde weg ontvangen. De genoemde beperkingen zouden een knelpunt voor telewerken kunnen vormen. Om dit te voorkomen zou voorafgaand aan de invoering van telewerken in kaart moeten worden gebracht welke politieambtenaren een autorisatie (moeten) hebben om bepaalde gegevens via geautomatiseerde weg te ontvangen. De mogelijkheid van geautomatiseerde gegevensverstrekking draagt bij aan de mogelijkheid van telewerken.

#### **5.2.13 CID regeling 1995**

De CID regeling bevat specifieke bepalingen met betrekking tot zogenaamde gevoelige gegevens, de groep van toegangsgerechtigden, beperkingen ten aanzien van verstrekking van gegevens uit het CID register en de bevoegdheden om systemen te koppelen.

Het feit dat dergelijke specifieke regels zijn vastgelegd, vloeit voort uit de aard van de opgeslagen gegevens en de functie van de CID leden. Indien telewerken zou worden ingevoerd bij de CID, zullen er zeer zware beveiligingen gerealiseerd moeten worden. Het is raadzaam te onderzoeken of telewerken voor zo'n specifiek onderdeel als de CID wenselijk is.

### **5.3 Europese regelgeving telewerken, arbeidsrechtelijke en arbeidsvoorwaardelijke aspecten**

Sinds medio 2000 richt de Europese Commissie zich op het onderwerp 'modernisering en verbetering van de arbeidsverhouding'. In het verlengde daarvan is in maart 2001 het aspect 'telewerken' belicht. De Commissie is van mening dat telewerken een flexibiliteitsfactor is, waarbij echter gezorgd moet worden dat de ontwikkeling daarvan niet ten nadele van de bescherming van de werknemers geschiedt.

De Commissie acht het nodig dat richtsnoeren worden opgesteld, zonder daarmee de ontwikkeling van telewerken te beteugelen. De Commissie heeft als aftrap algemene beginselen voor de vaststelling van een kader voor telewerken opgesteld.<sup>5</sup> De beginselen hebben betrekking op:

- Het vrijwillige karakter van het recht op terugkeer;
- De garantie van het behoud van de status werknemer;
- De garantie van gelijke behandeling;
- De aan een telewerker te verstrekken informatie;
- De betaling van de met telewerken verbonden kosten door de werkgever;
- De garantie van het verstrekken van een passende opleiding;
- De bescherming op het gebied van gezondheid en veiligheid;
- De arbeidstijd;
- De bescherming van de persoonlijke levenssfeer en de bescherming van de persoonsgegevens;
- Het behoud van het contact met het bedrijf;
- De collectieve rechten van telewerkers en de toegang tot telewerken.

Het voorstel van de Commissie is ter beoordeling aan de zogeheten sociale partners van de Europese Gemeenschap voorgelegd. De sociale partners zullen de Commissie een advies of een aanbeveling over het voorstel doen toekomen.

Aangezien Europese wetgeving nog niet voorhanden is, zijn de hiervoor opgesomde algemene beginselen een alternatief waaraan de haalbaarheid van telewerken bij de politie -op arbeidsrechtelijk en arbeidsvoorwaardelijk vlak- getoetst kan worden. De algemene beginselen zijn punten die goed in een arbeidsovereenkomst of CAO te verwerken zijn.

## **5.4 Europese regelgeving telewerken, overige juridische aspecten**

### **5.4.1 Europol Overeenkomst**

De Europol Overeenkomst betreft de samenwerking tussen de bevoegde instanties van de Lid-Staten met betrekking tot het voorkomen van bepaalde vormen van criminaliteit. De primaire taken van Europol hebben te maken met de verzameling, uitwisseling en bewerking van informatie en gegevens via een geautomatiseerd informatiesysteem dat door Europol wordt aangelegd en beheerd. Slechts bepaalde personen van een Lid-Staat kunnen het informatiesysteem raadplegen.

Elke Lid-Staat diende uiterlijk op het tijdstip van inwerkingtreding van de Overeenkomst in zijn nationale wetgeving met betrekking tot de verwerking van persoonsgegevens in bestanden in het kader van deze Overeenkomst, de nodige maatregelen ter waarborging van een niveau van gegevensbescherming dat ten minste gelijk is aan het niveau dat voortvloeit uit de toepassing van de beginselen van het Verdrag van de Raad van Europa van 28 januari 1981, rekening houdende met Aanbeveling R (87) 15 van het Comité van Ministers van de Raad van Europa van 17 september 1987 tot regeling van het gebruik van persoonsgegevens op politieel gebied. Nederland had de Wet persoonsregistraties en momenteel de Wet bescherming persoonsgegevens en daarvan afgeleide wetgeving, zoals de Wet en het Besluit politieregisters.

Artikel 25 Europol Overeenkomst betreft de beveiliging van de gegevens. Lid-Staten moeten *passende maatregelen* treffen om een aantal opgesomde handelingen te verhinderen of juist te waarborgen. Er zijn geen nadere eisen gesteld aan de passende maatregelen.

Gezien de niet specifieke, 'open' beveiligingsseis zal deze Overeenkomst geen direct knelpunt vormen voor de invoering van telewerken bij de sectorpolitie.

### **5.4.2 Europol geheime informatie**

In dit besluit worden de beveiligingsmaatregelen vastgesteld die worden toegepast op alle informatie die door of via Europol binnen zijn organisatie wordt verwerkt. De Lid-Staten verbinden zich ertoe te waarborgen dat dergelijke informatie op hun grondgebied een niveau van bescherming krijgt dat gelijkwaardig is aan het niveau dat geboden wordt door de maatregelen genoemd in het besluit.

---

<sup>5</sup> Publicatieblad Europese Gemeenschappen 2001/C318E/127).

Europol kent een basisbeschermingsniveau. De Lid-Staten waarborgen de toepassing van het basisbeschermingsniveau door middel van diverse maatregelen van uiteenlopende aard, overeenkomstig de nationale wet- en regelgeving, daaronder begrepen de zwijg- en geheimhoudingsplicht, het beperken van de toegang tot de informatie tot gemachtigde personeelsleden, vereisten inzake de bescherming van persoonsgegevens en algemene technische en proceduremaatregelen om de beveiliging van de informatie te waarborgen.

Aan informatie die extra beveiligingsmaatregelen vereist, wordt een Europol-beveiligingsniveau toegekend. Aan elk Europol-beveiligingsniveau is een specifiek beveiligingspakket verbonden dat binnen Europol wordt toegepast. De beveiligingspakketten omvatten verscheidene maatregelen van technische, organisatorische of administratieve aard, zoals omschreven in een beveiligingshandboek.

