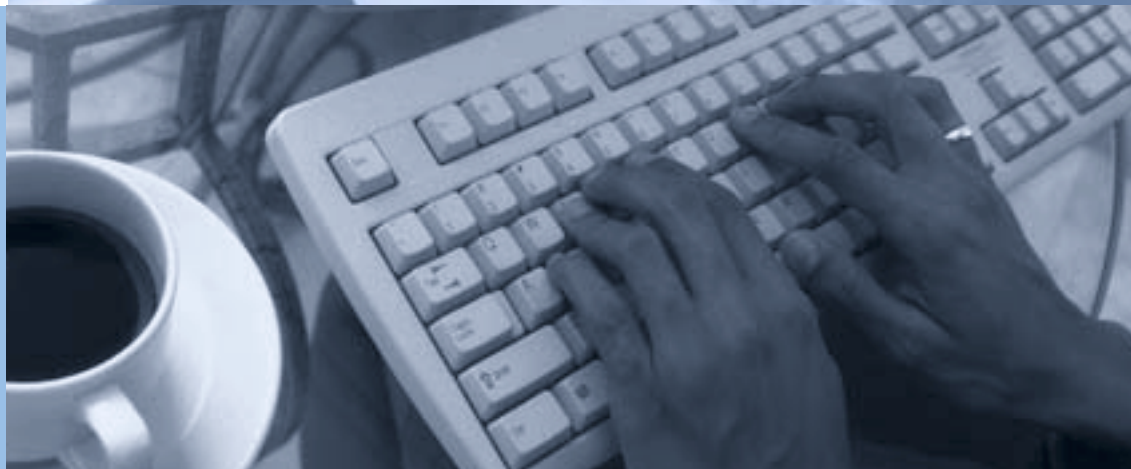


START

J.H.J. Terstegge

Goed werken in netwerken

Regels voor controle op
e-mail en internetgebruik
van werknemers



J.H.J. Terstegge

Regels voor controle op
e-mail en internetgebruik
van werknemers

Goed werken in netwerken

Tweede druk, herzien door drs. S. Lieon

Publicaties in de serie achtergrondstudies en verkenningen zijn het resultaat van onderzoeken uitgevoerd door of in opdracht van het College bescherming persoonsgegevens (CBP). Met het uitbrengen van deze publicaties beoogt het CBP de discussie en de meningsvorming te stimuleren over ontwikkelingen in de samenleving waarbij de persoonlijke levenssfeer van de burger in het geding is. In veel gevallen wordt in de publicaties het normatieve kader zoveel mogelijk praktisch uitgewerkt voor het onderwerp van de studie. Het CBP wil hiermee een handreiking geven voor het realiseren van de eigen verantwoordelijkheid die de wet een ieder geeft voor de bescherming van persoonsgegevens.

COLOFON

Goed werken in netwerken – Regels voor controle op e-mail en internetgebruik van werknemers. Tweede herziene druk.

ISBN 90 74087 30 2

COLLEGE BESCHERMING
PERSOONSGEGEVENS

Prins Clauslaan 20
Postbus 93374
2509 AJ Den Haag

TELEFOON 070 381 13 00

FAX 070 381 13 01

E-MAIL info@cbpweb.nl

INTERNET www.cbpweb.nl

College bescherming persoonsgegevens, Den Haag, april 2002.

Niets uit deze uitgave mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotocopie, microfilm of op welke wijze dan ook, zonder voorafgaande schriftelijke toestemming van het College bescherming persoonsgegevens.

Ontwerp: Proforma, strategie, ontwerp en management

Druk: Sdu Grafisch Bedrijf bv

Voorwoord

Het gebruik van e-mail en internet heeft binnen organisaties een grote vlucht genomen. Naast de evidente voordelen voor zowel werkgever als werknemer zoals productiviteit, bereikbaarheid en snelheid hebben ook de negatieve kanten van deze media zich gemanifesteerd. Werkgevers hebben derhalve behoefte om het voorheen vrijblijvende gebruik van e-mail en internet in goede banen te leiden. Daarvoor worden gedragscodes en gebruiksregels opgesteld, die ook middels controle worden gehandhaafd.

Elektronische controle van computergebruik roept vragen op met betrekking tot de bescherming van de persoonlijke levenssfeer van de werknemer. Een groot aantal werkgevers, ondernemingsraden en individuele werknemers heeft deze vragen in de afgelopen jaren voorgelegd aan de Registratiekamer. De Registratiekamer heeft daarom een studie verricht naar de controle op e-mail- en internetgebruik. Dit heeft geresulteerd in dit rapport *Goed werken in netwerken*.

Met voorbeelden en praktijkgevallen worden allereerst de feitelijke en juridische achtergronden van de problematiek geschetst. Daaruit vloeit een set vuistregels voort die de werkgever een handvat biedt om een behoorlijk en zorgvuldig beleid vast te stellen. Het mag voor zich spreken dat deze regels ook hun nut zullen hebben voor ondernemingsraden en individuele werknemers bij de beoordeling van het werkgeversbeleid en de consequenties daarvan voor hun privacy.

In deze herziene versie is het rapport *Goed werken in netwerken* aangepast aan de Wet bescherming persoonsgegevens die per 1 september 2001 van kracht is. In de nieuwe wet is het College bescherming persoonsgegevens (CBP) aangewezen als de opvolger van de Registratiekamer. Het rapport is tevens geactualiseerd aan de hand van recente jurisprudentie.

