

Internet-policies

Controlebevoegdheid

versus

privacy



Afstudeerscriptie
ir. L.J.M. Dullaart

Universiteit van Leiden
Faculteit der Rechtsgeleerdheid
Juni 2001

Internetpolicies

Controlebevoegdheid versus privacy

L.J.M. Dullaart

1. Inleiding

1.1 Waarom een Internet policy?

Met de groei van het Internet is ook het belang ervan toegenomen: steeds meer informatie wordt ontsloten via Internet. Voor werknemers is deze informatie vaak van belang voor hun functioneren. Dit is de reden dat steeds meer bedrijven en instellingen ertoe overgaan om Internet voor hun werknemers te ontsluiten.

Met de ontsluiting van het Internet neemt ook de kans op misbruik toe. (1) De angst voor misbruik is voor een aantal bedrijven en instellingen reden geweest om Internet-policies op te stellen. (2) Zo'n policy bevat regels waaraan het gebruik van Internet als medium gebonden is. Daarnaast hebben ook de FNV en VNO/NCW een voorbeeld-policy opgesteld. (3) Al deze policies stellen in meerdere of mindere mate grenzen aan het gedrag van de werknemer. Dergelijke grenzen zijn alleen effectief als ze gecontroleerd kunnen worden en er sancties op de overtredingen staan.

Het is nog niet eens zo lang geleden dat een leidinggevende zelf direct toezicht hield op de aanwezigheid en de gedragingen van zijn werknemers. Tegenwoordig wordt een deel van die controle automatisch uitgeoefend via toegangsbadges, gespreksstatistieken uit de telefoon-centrale en tegenwoordig ook via computerlogs van het Internet-gebruik. Waar in het verleden de werknemer enige invloed op de controle kon uitoefenen, bijvoorbeeld door activiteiten tijdens de afwezigheid van de leidinggevende te plannen, is tegenwoordig de controle omni-present, permanent en voorzien van een lang en gedetailleerd geheugen. Hierdoor is het voor de rechtszekerheid van de werknemer noodzakelijk, dat de gedragsregels duidelijk vastliggen en dat ook bekend is wat, wanneer en hoe er gecontroleerd wordt.

1.2 Wat is een Internet-policy?

Een Internet policy geeft aan hoe een werknemer zich op het Internet moet gedragen. De gedragingen van een werknemer zijn divers:

- Een werknemer kan surfen op het Web. Daarbij laat hij duidelijke sporen na die verwijzen naar de werkgever;
- Een werknemer maakt gebruik van e-mail;
- Een werknemer kan posten op een newsgroup of mailing-list;
- Een werknemer kan, gebruik makend van apparatuur van de werkgever, services aan derden verlenen of
- Een werknemer kan, gebruik makend van apparatuur van de werkgever, de wet overtreden.

Een Internet policy stelt grenzen aan wat een werknemer mag en kan doen op het Internet als eindgebruiker. De noodzaak hiervan wordt algemeen aanvaard. (4) Het aanbieden van diensten op Internet valt buiten het bereik van de Internet-policy.

Aan de andere kant geeft een werkgever aan welke controles hij uitvoert en welke registratie hij daarvoor aanlegt. Een werknemer zou op basis van die policy moeten kunnen bepalen wat voor privacy hij overhoudt.

1.3 Inhoud van deze scriptie

In deze scriptie wil ik nagaan wat de grenzen zijn aan de controlemogelijkheden van de werkgever. Ik zal mij daarbij beperken tot het civiel-rechtelijke gedeelte. Dit betekent dat strafrechtelijke sancties ten opzichte van de werkgever buiten het kader van deze scriptie vallen. De strafrechtelijke normen kunnen wel een rol spelen, bijvoorbeeld bij de vaststelling of een bepaalde gedraging onrechtmatig is. Ook de positie van ambtenaren, die op een aantal punten wezenlijk verschilt van de positie van de werknemer in de private sector, zal slechts zijdelings aan bod komen.

Het plan van de behandeling is als volgt:

- Eerst zullen de grenzen tussen de privacy van de werknemer en de controle-mogelijkheden van de werkgever verkend worden. Na een behandeling van de relevante wettelijke normen zullen de regels bij de al wat langer bestaande controles behandeld worden.

- Voor de traditionele controles zal ook even kort over de grens worden gekeken.
- Op basis van de regels voor traditionele controle zullen regels opgesteld worden voor de controle op Internet gebruik. Deze regels zullen vergeleken worden met recente publicaties van onder andere de FNV en de Registratiekamer. Ook zullen de regels vergeleken worden met de rechtspraak.
- Tot slot zal het effect van de grenzen in de rechtspraak onderzocht worden, met name in het kader van de bewijsvoering.

In deze scriptie wordt de term incident gebruikt als een verschijningsvorm van een overtreding van een regel. Een voorbeeld maakt dit duidelijker: Wanneer er een kastekort is, dan is er sprake van een incident. De overtreden regel kan een mathematische zijn (er is een rekenfout gemaakt) of bijvoorbeeld artikel 321 Wetboek van Strafrecht (verduistering).

2. Controles en privacy op de werkplek

2.1 De privacy van de werknemer

Het is moeilijk om, ook internationaal, een sluitende definitie van privacy te vinden. Bij de definitie van het privacy-begrip grijpt men steeds terug op een artikel van S.D. Warren en L.D. Brandeis waarin zij stellen dat: "Privacy is the right to be left alone". (5) Dit artikel is echter geschreven in een andere context dan de hedendaagse arbeidssituatie. Een veel bruikbaarere definitie wordt aangereikt door Blok en Vedder: privacy is de afwezigheid van ongerechtvaardigde betrekkingen tussen de persoon en anderen. (6) De nadruk ligt in dit geval niet op de afzondering van het individu van de maatschappij, maar op de noodzaak om deze interactie te reguleren.

In Nederland vindt men het recht op privacy terug in verschillende bepalingen van de Grondwet, als eerbiediging van de persoonlijke levenssfeer, het verbod op binnentreden van de woning, briefgeheim, etcetera. Ook in de voorstellen van de Commissie 'Grondrechten in het digitale tijdperk' staat het recht op privacy verspreid over verschillende bepalingen. De privacy die in de Grondwet is gedefinieerd is een privacy ten opzichte van de overheid. Het is duidelijk dat dergelijke regels overheidsingrijpen ten opzichte van burgers inperken. De machtspositie van de overheid maakt deze inperking noodzakelijk.

Minder duidelijk is of het recht op privacy ook horizontale werking, dat wil zeggen tussen burgers onderling, heeft (7) In het eindrapport van de Commissie Grondrechten in het digitale tijdperk geeft de commissie aan dat de privacy, voor zover het de eerbiediging van de persoonlijke levenssfeer betreft, zowel in de interpretatie van privaatrechtelijke begrippen als in wettelijke normen vastligt. (8) Voorbeelden van horizontale werking van het communicatiegeheim zijn de Commissie niet bekend.

Het belang van de horizontale werking van grondrechten is met name groot in een arbeidssituatie. Er is hier namelijk zowel sprake van een contract tussen burgers onderling als van een zekere machtsverhouding. Vanuit de positie van de werkgever kan aan de werknemer een beperking van zijn privacy opgelegd worden. De Registratiekamer formuleert dit als volgt: (9)

In werktijd geniet men niet dezelfde vrijheden als daarbuiten. De arbeidsverhouding brengt zekere beperkingen met zich mee voor de grondrechten van werknemers. Tegenover het loon staat de verplichting werkzaamheden te verrichten onder het gezag van de werkgever en hierbij diens aanwijzingen op te volgen. De werknemer is als gevolg daarvan in meer of mindere mate beperkt in zijn bewegings- en handelingsvrijheid en in zijn vrijheid van meningsuiting. Hetzelfde geldt voor zijn recht op privacy. Met het betreden van de werkplaats moet de werknemer een deel van zijn aanspraken op respect voor zijn persoonlijke levenssfeer inleveren. Dit betekent niet dat een werkgever bij het nastreven van zijn belang zonder meer aan de belangen en fundamentele vrijheden van zijn medewerkers voorbij kan gaan.

Er zijn dus grenzen aan de controle-bevoegdheid van de werkgever en de belangrijkste grens wordt gevormd door de inbreuk die een dergelijke controle op de persoonlijke levenssfeer van de werknemer maakt.

Hier komt ook een paradox naar voren. (10) Aan de ene kant is de werkgever bevoegd aanwijzingen te geven over de te verrichten werkzaamheden. (11) andere kant blijft de werknemer een recht op privacy houden. De werkgever koopt wel tijd en inspanning van de werknemer, maar niet zijn ziel.

2.2 Wettelijke normen

De persoonlijke levenssfeer van de werknemer wordt beschermd door verschillende verdrags- en wetteksten. De belangrijkste bescherming wordt gegeven door de grondrechten zoals vast gelegd in artikel 8 van het Europees Verdrag van de Rechten van de Mens (EVRM). De discussie over de horizontale werking van dit grondrecht wordt in de praktijk soms geheel overgeslagen. Zo overweegt de Kantonrechter in Zwolle: (12)

Voorop staat, dat VCVO als werkgeefster de persoonlijke levenssfeer van Drexhage als werknemer heeft te eerbiedigen, reeds omdat artikel 8, eerste lid, EVRM in de verhouding tussen werkgever en werknemer doorwerkt.

Daarnaast geeft de Europese Unie specifiek voor beeldscherm-medewerkers aan, dat er zonder medeweten van de werknemers geen gebruik mag worden gemaakt van een kwantitatief of kwalitatief controlemechanisme. (13)

In Nederland verplicht artikel 7:611 Burgerlijk Wetboek (BW) de werkgever zich te gedragen als een goed werkgever. Algemeen geaccepteerd wordt dat dit artikel tevens als schakelbepaling kan dienen als een directe horizontale werking van grondrechten niet of moeilijk kan worden vastgesteld. (14) De Wet Bescherming Persoonsgegevens (Wbp) biedt een specifieke vorm van privacy: de informationele privacy. De Wbp is een uitwerking van de Europese Richtlijn. (15) vergelijking tussen de materiële normen uit de Wbp en de Europese Richtlijn valt buiten het kader van deze scriptie. De Europese richtlijn is bedoeld om in Europa een uniforme regeling van de bescherming van de persoonlijke levenssfeer te creëren.

De Wbp wordt ook gezien als de opvolger van de WPR. Algemeen wordt aangenomen dat er geen grote materiële verschillen tussen de twee wetten zijn waar het gaat om de bescherming van het individu. Omdat de Wbp een kaderwet is met veel vage begrippen, zal de interpretatie hiervan waarschijnlijk conform de WPR gebeuren. Hierbij zal de jurisprudentie, die onder de WPR gewezen is, leidend blijven. (16) Eén van de verschillen tussen de Wbp en de WPR is, dat het verzamelen van gegevens onder de Wbp valt, ongeacht of deze gegevens in een persoonsregistratie voorkomen. (17)

Het verzamelen van gegevens viel alleen onder de WPR als er een persoonsregistratie werd aangelegd. Controle door de werkgever is een manier van verzamelen van gegevens en de verzamelde gegevens zijn persoonsgegevens in de zin van artikel 1 Wbp. Of de verwerking van de gegevens onder de Wbp valt, wordt in artikel 2 bepaald. Omdat een geautomatiseerde verzameling eigen is aan computer-logs zal controle van het Internet-gebruik altijd onder de Wbp vallen. Het staat de werkgever dus niet vrij om onbeperkt informatie over het Internet-gebruik van zijn werknemers te verzamelen.

Om te mogen controleren moeten de regels van de Wbp nageleefd worden. De gronden voor een dergelijke controle zijn te vinden in artikel 8 Wbp:

sub a: Ondubbelzinnige toestemming. De eisen aan de ondubbelzinnigheid zijn zeer streng. De toestemming moet in alle vrijheid gegeven worden. De werknemer mag niet de indruk hebben, dat hij gedwongen wordt tot de toestemming. Omdat een werkgever in een arbeidsrelatie een machtspositie heeft, kan de toestemming niet zonder meer als rechtvaardiging van de controle gehanteerd kan worden. Ook het opnemen van een toestemmingsbepaling in de arbeidsovereenkomst kan niet als toestemming gezien worden. In beide gevallen staat de werknemer immers 'onder druk [...] van de relatie waarin hij staat tot de verantwoordelijke'. (18)

Ook ad-hoc toestemming aan de werkgever, bijvoorbeeld in het kader van een disciplinair onderzoek, zal niet als ondubbelzinnige toestemming mogen gelden. (19)

sub b: Noodzakelijk voor de uitvoering van de overeenkomst. Een arbeidsovereenkomst is weliswaar een overeenkomst zoals bedoeld in artikel 8 sub b Wbp, maar het zal zelden zo zijn, dat de controles *noodzakelijk* zijn om de arbeidsovereenkomst uit te voeren.

sub c: Ter uitvoering van wettelijke verplichtingen. Omdat Internet Service Providers aan de overheid de mogelijkheid tot af luisteren moeten geven, kan het voorkomen dat ook een werkgever dergelijke gegevens zal moeten verstrekken. Dit rechtvaardigt echter nog geen reguliere controle.

sub f: Ter behartiging van een gerechtvaardigd belang. Het gerechtvaardigde belang van de werkgever kan bijvoorbeeld zijn dat de werknemer voldoende tijd overhoudt voor zijn normale werkzaamheden. Ook het voorkomen van ongewenste intimiteiten via e-mail is zo'n gerechtvaardigd belang. Maar het belang kan ook louter technisch zijn, zoals de beperking van het netwerk-verkeer. Deze belangen moeten afgewogen worden tegen het recht op privacy van de werknemer.

Volgens artikel 7 Wbp mag de verwerking van persoonsgegevens alleen plaatsvinden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Een omschrijving als 'controle op de naleving van de Internet-policy' is in het algemeen te vaag. Het doel moet de mate van controle rechtvaardigen. Het ligt voor de hand om de belangen, die in de afweging zoals bedoeld in artikel 8, sub f worden gebruikt, in het doel van de controle te laten doorklinken. Het doel van de controle bepaalt ook de manier waarop de controle kan plaatsvinden. Als het doel de beperking van het netwerk-verkeer is, dan zou geanonimiseerde verkeersanalyse voldoende controle zijn. Als de controle bedoeld is om te verzekeren dat klanten correct te woord gestaan worden, zou men kunnen

volstaan met steekproeven. Het is daarom belangrijk dat het doel van de controles duidelijk is aangegeven. Een werkgever mag alleen in specifieke gevallen hiervan afwijken. De gronden hiervoor staan vermeld in artikel 43 Wbp. Voor werkgevers is van belang dat, wanneer de artikel 43, sub e spreekt over 'rechten en vrijheden van anderen', de werkgever zelf bij 'de anderen' is inbegrepen.