Indien Nederland een vertegenwoordiger heeft afgevaardigd naar het Europol-beveiligingscomité zal deze persoon op de hoogte zijn van de specifieke beveiligingseisen. Ook bij de door iedere Lid-Staat opgerichte of aangewezen nationale eenheid zal voldoende kennis aanwezig zijn om te beoordelen welke maatregelen genomen moeten worden om telewerken bij de sector politie te laten slagen.

Het besluit levert in die zin knelpunten op dat meer inspanning en nauwkeurigheid vereist zal zijn om aan alle specifieke beveiligingseisen te voldoen. Om een goed overzicht van de specifieke eisen te verkrijgen dient geïnformeerd te worden bij een afgevaardigde of Europol. Het rechtstreeks benaderen van een 'insider' zal efficiënt werken.

## **5.5 Jurisprudentie**

Jurisprudentie die specifiek betrekking heeft op telewerken en waar in het kader van de invoering van telewerken bij de sector politie rekening mee gehouden zou moeten worden, is niet voorhanden. Dit geldt zowel op Nederlands als op Europees gebied.

## 6 Interviews

### 6.1 Inleiding

Door middel van het juridische onderzoek is inzicht verkregen in de mogelijke knelpunten in relevante wet- en regelgeving. Naast de theoretische kennis op het juridische vlak, is het van belang te inventariseren hoe er in de praktijk vanuit juridisch oogpunt tegen telewerken bij de sector politie wordt aangekeken. Daartoe is getracht enkele hoofdofficieren van justitie<sup>6</sup> te interviewen. Bij de arrondissementsparketten Utrecht en Groningen waren de reacties positief en kon op korte termijn een interview met de hoofdofficieren van justitie plaatsvinden. In Amsterdam en 's-Hertogenbosch is aangeboden het interview te houden met het hoofd bedrijfsbureau respectievelijk het hoofd bedrijfsvoering. Ook het College Bescherming Persoonsgegevens (verder: CBP) is benaderd voor een interview. Het CBP was niet bereid een gesprek aan te gaan. Wel konden er schriftelijk of telefonisch vragen worden gesteld. Telefonisch zijn enkele vragen gesteld over telewerken bij de sector politie. Het CBP moest echter de antwoorden schuldig blijven. De indruk bestaat dat slechts vragen met betrekking tot de Wet bescherming persoonsgegevens goed en op korte termijn beantwoord kunnen worden.

De geïnterviewde personen zijn:

- Mevrouw mr. Klopper-Gerretsen - hoofdofficier van justitie te Utrecht
- De heer mr. Moraal - hoofdofficier van justitie te Groningen
- De heer Jansen - hoofd bedrijfsvoering te 's-Hertogenbosch
- Hoofd bedrijfsvoering te Amsterdam

Het uitgangsdokument voor het interview, dat in paragraaf 6.2 is opgenomen, is opgesteld naar aanleiding van bevindingen uit het juridische onderzoek.

De resultaten van de interviews zijn samengevat weergegeven in paragraaf 6.3.

### 6.2 Uitgangsdokument interviews

Onderstaande vragen dienden als basis voor het interview.

Het hoofd bedrijfsbureau en het hoofd bedrijfsvoering hebben de vragen een week voor het interview ontvangen, zodat zij zonodig intern (o.a. bij de hoofdofficier van justitie) informatie konden vergaren.

1. Telewerken kan geassocieerd worden met on-line gegevens-uitwisseling.
  - Is dit een wenselijke ontwikkeling in het politiewezen in deze tijd?
  - Is dit een acceptabele ontwikkeling, gezien het feit dat tevens gewerkt wordt met gegevens die een rol kunnen spelen bij vervolging of rechtszaken?
2. In veel wetgeving is een eis met betrekking tot beveiliging van gegevens opgenomen, echter een bepaald niveau van beveiliging of technische specificaties worden niet gegeven. Is zo'n globale 'open' eis m.b.t. beveiliging afdoende in het kader van telewerken bij de sector politie?
3. De politie kent in veel wetgeving een uitzonderingspositie wat betreft de omgang met gegevens. De politie heeft veelal meer bevoegdheden.
  - Hoe is de verhouding tussen deze uitzonderingspositie en de 'open' beveiligingseis? Oftewel is de 'open' eis een probleem?
  - Zou er specifieke wetgeving moeten komen om telewerken bij de sector politie en/of soortgelijke sectoren in goede banen te leiden en veiligheid/vertrouwen te waarborgen?
  - Zou een regeling/richtlijn "Telewerken" voor de sector politie voldoende zijn om waarborgen te scheppen?
  - Zoja, op welk niveau zou een dergelijke regeling gemaakt moeten worden?
  - Welke persoon (functie) zou verantwoordelijk moeten zijn voor gebreken ten aanzien van beveiliging in systemen van telewerkende politie-medewerkers?

---

<sup>6</sup> De hoofdofficieren van justitie in de regio's waar telewerkprojecten gaande zijn, zijn benaderd. Het betreft de regio's: Utrecht, Groningen, Amsterdam en 's-Hertogenbosch.

4. Zou telewerken bij de politie in eerste instantie slechts mogelijk moeten zijn voor bepaalde functies?
  - Ja/Nee, welke redenen zijn daarvoor aan te voeren?
  - En in de toekomst?
  
5. Zou in het geval van thuiswerken de thuissituatie van een politiemedewerker een rol moeten/mogen spelen bij de beoordeling of een medewerker mag telewerken of niet?
  - Zou het antecedentenonderzoek gebruikt mogen worden bij een beoordeling over een bevoegdheid tot telewerken?
  
6. In het voorstel Wet Computercriminaliteit II is een wijziging van artikel 139b lid 2 Sr opgenomen. Het betreft aftappen/opnemen van gegevensoverdracht die elders dan in een woning, besloten lokaal of erf plaatsvindt... De wijziging is met name gericht op bescherming van telecommunicatie via bedrijfsnetwerken.
 

*“Met dezelfde straf wordt gestraft hij die met een technisch hulpmiddel opzettelijk en zonder daartoe gerechtigd te zijn heimelijk gegevensoverdracht aftapt of opneemt die, elders dan in een woning, besloten lokaal of erf, plaatsvindt door middel van een geautomatiseerd werk of door middel van telecommunicatie.”*

  - Zouden er voor het heimelijk aftappen of opnemen van gegevens die door telewerkende politiemedewerkers worden verwerkt hogere straffen moeten gelden dan voor hetzelfde misdrijf bij een ‘gewoon’ bedrijf?
  