Om de toepasbaarheid van de vuistregels van dit rapport te vergroten heeft het CBP een raamregeling voor het gebruik van e-mail en internet ontwikkeld. Deze raamregeling is bedoeld als instrument waarmee organisaties de vuistregels kunnen vertalen naar het eigen beleid. De concrete invulling van het beleid inzake het gebruik van e-mail en internet is maatwerk en dient in overleg tussen werkgever en ondernemingsraad tot stand te komen.

mr. P.J. Hustinx
voorzitter College bescherming persoonsgegevens

Inhoud

Voorwoord

1 Inleiding 7

2 Controle door de werkgever

- 2.1 Toegang tot internet 11
- 2.2 Vormen van internet 11
- 2.3 Content-filtering 16
- 2.4 Telewerken 16
- 2.5 Conclusie 17

3 Juridisch kader

- 3.1 Grondrechtelijk kader 19
- 3.2 Strafrechtelijk kader 20
- 3.3 Arbeidsrechtelijk kader 21
- 3.4 Wet bescherming persoonsgegevens 22
- 3.5 Telecommunicatiewet 24
- 3.6 Uitspraken van de Registratiekamer 24
- 3.7 Uitspraken van de rechter 27

4 Vuistregels voor controle

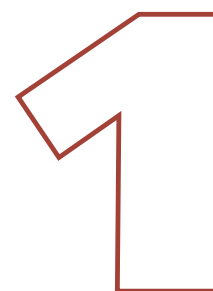
- 4.1 Online / off line 31
- 4.2 Ondernemingsraden 32
- 4.3 Publiceren regels 32
- 4.4 Privé-gebruik 32
- 4.5 Softwarematige oplossingen 32
- 4.6 Rapportages en gebruiksstatistieken 33
- 4.7 Back-up 33
- 4.8 Systeembeheerder 33
- 4.9 Bespreking met werknemer 33
- 4.10 Inzage 34
- 4.11 Evaluatie van regels 34
- 4.12 Zakelijke mail en privé-mail 34
- 4.13 Doeleinden en beperkingen 35
- 4.14 Maatwerk in controles 37
- 4.15 Logging en bewaartermijnen 38
- 4.16 Geprivilegieerde informatie 38

5 Samenvatting en overzicht vuistregels

6 Bijlagen

- 1 Deelnemers expertmeeting 45
- 2 Literatuur 46
- 3 Raamregeling 47
- 4 Achtergrondstudies en verkenningen 52

Inleiding



Gedurende de tweede helft van de jaren negentig is de elektronische snelweg een belangrijk communicatiemiddel geworden. E-mail is een snelle en doorgaans betrouwbare manier om iemand ergens van op de hoogte te stellen en op het World Wide Web (WWW) kan op een eenvoudige en snelle wijze informatie worden ontsloten die daarvoor moeilijk toegankelijk was. Ook binnen bedrijven heeft de elektronische snelweg opritten gekregen. Meer en meer werknemers hebben via de computer op hun bureau aansluiting op e-mail en internet. Veelal loopt deze aansluiting via het interne netwerk van de werkgever. Daarmee vervaagt ook het verschil tussen communicatie op het interne netwerk en via externe verbindingen. Bij het gebruik van een intranet binnen een organisatie kan er zelfs geen zichtbaar verschil meer tussen 'binnen' en 'buiten' zijn.

Deze nieuwe technologieën kennen ook schaduwzijden. Werknemers zijn van hun werktijd tegenwoordig een flink deel kwijt aan het maken, lezen en beantwoorden van e-mail en het zoeken naar relevante websites op het internet. Daarnaast worden e-mail en internet ook en soms vaak voor privé-doeleinden gebruikt. Even een nieuwtje laten weten aan je beste vriend(in), een geschikte vakantiebestemming zoeken, de laatste hits van je favoriete artiesten of de nieuwste drivers voor je computer thuis downloaden. De internettechniek maakt snelle en grenzeloze communicatie mogelijk.

Werkgevers ervaren privé-gebruik van de internetfaciliteiten als productiviteitsverlies en zijn bevreesd voor oneigenlijk gebruik van deze nieuwe middelen. Er zijn immers soms grote risico's aan verbonden. Zo kunnen virussen de computers beschadigen en zelfs hele computernetwerken lamleggen, liggen hackers op de loer en kunnen bedrijfsgeheimen uitlekken. Ook kan de goede naam van het bedrijf in diskrediet raken als een werknemer zich via een bedrijfsaccount inlaat met online gokken, (kinder)porno, discriminatie of inbreuken op auteursrechten. Aan de andere kant zijn juist door het gebruik van computers hiervoor, de controlemogelijkheden (achteraf of real-time) voor de werkgever groter dan het geval zou zijn als de werknemer hiervoor meer conventionele (off line) middelen zou gebruiken.

In de ogen van sommige werkgevers is er voor privacybescherming op het werk weinig of geen ruimte. Werknemers op hun beurt beschouwen controle door de werkgever als een inbreuk op hun persoonlijke levenssfeer. Controle op het gebruik van computersystemen is voor de werknemer immers onzichtbaar en is veelal continu aanwezig. Zij beroepen zich er op dat ook op de werkplek het recht op privacy geldt. Daarnaast beschouwen veel werknemers het privé-gebruik van bedrijfsfaciliteiten als een soort arbeidsvoorwaarde. Hier kan een vergelijking gemaakt worden met de telefoon of een auto van de zaak. In tegenstelling tot deze (bedrijfs)middelen bestaat er in veel bedrijven (nog) geen beleid voor het gebruik van e-mail- en internet voor privé-doeleinden. De verdergaande vervlechting tussen werk en privé (met name telewerken en mobiel werken) werkt het privé-gebruik van bedrijfsfaciliteiten in de hand en wordt daarvoor soms ook als rechtvaardiging gezien. De Kantonrechter Haarlem sprak in dat verband reeds van "privétisering van de werkplek" (zie paragraaf 3.8).

Dit rapport is bedoeld als handreiking voor werkgevers en werknemers bij de formulering van een bedrijfsbeleid voor de controle van e-mail- en internetgebruik door werkgevers op een manier die verantwoord is vanuit het oogpunt van privacybescherming. Het rapport geeft daarom een groot aantal vuistregels voor controle op e-mail en internetgebruik van werknemers. Het CBP heeft ook een raamregeling voor het gebruik van e-mail en internet ontwikkeld. Deze regeling is bedoeld als instrument voor organisaties, bedrijven en ondernemingsraden om de vuistregels in het eigen beleid toe te passen. De concrete

invulling van beleid voor e-mail en internetgebruik is maatwerk is en dient daarom in overleg tussen werkgever en ondernemingsraad tot stand te komen.

In hoofdstuk 2 zal eerst aan de hand van achtergronden en feiten de problematiek van e-mail en internet op de werkvloer worden belicht. Een aantal begrippen en verschijningsvormen van internet worden toegelicht. Vervolgens wordt in hoofdstuk 3 het juridisch kader geschetst waarbinnen controle mogelijk is. Zowel vanuit privacyrechtelijk als vanuit arbeidsrechtelijk perspectief zullen de grenzen worden aangegeven. In hoofdstuk 4 worden vuistregels geformuleerd aan de hand waarvan een zorgvuldig e-mail- en internetbeleid kan worden geformuleerd en getoetst. Deze vuistregels zijn in hoofdstuk 5 nog eens kort samengevat.