De doelbinding komt ook terug bij de bepaling van de bewaartermijn. Als de gegevens niet meer relevant zijn voor het doel waarvoor ze verzameld worden, dan moeten ze vernietigd worden. Het is moeilijk om aan te geven welke termijn voor de log-gegevens geldt. Uit het vrijstellingsbesluit bij de WPR blijkt dat gegevens voor het interne beheer van de organisatie zes maanden nadat de persoon de organisatie verlaten heeft, vernietigd moeten worden. (20)

De werknemer moet op de hoogte zijn van de controle. Dat volgt uit artikel 33 Wbp. Eventueel zou men kunnen betogen dat de gegevens niet bij de werknemer worden verkregen, maar bijvoorbeeld uit een centrale firewall. Volgens artikel 34 Wbp moet de werknemer dan op het moment van vastlegging van de gegevens gewaarschuwd worden (lid 1), tenzij dit onevenredig veel inspanning kost (lid 4). Niet valt in te zien hoe de kennisgeving van een voorgenomen controle vooraf onevenredig veel inspanning zou kosten.

De Wet op de Ondernemingsraden (WOR) garandeert geen materiële privacy van de werknemers ten opzichte van de werkgever, maar garandeert dat de vertegenwoordigers van de werknemers instemmen met de regelingen op dit gebied. (21) Een toestemming van de Ondernemingsraad om controles uit te voeren is overigens geen toestemming in de zin van artikel 8, sub a Wbp. Een werknemer kan zich verzetten tegen de controles, zelfs als de Ondernemingsraad hiermee heeft ingestemd. Dat blijkt uit FNV/KOMA. (22) De FNV kwam daar in kort geding met succes op tegen videocontrole, ondanks een goedkeuring voor het plaatsen van camera's door de Ondernemingsraad.

De werkgever kan instructies geven aan de werknemer. Deze bevoegdheid is geregeld in artikel 7:660 BW. In de instructie kan de werkgever voorschriften geven omtrent de 'goede orde' in zijn onderneming. Voorbeelden hiervan zijn een rookverbod en de verplichting om een helm te dragen. De werkgever kan dat vaak eenzijdig doen, maar in bepaalde gevallen heeft hij de medewerking van de ondernemingsraad. Dit betekent overigens nog niet dat het de werkgever vrij staat om te controleren: als een werkgever meent dat zijn belangen prevaleren boven het recht op persoonlijke levenssfeer van de werknemer, dan zal hij dat aannemelijk moeten maken. (23)

In het strafrecht verbieden de artikelen 139a-e SR het af luisteren van communicatie en het aftappen van gegevens. Opvallend is dat deze tap-verboden voor alle gegevensoverdrachten gelden. Deze normen zijn strafrechtelijke normen en vallen als zodanig buiten de reikwijdte van deze scriptie. Zij kunnen echter wel een rol spelen in het kader van de onrechtmatige daad; artikel 6:162 BW spreekt immers over 'doen of nalaten in strijd met een wettelijke plicht'.

2.3 Controles in de praktijk

De belangrijkste beperking aan de controleerbaarheid van Internet-gebruik is de inbreuk die een dergelijke controle maakt op de persoonlijke levenssfeer van de werknemer. Een werkgever maakt echter op verschillende andere terreinen inbreuk op de privacy.

2.3.1 De telefoon

Een onderdeel van de wettelijke bescherming van de privacy bestaat uit het telefoongeheim. In de Nederlandse Grondwet is het telefoongeheim geregeld in artikel 13, lid 2 GW. Volgens de Grondwet zijn er slechts twee mogelijke inbreuken:

- bij de wet bepaald of
- door of met machtiging van hen die daartoe bij wet zijn aangewezen.

Daarbij lijkt de werkgever geen recht te hebben om inbreuk te maken op dit telefoongeheim. De praktijk is echter anders. De bescherming van artikel 13 lid 2 GW is bedoeld voor de communicatie over publieke netwerken. In bedrijven loopt de communicatie veelal over de eigen infrastructuur van de werkgever. De werkgever is ook meestal de abonnee van de aansluiting op het publieke netwerk. Een horizontale werking van het telefoongeheim kan daarom niet zondermeer worden aangenomen.

Bij een enquête tijdens het in 1997 gehouden congres 'De werknemer achtervolgd' gaf 51% van de ondervraagden aan dat telefoongesprekken geregistreerd werden. (24) Werkgevers luisteren om verschillende redenen mee, bijvoorbeeld voor:

- Coaching en beoordeling van telefonistes;
- Het tegengaan van privé-gebruik of
- Het verzamelen van juridisch bewijs bij transacties of fraude.

In de beoordeling van het meeluisteren door de werkgever is een ontwikkeling te zien waarbij de privacy van de werknemer een grotere rol gaat spelen. Ter illustratie een drietal uitspraken:

In 1987 overweegt de Hoge Raad dat het enkele opnemen van telefoongesprekken niet voldoende inbreuk op de persoonlijke levenssfeer is om de bandopname onrechtmatig te maken. (25) Of het maken van zo'n bandopname onrechtmatig is, hangt mede af van de aard en de mate van intimiteit van de gevoerde conversatie.

In 1993 bepaalt de Centrale Raad van Beroep, dat een telefoniste/operatrice niet verwijtbaar werkeloos is wanneer zij, geconfronteerd met het feit dat zij afgeluisterd wordt, ontslag neemt. (26) De werknemster was van te voren niet op de hoogte van de controle.

In 1996 besluit L. een privé-detective in te huren om een van de directeurs af te luisteren. L. had vermoedens uit de tweede hand, dat de directeur apparatuur had meegenomen. Dergelijke vermoedens zijn volgens de Rechtbank Utrecht onvoldoende om een telefoon-tap te rechtvaardigen. (27) Het door de tap verkregen bewijsmateriaal is derhalve in beginsel onrechtmatig. Het wordt echter wel meegewogen.

De Registratiekamer geeft vuistregels voor het registreren en opnemen van telefoongesprekken. (28) Daarbij onderscheidt zij verschillende redenen voor deze registratie, elk met hun eigen voorwaarden en beperkingen. Globaal zijn de volgende regels te onderscheiden:

- Voor regelmatig registreren, mee- of afluisteren is toestemming van de ondernemingsraad noodzakelijk. De werknemer moet op de hoogte zijn.
- Incidenteel mag een werkgever gericht telefoongesprekken opnemen en analyseren zonder toestemming van de Ondernemingsraad. Er moet dan een dringende reden zijn, zoals ernstige bedreigingen of het leveren van bewijs van ernstige misdrijven.
- Managementinformatie moet zo snel mogelijk gedepersonaliseerd worden.
- Opnames en registraties moeten vernietigd worden zodra hun relevantie vervalst.
- Een geautomatiseerde verzameling gespreksopnames moet bij de Registratiekamer aangemeld worden.

Naast het werkelijke afluisteren is het mogelijk om uiterlijke kenmerken van een telefoongesprek vast te leggen. Men moet hierbij denken aan bijvoorbeeld tijdsduur, gebelde nummers en kosten. Ook het vastleggen van dergelijke gegevens maakt inbreuk op de privacy van de werknemer voor zover ze herleidbaar zijn tot de individuele werknemer. (29)

Naar aanleiding van een klacht heeft de Registratiekamer aangegeven, dat gespecificeerde nota's van een privé-aansluiting niet zomaar aan de werkgever gestuurd kunnen worden wanneer deze de telefoonkosten betaalt. (30) Dit ligt uiteraard anders bij het telefoneren vanaf de werkplek. Bij een privé-aansluiting is de verhouding tussen privé-gesprekken en zakelijke gesprekken anders. Daarnaast is bij een zakelijke aansluiting de werkgever (meestal) ook de abonnee. Toch gebruikt de Registratiekamer hier min of meer dezelfde criteria: de werknemer moet geïnformeerd zijn en er moet toestemming van de werknemer voor het verstrekken van de gegevens verleend zijn.

2.3.2 Briefgeheim

Het briefgeheim is vastgelegd in de Grondwet. De bescherming is sterker dan het telefoongeheim.

In de praktijk blijken er weinig problemen te zijn met het briefgeheim in de werksituatie. (31) Uitspraken zijn in ieder geval dun gezaaid. Als het briefgeheim ter sprake komt, is dit meestal een van het briefgeheim afgeleid recht.

Waar het briefgeheim op de werkplek ter sprake komt, wordt meestal verwezen naar een uitspraak van de Rechtbank in Amsterdam. (32) In dit vonnis worden faxen met een zakelijke inhoud die in een ordner op het bureau staan niet als behorende tot de persoonlijke levenssfeer beschouwd.

Ervaringsregels zoals voor de controle op het telefoon-gebruik gevonden zijn, zijn dan ook moeilijk te geven. Wellicht de enige regel is, dat duidelijk moet zijn wat wel en wat niet tot de persoonlijke levenssfeer van de werknemer behoort.

2.3.3 Camera's op de werkplek

Het plaatsen van camera's op de werkplek is de meest verregaande manier van automatische controle op de werkplek. Toch is de acceptatie van controle met een camera in Nederland steeds groter. In een uitgave van de Registratiekamer worden de regels voor de controle met camera's op de werkplek uitgelegd. (33) Daarbij wordt onderscheid gemaakt tussen het plaatsen van verborgen camera's en het gebruik van zichtbare camera's.

Het plaatsen van verborgen camera's is in principe niet toegestaan. De enige uitzondering die de Registratiekamer vermeldt, is een tijdelijke plaatsing die noodzakelijk is en waarvoor geen alternatieven bestaan.

In een arrest van 27 april 2001 woog de Hoge Raad de privacy van een werknemer af tegen het gebruik van een verborgen camera door de werkgever. (34) Het middels deze camera verkregen bewijsmateriaal was niet onrechtmatig, omdat 1) er een concreet vermoeden bestond dat de werknemster zich schuldig maakte aan strafbare feiten, 2) dit niet zonder camera bewezen zou kunnen worden, 3) de camera alleen de gedragingen bij de kassa vastlegde en 4) de camera slechts vier weken was opgesteld.

Volgens de Registratiekamer is het plaatsen van zichtbare camera's wel toegestaan. Daarbij gelden de volgende regels:

- Er moet een goede reden voor zijn. Met deze formulering van de Registratiekamer wordt verwezen naar de proportionaliteitseis. Uit de checklist van de Registratiekamer blijkt dat er een noodzaak moet zijn voordat cameratoezicht is toegestaan. (35)
- Werknemers (en eventuele klanten) moeten weten dat er camera's hangen.
- Opnames mogen niet langer dan 24 uur bewaard blijven.
- Als er digitale opnames gemaakt worden dan moet dit aangemeld worden bij de Registratiekamer (36)
- De Ondernemingsraad moet toestemming verlenen.
- Personeel moet de mogelijkheid hebben om persoonlijke activiteiten buiten het toezicht te laten plaatsvinden

De rechtspraak is minder veeleisend. Voor de plaatsing van een gesloten TV-circuit noemde de Rechtbank in Roermond slechts als eis dat de werkgever een gewichtiger belang dan de persoonlijke levenssfeer van werknemer moet hebben (dat wil zeggen 'een goede reden') en dat er afspraken met het betrokken personeel moeten zijn gemaakt over het gebruik van het TV-circuit en de controle daarop. (37) In 1997 volstond de mededeling dat een magazijn niet behoort tot het gebied dat tot de persoonlijke levenssfeer kan worden gerekend. (38) Eveneens in 1997 oordeelde het Kantongerecht in Schiedam dat een camera, gericht op een specifieke kast in een omgeving waar camera's gewoon waren, geen onredelijk middel is. (39) Januari 2001 oordeelde de Rechtbank in Arnhem dat de privacy van de vrijwillige brandweer ondergeschikt is aan de integriteit van het corps als er concrete aanwijzingen zijn dat er geld ontvreemd wordt. (40) Of deze concrete aanwijzing een harde eis is of slechts een van de mogelijke omstandigheden is niet duidelijk.

2.3.4 Andere privacy-schendingen

Naast de camera's, telefoontaps en het openen van brieven zijn er nog vele andere manieren waarop de werkgever inbreuk kan maken op de privacy van de werknemer. Zo komt het voor dat werkgevers privé-detectives inhuren om bepaalde werknemers te volgen. (41) Andere bedrijven fouilleren hun werknemers. (42)

In *Smyth vs. Pillsbury* (43) wordt aangegeven dat verschillende vormen van privacy-schendingen niet op één lijn staan. Dit naar Amerikaans recht gewezen vonnis is niet direct van toepassing op Nederland. De daar gebruikte argumenten zijn echter wel valide. Het vonnis gaat ervan uit dat er een verschil is tussen eenzijdige privacy-schendingen door een werkgever, zoals drugs- en alcoholtesten en zelf geïnitieerde communicatie, zoals een e-mail.

Het inschakelen van detectives, visitatie en drugs- en alcoholtesten lenen zich minder voor een automatische verwerking. Zij vallen in die zin dus niet onder de Wbp. (44) Bovendien zijn dit controles, die zich in de periferie van het werk afspelen. Het verschil tussen de controles op telefoon, (schriftelijke) correspondentie en camera-toezicht enerzijds en visitatie en het laten volgen door detectives anderzijds is dat de eerste direct ingrijpen op de manier waarop een werknemer zijn werk doet en daarbij eventueel privé-belangen behartigt. Deze controles zijn meer activiteitgericht, terwijl bijvoorbeeld visitatie meer persoonsgericht is. Dat maakt de schending van de persoonlijke levenssfeer weliswaar niet minder ernstig, maar hierdoor zijn zij minder geschikt voor een vergelijking met het gebruik van het Internet.

2.4 Tussenconclusie

De privacy-grondrechten van een werknemer zijn niet onverkort van toepassing in de beperkte scope van de arbeidsrelatie. De werkgever kan beperkingen opleggen die voortvloeien uit de arbeidsrelatie. Dit betekent echter niet dat de werknemer in het geheel geen privacy op de werkplek overhoudt.

De werkgever zal zich bij controles in ieder geval aan de wettelijke bepalingen van de Wbp en artikel 7:611 BW moeten houden. Op basis van de wettelijke normen en de onderzochte controlevormen kunnen algemene regels opgesteld worden waar elke vorm van controle aan onderworpen zou moeten zijn:

- Er moet een duidelijke reden zijn voor de controle; de controle moet een bedrijfsbelang dienen.
- De werknemers moeten van te voren op de hoogte zijn van de controle.
- De Ondernemingsraad moet toestemming hebben gegeven voor de controle.
- Er moet een beperkte bewaartermijn zijn van de gegevens.
- Incidenteel toezicht zonder toestemming is toegestaan bij beveiligingsincidenten of wetsovertredingen
- Er moet een mogelijkheid zijn om buiten de controle om enige persoonlijke activiteiten te verrichten.