7. Hoe moet er bij telewerken omgegaan worden met de aansprakelijkheid van politiemedewerkers?
  - Moeten er aparte afspraken gemaakt worden met de telewerker?
  - Zoja, in welke vorm?
  - Moet er een grotere verantwoordelijkheid komen te liggen bij de telewerker zelf in vergelijking met een ‘normale’ werksituatie?
  
8. Zijn er nog vragen en/of opmerkingen?

## 6.3. Resultaten interviews

### 6.3.1 Hoofdofficier van justitie - Utrecht

#### Vraag 1

De hoofdofficier van justitie (verder: HvJ) is van mening dat telewerken bij de sector politie zeker in deze tijd een wenselijke ontwikkeling is. Politieambtenaren hebben veel informatie nodig en het werkt efficiënt als zij dat op verschillende locaties kunnen opvragen, gebruik, etc..

Telewerken is naast een wenselijke ontwikkeling tevens een acceptabele ontwikkeling, echter met de beperking dat bepaalde informatie wel elektronisch opvraagbaar moet zijn en bepaalde informatie niet. Welke informatie elektronisch opvraagbaar moet c.q. mag zijn, dient praktisch bekeken te worden. Telewerken moet de efficiency in ieder geval bevorderen.

#### Vraag 2

De HvJ is onbekend met beveiligingsmogelijkheden en heeft derhalve geen mening over de mate van beveiliging en of de ‘open’ eis in wetgeving afdoende zal zijn.

#### Vraag 3

De HvJ is van mening dat de politie in wetgeving terecht meer bevoegdheden heeft wat betreft de omgang met gegevens. Over de mate van beveiliging heeft zij geen oordeel. Wel merkt zij op dat de toegang tot meer gegevensbestanden naar functie beperkt moet worden.

Specifieke wetgeving om telewerken bij de sector politie in goede banen te leiden zou goed zijn. Echter het wetgevingstraject is lang, dus de voorkeur gaat uit naar regelgeving. Dat dient er in ieder geval te komen. Binnen het OM speelt dit ook al. In regelgeving dient duidelijk vastgelegd te worden *wat kan en mag*. Bovendien moeten burgers de mogelijkheid krijgen om klachten in te dienen.

Misschien zou het toch goed zijn 1 basis wet op te stellen, waarbij wijzigingen en nadere regels bij besluit kunnen worden toegevoegd.

Een regeling of richtlijn moet op hoog niveau (ministerie) gemaakt worden. Zeker indien de politie toegang heeft/krijgt tot bestanden van derden, bijvoorbeeld van justitie. Controle en klachtbehandeling moeten ook plaatsvinden op hoog niveau.

Voor gebreken in de beveiliging bij telewerkers dient de korpsleiding / rijksrecherche verantwoordelijk te zijn. De verantwoordelijkheidsvraag moet centraal geregeld worden, niet zoals het nu gaat, dat iedere regio zijn eigen regeling heeft.

#### *Vraag 4*

Telewerken moet daar ingevoerd worden waar er de meeste behoefte aan is, bijvoorbeeld eerst bij de politie op straat en teams in het veld. Waar telewerken ingevoerd moet worden, moet praktisch bekeken worden. Eventueel kan gestart worden met een kleine experimentgroep.

Telewerken moet mogelijk zijn voor alle functies, voor zover het maar efficiënt is voor de betreffende functie.

#### *Vraag 5*

De thuissituatie mag geen rol spelen bij de beoordeling of een ambtenaar mag thuiswerken. Het antecedentenonderzoek mag niet gebruikt worden om te oordelen over de bevoegdheid tot telewerken. Indien er bezwaren zijn voor de bevoegdheid tot telewerken, zijn er ook bezwaren voor de uitoefening van de functie van politieambtenaar in het algemeen.

Indien een politieambtenaar niet geschikt is om te telewerken, moet de vraag gesteld worden of de persoon wel geschikt is als politieambtenaar.

#### *Vraag 6*

Voor het heimelijk aftappen of opnemen van gegevens die door telewerkende politiemedewerkers worden verwerkt moeten geen hogere straffen gelden dan voor hetzelfde misdrijf bij een 'gewoon' bedrijf. De politie moet zorgen voor afdoende beveiliging.

#### *Vraag 7*

Voor wat betreft de aansprakelijkheid van telewerkende politiemedewerkers zal er een protocol opgesteld moeten worden. Dit protocol kan afgeleid worden van eventueel toekomstige regelgeving.

De telewerker zelf moet geen grotere verantwoordelijkheid krijgen. De telewerker dient dezelfde zorgvuldigheid in acht te nemen als 'normaal'.

### **6.3.2 Hoofdofficier van justitie - Groningen**

#### *Vraag 1*

De HvJ is van mening dat de mogelijkheid tot telewerken en de wenselijkheid daarvan afhankelijk is van de taken van de politieambtenaar. Bereikbaarheid, zowel fysiek als telefonisch, is belangrijk.

Voor leidinggevend is telewerken niet wenselijk en/of acceptabel. Voor de politie op straat is telewerken toe te juichen.

Telewerken is, met inachtneming van voorgaande, acceptabel, maar beveiliging is daarbij van groot belang. Met name bij privacygevoelige gegevens. Een zware mate van beveiliging is noodzakelijk, zodat zelfs een professionele hacker niet bij bestanden kan.

#### *Vraag 2*

De 'open' beveiligingseis die in veel wetgeving voorkomt is niet afdoende. Elk korps heeft namelijk zijn eigen mening over beveiliging en de mate van beveiliging kan zodoende sterk verschillen. Om dit probleem op te vangen moeten er landelijke beveiligingsnormen worden afgesproken.

#### *Vraag 3*

De uitzonderingspositie wat betreft de omgang met gegevens die de politie in veel wetgeving kent, zorgt voor druk op de integriteit van de politieambtenaren. Politieambtenaren krijgen een opleiding waarin integriteit een belangrijke plaats inneemt. Naast de opleiding waarin de ambtenaar gevormd wordt, dient

technisch alles goed geregeld te worden. De vraag die daarna nog overblijft, is of de politieambtenaar met telewerken kan omgaan.