Controle door de werkgever



In dit hoofdstuk zal worden ingegaan op diverse begrippen uit de wereld van het internet. Om het gebruik van internet en de controle daarop te kunnen begrijpen, zullen eerst in het kort de diverse verschijningsvormen van internet worden beschreven. Daarbij wordt per vorm aangegeven welke risico's eraan kleven en op welke manier controle kan plaatsvinden.

Er is voor gekozen om alleen die vormen van internet aan de orde te stellen die op het moment van schrijven de belangrijkste toepassingen zijn van de internet-techniek. De regels die aan de orde komen, zijn uiteraard van overeenkomstige toepassing op oude toepassingen (bijvoorbeeld Telnet) en op zich aandienende toepassingen (Voice-over-IP, WAP).

Controle door de **2.1 Toegang tot internet**

Veel organisaties bieden hun werknemers e-mail- en internetfaciliteiten via het bedrijfsnetwerk. Een van de servers fungeert als schakel tussen het interne netwerk en het externe internet. Dit betekent dat al het dataverkeer tussen de PC van de werknemer en het internet de centrale server van de organisatie passeert. Het is voor de werkgever betrekkelijk eenvoudig om op de server controlesoftware te laten draaien of berichten te onderscheppen.

Het is ook mogelijk dat de werknemer toegang tot het internet verkrijgt via een stand-alone computer waarmee rechtstreeks bij een Internet Service Provider (ISP) wordt ingebeld. Bij deze vorm van toegang zit geen extra schakel waarop controlesoftware kan draaien. Eventuele controlemiddelen zullen in dat geval op de PC zelf moeten worden geïnstalleerd.

Om het opvragen van gegevens op internet te versnellen wordt gewerkt met proxyservers. Dat zijn servers waarop de webpagina's van veelbezochte websites worden opgeslagen. De gebruiker krijgt dus niet de echte pagina voorgeschoteld, maar de kopie zoals die zich op de proxyserver bevindt. Over het algemeen wordt surfen via een proxyserver als privacyvriendelijk beschouwd. De gebruiker hoeft immers niet echt het internet op zodat er geen informatie over hem wordt vrijgegeven. Controle van de werknemer is nog wel mogelijk maar minder noodzakelijk omdat binnen de organisatie reeds een selectie is gemaakt van sites die zijn toegestaan.

Op de scheiding tussen het interne netwerk en het externe internet wordt doorgaans een firewall geïnstalleerd. De firewall screent het inkomende (maar eventueel ook het uitgaande) dataverkeer op onder andere ongeautoriseerd gebruik. Op die manier kunnen bepaalde vormen van internetgebruik door werknemers worden tegengehouden. Zo kan een firewall het online spelen van spelletjes onmogelijk maken door de datapakketjes die daarvoor nodig zijn, niet te laten passeren.

Controle door de **2.2 Vormen van internet**

Internet kent vele verschijningsvormen. De bekendste en meest gebruikte daarvan zijn e-mail en het World Wide Web. Dit laatste is tegenwoordig voor velen zelfs synoniem voor internet. Toch zijn er ook andere vormen en er komen nog steeds nieuwe bij. Momenteel zijn de belangrijkste vormen: E-mail, World Wide Web (WWW), File Transfer (FTP), Usenet en Chat (IRC). Dit rapport beperkt zich dan ook tot die vormen.

Ondanks het feit dat de verschillende vormen ook verschillend gebruik mogelijk maken, is de controle ervan tot op zekere hoogte gelijk. De reden daarvoor is

dat controle in beginsel gebaseerd is op het TCP/IP-protocol waar alle vormen van internet gebruik van maken. Het TCP/IP-protocol zorgt voor de communicatie tussen de gebruiker en het internet. Omdat iedere computer een uniek IP-adres heeft, weet de server waar de datapakketjes vandaan komen of naar toe moeten. De gegevens die aan of door het IP-adres worden aangeboden, zijn in combinatie met de logging op de username te herleiden tot een bepaalde werknemer.

TCP/IP

Internet werkt op basis van het TCP/IP-protocol. TCP staat voor Transmission Control Protocol; IP staat voor Internet Protocol. Een bericht of bestand dat over internet wordt gestuurd, wordt in stukjes geknipt waarna ieder datapakketje door TCP/IP wordt voorzien van een code met daarin onder meer het afzendadres, het bestemmingsadres, en een volgnummer. Door deze code weet iedere computer die op de route ligt wat voor pakketje het betreft, waar het vandaan komt en waar het naar toe moet. Aan het eind worden de pakketjes weer keurig aan elkaar geplakt tot het oorspronkelijke bericht of bestand.

Computers die aan internet gekoppeld zijn, hebben ieder een uniek IP-nummer. Als een computer altijd hetzelfde IP-nummer heeft, spreken we van een vast IP-adres. Als een computer bij iedere verbinding met internet een ander IP-nummer krijgt, spreken we van een dynamisch IP-adres. Vaste IP-adressen komen vooral voor in interne netwerken binnen organisaties die ook op basis van het TCP/IP-protocol werken (intranet). Het is niet vereist dat het intranet ook aan internet gekoppeld is. Is dat wel het geval, dan moeten de gebruikte IP-nummers wereldwijd uniek zijn, omdat anders de communicatie met de buitenwereld niet goed kan verlopen. Een vast IP-adres is dus altijd herleidbaar tot één en dezelfde computer.

Dynamische IP-adressen worden vooral gebruikt bij inbelverbindingen via ISP's. Het zijn unieke adressen die niet permanent gekoppeld zijn aan een computer, maar per verbinding door de ISP worden toegekend aan de inbellende computer. Dynamische IP-adressen zijn dus niet herleidbaar tot een en dezelfde computer, maar kunnen in combinatie met de inbeltijd en het inbellende nummer wel achteraf tot een bepaalde computer worden herleid.

Naast TCP/IP is ook van belang welke vorm van internet door de werknemer wordt gebruikt. De applicatie waarmee hij dat doet, is niet zozeer van belang. Wel de protocollen waaraan de verschijningsvorm te herkennen is en aan de hand waarvan het verkeer door de server wordt afgehandeld. Een werkgever kan besluiten bepaalde protocollen niet door de server te laten afhandelen. Daarmee worden bepaalde vormen van internet onmogelijk. Op de verschillende vormen van internet zal hieronder worden ingegaan.