Uit de onderzochte controlevormen is bovendien gebleken dat de rechter de wettelijke normen niet zo absoluut toepast als de wetgever ze formuleert. Er wordt veeleer een afweging gemaakt tussen de belangen van de werkgever en de werknemer.

3. De Europese horizon

3.1 Inleiding

Nederland is geen eiland. Veel regelgeving over de privacy wordt op Europees niveau vastgesteld. Een voorbeeld hiervan is natuurlijk artikel 8 EVRM. Maar alle wetgeving in de EU voor wat betreft de verwerking van persoonsgegevens zou aan de Europese Richtlijn moeten voldoen. (45)

Maar ook de Raad van Europa stelt regels. Van belang is hier de *Recommandation no R (89) 2 du Comité des Ministres du Conseil de l'Europe aux Etats membres sur la protection des données à caractère personnel utilisées à des fins d'emploi*, aangenomen door het Comité van Ministers op 18 januari 1989:

3. Information et consultation des employés

3.1. Conformément aux législations et pratiques nationales et, le cas échéant, aux conventions collectives, les employeurs devraient informer ou consulter leurs employés ou les représentants de ceux-ci préalablement à l'introduction ou à la modification de systèmes automatisés pour la collecte et l'utilisation de données à caractère personnel concernant les employés. Ce principe s'applique également à l'introduction ou à la modification de procédés techniques destinés à contrôler les mouvements ou la productivité des employés.

3.2. L'accord des employés ou de leurs représentants devrait être recherché avant l'introduction ou la modification de tels systèmes ou procédés lorsque la procédure de consultation mentionnée au paragraphe 3.1 révèle une possibilité d'atteinte au droit au respect de la vie privée et de la dignité humaine des employés, à moins que d'autres garanties appropriées ne soient prévues par la législation ou la pratique nationale.

De standaard Europese jurisprudentie over de privacy op het werk is de uitspraak in de zaak Niemietz/Duitsland. (46) Het Hof concludeert hierin dat er niet altijd een scherp onderscheid te maken is tussen *private life* en *activities of a professional or business nature*.^r Derhalve strekt de bescherming van artikel 8 EVRM zich ook uit tot de werkplek. In Halford/UK spreekt het Hof zich nog duidelijker uit:

[The Court] Holds unanimously that Article 8 of the Convention is applicable to the complaints [i.e. de schending van de privacy, ljm] concerning both the office and the home telephones;

In dit hoofdstuk komt de regelgeving in een aantal andere Europese landen aan bod. Dit 'rondje Europa' is verre van volledig. Het dient slechts als een korte verkenning en om een indruk te krijgen in hoeverre de Nederlandse regelgeving afwijkt van die in andere Europese landen.

3.2 Frankrijk

Het af luisteren van telefoongesprekken door een werkgever is in principe verboden wanneer dit *de mauvaise foi* gebeurt. (47) Voor het niet te kwader trouw zijn, is het in ieder geval noodzakelijk dat de Ondernemingsraad (*le comité d'entreprise*) vòòr de in gebruikname van af- of meeluisterapparatuur op de hoogte wordt gebracht. (48) Bovendien moet autorisatie aangevraagd worden bij het ministerie van defensie. (49)

Het is nog maar de vraag of de kwade trouw opgeheven wordt door het personeel van te voren op de hoogte te stellen. Vaak zullen additionele maatregelen genomen moeten worden, zoals toegang tot een vrije lijn en/of inzage in de transcripties van de telefoongesprekken.

Voor wat betreft het monitoren van telefoongesprekken bepaalt *la délibération no94-113 du 20 décembre 1994* welke maatregelen genomen moeten worden. Het belangrijkste is dat *représentatives du personnel* vòòr de installatie van de apparatuur op de hoogte gebracht moeten worden over:

- welke controles uitgevoerd worden;
- voor wie de informatie bedoeld is en
- hoe een werknemer toegang heeft tot zijn eigen gegevens en hoe deze gecorrigeerd kunnen worden.

De maximale bewaartermijn van de gegevens is zes maanden. Bepaalde werknemers, zoals Ondernemingsraad-leden, moeten toegang hebben tot een vrije lijn.

In Frankrijk kent men, als een van de weinige landen in Europa, een eigen, wijd verbreid netwerk voor het opvragen van informatie: de minitel. Met enige regelmaat duikt in de arbeidsrechtspraak het privé-gebruik van de minitel op. De discussie daarbij lijkt voornamelijk gericht op de vraag of privé-gebruik een *faute grave* is en of op basis van het privé-gebruik ontslag mogelijk is. Aan het controle-aspect wordt vreemd genoeg grotendeels voorbij gegaan.

Video-bewaking is in Frankrijk aan duidelijk minder regels gebonden dan de Registratiekamer in Nederland voorstaat. (50) In Frankrijk maakt men onderscheid tussen publiek toegankelijke plaatsen (banken, warenhuizen) en *lieux qualifiés juridiquement de privés*. Voor publiek toegankelijke plaatsen moet toestemming van de overheid verkregen worden. De opnames mogen maximaal een maand bewaard blijven.

Voor niet publiek toegankelijke werkplekken moet de Ondernemingsraad van te voren geïnformeerd en geraadpleegd worden. De werknemer moet van te voren geïnformeerd worden. De eis dat de werknemer geïnformeerd moet worden, wordt ook door de rechter gevolgd. (51)

De CNIL heeft hier slechts een rol wanneer de beelden via computers verwerkt worden.

Het briefgeheim is in Frankrijk duidelijk afgebakend. Reeds in 1938 heeft het Cour d'Appel in Parijs een werkgever veroordeeld, omdat hij een gesloten enveloppe had opengemaakt. (52) rechtspraak hierover is sindsdien consistent. Het briefgeheim is in Frankrijk dus absoluut, niet alleen ten opzichte van de staat, maar ook ten opzichte van de werkgever. Wel moet duidelijk zijn dat de correspondentie privé is, bijvoorbeeld omdat zij *sous pli fermé* is of de melding

3.3 Engeland

De Data Protection Commissioner heeft een uitgebreide *Code of Practice* opgesteld over het gebruik van gegevens in een arbeidsrelatie. (53) Een onderdeel van deze *Code of Practice* bevat aanbevelingen voor het volgen van het personeel. Een overtreding van de regels in de *Code of Practice* is overigens niet automatisch een overtreding van privacy-wetgeving.

Bij de beoordeling van de volgsystemen wordt niet alleen rekening gehouden met inbreuk op de privacy van de werknemer, maar ook met inbreuk op de autonomie van de werknemer. Ook wordt een onderscheid gemaakt tussen *performance monitoring* en *behavioural monitoring*.

Voor elke vorm van monitoring stelt de Data Protection Commissioner de volgende standaarden voor:

- Reeds bij de afweging tussen het bedrijfsbelang enerzijds en de privacy en autonomie van de werknemer anderzijds moet overleg gevoerd worden met vertegenwoordigers van het personeel.
- Monitoring moet beperkt blijven tot wat absoluut noodzakelijk is voor het bedrijfsbelang.
- Het gehele personeel moet op de hoogte van de monitoring zijn.
- De gegevens mogen alleen voor het doel waarvoor ze ingewonnen worden gebruikt worden.

Uitzonderingen op deze regels zijn beperkt tot *behavioural monitoring* in verband met criminele activiteiten.

Voor het meeluisteren bij of opnemen van telefoongesprekken worden additionele regels voorgesteld:

- Luister alleen mee als het bedrijfsbelang onvoldoende informatie krijgt op basis van het call-record.
- Zorg ervoor, dat beide partijen in de conversatie op de hoogte zijn van het meeluisteren of opnemen en van de reden waarom dit gebeurt.
- Zorg dat werknemers toegang hebben tot een lijn voor privé-gesprekken, bijvoorbeeld via een muntjes-telefoon. (54)

Voor camera-bewaking worden andere regels gegeven:

- Maak een gescheiden analyse voor de noodzaak van video- en audiobewaking. Het is zeer zelden noodzakelijk om beide tegelijk te gebruiken.

— Zorg dat iedereen, ook niet-personeel, op de hoogte is van de videobewaking.

3.4 België

Voor wat betreft de privacy-regelgeving steunt de Commissie voor de bescherming van de persoonlijke levenssfeer sterk op de Europese regels. Daarbij wordt met name naar het Nederlandse en het Franse recht gekeken.

Basis voor het Belgische recht is de wet van 8 december 1992, de Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens. Waar sprake is van inbreuken op de privacy wordt verwezen naar het proportionaliteitsbeginsel. (55)

De Belgische Commissie voor de bescherming van de persoonlijke levenssfeer is zeer afkerig van het af- of meeluisteren van telefoongesprekken. (56) Zij stelt vast dat dit weliswaar in Nederland en Frankrijk onder bepaalde voorwaarden geaccepteerd is, maar blijft verwijzen naar artikel 314bis van het Belgisch strafwetboek. (57) Tegen het registreren van welke gesprekken gevoerd worden en met wie heeft de commissie minder bezwaar, mits het proportionaliteitsbeginsel gerespecteerd wordt.

Camera-toezicht is toegestaan als het finaliteitsbeginsel en proportionaliteitsbeginsel gerespecteerd worden. (58) Wel rust er een informatieplicht op de werkgever. Deze informatieplicht beslaat niet alleen het feit dat er camera's geplaatst zijn, maar ook de reden waarom, dat wil zeggen het doel van de observatie. Het toestemmingsvereiste wordt door de Commissie in het kader van de proportionaliteit gezien.

3.5 Korte rechtsvergelijking

Net als in Nederland is er in de genoemde landen een aparte organisatie die toeziet op de verwerking van persoonsgegevens. Deze organisaties stellen, vaak op eigen initiatief, richtlijnen op voor toezicht in de werksituatie. De regels in Europa wijken, zoals al verwacht kon worden, niet veel af van de Nederlandse regels. Wel ziet men accentverschillen. In de rest van Europa wordt nog meer expliciet de nadruk gelegd op de proportionaliteit. In Engeland wordt aangeraden de proportionaliteit van het toezicht af te wegen samen met de werknemers. In Frankrijk en Engeland legt men meer nadruk op de verplichting om in een vroeg stadium te overleggen met de Ondernemingsraad. De Engelse regels zijn strenger in de scheiding tussen privé en zakelijk gebruik van communicatiemiddelen. Wanneer het niet zonneklaar is dat het om zakelijke communicatie gaat, mag niet afgeluisterd worden. (59) Wellicht het grootste verschil is gelegen in de Belgische aversie tegen het af luisteren van telefoons.

4. Regels voor de Internet-policy

4.1 Inleiding

Er zijn verschillende redenen waarom een werkgever het Internet-gebruik van zijn werkgevers zou willen reguleren:

- Technische redenen. Een onbeperkte toegang van werknemers tot Internet-faciliteiten vergt investering in apparatuur en netwerken.
- Toezicht op het functioneren van de werknemer. Een werknemer die surft op Internet is niet (altijd) bezig met de werkzaamheden waarvoor hij betaald wordt.
- Wettelijke noodzaak. Als een werknemer bijvoorbeeld racistische teksten of pornografie via e-mail verspreidt, kan een werkgever er onder omstandigheden aan gehouden zijn maatregelen te nemen ter voorkoming van deze gedragingen. (60)
- Ter voorkoming van aanspraken Het kan hierbij gaan om aanspraken van zowel derden als andere werknemers.
- Ter voorkoming van imago-schade. Het taalgebruik en de inhoud van e-mail kunnen bepalend zijn voor het imago van een bedrijf.

Het gebruik van een Internet-policy maakt aan werknemers duidelijk welke grenzen er aan het gebruik van het Internet gesteld worden. Omdat er een duidelijke relatie met de privacy van de werknemer is, moet zo'n policy aan verschillende eisen voldoen. Deze eisen zijn te splitsen in inhoudelijke eisen (wat mag er gecontroleerd worden) en eisen aan de omgang met de policy (publicatie, inspraak en dergelijke).

In dit hoofdstuk zullen, naast de eerder gevonden regels bij de verkenning van de privacy van de werknemer, de richtlijnen van de Registratiekamer onder de loep worden genomen. Ook zal weer een korte blik op de Europese horizon worden gegeven.

4.2 Techniek-onafhankelijkheid of niet?

De hiervoor bestudeerde technieken zijn conventionele manieren om de werknemer te monitoren. De Commissie Grondrechten in het digitale tijdperk heeft ervoor gekozen om de grondrechten techniek-onafhankelijk te formuleren. De Commissie meent dat alleen een techniek-onafhankelijke formulering de tijd kan bij houden. (61)

Doordat alles op Internet zich in de wereld van de 'bits' afspeelt, (62) is het relatief eenvoudig om een hoge mate van controle uit te oefenen. Sterker: het loggen van gegevens is inherent aan het gebruik van moderne computers. Elke toegang tot Internet levert mogelijkheden tot logging op. In de meeste bedrijven zullen firewalls en proxies staan. Deze zijn gewoonlijk zo geconfigureerd dat er vele gigabytes logging per dag gegenereerd worden. In deze logs staat, naast de inbraakpogingen vanaf het Internet, uiteraard ook het browse- en e-mail-gedrag van de werknemers.

Met de huidige prijzen van harde schijven zijn bovendien de kosten van het loggen en het on-line houden van de log verwaarloosbaar. Ook de kosten van extra apparatuur zijn vele malen lager dan van bijvoorbeeld video-observatie. Uit de logs worden verschillende uittreksels gemaakt zoals:

- Lijsten van aanvallen van buiten (bijvoorbeeld portscans of denial of service-attacks);
- Performance gegevens over de netwerkcapaciteit en de computercapaciteit van bijvoorbeeld de firewall of
- Beschikbaarheidsrapportages.

Het is zonder meer mogelijk om rapportages te genereren over de meest bezochte sites, de sites met *explicit content*, al dan niet met de namen van de werknemers die deze sites bezocht hebben. Ook kan per gebruiker een rapport van zijn activiteiten gemaakt worden.

In tegenstelling tot de conventionele controletechnieken, zoals af luisteren en cameratoezicht, is het dus mogelijk om uit een grote stroom data werkelijke informatie te krijgen over het gedrag van werknemers. Dergelijke rapportages kunnen door ervaren systeembeheerders met relatief weinig inspanning gegenereerd worden. (63) Technisch gezien is de controle op Internet-gebruik dus eenvoudiger, gedetailleerder en goedkoper dan de conventionele controles.

Dit geeft echter geen aanleiding voor een ander privacy-beleid wanneer het gaat om Internet-toegang; het onderstreept veeleer de noodzaak de grenzen aan de controle duidelijk te stellen.

Bepaalde technieken leveren wel extra gevaren op. Zo levert e-mail met attachments bij sommige mail-lezers (64) het verspreidingsrisico van virussen op. Wanneer men ongecontroleerde programma's via FTP downloadt kan men ook virussen verspreiden of zelfs de computer voor hackers toegankelijk maken. Dit betekent dat elke techniek zijn eigen gevaren meebrengt en dat voor elke techniek een aantal eigen regels zal gelden.