Specifieke wetgeving is niet wenselijk. Het gaat om de beroepsethiek. Er zouden wel dwingende regels opgelegd kunnen worden. Het aanvullen van de Politiewet met een AMvB kan een optie zijn. De AMvB moet specifiek zijn en voor alle korpsen gelden.

Een regeling/richtlijn "Telewerken" voor de sector politie kan voldoende zijn. De regeling zou door BZK opgesteld moeten worden.

Voor gebreken in de beveiliging bij telewerkers dient de korpschef verantwoordelijk te zijn.

#### *Vraag 4*

Telewerken zou in eerste instantie slechts voor bepaalde functies mogelijk moeten zijn. Niet alle functies zijn geschikt voor telewerken. Bij sommige functies bestaan er praktische bezwaren, denk bijvoorbeeld aan een verbalisant of iemand die dossierwerk doet. Voor andere functies bestaan er principiële bezwaren, bijvoorbeeld voor lijnfuncties.

Ook voor de toekomst is/blijft het bezwaarlijk dat leidinggevendenden gaan telewerken. De vervangingsvraag speelt echter wel een belangrijke rol. Leidinggevendenden kunnen elkaar bijvoorbeeld afwisselen op kantoor, zodat er in ieder geval altijd iemand aanwezig is. Het laatste is een vereiste.

#### *Vraag 5*

De thuissituatie mag geen rol spelen bij de beoordeling of een ambtenaar mag thuiswerken. Het antecedentenonderzoek mag niet gebruikt worden om te oordelen over de bevoegdheid tot telewerken. Integriteit wordt bij een politieambtenaren aangenomen. Er kunnen wel bepaalde categorieën gegevens uitgesloten worden voor telewerken.

#### *Vraag 6*

Voor het heimelijk aftappen of opnemen van gegevens die door telewerkende politiemedewerkers worden verwerkt zou een hogere strafmaat kunnen gelden dan voor hetzelfde misdrijf bij een 'gewoon' bedrijf. Veelal worden al hogere straffen geëist bij bepaald gedrag richting de politie. In het geval van gegevensverwerking zou dit ook op kunnen gaan.

#### *Vraag 7*

Voor wat betreft de aansprakelijkheid van telewerkende politiemedewerkers zal er een protocol opgesteld moeten worden. Op grond daarvan kunnen dan bij afwijking van de regels disciplinaire maatregelen volgen.

Er moet met betrekking tot het naleven van het protocol een grotere verantwoordelijkheid komen te liggen bij de telewerker. De politieorganisatie moet echter zorgen voor de nodige voorzieningen, bijvoorbeeld alarm en een kluis. De verantwoordelijkheid voor de te treffen maatregelen ligt niet bij de telewerker, maar bij de politieorganisatie. Verantwoordelijkheid van de telewerker moet deel uitmaken van het contract dat wordt aangegaan voor telewerken.

#### *Vraag 8*

Tot slot merkt de HvJ op dat hij een voorstander is van telewerken in de auto. Wat betreft het thuiswerken is hij een stuk terughoudender.

### **6.3.3 Hoofd bedrijfsvoering - 's-Hertogenbosch**

#### *Vraag 1*

Het hoofd bedrijfsvoering (verder: HB) merkt vooraf op dat hij bij telewerken niet alleen denkt aan online gegevensuitwisseling, maar aan een hele on-line werkplek, waar alle taken verricht kunnen worden, als ware het een 'normale' vaste werkplek. HB wordt verteld dat het laatste ook het uitgangspunt geweest is bij het onderzoek.

HB vindt telewerken een wenselijke ontwikkeling, flexibiliteit is in deze tijd van belang. Telewerken is bovendien acceptabel. Daarbij moet wel de beveiliging strikt gehanteerd worden. Beveiliging is echter goed te realiseren.

### Vraag 2

De HB laat zich niet specifiek uit over de 'open' beveiligingseis die in veel wetgeving voorkomt, maar meldt dat beveiligingstechnieken goed zijn, niet 100%, maar wel voldoende. Daarnaast moet procedureel het nodige gedaan worden, denk aan verantwoordelijkheden aangeven en autorisaties regelen. De 'open' beveiligingseis moet goed ingevuld worden, dat wil zeggen organisatorisch, procedureel (integriteit) en technisch.

Specifieke wetgeving met betrekking tot informatiebeveiliging is wenselijk en gemakkelijk bij eventuele overtredingen. Uitwerkingen kunnen beter in regelingen worden opgenomen om teveel wijzigingen en/of aanvullingen in een wet te voorkomen. Regelingen/richtlijnen moeten door BZK opgesteld worden.

Voor gebreken in de beveiliging bij telewerkers dient verantwoordelijk te zijn:

- voor fysieke beveiliging (bijvoorbeeld toegangscontrole) een *Beveiliging functionaris*;
- voor gegevensbeveiliging een *Beveiligingsfunctionaris informatiebeveiliging* (deze functie is betrekkelijk nieuw en is onder andere ontstaan in verband met telewerken).

De twee functies zullen elkaar gedeeltelijk overlappen.

### Vraag 4

Voor de invoering van telewerken moet je geen functies gaan benoemen. Er moet gekeken worden naar de toegevoegde waarde van telewerken voor de functie. In principe moet telewerken voor alle functies mogelijk zijn, met als voorwaarde dat het een toegevoegde waarde heeft.

### Vraag 5

De thuissituatie mag geen rol spelen bij de beoordeling of een ambtenaar mag thuiswerken. Het antecedentenonderzoek mag niet gebruikt worden om te oordelen over de bevoegdheid tot telewerken. Integriteit staat voorop. Telewerken, of niet, mag geen verschil uitmaken.

### Vraag 6

Voor het heimelijk aftappen of opnemen van gegevens die door telewerkende politiemedewerkers worden verwerkt mogen geen hogere straffen gelden dan voor hetzelfde misdrijf bij een 'gewoon' bedrijf.

### Vraag 7

Er moeten afspraken gemaakt worden in de vorm van een protocol, waarbij de integriteit extra benadrukt moet worden. De aansprakelijkheid van de politieregio moet vergroot worden, niet die van de telewerker zelf.

De telewerker zelf dient een grotere verantwoordelijkheid te krijgen om de bewustwording van de integriteit te stimuleren.

### Vraag 8

Bij het OM loopt ook een telewerkpilot. Er wordt gewerkt met computers zonder programmatuur of gegevens erop, zodat bij verlies of diefstal geen gegevenslek kan ontstaan. Alle programmatuur en gegevens waar mee gewerkt wordt en gegevens die geproduceerd worden, komen rechtstreeks van of gaan naar de 'moedercomputer' op een kantoor. De beveiliging van de moedercomputer is optimaal.