E-mail

E-mail is het versturen van een bericht door de afzender dat wordt geplaatst in de mailbox van de ontvanger. Voor het versturen wordt gebruik gemaakt van het SMTP-protocol (Simple Mail Transfer Protocol). Vervolgens wordt het bericht opgeslagen bij de ISP van de ontvanger totdat de ontvanger het bericht ophaalt. Het ophalen geschiedt via het POP-protocol (Post Office Protocol), waarbij het bericht in de mailbox op de server wordt bewaard totdat de gebruiker de post ophaalt en lokaal opslaat.

Een andere manier om de post op te halen is het gebruik van het IMAP-protocol (Internet Message Access Protocol). In dit laatste geval kan men kiezen of de

berichten aan de ontvanger worden overgedragen of dat de berichten op de server achterblijven.

(Webmail waarbij de post via het World Wide Web wordt opgehaald blijft hier verder buiten beschouwing). Worden deze protocollen geblokkeerd, dan is regulier e-mailverkeer onmogelijk.

Mailberichten zijn platte tekstbestanden die doorgaans met een eenvoudig mailprogramma gelezen kunnen worden. Om het lezen door onbevoegden te voorkomen kan de verzender het bericht versleutelen. In dat geval is alleen de header (het 'briefhoofd' met daarin de gegevens over de afzender, de bestemming en het onderwerp) nog voor derden leesbaar. Een mailbericht kan voorzien zijn van een attachment (een bijlage). Een attachment kan een bestand zijn in ieder willekeurig formaat. Bijlagen moeten door de ontvanger (tijdelijk) worden bewaard op zijn computer alvorens gelezen of gebruikt te worden.

Controle

Een e-mailbericht kan gecontroleerd worden op onder meer: afzender, ontvanger, onderwerp, datum, tijd en inhoud. De bijlagen kunnen worden gecontroleerd op extensie en inhoud. De controle kan onder meer geschieden door content-filtering (zie hierna 2.3) en door het maken van kopieën.

Risico's

Zowel de inhoud van de berichten als de bijlagen kunnen 'verboden' materiaal, virussen en dergelijke bevatten. Deze kunnen de belangen van de werkgever schaden. Het versturen van e-mail brengt voor de werknemer echter het risico met zich mee dat de berichten kunnen worden gekopieerd of worden gelezen alvorens hij het bericht ontvangt of het bericht daadwerkelijk wordt verstuurd. Dit kan zijn privacy maar ook zijn vrijheid van meningsuiting schaden.

World Wide Web

Het World Wide Web (WWW) is momenteel de meest bekende verschijningsvorm van internet. Op het WWW staan websites met webpagina's. Het WWW werkt op basis van het HTTP-protocol. HTTP staat voor Hypertext Transfer Protocol. Websites zijn via een browser toegankelijk door het gebruik van unieke adressen (URL's, Uniform Resource Locator). Binnen de pagina kan de gebruiker via hyperlinks doorklikken naar andere pagina's of websites. Hyperlinks kunnen zich voordoen als woorden in de tekst of (gedeelten van) plaatjes.

Controle

Het bezoek van websites kan worden gecontroleerd op onder meer datum, tijd, duur en inhoud. Ook de bestanden die worden gedownload, kunnen worden gecontroleerd. Behalve het loggen van de verkeersgegevens, is controle mogelijk door het loggen van de adressen van websites of het opslaan van (de onderdelen van) de webpagina's. Onder logging wordt verstaan het bijhouden van gegevens over het gebruik van (computer)systemen en/of programma's. Sommige controlemiddelen geven de werkgever de mogelijkheid om websites af te sluiten of - juist omgekeerd - om alleen het bezoek aan bepaalde websites toe te staan.

Risico's

De inhoud van websites is niet altijd van tevoren even duidelijk. Een werknemer kan tijdens het surfen makkelijk verdwalen en via 'onschuldige' hyperlinks terecht komen op een site waarvan de inhoud door de werkgever als onwenselijk wordt beschouwd (hierna: een 'verboden' site). Dit geldt ook voor de adressen van websites. Als een werknemer op goed geluk het adres van een organisatie intikt, loopt hij het risico om op een verboden site te komen. Dubieuze sites maken nogal eens gebruik van het feit dat iemand (tik)fouten maakt bij het intikken van de naam van een website. Zo is www.whitehouse.gov de website van het Witte Huis in Washington, maar verwijst www.whitehouse.com naar een sekssite.

Een ander punt dat de aandacht verdient, is het feit dat de onderdelen van een webpagina niet allemaal van hetzelfde webadres hoeven te komen. Zo kan de gevraagde pagina komen van website A, terwijl de plaatjes binnen die pagina komen van website B. Als alle onderdelen zijn opgehaald, stelt de browser de pagina samen en geeft die weer. Een bezoeker van een website kan dus ongewild bestanden ophalen van een verboden site. Hij heeft daar in principe geen controle over. Een bekend voorbeeld hiervan is het plaatsen van een zogeheten banner, een reclameplaatje voor een doorgaans commerciële website waarop de gebruiker kan klikken om te worden doorgeschakeld naar die site. Ook kan ongemerkt informatie worden opgehaald via zogeheten meta-informatie, informatie die niet visueel wordt weergegeven door de browser. Dit geschiedt bijvoorbeeld bij het plaatsen van cookies door websites voor andere websites dan de website die door de gebruiker wordt bezocht.

Controle op de herkomst van informatie kan leiden tot de onterechte conclusie dat een medewerker zich niet aan de afspraken heeft gehouden.

FTP

FTP staat voor File Transfer Protocol en is met name bedoeld om (grote) bestanden over een netwerk te transporteren. Het is vergelijkbaar met het verplaatsen van bestanden binnen een computer van de ene naar de andere directory. Bij FTP maakt de computer van de gebruiker verbinding met een FTP-server. Bestanden kunnen nu over en weer worden uitgewisseld (zogenaamd uploaden en downloaden). Vaak is voor het uploaden een username en een password vereist. Het wordt dan ook bij voorkeur gebruikt bij het onderhoud van websites. Downloaden is vaak voor iedereen mogelijk. Voor FTP zijn aparte programma's nodig, hoewel alle webbrowsers bestanden van FTP-servers kunnen downloaden.