Het moge onderhand voldoende bekend zijn dat privacy op het Internet nauwelijks bestaat. (65) De volgende lijst geeft een, overigens verre van uitputtende, opsomming van manieren weer waarop men zonder maatregelen zijn privacy op Internet prijsgeeft:

- Het openstellen van Windows-shares op de eigen computer. Veel PC's, met name privé-installaties, laten onbeperkte toegang tot de gegevens op de harde schijf vanaf het Internet toe. (66)
- Wanneer men cookies in de browser accepteert, schept men de mogelijkheid voor aanbieders om deze cookies uit te lezen. Hierdoor is het geen probleem om de voorkeuren van een Internet-gebruiker te achterhalen.
- E-mail gaat langs een groot aantal tussenliggende computers en netwerken. (67) Alleen door encryptie kan men garanderen dat geen van de tussenliggende partijen het bericht inziet. Toch is het versleutelen van e-mail niet gebruikelijk.
- Wanneer men mail aan verschillende personen stuurt, komen de adressen van al deze personen in de header te staan. Niet iedereen met wie gecorrespondeerd wordt, hoeft het op prijs te stellen dat alle andere ontvangers ook zijn e-mail adres krijgen.
- In toenemende mate worden bijdragen aan, ook serieuze, discussie-groepen geanonimiseerd. Als men dit niet doet is levert men weer wat privacy in. (68)

Wanneer men zich zo gedraagt, kan men niet spreken van een *reasonable expectation of privacy*. De persoonlijke informatie, die zo kwistig wordt rondgestrooid, wordt door veel bedrijven en instellingen verzameld en geadministreerd. In Europa gelden er regels voor het aanleggen en verwerken van dergelijke administraties, buiten Europa is de regelgeving duidelijk minder scherp.

Wanneer zoveel bedrijven informatie over het surfgedrag en het overige Internet-gebruik verzamelen, waarom zou de werkgever dit niet mogen? Het antwoord ligt mijns inziens deels in de aard van de sociale verhoudingen. Een werkgever heeft ten opzichte van de werknemer een machtspositie. Juist deze machtspositie maakt het noodzakelijk dat de werkgever bepaalde grenzen niet overschrijdt.

In Nederland bestaat sterk de neiging om de privacy als een absoluut recht te zien, onafhankelijk van technieken. Deze wens komt nadrukkelijk ook tot uiting in het *Rapport van de Commissie grondrechten in het digitale tijdperk*. In de huidige Grondwet is deze techniek-onafhankelijkheid nog niet gerealiseerd.

Er is bovendien een verschil tussen de Grondwet en een bedrijfspolicy. Een bedrijfspolicy is relatief snel op te stellen. De, door werkgevers als langdurig ervaren, procedures van consultatie en instemming van de Ondernemingsraad zijn vele malen eenvoudiger dan de wijziging van de Grondwet. Ook staat het management van bedrijven, hoe a-technisch het ook is, dichter bij de techniek dan politici, waardoor het traject vereenvoudigd wordt.

Het heeft echter geen zin om de werknemers te overladen met boekwerken vol regels. Als voor elke communicatietechniek aparte regels en controles gelden, dan ziet de werkgever door de bomen het bos niet meer. Controles vinden dan plaats zonder medeweten van de werknemer, wat strijdig is met de Europese Richtlijn voor beeldschermmedewerkers. (69) Ook wordt het moeilijker om een *begrijpelijk* overzicht te geven van de verzamelde persoonsgegevens. (70)

Ook is het moeilijk uit te leggen, waarom privé-telefoontjes wel toegestaan zouden zijn, maar privé-e-mails niet. Als er grote verschillen zijn tussen de toepassingsregels van de verschillende communicatie-technieken, dan krijgt men een technologie-vlucht van een verboden techniek naar een geoorloofde, bijvoorbeeld van e-mail naar telefoon. Het kosten-aspect hiervan hoeft niet altijd gunstig voor de werkgever te zijn. Een technologische afhankelijkheid van de regels werkt dus contraproductief. (71)

Bij elke vorm van communicatie geeft men iets van zijn privacy prijs. Ook loopt men bij elke vorm van communicatie het risico dat derden, zoals de werkgever, op de hoogte raken van de communicatie.

Bedrijven gebruiken voor de keuze van communicatiekanalen vaak een data-classificatie. Zo zullen niet-geheime gegevens makkelijk via een e-mail verstuurd kunnen worden en mogen zeer geheime gegevens alleen persoonlijk afgegeven worden. Intuïtief doet men in zijn privé-leven hetzelfde: bepaalde communicatie gaat in een gesloten enveloppe, andere mag op de achterkant van een prentbriefkaart. Door de keuze van de wijze van verzending bepaalt men zijn behoefte aan beslotenheid. Zo zou een werknemer zijn privacy-verwachting moeten afstemmen op zijn gebruik van encryptie, de keuze om vanuit huis of vanuit werk te mailen, enzovoorts.

Omdat alle verschillende communicatiemogelijkheden hun eigen risico's en kosten met zich meebrengen, zal een gedeelte van de policy techniek-afhankelijk zijn. Een groot deel, met name waar het de privacy van de werknemer betreft, zal techniek-onafhankelijk kunnen blijven.

4.3 De Registratiekamer

In een recent rapport heeft de Registratiekamer, onder andere op basis van een bijeenkomst van experts, regels geformuleerd voor het gebruik van Internet. (72) Zij komt daarbij tot een uitgebreidere set regels dan op basis van de andere controles (mee- of af luisteren, camera-toezicht) verwacht mocht worden.

Een nadere analyse van de additionele regels geeft ons daarvoor drie redenen:

- De zorg voor de beheersmatige aspecten: de integriteit van de systeembeheerder, het bestaan van backups.
- De mogelijkheden die de techniek biedt: het zoveel mogelijk softwarematig onmogelijk maken van misbruik, anonimisering ten behoeve van gebruiksstatistieken, vaststellen welke software gebruikt mag worden, het scheiden van zakelijke mail en privé-mail.
- Additionele inzichten of aspecten die blijkbaar tot op heden tot weinig problemen aanleiding hebben gegeven: het bieden van inzicht in de gegevens, evaluatie van de regels, het ontzien van geprivilegieerde informatie.

Het rapport van de Registratiekamer wekt de indruk in de haast in elkaar gezet te zijn. Delen van de tekst zijn letterlijk gecopieerd uit andere stukken. Verder maakt het rapport, ook wat structuur betreft, weinig indruk. De opmerkingen en adviezen zijn blijkbaar gebaseerd op een 'expert-meeting'.

De Registratiekamer heeft daarnaast ook een aantal uitspraken gedaan die een indruk geven van de regels die de Registratiekamer hanteert. Als een computerbedrijf zijn werknemers voorhoudt dat het gerechtigd is om alle e-mails te openen *for any purpose* en stelt dat de werknemers geen *reasonable expectation of privacy* hebben bij het gebruik van e-mail, constateert de Registratiekamer dat dit in strijd is met de WPR. (73) In ieder geval dient het doel van de registratie aangegeven te worden, zodat de redelijkheid van het belang van de werkgever getoetst kan worden (proportionaliteit). Voorts wijst de Registratiekamer op de noodzaak van transparantie en op het instemmingsrecht van de ondernemingsraad. (74)

In Computerrecht wordt een uitspraak van de Registratiekamer vermeld, waarbij onder voorwaarden het openen van e-mails bij een incident is toegestaan. (75) Na de melding van het incident (het ontvangen van ongewenste e-mails met pornografisch materiaal) werd op een vaste peildatum alle e-mail met attachment geopend om vast te stellen of het een programma, filmpje of plaatje bevatte. Overige e-mails werden niet geopend, tenzij de titel aangaf dat het om pornografisch materiaal ging. Een dergelijke werkwijze werd door de Registratiekamer behoorlijk en zorgvuldig genoemd. Daarbij heeft de Registratiekamer de belangen van de werkgever, namelijk de controle op misbruik, afgewogen tegen de inbreuk die een dergelijke controle op de persoonlijke levenssfeer van de werknemers heeft.

Als een korpschef aan de Registratiekamer vraagt of hij naar aanleiding van een incident (e-mailberichten die gezien hun inhoud door met name vrouwelijke collegae als intimiderend en ongewenst worden beschouwd) verdergaande controle op het e-mail gebruik mag uitvoeren, stelt de Registratiekamer een aantal eisen aan het onderzoek. (76) Allereerst moet er een concrete verdenking zijn, er mag geen minder ingrijpende weg open staan en de gevonden gegevens mogen niet buiten het onderzoek gebruikt worden. De Registratiekamer stelt dus de eis van proportionaliteit, waarbij zij stelt, dat voor zo'n inbreuk op de privacy een groot werkgeversbelang nodig is dat bovendien op geen andere wijze gerealiseerd kan worden.

Uit de uitspraken blijkt dat de Registratiekamer let op de proportionaliteit, de beperking van het gebruik van de gegevens tot het aangegeven doel, de transparantie en het instemmingsrecht van de Ondernemingsraad.

4.4 Internet-regels elders in Europa

In andere landen van Europa wijken de adviezen alleen op nuances af als het gaat om het stellen van regels voor het Internet-gebruik. Het duidelijkst zijn de regels uit de *draft* van de Employment COP. (77) De Engelse Data Protection Commissioner geeft regels die gelden voor alle vormen van monitoring. Voor Internet-gebruik, met name e-mail en web-browsen, worden specifieke regels gegeven. In Engeland wordt in het geval van het gebruik van Internet-diensten, nog meer dan bij andere communicatie-vormen, een duidelijke scheiding aangebracht tussen de communicatie voor zakelijke doeleinden, die wellicht eventueel zou mogen worden gemonitord, en de privé-communicatie, die ontzien moet worden.

In Frankrijk is de discussie over het volgen van Internet-gebruik in een onderneming in volle gang. De CNIL heeft recentelijk een discussiestuk opgeleverd (78) waarin de privacy van de werknemer aan de orde wordt gesteld. Het discussie-stuk is geen vertaling van de privacy-regels op ander gebied, maar probeert wel een algemeen geldende norm te geven. Er worden drie grenzen aan de controle door de werkgever gesteld:

- *La transparence et la loyauté*: de verplichting om te melden welke registraties en controles de werkgever uitvoert en ook alleen die controles uit te voeren.
- *La proportionnalité*: er dient een afweging gemaakt te worden tussen de belangen van de werkgever enerzijds en het recht op privacy anderzijds.
- *La discussion collective*: vanwege de afhankelijke positie van de werknemer is het van belang dat de discussie met de werkgever niet door individuele werknemers gevoerd hoeft te worden.

Alleen de proportionaliteitseis stelt grenzen aan de inhoud van de policy; de overige twee eisen geven aan hoe er met de policy omgegaan moet worden.

In België onderscheidt de Commissie voor de bescherming van de persoonlijke levenssfeer ook drie grenzen aan de controlebevoegdheid van de werkgever op het IT-gebruik door de werknemer: (79)

- Transparantie: voor de werknemer moet het duidelijk zijn welke regels er gelden. Daarbij dienen de volgende aspecten aan de orde te komen:
 - in hoeverre privé-gebruik is toegestaan,
 - hoe gecontroleerd wordt,
 - of er een opslag van de gegevens plaatsvindt en wat de bewaartermijn van de gegevens is,
 - welke beslissingen de werkgever kan nemen op basis van deze gegevens en
 - het recht van toegang van de werknemer tot de gegevens.

Een groot deel van de discussie zal zich afspelen in de collectieve sfeer, dus niet met de werknemers afzonderlijk.

- Proportionaliteit: iedere controle moet steunen op een aanwijzing dat er misbruik van de werkinstrumenten wordt gemaakt. De Commissie maakt hierbij een onderscheid tussen e-mail en het raadplegen van Internet-sites. Voor e-mail verkeer is het kennismaken van de inhoud, behalve bij incidenten, altijd disproportioneel. Wel is het mogelijk om verkeersgegevens bij te houden. Het raadplegen van Internet-sites mag ook niet permanent gemonitord worden. Wel is het toegestaan om afwijkend gedrag vast te stellen op basis van bijvoorbeeld geraadpleegde sites of keywords.

- Gelimiteerde bewaartermijn. de gegevens mogen niet langer bewaard worden dan noodzakelijk is voor de controles. De Commissie doet geen aanbeveling voor een maximale bewaartermijn.

4.5 De regels voor een Internet-policy

De uiteindelijke keuze voor een Internet-policy is een keuze van de werkgever in overleg met de Ondernemingsraad. Men zal er niet aan kunnen ontkomen om bepaalde regels en beperkingen te stellen. En waar regels gesteld worden, moet controle plaatsvinden.

Bij de vaststelling van de regels is er onderscheid gemaakt tussen de inhoud van een Internet-policy en de wijze waarop er mee omgegaan moet worden. Uit een korte blik op wat in andere Europese landen plaatsvindt, valt te concluderen dat de gevonden regels niet of nauwelijks aangepast hoeven te worden aan de rechtssystemen van andere landen.

1. Enige vorm van privé-gebruik door de werknemer moet toegestaan worden. Dit volgt uit het arrest Halford/UK (80) en uit Niemietz/Duitsland. (81)
2. De werkgever kan beperkingen aan het Internet-gebruik van de werknemer stellen. Dit volgt uit artikel 7:660 BW. De Registratiekamer verwoordt dit als: "In werktijd geniet men niet dezelfde vrijheden als daarbuiten". Uit de policy moet duidelijk blijken welke beperkingen en regels er gesteld worden.
3. Wanneer de werkgever controles uitvoert, moet hij een duidelijk doel hebben voor het registreren van het Internet-gedrag van de werknemer. Dit doel moet uit de policy blijken. Artikel 7 Wbp stelt deze eis van doelbinding.
4. De controles door de werkgever moeten in verhouding staan tot het doel wat hij probeert te bereiken. Er moet een afweging plaatsvinden tussen het bedrijfsbelang en het recht op privacy van de werknemer. Deze eis van belangenafweging volgt uit artikel 8, sub f Wbp.
5. Er is een maximale bewaartermijn van de loggegevens. Dit volgt uit artikel 10 lid 1 Wbp. Deze termijn moet in de policy vermeld staan.
6. De policy behoeft instemming van de Ondernemingsraadingsraad. De reden hiervoor is dat de Internet-policy een controlebevoegdheid aan de werkgever geeft waarmee hij de persoonlijke levenssfeer van de werknemer inperkt. Artikel 27 lid 1, sub k en l geeft de Ondernemingsraad in dergelijke gevallen instemmingsrecht.
7. De policy moet bekend zijn bij alle werknemers die het aangaat. Hier speelt een element van rechtszekerheid mee, maar ook artikel 7:660 BW stelt deze eis.
8. De werkgever moet de policy loyaal uitvoeren, ook waar het beperkingen aan de controlebevoegdheid stelt. Dit volgt niet alleen uit de eis van goed werkgeverschap, maar ook uit artikel 9 lid 1 Wbp.
9. De controle moet in principe bij de Registratiekamer aangemeld worden.
10. Bij incidenten mag een verdergaande controle plaatsvinden. Daarbij moet sprake zijn van concrete verdenkingen. De gegevens van de extra controles moeten vernietigd worden zodra ze geen relevantie meer hebben voor het onderzoek. Dit volgt uit artikel 43 Wbp.
11. Waar mogelijk, moet geprobeerd worden misbruik technisch onmogelijk te maken.