## 6.3.4 Hoofd bedrijfsvoering – Amsterdam

Het Hoofd bedrijfsvoering (verder: HB) heeft de vragen enige tijd voor het interview toegestuurd gekregen en heeft de vragen gezamenlijk met de Hoofdofficier van justitie (verder: HvJ) te Amsterdam voorbereid.

### Vraag 1

Het HB en de HvJ zijn van mening dat telewerken bij de sector politie wenselijk en acceptabel is, mits er voldoende maatregelen zijn getroffen op het gebied van beveiliging en er wordt voldaan aan wettelijke privacyeisen. Een kanttekening die het HB en de HvJ maken, is dat telewerken slechts voor bepaalde functies acceptabel is. Het verwerken van processen-verbaal zou bijvoorbeeld niet thuis mogen gebeuren. Politieambtenaren die dergelijke werkzaamheden verrichten zijn derhalve beperkt in de mogelijk-

heid tot telewerken. Ook voor ambtenaren met een specialisme, bijvoorbeeld CID-leden, zou telewerken niet vanzelfsprekend mogen zijn en eigenlijk gewoonweg niet mogen.

#### *Vraag 2*

De 'open' beveiligingseis die in veel wetgeving voorkomt, is in geen geval afdoende. Het is van groot belang dat er zware beveiligingscriteria worden opgesteld en dat er vervolgens monitoring plaatsvindt. Beveiliging moet op diverse punten goed geregeld worden, de techniek is een hele belangrijke.

#### *Vraag 3*

De uitzonderingspositie wat betreft de omgang met gegevens die de politie in veel wetgeving kent, maakt zware beveiligingscriteria nog meer van belang. Buiten de beveiligingsvraag zou men zich moeten afvragen of ambtenaren die met bepaalde gevoelige gegevens werken überhaupt de mogelijkheid tot telewerken moeten krijgen.

Dat telewerken bij de sector politie via wet- of regelgeving in goede banen moet worden geleid, is een feit. Wetgeving is niet noodzakelijk. Gezien de termijnen voor het vervaardigen en het inwerkingtreden van wetgeving, is regelgeving een goede optie. Een regeling/richtlijn moet op ministerieel niveau gemaakt worden.

Voor gebreken in de beveiliging bij telewerkers dient de korpschef verantwoordelijk te zijn.

#### *Vraag 4*

Het HB en de HvJ zijn van mening dat telewerken in eerste instantie slechts voor bepaalde functies mogelijk moet zijn, bijvoorbeeld in het kader van een pilot. Echter ook in de toekomst zal telewerken slechts voor bepaalde functies mogelijk moeten zijn. Niet elke functie is geschikt voor telewerken, dit is grotendeels afhankelijk van de aard van de werkzaamheden die door de betreffende ambtenaar worden verricht. De aard van de te verrichten werkzaamheden zou bepalend moeten zijn bij de beoordeling of telewerken voor een bepaalde functie mogelijk moet zijn. Beleidsfuncties komen volgens het HB en de HvJ wel in aanmerking voor telewerken.

#### *Vraag 5*

In het geval van thuiswerken is de thuissituatie een zeer belangrijk aspect. Het gebruiken van een antecedentenonderzoek om de thuissituatie van een ambtenaar te beoordelen is een te licht middel. Het HB en de HvJ denken meer in de richting van een veiligheidsonderzoek. Een en ander is mede afhankelijk van de aard van de werkzaamheden die een telewerker verricht en de aard van de gegevens waarmee hij/zij kan werken. Een voorbeeld van een situatie waarbij een ambtenaar niet in aanmerking zou komen voor thuiswerken, is het feit dat hij/zij in een studentenhuus woont. Op grond van de aard van een dergelijke woonsituatie zou telewerken niet mogelijk moeten zijn.

#### *Vraag 6*

Voor het heimelijk aftappen of opnemen van gegevens die door telewerkende politiemedewerkers worden verwerkt, zou een hogere strafmaat moeten gelden. Dit moet niet in de wet verankerd worden, maar zal in de praktijk moeten gebeuren, zoals ook op andere rechtsgebieden veelal hogere straffen worden geëist bij bepaald gedrag richting de politie. Een hacker die bewust het risico aangaat om politiegegevens te onderscheppen, mag hiervoor zwaarder gestraft worden dan dat het andere gegevens, niet zijnde politiegegevens, zou betreffen.

#### *Vraag 7*

Voor de mogelijkheid tot telewerken zullen er aparte afspraken met de telewerker moeten worden gemaakt. Dit kan in de vorm van een protocol. Een telewerker moet zich beseffen dat telewerken risicovoller kan zijn dan het werken vanaf de vaste (kantoor)werkplek. Dit wil niet zeggen dat de telewerker een grotere verantwoordelijkheid moet krijgen. De verantwoordelijkheid komt met name bij de werkgever te liggen. Deze moet zorgdragen voor goede voorzieningen.

#### *Vraag 8*

Het HB merkt nog op dat hij en de HvJ het lastig vonden de vragen te beantwoorden. Het is moeilijk om de uitwerking c.q. gevolgen van telewerken bij de sector politie in te schatten. Er wordt momenteel huiverig tegen aangekeken. Misschien is het koudwatervrees, maar dat zal de toekomst leren, aldus het HB en de HvJ.

Bij het OM zijn twee pilots geweest, die inmiddels zijn afgerond. Vanuit het ministerie van Justitie is de kaderregeling telewerken opgesteld. Door een werkgroep, waaraan het HB deelneemt, wordt momenteel aan de genoemde kaderregeling een nadere invulling gegeven ten behoeve van het OM. Op het niveau van het OM is derhalve de nodige ervaring en kennis aanwezig op het gebied van telewerken.

Het HB staat open voor vragen van BZK op het gebied van telewerken, ook een eventuele samenwerking zal positief ontvangen worden. Het HB is zeer geïnteresseerd in resultaten en eventuele plannen op het gebied van telewerken bij de sector politie.

## 7 Conclusies en aanbevelingen

### 7.1 Deelconclusies

#### 7.1.1 Algemeen

- De literatuur op het gebied van de juridische aspecten van telewerken is beperkt. Een belangrijke reden is dat in weinig wet- en/of regelgeving wordt ingegaan op deze specifieke werksituatie.
- Telewerken bij de sector politie moet specifiek bekeken worden in verband met haar takenpakket en haar positie in de maatschappij.