Controle

Bestanden die via FTP worden uitgewisseld kunnen onder meer worden gecontroleerd op datum, tijd en duur.

Risico's

Middels FTP kunnen op een snelle wijze gevaarlijke of verboden bestanden worden uitgewisseld. Als de bestanden middels encryptie zijn beveiligd, kan de inhoud van de bestanden niet gecontroleerd worden.

Usenet

Usenet is een vorm van internet die bestaat uit zogeheten nieuwsgroepen. Er zijn duizenden nieuwsgroepen waarin mensen berichten uitwisselen over uiteenlopende onderwerpen. Aan de naam van de nieuwsgroep kan doorgaans goed worden afgeleid waar hij over gaat. Zo gaat alt.privacy over problemen op

het gebied van privacy en kunnen mensen voor informatie over kanker terecht in alt.support.cancer.

De meeste nieuwsgroepen zijn openbaar en dus voor iedereen toegankelijk. Om het zoeken nog eenvoudiger te maken, werkt Usenet met een hiërarchische structuur, dat wil zeggen dat elke nieuwsgroep in een cluster van soortgelijke nieuwsgroepen zit.

Een bericht aan een nieuwsgroep is het best te omschrijven als "een e-mail aan de rest van de wereld". Het kan dan ook niet alleen vanuit nieuwsgroepenlezers, maar ook vanuit mailprogramma's verstuurd worden. Als iemand het bericht leest, kan hij erop reageren door een bericht terug te sturen naar de afzender en/of naar de nieuwsgroep zelf. Ook berichten in nieuwsgroepen kunnen attachments bevatten van allerlei soort. Vanwege de grote hoeveelheid berichten die dagelijks verstuurd worden, worden de berichten in nieuwsgroepen doorgaans slechts enkele dagen bewaard. Bedrijven zoals DejaNews verzamelen alle berichten en bewaren ze gedurende een veel langere tijd. De database kan door iedereen worden geraadpleegd.

Controle

Het versturen van berichten aan nieuwsgroepen kan op dezelfde wijze worden gecontroleerd als het versturen van e-mail. Het lezen van nieuwsgroepen kan worden gecontroleerd op onder meer datum, tijd en inhoud. De werkgever kan ook relatief eenvoudig nieuwsgroepen afsluiten voor werknemers.

Risico's

Via Usenet heeft een werknemer gemakkelijk toegang tot berichten met een 'verboden' of gevaarlijke inhoud of bijlage. Deze berichten zijn niet altijd vooraf als zodanig herkenbaar. Omdat de meeste nieuwsgroepen niet worden beheerd, komt het nogal eens voor dat nieuwsgroepen berichten bevatten die niets met het onderwerp van de nieuwsgroep te maken hebben. Het lezen van deze berichten kan dan ook ongewild leiden tot een overtreding van het bedrijfsbeleid.

Controle op het lezen van nieuwsgroepen kan leiden tot inbreuken op de privacy en de informatievrijheid van de werknemer. Zo kan vaak uit de naam van de bezochte nieuwsgroepen informatie worden verkregen over de interesses van de werknemer.

Voor de werkgever kunnen nieuwsgroepen ook een risico vormen. Door het open karakter van Usenet kan een werknemer relatief eenvoudig schade toebrengen aan de goede naam van de organisatie door 'verboden' informatie te verspreiden met gebruikmaking van het zakelijke e-mailadres. Dit wordt immers vermeld bij het bericht.

Chat

Met een chat-programma kan de gebruiker contact maken met andere internetgebruikers en in groepen of apart real-time informatie uitwisselen. Ook kunnen deelnemers binnen deze babbelboxen bestanden met elkaar uitwisselen. Veel werkgevers staan niet toe dat werknemers chatten omdat dit doorgaans gepaard gaat met een aanzienlijk tijdsbeslag. Chatsessies kunnen eenvoudig worden geblokkeerd. Er hoeft dan ook geen controle plaats te vinden op de inhoud.

Controle door de werkgever **2.3 Content-filtering**

Het is betrekkelijk eenvoudig om de datapakketjes die de server passeren, te screenen op inhoud (content-filtering). Dit houdt in dat geautomatiseerd gekeken wordt of bestanden woorden of teksten bevatten die door de werkgever verboden zijn. Ook kan worden gekeken of de extensie is toegestaan (extensies voor plaatjes zoals *.jpg, *.gif of *.bmp, voor filmpjes zoals *.mpg, *.mov of *.avi, voor programma's zoals *.exe of voor ingepakte bestanden zoals *.zip of *.arj). Indien bestanden worden gevonden die voldoen aan de zoektermen zal door het systeem 'alarm' geslagen worden. De bestanden kunnen worden tegengehouden, teruggestuurd, apart gezet, gekopieerd, gelogd, etc.

Content-filtering kan de communicatievrijheid en de persoonlijke levenssfeer van de gebruiker aantasten. Voor het gebruik zal de werkgever een gerechtvaardigd belang moeten hebben. Ook zal het gebruik ervan moeten voldoen aan de eisen van proportionaliteit en subsidiariteit. Dit betekent dat onder meer zal moeten worden bezien in hoeverre content-filtering noodzakelijk is, welke zoektermen worden gebruikt, welke actie wordt ondernomen nadat een 'hit' is gevonden, en welke procedures er bestaan om gerechtvaardigd gebruik van aangewezen zoektermen mogelijk te maken. Zo zal een zoekvraag naar 'breasts' of 'borsten' doorgaans leiden tot een alarm, maar zal iemand wel een zoekvraag of 'breastcancer' of 'borstkanker' moeten kunnen stellen. Een zoekterm in het systeem naar 'breast' of 'borst' zal voor beide alarm slaan. In het laatste geval zullen werknemers die op internet zoeken naar informatie over borstkanker, mogelijk in hun privacy worden geschaad.

Content-filtering kan dus alleen worden ingezet als de zoektermen vanuit het belang van de werkgever gerechtvaardigd zijn en ook zo nauwkeurig zijn dat gerechtvaardigd gebruik zoveel mogelijk ongemoeid wordt gelaten. Mits het met de nodige zorgvuldigheid wordt ingezet, zal content-filtering als controle-middel in mindere mate inbreuk maken op de privacy en de communicatievrijheid van de gebruiker dan andere vormen van controle, zoals volledige inhoudscontrole of steekproefsgewijze inhoudscontrole.