De gevonden regels zijn bewust beperkt gehouden tot het gebruik van Internet door werknemers als eindgebruiker. Dit is namelijk de situatie waar de meeste werknemers zich in bevinden. Naast deze eindgebruikersfunctie zijn er verschillende andere manieren van Internet-gebruik te onderscheiden zoals bijvoorbeeld:

- Het plaatsen van een http- of ftp-server. In dergelijke gevallen spelen aspecten als het imago van het bedrijf, respect voor copyrights en dergelijke een grotere rol dan in de hier voorgestelde policy.
- Het maken van een extra connectie naar het Internet, zoals bijvoorbeeld in Wierdens/Kunst gedaan werd. (82)

Veel bedrijven verbieden expliciet, overigens buiten hun Internet-policy om, dergelijke handelingen. Zij vallen dan terug op een algemene bedrijfspolicy over computer- en netwerkbeveiliging. Ook in deze algemene policies worden er grenzen aan het gedrag van de werknemers gesteld. En ook daar worden controlemogelijkheden aangegeven waarbij de privacy van de werknemer in het geding kan zijn. De behandeling hiervan in het kader van deze scriptie zou echter te ver gaan.

5. De praktijk

5.1 Inleiding

In dit hoofdstuk zullen de gevonden regels worden vergeleken met regels zoals deze in voorstellen voor Internet-politicies voorkomen. Vervolgens wordt een blik geworpen op de jurisprudentie.

5.2 FNV

De FNV heeft een voorbeeld-protocol opgesteld dat als basisstuk voor de discussie van een Ondernemingsraad met de werkgever kan dienen. (83) Bij de invoeringsregels gaat de FNV er vanuit dat het initiatief bij de Ondernemingsraad ligt.

Het protocol van de FNV beteedt veel aandacht aan de privacy en de rechten van de werknemer. E-mail en overig Internet-gebruik voor niet-zakelijke activiteiten is toegestaan, zolang het niet storend is voor de dagelijkse werkzaamheden. De belangen van de werkgever komen eigenlijk niet aan bod. Van een reële afweging is geen sprake. Dat hoeft ook niet: een Ondernemingsraad brengt dit stuk in als vertegenwoordigend orgaan van het personeel.

De enige controle die het protocol toestaat, is een gerichte controle bij incidenten. Er moet dan sprake zijn van een reële verdenking tegen een of meer werknemers. In een dergelijk geval acht de FNV ook heimelijke observatie geoorloofd.

Doordat de FNV geheel voorbij gaat aan bedrijfsbelangen en het recht van de werkgever om regels te stellen, is deze policy praktisch van weinig nut. Zo ontbreekt de eis, dat de werkgever een duidelijk doel moet hebben voor registratie en controle. Ook ontbreekt de proportionaliteitseis. Bovendien ontbreekt een suggestie over de bewaartermijn van de controlegegevens.

De FNV bewijst zijn leden geen goede dienst met deze policy. Door de rechten van de werkgever te ontkennen, berooft zij de leden van het inzicht waar de grens getrokken moet worden.

5.3 Werkgeversorganisaties

De werkgeversorganisaties hebben twee documenten ontwikkeld; een algemeen privacy-document en een voorbeeld-policy. Voor alle registraties en controles bevelen de werkgeversorganisatie aan: (84)

- Helder en redelijk doel: Bij het vaststellen van het doel moet het belang van de werkgever tegen de privacy van de werknemer worden afgewogen. Daarbij moet ook het kostenaspect een rol spelen.
- Open vizier: iedere reden waarom informatie over het personeel wordt bijgehouden, moet bekend zijn bij het personeel.
- Zorgvuldig gebruik: de gegevens mogen niet buiten het doel waarvoor ze verzameld worden gebruikt worden.
- Kwaliteitscontrole: van tijd tot tijd moet de werkgever de gegevens controleren. Ook de werknemer heeft inzage- en correctierecht.

Volgens de werkgeversorganisaties berust het op een misverstand dat werkgevers een dringende reden zouden moeten hebben om het Internet en e-mail gebruik te controleren. De verwijzing daarbij naar het briefgeheim vinden zij "nagal overtrokken".

Bij het opstellen van een voorbeeld-policy gaan VNO-NCW uit van een restrictief beleid. (85) Internet-gebruik voor privé-doeleinden is niet toegestaan. Mocht de werkgever dit toch toe willen staan, dan suggereert de gebruiksaanwijzing enkele wijzigingen. In dat geval mag de werkgever controle uitoefenen bij een vermoeden van ongeoorloofd handelen.

De voorbeeld-policy geeft expliciet aan, dat het Internet-gebruik wordt vastgelegd:

Het gebruik van internet en e-mail wordt vastgelegd. Deze registratie geschiedt om de continuïteit van de technische infrastructuur te waarborgen, verstoring van bedrijfsprocessen en andere (financiële) schade tegen te gaan en om toezicht te houden op de naleving van de gedrags- en gebruiksregels door de gebruiker.

In de regels over controle blijkt dat de werkgever controle op drie manieren moet kunnen uitoefenen:

- statistische, anonieme controle om te bepalen in hoeverre de regels overtreden worden,
- steekproeven en
- uitgebreide controles bij incidenten.

Deze policy is duidelijk opgesteld vanuit het perspectief van de werkgever. Alhoewel in principe geen privé-gebruik wordt toegestaan, wordt wel aangegeven welke aanpassingen nodig zijn als de werkgever wel privé-gebruik toe wil staan.

Uit de policy blijkt duidelijk welke grenzen er getrokken worden. Zo wordt het downloaden van software verboden, wordt het versturen van vertrouwelijke of bedrijfskritische gegevens verboden en wordt de toegang tot bepaalde Internet-sites geblokkeerd. Ook geeft de policy aan welke sancties er genomen kunnen worden. Dit bevordert de rechtszekerheid.

Het doel van controles wordt ook duidelijk aangegeven. Daarnaast wordt ook aangegeven hoe de controles worden uitgevoerd. Hierdoor is het mogelijk om een oordeel over de proportionaliteit te vormen. Surf-gedrag en e-mail wordt anoniem bekeken. Als blijkt dat er (grote) overtredingen zijn of wanneer er klachten komen, worden de gegevens van de betrokken werknemer bekeken. Dit betekent dat er in principe geen persoonlijke controle plaatsvindt. Dit zal over het algemeen geen grote inbreuk op de privacy van de werknemer betekenen.

Het enige wat in de policy ontbreekt, is de bewaartermijn van de loggegevens.

Ook de wijze waarop er met deze policy omgegaan moet worden, is consistent met de regels. Uitgebreid wordt ingegaan op het traject met de Ondernemingsraad (gebruiksaanwijzing onder 3b). Ook de noodzaak van publicatie komt aan bod (gebruiksaanwijzing onder 1). Er wordt op gewezen dat registratie van het Internet-gebruik aangemeld moet worden bij de Registratiekamer (gebruiksaanwijzing onder 3c). Het technisch afschermen van ongewenst gebruik wordt als vanzelfsprekend aangenomen (gedragscode 2.2). Ook de mogelijkheid om bij incidenten een gericht, verdergaand onderzoek uit te voeren, wordt in de gedragscode vermeld (onder 4.3). Door deze bevoegdheid in de gedragscode op te nemen, wordt bovendien bijgedragen aan de rechtszekerheid.

Wat ontbreekt, is een referentie naar de loyaliteit van de werkgever bij het uitvoeren. Maar dit is, vanuit het oogpunt van de opstellers van de policy, logisch. Erger is de aanname dat een werkgever geen dringende reden nodig zou hebben om e-mails te controleren. Natuurlijk kan het voor komen dat het bedrijfsbelang een dergelijke controle nodig maakt, maar de stelling dat verwijzing naar het briefgeheim overtrokken is, is onjuist.

5.4 Jurisprudentie

De Nederlandse rechter is, wanneer het om Internet gaat, nog zoekende naar consistentie. De onzekerheid van de rechter is het grootst in Wierdens/Kunst: (86)

Dat het ongeoorloofd internetten niet als dringende reden in het bestek van deze procedure kan worden aangenomen ligt vooral aan de onkunde van de kantonrechter en Wierdens Houthandel inzake informatietechnologie.

Maar over de eventuele schending van de privacy van de werknemer is de rechter van oordeel:

Dat Wierdens Houthandel mogelijkwerwijs de privacy van Kunst heeft geschonden, mag Kunst niet aan haar tegenwerpen. In het kader van het onderzoek naar misbruik van het internet bij Wierdens Houthandel, valt niet te ontkomen aan een onderzoek naar het persoonlijk gebruik dat van het internet is gemaakt.

Of, en in hoeverre de privacy van Wierdens is geschonden, komt echter niet aan bod. Kunst mag het privacyargument niet gebruiken.

Soms grijpt de rechter terug op een vergelijking met de bekende technieken, zoals de rechtbank in Utrecht doet. (87) De conclusie is dan tegengesteld:

Anders dan NPI is de rechtbank van oordeel, dat analoog aan artikel 13 van onze Grondwet, het briefgeheim zich ook uitstrekt tot de met een persoonlijke brief vergelijkbare moderne communicatievormen zoals in casu de betreffende E-mails. Daaraan doet niet af, dat Pijpers voor de verzending van zijn privé-correspondentie gebruik heeft gemaakt van de E-mail-aansluiting van NPI [...] Voorts kan niet worden geoordeeld dat Pijpers, door gebruik te maken van de E-mail aansluiting van NPI, het vertrouwelijke karakter van de E-mails heeft prijsgegeven.

De Kantonrechter in Haarlem oordeelde, dat de inhoud van de privé-e-mail niet meegewogen mag worden, maar de attachments wel. (88) De reden is, dat de attachments gewelddadige en pornografische afbeeldingen bevatten. Het gemaakte onderscheid tussen inhoud van de mail en de inhoud van de meegestuurde afbeeldingen komt nogal kunstmatig over.

Het beperkte aantal uitspraken maakt het niet mogelijk om een vaste lijn in de jurisprudentie te vinden als het gaat om het gebruik van Internet. De privacy van werknemers bij het gebruik van andere communicatiemiddelen is hiervoor uitgebreid aan bod gekomen. Daarbij is geconcludeerd, dat de rechter bij de beoordeling van de onrechtmatigheid van de controles minder strenge normen hanteert dan op grond van de wet en de publicaties van de Registratiekamer verwacht zou mogen worden.

6. Controles in het arbeidsconflict

6.1 Inleiding

Wanneer een bedrijf een Internet-policy hanteert, mag verwacht worden dat deze ook gerespecteerd zal worden. Als dit niet gebeurt, heeft de werkgever een scala aan sancties voor handen die hij aan de werknemer kan opleggen. Afhankelijk van de managementstijl, de relaties binnen het bedrijf en de ernst van de overtreding kan de werkgever kiezen voor informele of meer formele maatregelen, bijvoorbeeld:

- Een "goed gesprek" heeft alleen informele betekenis.
- Een functioneringsgesprek heeft geen directe juridische betekenis. Het gespreksverslag kan echter wel in een vervolgtraject gebruikt worden, bijvoorbeeld om aan te tonen dat de werknemer op de hoogte had moeten zijn van de policy.
- De werkgever kan een boete opleggen. Voorwaarde is wel dat deze mogelijkheid in de policy een onderdeel uitmaakt van de arbeidsovereenkomst.
- Schorsing van de werknemer.
- Ontslag. Daarbij zijn ontslag wegens dringende of gewichtige reden de belangrijkste maatregelen. (89)
- Ook kan de werkgever nog een schadevergoeding van de werknemer eisen. Dit kan alleen bij opzet of bewuste roekeloosheid. (90) Daar is slechts zelden sprake van. (91)

Als een werkgever de werknemer wil ontslaan, dan zal hij bewijzen moeten geven van de gedragingen van de werknemer. De bewijzen hiervoor zijn, behoudens toevalstreffers, alleen door controles door de werkgever te achterhalen.

Een werkgever die de grenzen van zijn controlebevoegdheid overschrijdt, handelt onrechtmatig ten opzichte van de werknemer. Het is de vraag wat daar de consequenties van moeten zijn: mag het bewijs mee gewogen worden in de ontslagprocedure? En, zo ja, welke voorwaarden zijn hieraan verbonden? Volgens Hugenholtz/Heemskerk valt deze vraag uiteen in twee sub-vragen: (92)

- Wanneer is er sprake van bewijs dat op onrechtmatige wijze is verkregen, en
- Kan onrechtmatig verkregen bewijs als bewijs in een burgerlijk proces worden toegelaten?

Een werkgever die zijn controlebevoegdheid niet overschrijdt, kan de logs zonder problemen inbrengen in de ontslagprocedure. De vraag is dan: welke waarde hebben de computerlogs? Logs kunnen eenvoudig gemanipuleerd worden, zowel tijdens het verzamelen als achteraf.

Een werknemer hoeft het niet eens te zijn met het feit dat de werkgever controles uitvoert. Hij kan hiertegen actie ondernemen. Als de ontslagprocedure begonnen is, kan de werknemer weinig doen tegen het inbrengen van de controleresultaten als bewijs.

6.2 De onrechtmatigheid van de controles

Een werkgever die zijn controlebevoegdheid overschrijdt, handelt onrechtmatig ten opzichte van zijn werknemer. Een dergelijke onrechtmatige daad valt binnen het bereik van artikel 6:162 BW: het is een inbreuk op een recht, namelijk het recht op bescherming van de persoonlijke levenssfeer. Een verregaande controle bij incidenten kan overigens conform de wet zijn; de Wbp geeft daar in artikel 43 sub e een regeling voor: hij kan de extra controles uitvoeren ter bescherming van zijn eigen rechten.

De overschrijding van de controlebevoegdheid hoeft echter niet altijd onrechtmatig te zijn. Lid 2 van artikel 6:162 BW stelt: "...behoudens de aanwezigheid van een rechtvaardigingsgrond". Ook het genoemde artikel 43, sub e verwijst in feite naar een rechtvaardigingsgrond. Bij de bepaling van rechtvaardigingsgronden wordt in eerste instantie aansluiting gezocht bij artikel 40 e.v. SR. (93) De daar genoemde rechtvaardigingsgronden zijn overmacht, noodweer, wettelijk voorschrift en ambtelijk bevel. Daarbij komt voor de bepaling van de onrechtmatigheid van

bewijs alleen noodweer als rechtvaardigingsgrond in aanmerking.