#### 7.1.2 Arbeidsrechtelijk / arbeidsvoorwaardelijk

- Bij de politie zullen de telewerkplekken zich op diverse locaties bevinden en mobiel kunnen zijn. Bij een mobiele telewerkplek zal het voor de werkgever complex zijn om aan alle verplichtingen uit de Arbo-wet te voldoen.
- Het Arbobesluit geeft de politie en brandweer een uitzonderingspositie, in die zin dat een aantal artikelen van de Arbo-wet slechts van toepassing zijn voor zover door de toepassing een goede taakuitoefening door politie en brandweer niet wordt belemmerd. Bij de invoering van telewerken kan deze uitzondering gunstig uitvallen.
- De bepalingen betreffende beeldschermwerk (afdeling 2 Arbobesluit) zijn niet van toepassing op zogenoemde draagbare systemen die niet aanhoudend worden gebruikt op een werkplek. Een positief aspect voor mobiele telewerkplekken.
- De Arbeidstijdenwet voorziet in flexibele arbeidspatronen. Controle door de werkgever op de naleving van de wet is mogelijk door gebruik te maken van geautomatiseerde toezichtssystemen. De privacy van medewerkers moet in acht genomen worden.
- Hoofdstuk III van het Barp bevat voor de politieambtenaren specifieke bepalingen over Arbeids- en Rusttijden.
- In de Politiewet en het Barp is de ambtenarenstatus van de politie vastgelegd, waardoor er met de invoering van telewerken geen discussie kan ontstaan over de arbeidsverhouding.
- De in het Barp voorkomende begrippen *aebouw*, *gebouwencomplex* en *terrein* vormen geen belemmering voor telewerken. De zinsnede '*waar de ambtenaar gewoonlijk zijn werkzaamheden verricht*' biedt zelfs ruimte voor telewerken. 'Standplaats' vormt geen knelpunt.

#### 7.1.3 Overig juridisch

- Op grond van de Regeling informatiebeveiliging politie moet een informatiebeveiligingsbeleid worden vastgesteld. In het kader van telewerken is het noodzakelijk voor de politie aandacht te besteden aan de beveiliging van de informatievoorziening en om de informatiebeveiliging aan te pakken op een gemeenschappelijke basis.
- De Wet bescherming persoonsgegevens is niet van toepassing op:
  - *verwerking van persoonsgegevens ten behoeve van de inlichtingen- en veiligheidsdiensten, bedoeld in de Wet op de inlichtingen en veiligheidsdiensten;*
  - *verwerking van persoonsgegevens ten behoeve van de uitvoering van de politietaak, omschreven in artikel 2 van de Politiewet 1993.*
- De niet toepasselijkheid van de wet geldt tevens voor het verbod om strafrechtelijke persoonsgegevens te verwerken.
- In de lijn van de Wet bescherming persoonsgegevens moet de sector politie de Wet politieregisters in acht nemen, waarin regels met betrekking tot de omgang met persoonsgegevens zijn opgenomen.
- Op grond van de Wet bescherming staatsgeheimen 1951 zou het mogelijk kunnen zijn dat een bepaalde (toekomstige) telewerklocatie niet gebruikt mag worden, omdat de locatie als een 'verboden plaats' is aangewezen.
- Artikel I sub G van het Voorstel Wet computercriminaliteit II biedt bescherming voor telecommunicatie via bedrijfsnetwerken en levert daarmee een positieve bijdrage voor telewerken.
- De beveiligingseis in de wet op de inlichtingen en veiligheidsdiensten is strikter/minder 'open' dan in andere wetgeving. De invoering van telewerken, voor de ambtenaren van de inlichtingen en veiligheidsdiensten, vereist op beveiligingsgebied een grotere inspanning vanwege de grotere mate van complexiteit.

- Op grond van de Wet justitiële gegevens mogen justitiële gegevens door middel van telecommunicatie worden verstrekt. De ontvanger van de gegevens, die verstrekt zijn via telecommunicatie, mag deze niet op geautomatiseerde wijze vastleggen of vermenigvuldigen, tenzij dit noodzakelijk is voor de uitvoering van een bepaalde taak. In het laatste geval moeten passende technische en organisatorische maatregelen ten uitvoer gelegd worden, waarvoor de Minister van Justitie verantwoordelijk is.
- Telewerken in vertrouwensfuncties ingevolge de Wet op de veiligheidsonderzoeken draagt het risico de veiligheid of andere gewichtige belangen van de staat te schaden.
- De Wet politieregisters kent een 'open' beveiligingseis. Iedere beheerder kan deze eis naar eigen inzicht invullen. Met de invoering van telewerken zal de beveiliging verzawaard c.q. aangepast moeten worden en zullen de te treffen voorzieningen complexer worden.
- Het Besluit politieregisters bevat beperkingen ten aanzien van gegevensverstrekking langs geautomatiseerde weg. Slechts personen die van de beheerder een schriftelijke autorisatie voor een daarbij bepaald omschreven doel hebben gekregen, kunnen gegevens langs geautomatiseerde weg ontvangen.
- De CID regeling bevat specifieke bepalingen met betrekking tot zogenaamde gevoelige gegevens, de groep van toegangsgerechtigden, beperkingen ten aanzien van verstrekking van gegevens uit het CID register en de bevoegdheden om systemen te koppelen. De aard van de opgeslagen gegevens en de functie van de CID leden maken dit noodzakelijk.
- Europese wetgeving met betrekking tot telewerken is niet aanwezig. De door de Europese Commissie opgestelde 'algemene beginselen voor de vaststelling van een kader voor telewerken' kunnen als aanknopingspunt worden gebruikt om de haalbaarheid van telewerken bij de politie -op arbeidsrechtelijk en arbeidsvoorwaardelijk vlak- te toetsen.
- De Europol Overeenkomst bevat een 'open' beveiligingseis: Lid-Staten moeten *passende maatregelen* treffen om een aantal opgesomde handelingen te verhinderen of juist te waarborgen. Nadere eisen met betrekking tot de passende maatregelen worden niet gesteld.
- Europol kent diverse beveiligingsniveaus. Uitwerkingen zijn opgenomen in een beveiligingshandboek. Om aan alle specifieke beveiligingseisen te voldoen zal meer inspanning en nauwkeurigheid vereist zijn.