Met behulp van content-filtering zal verboden gebruik waarbij berichten worden opgesteld in codetaal of met versleuteling, niet kunnen worden opgespoord.

Controle door de werkgever **2.4 Telewerken**

De controle door de werkgever van het computergebruik van de werknemer vormt in situaties waarin de werknemer vanuit zijn eigen huis inlogt op het computersysteem van het werk (telewerken) een extra probleem. Voor zover de werknemer uitsluitend ten behoeve van het werk inlogt, zullen de regels in dit rapport van overeenkomstige toepassing zijn. De computer van de werknemer thuis maakt dan immers logisch gezien deel uit van het computernetwerk en de werknemer bevindt zich in een situatie waarin ook de gezagsbevoegdheid van de werkgever geldt.

Dit is anders als de werknemer het bedrijfsaccount kan en mag gebruiken om privé e-mail te versturen of in zijn eigen tijd over het internet te surfen. Voor logging van hetgeen hij privé doet, is geen grond. Dit geldt zeker indien ook zijn gezinsleden van de faciliteiten gebruik mogen maken. Met hen heeft de werkgever immers geen arbeidsrelatie waarin hij zijn gezag kan uitoefenen. Zijn positie is in deze vergelijkbaar met een ISP. De werkgever dient hiermee

rekening te houden bij het opzetten en de uitvoering van het telewerkbeleid. (Voor meer informatie over de relatie tussen een gebruiker en Internetprovider zie, M.J.T. Artz en M.M.M. van Eijk, *Klant in het web*, Registratiekamer, Den Haag 2000).

Controle door de werkggever **2.5 Conclusie**

Internet kent een grote verscheidenheid aan verschijningsvormen. Deze maken echter allemaal gebruik van het TCP/IP-protocol waardoor controle op het gebruik relatief eenvoudig is te realiseren. De werkgever kan het gebruik van bepaalde vormen van internet onmogelijk maken door datapakketjes met vormspecifieke protocollen op de server tegen te houden. Verder is controle tot in ieder detail mogelijk. Van ieder gebruik kan de datum, de tijd en vaak ook de inhoud worden gecontroleerd.

Internetgebruik leidt per verschijningsvorm tot andere risico's voor de werkgever en de werknemer. Voor de werkgever kan het gaan om de beveiliging van het netwerk, het tegengaan van 'verboden gebruik' of het beschermen van andere bedrijfsbelangen zoals bedrijfsgeheimen of de goede naam van de organisatie. Voor de werknemer staat vaak het privacybelang door de controle onder druk, maar ook de vrijheid van meningsuiting of de informatievrijheid kan in het geding zijn. De werkgever dient zich hiervan bewust te zijn, als hij overgaat tot controle van e-mail- en internetgebruik van zijn werknemers.

Juridisch kader

3

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 handelvrijheid 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. Dit geldt ook voor de controle van het e-mail- en internetgebruik van werknemers.

Juridisch kader **3.1 Grondrechtelijk kader**

Artikel 8 van het Europese verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM) bepaalt dat een ieder recht heeft op respect voor zijn privé-leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. De verzamelterm voor deze niet duidelijk te scheiden rechten is het 'recht op privacy'.

Het Europese hof van de Rechten van de Mens (EHRM) oordeelde in de zaak Niemietz – Duitsland dat activiteiten op de werkplek onder de bescherming van artikel 8 EVRM vallen (EHRM 16 december 1992, NJ 1993, 400 Niemietz). Werknemers hebben een gerechtvaardigd belang om ook gedurende het uitvoeren van bedrijfsmatige activiteiten relaties met andere mensen aan te kunnen gaan. Een zekere mate van vrijheid om met anderen al dan niet persoonlijk te kunnen communiceren zonder inmenging door de werkgever is in dat kader onontbeerlijk. Hieruit kan het uitgangspunt gedestilleerd worden dat een werknemer het recht heeft in beperkte mate gebruik te maken van communicatiefaciliteiten op de werkplek voor privé-communicatie.

Artikel 8 EVRM beschermt het individu niet alleen tegen inbreuken op dergelijke privacyaanspraken door de overheid maar ook wanneer deze afkomstig zijn van particulieren, zoals werkgevers. Bovendien zijn de verdragsstaten verplicht om het recht op privacy zo goed mogelijk te waarborgen in hun wetgeving, rechtspraak en bestuur.

In Nederland ligt het brief-, telefoon- en telegraafgeheim vast in de Grondwet (artikel 13). Deze bescherming van de communicatievrijheid kan gezien worden als een onderdeel van het meer omvattender recht op eerbiediging van de persoonlijke levenssfeer (artikel 10 Grondwet). De komst van e-mail heeft geleid tot de vraag of deze ook onder de reikwijdte van artikel 13 van de Grondwet valt; met name het briefgeheim. Aanvankelijk beschouwde het kabinet e-mail als een soort briefkaart met een daarbij passend laag beschermingsniveau. In het vervolg van de voorstellen van de Commissie Grondrechten in het digitale tijdperk is het Kabinet in 2001 met voorstellen gekomen om de grondrechten aan te passen (Kamerstukken II, 2000-2001, 27 460). Het voorstel is het brief-, telefoon- en telegraafgeheim te vervangen door een recht op vertrouwelijke communicatie, waaronder ook vertrouwelijke communicatie via e-mail, SMS en fax. Nadat de wetsvoorstellen zijn behandeld door de Raad van State, zullen zij vervolgens bij de Tweede Kamer ingediend worden.

Het communicatiegeheim betreft met name de inhoud van de boodschap. Uitgangspunt hierbij is dat de deelnemers anderen (de overheid of derden)

in beginsel niet tot hun communicatie hoeven toe te laten en gevrijwaard zijn van inbreuken hierop. Controle van e-mail raakt vooral de vrijheid om met anderen te communiceren. Van het vastleggen van uiterlijke kenmerken van het communicatieverkeer gaat eveneens een 'chilling effect' uit voor de communicatievrijheid. Het vastleggen van gegevens die inzicht bieden in de activiteiten van de werknemer, raakt niet alleen diens persoonlijke levenssfeer maar ook de arbeidsverhouding in het algemeen; het kan in zekere zin de handelingsvrijheid van de werknemer beperken om de werkzaamheden naar eigen inzicht uit te voeren (autonomie). Het inperken van dergelijke vrijheden door de werkgever behoeft een rechtvaardigingsgrond terwijl tevens zo terughoudend mogelijk te werk moet worden gegaan (de zogeheten 'eisen van proportionaliteit en subsidiariteit').