In het civiele recht worden echter meer rechtvaardigingsgronden geaccepteerd. Bij de parlementaire behandeling is ervan uitgegaan dat ook normen uit het ongeschreven recht rechtvaardigingsgronden kunnen opleveren. Hartkamp noemt als voorbeelden onder andere de toestemming, onder bepaalde omstandigheden de eigenrichting en de compensatie.

In het geval van Internet-polices is er toestemming verleend door de ondernemingsraad. Een dergelijke toestemming wordt in de rechtspraak niet zonder meer geaccepteerd in plaats van de toestemming door individuele werknemers. (94) Toestemming dient bovendien in vrijheid gegeven te worden. Er lijkt een duidelijke overeenkomst met de eisen die aan de toestemming in het kader van artikel 8 Wbp gesteld worden. Dit disqualificeert de toestemming als rechtvaardigingsgrond.

Bij compensatie als rechtvaardigingsgrond denkt men wellicht in eerste instantie aan overheidsoptreden. (95) Toch zou in een arbeidsconflict wel degelijk sprake kunnen zijn van compensatie. Zo zou een werkgever af kunnen zien van schade-claims. Deze situatie is echter uitzonderlijk. Ook zou de rechter de compensatie kunnen laten doorklinken in de correctiefactor in de Kantonrechtformule, die doorgaans bij ontbindingen van de arbeidsovereenkomst ex artikel 7:685 BW gebruikt wordt.

Bij de bepaling van de onrechtmatigheid probeert Kremer aansluiting te zoeken bij de noodweer en de eigenrichting. (96) Hij vindt het evident dat een stringente interpretatie van noodweer de verkrijging van onrechtmatig bewijs niet zal rechtvaardigen. (97) Het probleem daarbij wordt gevormd door het feit dat er sprake moet zijn van een ogenblikkelijke, wederrechtelijke aanranding. De eis van ogenblikkelijkheid betekent dat de aanranding in de nabije toekomst moet plaatsvinden. Maar de werkelijke aanranding, zo daar al sprake van is, zal pas plaatsvinden bij de uitspraak van de rechter. Kremer ziet een oplossing voor het probleem van de ogenblikkelijkheid door dit te bepalen tijdens het proces: de eigenlijke aanranding zou pas plaatsvinden met en door de rechterlijke uitspraak. Hij komt tot vier, wat hij basiscontouren van een rechtvaardigingsgrond noemt. Toegepast op Internet-polices:

- Bewijsdoel of bewijsintentie. De additionele controle moet tot doel hebben bewijs te verzamelen. Dit houdt in, dat additionele verzameling van logging alleen bij concrete verdenkingen toegestaan is.
- Er moet een redelijke verdenking zijn dat de werknemer zijn processuele verplichtingen niet na zal komen of informatie zal achterhouden of ontkennen. Omdat de werknemer in ontslagzaken er geen enkele baat bij heeft zijn misdragingen op Internet in te brengen, zal aan deze voorwaarde snel voldaan zijn.
- Er moet een situatie van bewijsnood ontstaan. Wanneer er voldoende bewijs zou zijn zonder de additionele controle, is een verdere inbreuk op de privacy van de werknemer niet noodzakelijk. Dus: liever getuigenverklaringen dan onrechtmatige controles.
- Proportionaliteit en subsidiariteit. Volgens Kremer is dit geen afzonderlijke eis, omdat hij geldt voor alle bewijsvoering.

6.3 Het gebruik van onrechtmatige controles als bewijs

Dijksterhuis-Wieten ziet geheel niets in een afzonderlijke bepaling van de onrechtmatigheid van de verkrijgingshandeling van het bewijs. (98) Zij stelt dat uit de jurisprudentie gebleken is dat in de praktijk onrechtmatig verkregen bewijsmateriaal gewoon gebruikt wordt en dat rechtmatig verkregen bewijsmateriaal soms uitgesloten wordt. Zij heeft daarin gelijk; als voorbeeld een tweetal uitspraken:

In Driessen/van Gelder (99) geeft de Hoge Raad als opmerking aan, dat:

(...) verwerping van de stelling "dat aan de onderwerpelijke bandopname geen enkel bewijs mag worden ontleend", niet zonder meer meebrengt dat de vraag of te dezen aan die band bewijs kan worden ontleend, bevestigend moet worden beantwoord (...)

en de Rechtbank Utrecht in LBP/Kupers: (100)

In beginsel is daarom het uit het 'aftappen' van Kupers' telefoon verkregen bewijsmateriaal als onrechtmatig verkregen aan te merken.

Dit betekent echter niet, dat bewijsmateriaal als het onderhavige, ongeacht de inhoud daarvan, onder alle omstandigheden door de rechter buiten beschouwing moet worden gelaten.

Dit houdt in dat er geen directe relatie tussen de onrechtmatigheid van het bewijs en de bruikbaarheid in het proces zou zijn.

Bij de toelating van onrechtmatig verkregen bewijs wordt een beperkt aantal arresten genoemd: het al eerder genoemde Driessen/van Gelder, Slemptes/Nool (101), het Codicil-arrest (102) en S. en O./Gemeente Wierden. (103) Opvallend is dat de Hoge Raad in al deze arresten het gebruik van het bewijs niet afwijst. Ook Kremer vindt geen argument dat hem zelf overtuigt. (104) De Vries stelt dan ook correct: privacy is geen alibi. (105)

De Vries geeft echter ook aan dat er grenzen moeten zijn. Daarbij haalt zij Asser aan wanneer zij stelt dat de rechter niet mag vervallen in een Pilatus-rol. Als een duidelijk grens noemt zij artikel 6 EVRM. Ook Kremer ziet een uiterste grens, bijvoorbeeld bij de overtreding van artikel 3 EVRM ter verkrijging van het bewijs. (106)

Anderzijds dient er voldoende correct materiaal voorgelegd te worden aan de rechter zodat deze een juist oordeel kan vormen. Een oordeel als in Wiedens/Kunst: (107)

Dat het ongeoorloofd internetten niet als dringende reden in het bestek van deze procedure kan worden aangenomen ligt vooral aan de onkunde van de kantonrechter(...)

is hoe dan ook onbevredigend.

De partijen in de discussie over de eventuele bewijsuitsluiting in het geval van onrechtmatig verkregen bewijs zijn nog ver verwijderd van een consensus. Wat in het kader van deze scriptie van belang is, is dat tot nu toe de privacy zelden een reden is geweest voor bewijsuitsluiting. De conclusie moet dan ook zijn dat, wanneer een werkgever te ver gaat in zijn controles, de resultaten van de controles gewoon gebruikt mogen worden.

De werknemer hoeft ook niet op compensatie te rekenen. Kremer verwijst hiervoor naar van Bavel/Duco. (108) Een gunstigere correctiefactor in de Kantonrechters-formule is dan ook niet te verwachten. De werknemer staat in dit geval met lege handen. Dit betekent overigens dat compensatie niet als rechtvaardigingsgrond kan dienen. (109)

6.4 De waarde van logs als bewijs

In een ontslagprocedure zal de werkgever zijn bewijzen moeten overleggen. Deze bewijzen bestaan, naast eventuele getuigenverklaringen, voornamelijk uit computer-logs. Deze computer-logs moeten gezien worden als geschriften-niet-akten, in welke vorm zij ook worden aangeleverd (CD-ROM, tape of misschien zelfs papier). (110)

Als een werkgever geen logging kan overleggen, is zijn positie behoorlijk verzwakt. De Kantonrechter in Zwolle oordeelde dat een ernstige controle van de bedrijfsregels, in casu het downloaden van software uit ongescreende bron, onvoldoende reden was voor ontslag op staande voet, omdat de werkgever geen, althans onvoldoende, controle had uitgevoerd. (111) Aardig is, dat het behalen van het ISO-9000 certificaat hier ten nadele van de werkgever werkte.

De basis van bijna alle logging op computers is dat log-records weggeschreven worden bij een min of meer nauwkeurig omschreven gebeurtenis. Voor het daadwerkelijk volgen van de activiteiten van een werknemer op Internet kan een zeer grote hoeveelheid logging nodig zijn. In de regel zal dan ook een selectie uit of bewerking van de log gepresenteerd worden. Dit levert gelijk een probleem op: degene die de log bewerkt, is dezelfde die het inbrengt als bewijs.

Het wijzigen van een (login-) naam in een log is al relatief eenvoudig, hier rekening mee houden met het bewerken van de log is helemaal een fluitje van een cent. Het is dan ook verwonderlijk dat de inhoud van de logs in de meeste uitspraken eigenlijk niet ter discussie wordt gesteld. De discussie lijkt zich voornamelijk af te spelen op het terrein van de onrechtmatige bewijsgaring. Zoals hierboven gesteld is dat voor de werknemer een heilloze weg.

Een werkgever zal proberen, wanneer er twijfel over de inhoud van de logs is, deze twijfel zoveel mogelijk weg te nemen. Dat kan door bijvoorbeeld een EDP-auditor een onderzoek naar het logging- en rapportageproces te laten doen. Een EDP-audit is echter een momentopname; het garandeert weinig over de situatie ervoor. Ook de financiële aspecten kunnen prohibitief zijn voor het inzetten van dit middel. Een bewijsovereenkomst lijkt dan ook het aangewezen middel. De bewijsovereenkomst zou opgenomen kunnen worden in het arbeidscontract. Het feit dat de computer-logs volledig onder beheer van de werkgever staan hoeft daarbij geen probleem te zijn; dit is af te leiden uit het arrest over de "boekenclausule". HR 7 december 1934, NJ 1935, p.443. Hierin wordt bepaald, dat een clausule waarbij de schuldenaar zich op voorhand neerlegt bij het bedrag dat in de boeken bij de geldgever staat, rechtsgeldig gevonden. Een clausule, die de werknemer in zijn bewijsvoering uitsluit of beperkt zal echter, naar analogie van artikel 6:236 onder k, als onredelijk bezwarend buiten beschouwing blijven. Tevens moet worden opgemerkt, dat het hier gaat om een overeenkomst; een clausule in een algemene Internet-policy zal onvoldoende zijn. De combinatie van een dergelijke clausule en een handtekening van de werknemer, bijvoorbeeld op een aanvraagformulier voor een Internet-account, kan wel voldoende zijn. Om latere discussies te vermijden, is het aan te bevelen om een dergelijke bewijs-overeenkomst deel uit te laten maken van de procedure waarmee een werknemer toegang tot Internet krijgt.

Een volgend probleem bij het gebruik van de logs is hun interpretatie. Logs in ruwe vorm zijn vaak lastig te lezen. (112) De rechter kan hiervoor onvoldoende kennis hebben. (113) Ook bijvoorbeeld de tijd in de tijdsaanduidingen in de verschillende logs hoeven niet hetzelfde te zijn; de ene computer kan "achter lopen" ten opzichte van de andere. Doordat de inhoud van de logs door de werknemer niet in twijfel worden getrokken is er nog geen noodzaak geweest om de logs nader te analyseren. In voorkomende gevallen zal de rechter een beroep moeten doen op deskundigen. (114) Ook wanneer de logs technisch-inhoudelijk duidelijk zijn is nog een interpretatieslag nodig. In een aantal bedrijven is het, bijvoorbeeld ten behoeve van de continuïteit, de gewoonte om de wachtwoorden van een aantal collega's te weten. Het is dan eenvoudig om zijn eigen sporen uit te wissen ten koste van collega's. (115)

6.5 De positie van de werknemer

Bij een persoonsregistratie heeft de geregistreerde het recht van correctie. Een wijziging, daarbij inbegrepen verwijdering, is toegestaan indien:

- de gegevens feitelijk onjuist zijn
- voor het doel of de doeleinden van de verwerking onvolledig of niet ter zake dienend zijn;
- dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt. (116)

Bij reguliere controles, dat wil zeggen volgens de regels uit de Internet-policy, kan de werknemer verlangen dat bepaalde log-gegevens verwijderd worden.

Dat ligt anders voor controles bij incidenten. Vaak worden deze controles heimelijk uitgevoerd, dus zonder medeweten van de werknemer. De vraag is of in dergelijke gevallen de werkgever verplicht is om op verzoek van de werknemer mede te delen welke gegevens verzameld worden. De werkgever heeft hier, volgens de wet, vier weken de tijd voor. Een uitgebreidere controle zal slechts voor een beperkte termijn acceptabel zijn. (117) Als een werkgever gedurende een langere termijn additionele logging verzamelt, dan heeft dit meer weg van de reguliere controle. De werknemer dient dan op de hoogte te zijn. De werknemer kan dan proberen invloed uit te oefenen op de controles zodra hij weet dat ze plaatsvinden.

In het arbeidsconflict staat de werknemer niet sterk tegenover een werkgever die bovenmatig controleert. De werknemer moet derhalve zorgen dat de werkgever in het gareel blijft lopen, bijvoorbeeld door te eisen dat de controlemaatregelen teniet gedaan worden. In de Distrivox-zaak kwam de Ondernemingsraad met succes op tegen het gebruik van de extra controlemogelijkheden die een nieuwe telefooncentrale had "KG_1990_33.txt". Pres. Rb Amsterdam 14 december 1989, KG 1990, 33. en ook de KOMA moest de camera's na een kort geding met de FNV verwijderen. (118) Een werknemer heeft het recht om met redelijke tussenpozen aan de werkgever te vragen of er persoonsgegevens van hem worden verwerkt. De werkgever moet dan, volgens artikel 35 lid 2 Wbp binnen vier weken een *volledig* overzicht geven van de gevoerde registraties en hun doelen. Naast volledig dient dit overzicht ook nog begrijpelijk te zijn.

Een werknemer heeft dus wel degelijk mogelijkheden om de controles door de werkgever te beperken. Doet hij dit niet, dan kan hij bij een arbeidsconflict geconfronteerd worden met controles waar hij nauwelijks weet van had. De moraal voor de werknemer is dan ook: let op de werkgever.

7. Afsluiting

7.1 De Internet-policy

Op basis van de Wbp, de jurisprudentie en de uitspraken van de Registratiekamer zijn regels gevonden voor het opstellen van Internet-polities. Uit een korte blik over de grens is gebleken, dat de regels elders in Europa niet veel afwijken van de ontwikkelingen in Nederland. Dat was ook niet te verwachten: de privacy-wetgeving is grotendeels gebaseerd op Europese richtlijnen.