#### 7.1.4 Interviews

- Telewerken bij de sector politie is wenselijk en acceptabel. Daarbij moet wel voldoende aandacht besteed zijn/worden aan beveiliging.
- De mogelijkheid tot telewerken moet gelden voor (diverse meningen):
  - Alle functies, mits efficiënt voor de functie en/of het moet een toegevoegde waarde hebben;
  - Bepaalde functies, afhankelijk van het takenpakket; leidinggevenden in ieder geval niet.
- De 'open' beveiligingseis - die in veel wetgeving voorkomt - is onvoldoende, omdat ieder korps zijn eigen invulling hanteert; er moeten landelijke beveiligingsnormen komen.
- Beveiliging is goed realiseerbaar, maar de 'open' eis moet wel goed ingevuld worden, d.w.z. organisatorisch, procedureel en technisch.
- Dat de politie op het gebied van gegevensverwerking veelal meer bevoegdheden heeft is goed. Wel moet hiermee rekening worden gehouden bij de beveiliging van systemen. De toegang tot systemen/gegevens zou naar functie beperkt moeten worden. Het hebben van meer bevoegdheden leidt tot druk op de integriteit.
- Specifieke regelgeving voor telewerken bij de sector politie is een must. Over de vorm waarin dit moet gebeuren zijn de meningen verdeeld:
  - Wetgeving is wenselijk, maar kost veel tijd. Het zou kunnen in de vorm van een basiswet met de mogelijkheid tot het nemen/vervaardigen van Besluiten.
  - Specifieke nieuwe wetgeving is niet gewenst. Een aanpassing van de Politiewet plus een regeling/richtlijn zou wel een optie kunnen zijn.
- Een regeling moet op hoog niveau (ministerie BZK) gemaakt worden.
- De verantwoordelijkheid voor gebreken in de beveiliging van systemen van telewerkende politie-ambtenaren moet liggen bij de korpsleiding.
- Telewerken moet ingevoerd worden, daar waar er de meeste behoefte aan is. In principe moet het mogelijk zijn voor alle functies. Er moeten geen functies benoemd worden, er moet gekeken worden naar de toegevoegde waarde. Dit is de overheersende gedachte. Een andere mening is dat slechts bepaalde functies in aanmerking kunnen komen voor telewerken. Het moet praktisch bekeken worden. Lijnfuncties komen niet in aanmerking voor telewerken.
- Het antecedentenonderzoek mag niet gebruikt worden om te oordelen over de bevoegdheid tot telewerken.

- De aansprakelijkheid bij telewerken moet geregeld worden via een protocol. De integriteit moet daarbij benadrukt worden.
- De verantwoordelijkheid van een telewerker moet vergroot worden, in het kader van naleving van het protocol en bewustwording van de integriteit. De verantwoordelijkheid van de politieregio moet vergroot worden met betrekking tot de te leveren voorzieningen.

## 7.2 Eindconclusie

De invoering van telewerken bij de sector politie is in principe haalbaar. De knelpunten, die voornamelijk worden gevormd door de grotere complexiteit van beveiliging bij telewerken en de verplichtingen in de Arbo-wet, zijn met de nodige inspanning op te lossen. Hiervoor zal op diverse vlakken onderzoek verricht moeten worden naar de mogelijkheden en de gewenste mate van beveiliging en de haalbaarheid van de Arboverplichtingen. Onderzoek is onder andere noodzakelijk op het gebied van inlichtingen en veiligheidsdiensten, de vertrouwensfunctie (Wet veiligheidsonderzoeken), de CID, het Besluit politieregisters en de Arbo-wet (uitwerking in aanbevelingen). De vervolgens op te stellen beleidsplannen op het gebied van beveiliging en Arbo moeten de invoering van telewerken bij de sector politie in goede banen leiden. Afstemming met een Europol 'insider' is zeer wenselijk om inzicht te krijgen in de Europese beveiligingsniveaus en -eisen. Gezien de soms verdeelde meningen van Justitie/OM medewerkers over telewerken bij de sector politie is ook afstemming met Justitie/OM en/of andere Ministeries of partijen gewenst.

## 7.3 Aanbevelingen

- Bij mobiele telewerkplekken zal een goed vooronderzoek verricht moeten worden om te kunnen bepalen of en op welke wijze verplichtingen uit de Arbo-wet haalbaar zijn. Indien er niet haalbare verplichtingen naar boven mochten komen, dient gekeken te worden of de betreffende verplichting onder een 'uitzondering'<sup>7</sup> voor de politie gebracht kan worden. Indien de verplichtingen in kaart zijn gebracht moeten procedures, rechten en verplichtingen eenduidig vastgelegd worden. Dit kan gebeuren in een arbeidsomstandighedenbeleidsplan, waarmee een goede basis voor de uitvoering gelegd wordt.
- Om controle op de naleving van arbeids- en rusttijden te realiseren, zonder daarbij de privacy van medewerkers te schenden, dient onderzocht te worden op welke wijze (geautomatiseerde) controle plaats kan vinden. Bekeken moet worden of controle wenselijk/noodzakelijk is; met welk systeem of welke middelen men controle wil gaan uitoefenen; of met de gekozen controlemogelijkheid de doeleinden worden vervuld (en niet meer). E.e.a. moet kenbaar gemaakt worden aan de medewerkers.
- De zinsnede uit het Barp '*waar de ambtenaar gewoonlijk zijn werkzaamheden verricht*' duidt op één locatie. Indien in een overeenkomst een plaats van tewerkstelling moet worden opgenomen, kunnen meerdere plaatsen van tewerkstelling worden aangewezen, om problemen in het kader van telewerken te voorkomen.
- Om te voorkomen dat telewerken het beheer van archiefbescheiden bemoeilijkt, is het raadzaam de zogeheten "zorgdrager"<sup>8</sup> te informeren over de invoering van telewerken bij de politie. De zorgdrager kan vervolgens aangeven of er specifieke zaken geregeld moeten worden of dat er bepalingen in bijvoorbeeld een regeling of richtlijn opgenomen moeten worden.
- Er moet een duidelijk standpunt ingenomen worden over het al dan niet opnieuw mogen uitvoeren van een antecedentenonderzoek bij invoering van telewerken.
- Op grond van de Regeling informatiebeveiliging politie moet een informatiebeveiligingsbeleid worden vastgesteld. Het is aan te bevelen dit op gemeenschappelijke basis uit te voeren; gedacht kan worden aan landelijke beveiligingsnormen.
- Indien invoering van telewerken voor de ambtenaren van de inlichtingen en veiligheidsdiensten wordt overwogen, dient in verband met de aard van de functie en de te verwerken gegevens onderzocht te worden op welke wijze aan de beveiligingsseis voldaan kan worden.
- Gezien het risico dat een vertrouwensfunctie (Wet op de veiligheidsonderzoeken) draagt, moet beoordeeld worden of telewerken bij dergelijke functies gewenst respectievelijk acceptabel is. De wet zelf geeft geen duidelijkheid. Het besluit zal mede afhankelijk moeten zijn van de aard en de mate van beveiliging die gerealiseerd kan worden.
- In verband met de beperkingen uit het Besluit politieregisters is het aan te bevelen voorafgaand aan de invoering van telewerken in kaart te brengen welke politieambtenaren een autorisatie (moeten) hebben om bepaalde gegevens via geautomatiseerde weg te ontvangen.