Uit de jurisprudentie op artikel 8 EVRM is eveneens duidelijk dat de inbreuk kenbaar moet zijn voor de betrokkene. Heimelijke controle waaraan geen waarschuwing aan vooraf is gegaan of als uitvoering van een geldende gedragscode is in strijd met deze regels.

Het enkele bekend zijn van de mogelijkheid tot meeluisteren of opnemen rechtvaardigt het gebruik daarvan evenwel niet. Een geval uit de Europese jurisprudentie kan dit verduidelijken (EHRM 25 juni 1997, NJ 1998, 506 Halford). Mevrouw Halford was Assistant Chief Constable bij een Engels politiekorps. In verband met een rechtszaak tegen haar werkgever wegens ongelijke behandeling had zij de beschikking over een tweede telefoon die was uitgezonderd van de standaard controle van de telefoons van het politiebureau. Uit het bewijs dat in de rechtszaak was overlegd, kon worden afgeleid dat de werkgever de gesprekken die via de speciale telefoon waren gevoerd, waarschijnlijk had afgeluisterd. Het Hof overwoog dat 'the right to private life and correspondence' zich ook uitstrekt tot de werkplek. Omdat er geen waarschuwing was gegeven dat de telefoongesprekken werden opgenomen, had zij een 'reasonable expectation of privacy', hetgeen werd versterkt door bijkomende factoren waaronder het feit dat de telefoon specifiek ter beschikking was gesteld voor privé-gebruik.

Een werknemer heeft op zijn werkplek recht op de bescherming van zijn privacy – zo kan uit dit oordeel van de rechter worden afgeleid - en hij mag uit de omstandigheden afleiden dat dit recht in redelijke mate wordt beschermd. Kenbaarheid van de (mogelijkheid tot) controle is een basisvoorwaarde voor de rechtmatigheid ervan. Bijkomende factoren kunnen de controle echter alsnog onrechtmatig maken.

Juridisch kader **3.2 Strafrechtelijk kader**

De bescherming van de privacy en van het communicatiegeheim bij het gebruik van computers is uitgewerkt in het Wetboek van Strafrecht (artikel 138a: computervredebreuk; artikel 139b: aftappen / opnemen van gegevensoverdracht; artikel 139c: aftappen / opnemen van gegevensoverdracht via telecommunicatienetwerk; artikel 350a: ontoegankelijk maken computergegevens). Wanneer de controle op het gebruik van e-mail en internet geschiedt in opdracht van de werkgever die tevens de verantwoordelijke is voor zijn gedeelte van het telecommunicatienetwerk, zal van strafbaarheid geen sprake zijn, behalve natuurlijk in geval van misbruik. Ook als de controle niet strafbaar is, kan deze nog wel onrechtmatig zijn jegens de betreffende werknemers. Dat is het geval indien de werkgever niet handelt zoals een goed werkgever betaamt.

Juridisch kader 3.3 Arbeidsrechtelijk kader

Burgerlijk wetboek (BW)

De werkgever is gerechtigd tot het geven van voorschriften voor het verrichten van de arbeid en het nemen van maatregelen ter bevordering van de goede orde in de onderneming (artikel 7:660 BW). Regels voor het gebruik van e-mail en internet en de maatregelen voor de controle daarop vallen onder deze bepaling.

Een werkgever en een werknemer dienen zich ten opzichte van elkaar te gedragen als een goed werkgever en een goed werknemer (artikel 7:611 BW). Dit impliceert dat ook als er geen sprake is van een strafbaar feit, de controle toch onrechtmatig kan zijn. Dat is het geval als de werkgever niet handelt zoals het een goed werkgever betaamt. Hiervan is met name sprake als zonder noodzaak of gerechtvaardigd belang dan wel met onevenredige middelen inbreuk wordt gemaakt op de persoonlijke levenssfeer van werknemers. Hiervan is ook sprake als niet voldoende zorgvuldigheid wordt betracht bij het beoordelen van individuele werknemers op basis van de aldus verkregen gegevens. Bij dat laatste geldt als uitgangspunt, dat een werknemer zich moet kunnen verdedigen indien er bezwaren rijzen tegen zijn functioneren. Hiervoor is essentieel dat hij weet op grond van welke feiten en omstandigheden hij wordt beoordeeld.

Werknemers dienen zich als een goed werknemer te gedragen. Dit betekent onder andere dat redelijke gedragsregels ten aanzien van het gebruik van e-mail en internet behoren te worden nageleefd.

Arbeidsomstandighedenwetgeving

Het gebruik van controlemiddelen voor computers wordt arbeidsrechtelijk uitsluitend expliciet genormeerd in het Besluit beeldschermwerk dat thans integraal is opgenomen in de artikelen 5.1 tot 5.3 van de Arbeidsomstandighedenregeling. De bepalingen zijn een uitvoering van een Europese richtlijn voor arbeidsomstandigheden (90/270/EEG, 29 mei 1990, vijfde bijzondere Richtlijn). De regeling bepaalt dat zonder medeweten van de werknemer geen gebruik mag worden gemaakt van een kwalitatief of kwantitatief controlemechanisme. Voorts moet het systeem de werknemer duidelijkheid verschaffen over de werking ervan.

Wet op de ondernemingsraden (WOR)

Met betrekking tot de verwerking van persoonsgegevens en het gebruik van personeelsvolgsystemen heeft de ondernemingsraad het recht van instemming (artikel 27, lid 1, onder k en l). Onder personeelsvolgsysteem verstaat de wet "voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag of prestaties van de in de onderneming werkzame personen; en en ander voor zover betrekking hebbende op alle of een groep van de in de onderneming werkzame personen." De controle op e-mail en internet is derhalve een personeelsvolgsysteem waarover de ondernemingsraad instemmingsrecht heeft. De instemming van de ondernemingsraad bindt echter de individuele werknemers niet.