In paragraaf 4.5 zijn de regels voor de Internet policy weergegeven. Het is gebleken, dat de manier van omgang met de policy net zo belangrijk is als de inhoud van de policy. In hoofdstuk 6 kwamen de bewijsrechtelijke aspecten van controles aan de orde. De belangrijkste aanbeveling voor de Internet-policy was dat een bewijsovereenkomst opgenomen kan worden. (119)

Voor de werkgever is het belangrijk te weten dat hij het recht heeft beperkingen te stellen aan het Internet-gebruik van zijn werknemers. In de Internet-policy kan hij aangeven wat de grenzen zijn. Dit kan betrekking hebben op het taalgebruik, het niet verspreiden van informatie, het niet-downloaden van software of het beperken van het privé-gebruik. Hij zal echter altijd een bepaald privé-gebruik moeten toestaan. De werkgever heeft bovendien het recht om controles uit te voeren zolang deze controles voldoen aan de proportionaliteitseis. Bij incidenten heeft hij het recht verdergaande controles uit te voeren; er dient dan wel een concrete verdenking te zijn.

Voor de werknemer is het belangrijk te weten dat hij gecontroleerd wordt. Uit de policy weet hij welke controles er plaatsvinden. Op basis van de gestelde grenzen zou een calculerend werknemer de keuze kunnen maken tussen het privé Internet-gebruik op het werk (besparing telefoonkosten) of thuis (grotere privacy). Een werknemer die bij deze keuze de aangekondigde controles meeweegt komt van de koude kermis thuis: bij incidenten mag de werkgever veel meer gegevens verzamelen en ook onrechtmatig verkregen gegevens over het Internet-gebruik zullen in een arbeidsconflict gewoon meegewogen worden. Een beroep op onrechtmatig verkregen bewijs zal zelden slagen.

Ook bewijs-technisch kan de Internet-policy voordelen bieden. Alle bewijs uit reguliere controles zal zonder problemen gebruikt kunnen worden. Ook verdergaande controle, mits aangekondigd in de Internet-policy, zal geaccepteerd worden. De discussie over de waarde van bepaalde computer-logs kan beperkt worden door een bewijsovereenkomst-clausule op te nemen.

7.2 Alternatieven

In deze scriptie is ervan uitgegaan, dat de werkgever de Internet-policy als instrument hanteert om Internet-gebruik te reguleren. Dat hoeft echter niet: er zijn verschillende alternatieve mogelijkheden. De meest voorkomende is waarschijnlijk: geen Internet. Een groot aantal middelgrote en kleine bedrijven is, ondanks de reclames van het Ministerie van Economische Zaken, nog steeds niet on-line. Andere bedrijven hebben alleen een server bij een provider staan en nemen daar een complete dienst, van ontwerp tot web-hosting, af. Uiteraard speelt het probleem van de privacy van de werknemer bij het gebruik van Internet hier in het geheel niet.

Een werkgever kan ook onbeperkte toegang tot het Internet toestaan, zonder controles. Deze variant ziet men wel in de academische wereld. De grenzen voor de werknemer zijn in dit geval de wettelijke grenzen, bijvoorbeeld de intellectuele eigendomsregels. Doordat het niet mogelijk is eigen grenzen te stellen, is dit alternatief voor het bedrijfsleven minder geschikt. Een werkgever zal in ieder geval invloed willen hebben op de uitstraling die zijn bedrijf op Internet heeft.

De KPN heeft ervoor gekozen om geen Internet-policy op te stellen. Door geen beperkingen op te leggen hoopt de KPN, via het Internet-gebruik, de kennis van de medewerkers te vergroten. Bij incidenten, zoals vastlopende systemen of het ontdekken van porno, valt de KPN terug op algemene CAO-bepalingen. (120) Een groot voordeel is, dat er geen controle-infrastructuur aangelegd en beheerd hoeft te worden. Het gebrek aan reguliere logging kan echter proces-rechtelijke consequenties hebben. (121)

7.3 Afsluitende opmerkingen

Een Internet-policy moet geen op zich zelf staand document zijn. De policy mag niet buiten de grenzen van de arbeidsovereenkomst of de CAO treden; daar buiten mag de werkgever geen beperkingen opleggen aan de werknemer. De bevoegdheid van de werkgever tot grenzen stellen vloeit namelijk voort uit artikel 7:660 BW dat de bevoegdheid beperkt zich tot binnen de grenzen van algemeen verbindende voorschriften, overeenkomst of reglement. Een Internet-policy zal zich ook moeten conformeren aan het algemene informatie-beveiligingsbeleid van het bedrijf. Het technisch deel van de beperkingen aan het Internet-gebruik zullen bepaald worden door dit beveiligingsbeleid.

Bij verdergaande controles moet een concrete verdenking zijn. In tegenstelling tot het strafrecht, waar een rechter toestemming moet geven voor inbreuken op de persoonlijke levenssfeer, is de werkgever zelf gerechtigd deze beslissing te nemen. De werkgever stelt dus de regels op, bepaalt wanneer en hoe er gecontroleerd wordt en kan bovendien zelf de straf bepalen. (122) Gelukkig zijn er beperkingen. De belangrijkste beperking is dat de werkgever zich als goed werkgever moet gedragen. Doet hij dit niet, dan kan de werknemer zich tot de rechter wenden. De macht van de werkgever beperkt zich bovendien tot de arbeidssituatie. Een werknemer die zijn arbeidscontract opzegt, wordt bevrijd van de inbreuk die door de werkgever wordt gemaakt op zijn privacy. Voor de invoering van reguliere controles is bovendien toestemming van de Ondernemingsraad nodig. Door deze grenzen aan de macht hoeft het gebrek aan machtscheiding geen probleem te zijn.

Herhaaldelijk is in deze scriptie aangegeven dat de rechtspraak, ondanks de inbreuk op de privacy, de resultaten van controles als bewijs accepteert in een ontslagzaak. Aan de andere kant blijkt een ontslag op staande voet vaak ongedaan gemaakt te worden. Zelfs bij een beveiligingstechnische doodzonde, zoals het downloaden van met virus besmette software (123) of het aanleggen van een eigen Internet-verbinding (124) is ontslag op staande voet niet goedgekeurd. Ook als de werknemer de verspeiding van porno via e-mail toegeeft blijkt de Kantonrechter de arbeidsovereenkomst te ontbinden wegens verandering van omstandigheden. (125)

7.4 Conclusie

Het is moeilijk om een eindconclusie te geven van een onderwerp dat zo in beweging is. Ook is er niet een vaste algemene maatschappelijke tendens te vinden. Als voorbeeld: enerzijds legt men steeds meer nadruk op de privacy, anderzijds worden steeds meer controles, zoals bijvoorbeeld camera-bewaking in openbare gelegenheden, geaccepteerd. Ook het beleid van de overheid is niet consistent: aan de ene kant wil zij e-mails, net als andere vormen van communicatie, besloten houden, aan de andere kant verplicht zij Internet Service Providers aftappunten te realiseren zodat de e-mail eenvoudig gelezen kan worden.

In de jurisprudentie vindt men een tendens naar meer respect voor de persoonlijke levenssfeer van de werknemer. Deze trend is echter niet zó duidelijk dat er harde conclusies aan verbonden kunnen worden. In een rechtszaak, waar de werknemer geconfronteerd wordt met de resultaten van de schendingen van zijn persoonlijke levenssfeer, mogen deze resultaten wel tegen hem gebruikt worden. Een ontslag wegens dringende reden is echter zeldzaam; meestal wordt de arbeidsovereenkomst ontbonden wegens verandering van omstandigheden. De Nederlandse rechter lijkt de kool en de geit te willen sparen; hij maakt daardoor een onzekere indruk als het gaat om het Internet-gebruik.

Ook de techniek staat niet stil. Het gebruik van encryptie-technieken maakt het mogelijk om voor de werkgever onleesbare e-mail te versturen. De privacy is dan gegarandeerd tot het moment dat de werkgever de encryptie-sleutels heeft gekregen. Logging kan opgeslagen worden via "three handed games". Elk van de drie handen krijgt een deel van de informatie. Voor de reconstructie van het bericht zijn alle drie de delen nodig. Geen van de delen bevat voldoende informatie om de inhoud van het bericht te kennen. Een werkgever is dan nooit in staat om in zijn eentje de controles te initiëren. Partroon-herkenning en log-correlatie mechanismes maken de controles weer eenvoudiger. Het kost weinig moeite om alle e-mails met onwelvoeglijke termen erin op te sporen.

Wellicht de duidelijkste conclusie die getrokken kan worden is dat het probleem bij Internet-polities ligt bij het spanningsveld tussen de bevoegdheid van de werkgever en de privacy van de werknemer. Dit verklaart ook de aandacht voor Internet-polities: het onderwerp combineert de stijgende behoefte aan privacy op de werkplek met de hype van het Internet.

Een Internet-policy heeft een duidelijke functie. De policy stelt regels waar de werknemer zich aan moet houden. De policy zorgt ervoor dat de werkgever aan zijn verplichting voldoet om aan de werknemer aan te geven welke controles er plaatsvinden. Ook bewijsrechtelijk heeft de policy voordelen. Veel bedrijven zullen dan ook overgaan tot het opstellen van Internet-policies.

Eindnoten

- (1) Zie bijvoorbeeld A. van Oorschot, Let op je personeel! Maar hoe doe je dat? Nieuwe privacywetgeving vraagt om zorgvuldige aanpak fraude werknemers, VNO-NCW Forum 99-019.
- (2) Bijvoorbeeld: <https://www.computable.nl/2000/11/23/tegenwind-voor-kantoorsurfers/> CMG <http://www.computable.nl/artikels/binnlan0/n4700t07.htm>.
Auke Schouwstra, Tegenwind voor kantoorsurfers in: Computable, 24 november 2000, p. 34, 35.
- (3) Voorbeeldprotocol: Privacy bij internet- en email-gebruik, FNV Bondgenoten, 1999
Surfen op de werkplek. Een modelgedragscode voor Internet en e-mailgebruik, FME-CWM, VNO-NCW, maart 2001.
- (4) Anders: Herbert Blankesteijn, "Surfen op kantoor is verre van schadelijk voor de baas", NRC Handelsblad 13 januari 2001, p. 7.
- (5) S.D. Warren, L.D. Brandeis, "The right to privacy. The implicit made explicit.", Harvard Law Review 1890, p. 193-220.
- (6) P.Blok, A. Vedder, "Privacy in ontwikkeling", in: <https://research.tilburguniversity.edu/en/publications/privacy-en-de-bescherming-van-persoonsgegevens> Prins & Berkvens, p. 23.
- (7) Zie voor een algemene discussie: Van der Pot-Donner, Handboek van het Nederlandse staatsrecht, Zwolle: Tjeenk Willink, 1995.
- (8) https://www.denederlandsegrondwet.nl/id/vlt2198inlwf/commissie_franken Grondrechten in het digitale tijdperk, p. 53.
- (9) De hier geciteerde tekst is een standaardformulering van de Registratiekamer. Zie paragraaf 3.1 in ["Als_de_telefoon.html"](#) Hulsman en ["top_1_5_35_18.html"](#) Goed werken in netwerken.
- (10) P.F. van der Heijden, "Tussen paradox en paranoia", in: P.F. van der Heijden (red.), Privacy op de werkplek, 's-Gravenhage: SDU, p. 9-23.
- (11) Deze bevoegdheid heeft hij op basis van ["BW7titel10.htm#660"](#) art. 7:660 BW.
- (12) ["JAR_1999_25.txt"](#) Kr Zwolle, 30 december 1998, JAR 1999, 25.
- (13) ["nl_390L0270.html"](#) Art. 3, sub b, bijlage bij Richtlijn 90/270/EEG, 11-3-1999.
- (14) Bijvoorbeeld: Van der Heijden 1998 (Tekst & Commentaar BW), art. 7:611 BW, aant. 1.
- (15) EG Richtlijn 95/46 van 24 oktober 1995.
- (16) Zie bijvoorbeeld: J. Terstegge, De nieuwe Wet bescherming persoonsgegevens. Handleiding voor de praktijk, Alphen aan den Rijn: Samson 2000, p. 18, 19.
- (17) J.E.J. Prins, J.M.A. Berkvens, "De Wet bescherming persoonsgegevens", in <https://research.tilburguniversity.edu/en/publications/privacy-en-de-bescherming-van-persoonsgegevens> Prins & Berkvens, p. 80.
- (18) ["wbp_mvt.htm"](#) MvT Wbp, toelichting art. 1, onderdeel i.
- (19) Een verzoek, zoals gedaan door de districtschef van de politie Rotterdam-Rijnmond in ["AB0812.txt"](#) AB0812 is dan ook niet geldig als toestemming in deze zin. (Rb. Rotterdam, 29 maart 2001, ELRO: AB0812).
- (20) ["vrijstellingsbesluit.html"](#) Besluit genormeerde vrijstelling, Stb. 1990, 16, tekst van het besluit per 1 april 1995, art. 20.

- (21) "WOR.html" Art. 27 lid 1 sub k en l WOR.
- (22) "KG_1985_299.txt" Pres. Rb Roermond 12 september 1985, KG 1985, 299.
- (23) "JAR_1999_25.txt" Kr Zwolle, 30 december 1998, JAR 1999, 25.
- (24) J.H.J. Terstegge, H.H. de Vries, De werknemer achtervolgd? Over personeelsvolgsystemen, verzuimcontrole en de nieuwe bevoegdheden van de OR, Den Haag: SDU, 1998. In de Verenigde Staten blijkt 44% van de werkgevers lijsten van gebelde nummers bij te houden (American Management Association: Workplace Testing, Monitoring & Surveillance, AMA, 2000).
- (25) Hoge Raad, 16 oktober 1987, NJ 1988, 850.
- (26) CRvB 9 februari 1993, PG 1993, 3871.
- (27) "JAR_1997_6.txt" Rb Utrecht, 25 september 1996, JAR 1997, 6.
- (28) "Als_de_telefoon.html" Hulsman, hoofdstuk 5.
- (29) Zie ook het antwoord van Minister Sorgdrager op vragen van de heer Rabbae, NJB 13 oktober 1995, p. 1351.
- (30) "z1999-1140-19.html" Registratiekamer, 24 juli 2000, kenmerk z1999-1140-19.
- (31) Tot deze conclusie komt ook Van Tongeren: W.J.M. van Tongeren, Het briefgeheim op de werkplek, ArbeidsRecht, 1999 6/7, p. 5.
- (32) "JAR_1998_135.txt" Rb Amsterdam, 20 mei 1998, JAR 1998, 135.
- (33) "top_1_4_2_3.html" Registratiekamer, 'Camera's op de werkplek', Informatieblad 3, april 1999.
- (34) "JOL2001_295.txt" HR 27 april 2001, JOL 2001, 295.
- (35) Checklist videocameratoezicht van de Registratiekamer, zoals geciteerd in H.H. de Vries, (Verborgen) cameratoezicht op de werkplek, Privacy & informatie, 1999-6, p. 262.
- (36) Dat een goede analoge opname bedreigender voor de privacy is dan eenvoudige digitale opnames lijkt niet terzake te doen. Ook is een analoge opname naderhand eenvoudig te digitaliseren. Onder de Wbp wordt ook het opnemen met analoge apparatuur aangemerkt als het verzamelen van persoonsgegevens.
- (37) "KG_1985_299.txt" Pres. Rb Roermond, 12 september 1985, KG 1985, 299.
- (38) "JAR_1997_204.txt" Kr Utrecht, 20 augustus 1997, JAR 1997, 204. Deze uitspraak is niet zonder commentaar(bijvoorbeeld H.H. de Vries, (Verborgen) cameratoezicht op de werkplek, Privacy & Informatie nr. 6, december 1999, p. 257: "Deze motivering is wel heel kort door de bocht").
- (39) "JAR_1997_189.txt" Kr Schiedam, 8 juli 1997, JAR 1997, 189.
- (40) "AB1825.txt" Rb Arnhem, 18 januari 2001, ELRO AB1825.
- (41) "PRG_1998_4946.txt" Zie bijvoorbeeld Kr Rotterdam 19 december 1997, PRG 1998, 4946.
- (42) Dit is gebruikelijk bij onder andere winkelpersoneel. De schrijver dezes heeft dat aan den lijve ondervonden tijdens een vakantiebaantje bij de Bijenkorf.
- (43) "Smyth_v_Pillsbury.html" US District Court for the Eastern District of Pennsylvania, 18 januari 1996. Met deze uitspraak wordt in Amerika het verschil in privacy-schendingen beargumenteerd.
- (44) Tenzij de resultaten in een registratie worden opgenomen.
- (45) "95-46-EG.txt" Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, Publikatieblad nr L 281 van 23-11-1995, blz. 0031 - 0050.