<sup>7</sup> Hiervoor dient het Arbobesluit geraadpleegd te worden.

<sup>8</sup> Zorgdrager: degene die bij of krachtens de wet belast is met de zorg voor de archiefbescheiden.

- Gezien de aard van de gegevens en de functie van de CID leden moet beoordeeld worden of telewerken bij de CID gewenst respectievelijk acceptabel is. Er dient rekening gehouden te worden met het realiseren van een zeer zware beveiliging.
- Indien er nieuwe arbeidsovereenkomsten of een nieuwe CAO worden/wordt gevormd is het aan te bevelen om daarbij rekening te houden met de Europese algemene beginselen voor de vaststelling van een kader voor telewerken.
- Wat betreft de Europol beveiligingseisen is het raadzaam een Nederlandse vertegenwoordiger (indien afgevaardigd) te raadplegen over de verschillende niveaus en het beveiligingshandboek. Ook bij de door iedere Lid-Staat opgerichte of aangewezen nationale eenheid zal voldoende kennis aanwezig zijn om te beoordelen welke maatregelen getroffen moeten worden om telewerken bij de sector politie te laten slagen.
- Op het moment dat er duidelijke ideeën zijn over de wijze van invoering van telewerken bij de sector politie, met name op het vlak van beveiliging, zou het College Bescherming Persoonsgegevens gevraagd kunnen worden hun visie op (concept) plannen te geven.
- Het is aan te bevelen de resultaten van de pilot telewerken bij het OM te volgen c.q. op te vragen, evenals het protocol dat momenteel wordt opgesteld.

# BIJLAGE

## Telewerken politie: relevante wet- en regelgeving

1. Arbeidsomstandighedenwet 1998 (Arbowet)
  - Wet van 13 december 2000 tot wijziging van de Arbowet 1998
  - *Stb. 2000, 595.*
  - Beleidsregels Arbowet 1998.
2. Arbeidsomstandighedenbesluit (Arbobesluit) *Stb. 1999, 451*
3. Arbeidstijdenwet *Stb. 1995, 598*
4. Arbeidstijdenbesluit *Stb. 1998, 407*
5. Archiefwet 1995 *Stb. 1995, 276*
6. Archiefbesluit 1995 *Stb. 1995, 671*
7. Besluit algemene rechtspositie politie (Barp)
  - Besluit van 23 februari 1998, houdende wijziging van het Barp, het Besluit rechtspositie vrijwillige politie en het Besluit politieregisters in verband met het antecedentenonderzoek voor de politie *Stb. 1998, 144.*
  - Besluit van 7 september 1998, houdende wijziging van het Barp, het Besluit rechtspositie vrijwillige politie in verband met onder meer de invoering van de Wet op de medische keuringen *Stb. 1998, 586.*
8. Burgerlijk Wetboek (artikel 7:658; titel 3 van boek 6)
9. CID regeling 1995 *Stcrt. 1995, 74*
10. Comptabiliteitswet
11. Europol overeenkomst
12. Europol geheime informatie
13. Politiewet 1993
  - Aanpassingsbesluit Politiewet 1993.
  - Wet van 22 december 1999 tot wijziging van de Politiewet 1993 en de Wet politieregisters in verband met de overdracht van het beheer van het KLPD aan de Minister van BZK.
14. Regeling informatiebeveiliging politie *Stcrt. 1997, 60*
  - Wijziging Regeling informatiebeveiliging politie *Stcrt. 1998, 134*
15. Regeling uitvoering antecedentenonderzoek door de politie *Stcrt. 1999, 17*
16. Wet bescherming persoonsgegevens *Stb. 2000, 302*
17. Wet bescherming Staatsgeheimen 1951
18. Voorstel van Wet Computercriminaliteit II
19. Gewijzigd voorstel van Wet op de inlichtingen en veiligheidsdiensten
  - Artikel "De oude en de nieuwe Wet op de Inlichtingen- en veiligheidsdiensten".
20. Gewijzigd voorstel van Wet justitiële gegevens
  - Derde nota van wijziging (10 oktober 2001)
21. Wet veiligheidsonderzoeken *Stb. 1996, 525*
  - Beleidsregels veiligheidsonderzoeken voor de politie *Stcrt. 2001, 241*
22. Wet openbaarheid van bestuur
  - Wet van 12 maart 1998 tot wijziging van de WOB in verband met de implementatie van de richtlijn nr. 90/313/EEG van de Raad van de Europese Gemeenschappen van 7 juni 1990 inzake de vrije toegang tot milieu-informatie *Stb. 1998, 180.*
23. Wet politieregisters *Stb. 1990, 414.*
  - Wet van 27 mei 1999 – bijzondere politieregisters *Stb. 1999, 244.*
24. Besluit politieregisters
  - Besluit van 5 juli 1997, houdende wijziging van het Besluit politieregisters *Stb. 1997, 326.*
  - Besluit van 12 oktober 1999, houdende wijziging van het Besluit politieregisters in verband met het stellen van nadere regels voor bijzondere politieregisters, het uitbreiden van de kring van informatiege-rechtigden en het aanbrengen van enige wijzigingen van technische aard *Stb. 1999, 455.*
  - Besluit van 30 januari 2001, houdende wijziging van het Besluit gebruik sofi-nummer en het Besluit poli-tieregisters met het oog op het verbeteren van de mogelijkheden tot het controleren van de juistheid van gegevens en het aanbrengen van enkele andere wijzigingen *Stb. 2001, 54.*
25. Aanwijzingen voor de beveiliging van staatsgeheimen en vitale onderdelen bij de Rijksdiensten *Circulaire van 20 januari 1989.*
  - Tevens 2 documenten in het kader van de aanwijzingen voor beveiliging overheid