- (46) "NJ_1993_400.txt" EHRM, 16 december 1992, NJ 1993, 400.
- (47) Article 226-15 du code pénal.
- (48) Article L 432-2-1 du code du travail.
- (49) Article 226-3 du code pénal.
- (50) "travail_video1a.pdf" Commission Nationale de l'Informatique et des Libertés, La vidéosurveillance sur le lieu de travail, versie 1.0-011297, <http://www.cnil.fr>.
- (51) Cour de Cassation, 20 novembre 1991, Droit Social 1992, p. 28.
- (52) Paris, 17 juni 1938, DH 1938.520, geciteerd in "cybersurveillance.pdf" Bouchet p. 29.
- (53) "GB_employ2.pdf" The use of personal data in employer/employee relationships, Draft Code of Practice issued for consultation by the Data Protection Commissioner, oktober 2000.
- (54) Deze lijn mag dan niet afgeluisterd worden "NJ_1998_506.txt" (EHRM 25 juni 1997, NJ 1998, 506).
- (55) Wet van 8 december 1992, art. 5, sub f.
- (56) Commissie voor de bescherming van de persoonlijke levenssfeer, 30 januari 1998, RZ981U2_1.
- (57) En dan met name § 1:
Met gevangenisstraf van zes maanden tot één jaar en met geldboete van tweehonderd frank tot tienduizend frank of met een van die straffen alleen wordt gestraft hij die 1° ofwel, opzettelijk, met behulp van enig toestel privé-communicatie of -telecommunicatie, waaraan hij niet deelneemt, tijdens de overbrenging ervan, afluistert of doet afluisteren, er kennis van neemt of doet van nemen, opneemt of doet opnemen, zonder de toestemming van alle deelnemers aan die communicatie of telecommunicatie;
- (58) Commissie voor de bescherming van de persoonlijke levenssfeer, advies Nr 34/1999 van 13 december 1999.
- (59) Dit is waarschijnlijk een gevolg van de veroordeling van het Verenigd Koninkrijk door het EHRM. "NJ_1998_506.txt" EHRM 25 juni 1997, NJ 1998, 506.
- (60) Vergelijk "NJ_1987_321.txt" HR 16 december 1986, NJ 1987, 321 (Slavenburg II), waarin gesteld wordt dat van feitelijk leidinggeven aan verboden omstandigheden sprake kan zijn als "de desbetreffende functionaris - hoewel daartoe bevoegd en redelijkerwijs gehouden - maatregelen ter voorkoming van deze gedragingen achterwege laat en bewust de aanmerkelijke kans aanvaardt dat de verboden gedragingen zich zullen voordoen".
- (61) "rapport_gdt_5-00.pdf" Grondrechten in het digitale tijdperk, p. 4.
- (62) Nicholas Negroponte stelt de wereld van de bits tegenover de wereld van de atomen (Nicholas Negroponte, Being Digital, London: Hodder and Stoughton, 1995).
- (63) Hiervoor zijn zelfs speciale tools en computertalen ontwikkeld zoals SAS (Statistics Application System), PERL (Practical Extraction and Report Language), Python, awk (Aho, Weinberger, Kernighan).
- (64) Met name Microsoft Outlook.
- (65) La Commission Nationale de l'Informatique et des Libertés heeft op haar web-site een aardige demonstratie "www.cnil.fr"
- (66) Sommige ISP's, zoals XS4all, blokkeren dit verkeer, omdat zij het een te groot risico voor onnadenkende klanten vinden.
- (67) Ter illustratie: een e-mail van mijn privé-adres naar de universiteit gaat via de netwerken van XS4all, UUnet, SURFnet en de universiteit.
- (68) Overigens is de inhoud van het bericht sowieso openbaar. Maar het feit dat men een bijdrage geeft aan bijvoorbeeld alt.support.aids.partners hoeft niet algemeen bekend te zijn.

- (69) "nl_390L0270.html" Art. 3, sub b, bijlage bij Richtlijn 90/270/EEG, 11-3-1999 stelt: "[...] er mag zonder medeweten van de werknemers geen gebruik worden gemaakt van een kwantitatief of kwalitatief controlemechanisme"
- (70) "wbp.htm" Art. 35 lid 2 Wbp.
- (71) De Registratiekamer beveelt dan ook aan: "Behandel zaken online op dezelfde manier als offline" "top_1_5_35_18.html" (Goed werken in netwerken).
- (72) "top_1_5_35_18.html" Goed werken in netwerken, hoofdstuk 5.
- (73) "top_1_6_2_35.html" Registratiekamer, 24 juni 1999.
- (74) Deze noodzaak, vastgelegd in art. 27 lid 1, sub k en l WOR, is ook in §2.2 aan bod gekomen.
- (75) J.P.R. Bergfeld (ed.), Controle e-mailverkeer door werkgever, Computerrecht 2000/2, p. 109. Het is vervelend dat de schrijver van het artikel geen referentie van de uitspraak van de Registratiekamer geeft.
- (76) Brief van de Registratiekamer d.d. 14 oktober 1997, gepubliceerd in Computerrecht 1998-5, p.252.
- (77) "GB_employ2.pdf" The use of personal data in employer/employee relationships, Draft Code of Practice issued for consultation by the Data Protection Commissioner, oktober 2000.
- (78) "cybersurveillance.pdf" Bouchet
- (79) "be_itopwerk.html" Commissie voor bescherming van de persoonlijke levenssfeer, Advies uit eigen beweging betreffende het toezicht door de werkgever op het gebruik van het informaticasysteem op de werkplaats, nummer Z00433_1, 3 april 2000.
- (80) "NJ_1998_506.txt" EHRM 25 juni 1997, NJ 1998, 506.
- (81) "NJ_1993_400.txt" EHRM 16 december 1992, NJ 1993, 400.
- (82) "PRG_1999_5365.txt" Kr Almelo, 30 september 1999, PRG 1999, 5365.
- (83) "vb-prtcl_fnv.htm" Voorbeeldprotocol: privacy bij het internet- en email-gebruik, FNV Bondgenoten, 1999.
- (84) Privacy in bedrijf, Een uitleg van de nieuwe Wet Bescherming Persoonsgegevens, AWWN, FME-CWM, VNO-NCW, augustus 2000.
- (85) "vnoncw-surfen.pdf" Surfen op de werkplek. Een modelgedragscode voor internet en e-mailgebruik, FME-CWM, VNO-NCW, maart 2001.
- (86) "PRG_1999_5365.txt" Kr Almelo, 30 september 1999, PRG 1999, 5365.
- (87) Rb Utrecht 16 september 1998, NJ-kort 1998, 83.
- (88) Kr Haarlem 16 juni 2000, Computerrecht 2001/1, p. 37.
- (89) "BW7tite110.htm" Art. 7:677 BW resp. art. 7:685 BW.
- (90) "BW7tite110.htm" Art. 7:661 BW.
- (91) Een extreem geval is Pollemans/Hoondert, HR 20 september 1996, JAR 1996, 203 of "NJ_1997_198.txt" NJ 1997, 198.
- (92) "hugen.html" Hugenholtz, nr 124.
- (93) Asser-Hartkamp 4-III, nr. 58 e.v.
- (94) "KG_1985_299.txt" Vergelijk Pres. Rb Roermond, 12 september 1985, KG 1985,299.
- (95) Bijvoorbeeld: "NJ_1992_638.txt" Leffers/Staat, HR 18 januari 1991, NJ 1992, 638.

- (96) "kremer.html" Kremer, p. 129.
- (97) "kremer.html" Kremer, p. 129.
- (98) H.L.G. Dijksterhuis-Wieten, "Onrechtmatig verkregen, toch gebruiken", Advocatenblad 2000, p. 606-609.
- (99) "NJ_1988_850.txt" HR 16 oktober 1987, NJ 1988, 850.
- (100) "JAR_1997_6.txt" Rb Utrecht, 25 september 1996, JAR 1997, 6.
- (101) "NJ_1993_78.txt" HR 7 februari 1992, NJ 1993, 78.
- (102) "NJ_1983_682.txt" HR 1 juli 1982, NJ 1983, 682.
- (103) "NJ_1995_400.txt" HR 11 november 1994, NJ 1995, 400.
- (104) "kremer.html" Kremer, p. 233 e.v.
- (105) H.H. de Vries: Hoe werkt informationele privacy?, Sociaal Recht 2000/5, p. 133-140.
- (106) "href=kremer.html" Kremer, p. 221.
- (107) "PRG_1999_5365.txt" Kr Almelo, 30 september 1999, PRG 1999, 5365.
- (108) "href=kremer.html" Kremer, p. 238; "NJ_1979_263.txt" Hof 's-Hertogenbosch 14 november 1978, NJ 1979, 263.
- (109) Compensatie was één van de mogelijke civielrechtelijke rechtvaardigingsgronden in §6.2.
- (110) "hugen.html" Hugenholtz nr. 125 formuleert het als "dragers van verstaanbare leestekens die in onderling verband een gedachte tot uitdrukking brengen. Van welke aard de leestekens zijn of op welk materiaal zij zijn gesteld is onverschillig".
- (111) "JAR_1998_22.txt" Kr Zwolle 18 november 1997, JAR 1998, 22.
- (112) Kolkman en Van Kralingen geven een voorbeeld in P.J.M. Kolkman, R.W. van Kralingen, "Privacy en nieuwe technologie" in: "https://research.tilburguniversity.edu/en/publications/privacy-en-de-bescherming-van-persoonsgegevens" Prins & Berkvens
- (113) Dit was ook het geval in: "PRG_1999_5365.txt" Kr Almelo 30 september 1999, PRG 1999, 5365.
- (114) "burgrv.txt" Art. 221-225 RV.
- (115) Zie ook J.R. Prins, M.W. van Marel, "Forensische informatietechnologie", De EDP-Auditor, 2001-1, p. 33-36.
- (116) "wbp.htm" Art. 35 Wbp.
- (117) Vergelijk bijvoorbeeld de heimelijke camera-observatie.
- (118) "KG_1985_299.txt" Pres. Rb Roermond, 12 september 1985, KG 1985, 299.
- (119) Zo kan in de policy een clause opgenomen worden waarbij de log van de firewall als vaststaand wordt beschouwd waar het gaat om de vastlegging van het Internet-verkeer. In het aanvraagformulier voor een Internet-account geeft de werknemer aan zich te verenigen met de Internet-policy.
- (120) En met name art. 1.5: Verplichtingen van de werknemer: (1) De werknemer is gehouden zijn functie naar behoren te verrichten en al datgene te doen of na te laten wat een goed werknemer behoort te doen of na te laten. (2) De werknemer is gehouden aan de door of namens de werkgever vastgestelde te zijner kennis gebrachte voorschriften, richtlijnen en aanwijzingen.
- (121) "JAR_1998_22.txt" Zie Kr Zwolle 18 november 1997, JAR 1998, 22.
- (122) Volgens Montesquieu zouden deze drie bevoegdheden bij verschillende instanties moeten liggen. Montesquieu, L'esprit des lois XI: Des lois qui forment la liberté politique dans son rapport avec la constitution, Parijs: Gallimard, 1994, p. 396 e.v.

(123) "JAR_1998_22.txt" Kr Zwolle, 18 november 1997, JAR 1998, 22.

(124) "PRG_1999_5365.txt" Kr Almelo, 30 september 1999, PRG 1999, 5365.

(125) Bijvoorbeeld Kr Haarlem 16 juni 2000, Computerrecht 2001/1, p. 37, 38 en Kr Apeldoorn 6 september 2000, Computerrecht 2001/1, p. 38, 39.

Inhoudsopgave

1. Inleiding	2
1.1 Waarom een Internet policy?	2
1.2 Wat is een Internet-policy?	2
1.3 Inhoud van deze scriptie	2
2. Controles en privacy op de werkplek	4
2.1 De privacy van de werknemer	4
2.2 Wettelijke normen	4
2.3 Controles in de praktijk	6
2.4 Tussenconclusie	9
3. De Europese horizon	10
3.1 Inleiding	10
3.2 Frankrijk	10
3.3 Engeland	11
3.4 België	12
3.5 Korte rechtsvergelijking	12
4. Regels voor de Internet-policy	14
4.1 Inleiding	14
4.2 Techniek-onafhankelijkheid of niet?	14
4.3 De Registratiekamer	16
4.4 Internet-regels elders in Europa	17
4.5 De regels voor een Internet-policy	18
5. De praktijk	20
5.1 Inleiding	20
5.2 FNV	20
5.3 Werkgeversorganisaties	20
5.4 Jurisprudentie	21
6. Controles in het arbeidsconflict	24
6.1 Inleiding	24
6.2 De onrechtmatigheid van de controles	24
6.3 Het gebruik van onrechtmatige controles als bewijs	25
6.4 De waarde van logs als bewijs	26
6.5 De positie van de werknemer	27
7. Afsluiting	30

7.1 De Internet-policy	30
7.2 Alternatieven	30
7.3 Afsluitende opmerkingen	31
7.4 Conclusie	31
Eindnoten	34