Aparte aandacht verdient de communicatie per e-mail van leden van de ondernemingsraad ten behoeve van hun OR-werkzaamheden. Op grond van artikel 17 WOR hebben zij het recht om onderling te overleggen met gebruik van voorzieningen waarover het OR-lid als zodanig kan beschikken. De wetsgeschiedenis van artikel 17 WOR maakt duidelijk dat tussen de OR en de werkgever geen gezagsrelatie bestaat. Derhalve kan de werkgever zijn gezagsbevoegdheid niet aanwenden om het e-mailgebruik van OR-leden in functie te controleren. Dit betekent dat op e-mail van, aan en tussen OR-leden in functie de algemene wettelijke regels omtrent vertrouwelijke communicatie van toepassing zijn. Daarmee is dit soort e-mail geprivilegieerd en mag de werkgever er in beginsel geen kennis van nemen.

Juridisch kader **3.4 Wet bescherming persoonsgegevens**

Persoonsgegevens

De WBP is van toepassing als er sprake is van verwerking van persoonsgegevens (artikel 2, onder a). Gegevens met betrekking tot het e-mail- en internetgebruik van werknemers zijn in het algemeen te kwalificeren als persoonsgegevens. IP-adressen zijn in combinatie met de username en het password te herleiden tot een bepaalde gebruiker. De daaraan verbonden bestanden zijn aldus herleidbaar tot een werknemer. De verkeersgegevens geven inzicht in de afzender, de bestemming, de datum en de tijd van het bericht of van het internetgebruik. Ook de inhoud van het e-mailbericht is een persoonsgegeven als de werkgever dit tot zijn beschikking heeft om bijvoorbeeld te controleren of een werknemer de gebruiksafspraken nakomt.

Verwerking

De WBP hanteert een ruime definitie voor het begrip 'verwerking' (artikel 1, onder b). Het gehele proces van verzamelen tot aan vernietigen van gegevens valt onder het begrip. Bij het proces van e-mail en internetgebruik is voortdurend sprake van het vastleggen van gegevens in servers op de route tussen de gebruiker en de bestemming. Van belang is of de werkgever invloed kan uitoefenen op de vastleggingen. Alleen als het vastleggen een definitief karakter heeft en niet slechts voor de duur van de verbinding, zodat ook de mogelijkheid van raadplegen (achteraf) bestaat, zal kunnen worden gesproken van verwerking van gegevens en is de WBP mogelijk van toepassing.

Verantwoordelijke

Verantwoordelijke voor de verwerking van persoonsgegevens is degene die het doel en de middelen van de verwerking vaststelt (artikel 1, onder d). Of de werkgever in de zin van de WBP ook verantwoordelijke is voor de verwerking van de gegevens, hangt onder meer af van de vraag wie de faciliteiten aanbiedt en beheert. Een werkgever die zelf een e-mail- en/of internetserver beheert, zal verantwoordelijke zijn voor de verwerkingen van gegevens op die server. Indien het e-mail- en internetverkeer echter geheel verloopt via het telefonisch inbellen bij een ISP, zal de werkgever niet snel als verantwoordelijke kunnen worden gekwalificeerd, omdat de ISP zelf het doel en de middelen vaststelt. Dit is alleen anders voor eventuele logbestanden op de computer van de werknemer zelf.

Indien de werkgever het aanbieden van de computerfaciliteiten heeft uitbesteed aan een derde ('outsourcing'), kan sprake zijn van een 'bewerker'; de derde is dan niet zelfstandig verantwoordelijk voor de gegevensverwerkingen, maar het is de werkgever die jegens de werknemer als verantwoordelijke moet worden aangemerkt. Daarnaast kan het voorkomen dat de bewerker dermate veel invloed heeft op het proces, dat wellicht moet worden gesproken van (mede)verantwoordelijkheid.

Verzamelen/verwerken

De WBP bepaalt dat gegevens in overeenstemming met de wet en op een behoorlijke en zorgvuldige wijze moeten worden verwerkt (artikel 6). In zoverre geldt dit voorschrift als de privacyrechtelijke evenknie van de arbeidsrechtelijke norm van het goed werkgeverschap. Voorts mogen de gegevens alleen worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden (artikel 7). Controle via volgsystemen is dus alleen toegestaan als het doel van de controle vooraf is bepaald.

Als grondslag van de controle kan doorgaans worden aangewezen het gerecht-

vaardigd belang van de werkgever (artikel 8 onder f). Hierbij geldt wel dat hij een aantoonbare belangenafweging moet maken tussen zijn belangen en de (privacy)belangen van de werknemers. De aard, omvang en de vorm van de controlemaatregelen dienen derhalve in een redelijke verhouding te staan tot het doel van de controle.

Ten slotte is niet onbelangrijk dat de WBP voorschrijft dat gegevens niet bovenmatig mogen zijn (artikel 11, eerste lid). De controlemaatregelen dienen dus beperkt te zijn en gegevens niet onnodig vast te leggen. Indien het doel de vastlegging van gegevens op persoonsniveau niet vereist, moet worden volstaan met geaggregeerde of geanonimiseerde gegevens.

Gebruik

Een andere vraag is waarvoor de gegevens die door middel van de controle zijn verzameld, mogen worden gebruikt. Deze doelen mogen niet onverenigbaar zijn met het doel waarvoor de gegevens zijn verkregen. Dit betekent dat algemene personeelsbeoordeling alleen kan plaatsvinden als dit als doelstelling voor het systeem is geformuleerd of als dit verenigbaar is met de primaire doelstelling. Dit ligt anders bij incidenteel gebruik van de gegevens wegens verdenking van overtreding van de regels. In dat geval zal een werkgever er toe over mogen gaan om de gegevens voor zijn onderzoek te gebruiken als dat noodzakelijk is voor voorkoming, opsporing of vervolging van strafbare feiten binnen de organisatie (artikel 43). Daarbij dient hij wel zorgvuldig te werk te gaan en de controlemiddelen naar evenredigheid in te zetten.

Rechten en plichten

De werkgever is verplicht om de werknemers inlichtingen te verschaffen over het doel van de controlemiddelen, de manier waarop de gegevens worden verkregen en het gebruik dat ervan wordt gemaakt. Transparantie is een belangrijk beginsel voor privacybescherming. De informatieplicht is – afhankelijk van de situatie – gebaseerd op de artikelen 33 en 34 WBP. De verplichting vloeit ook voort uit de Arbowetgeving. Het enkele overleg met de ondernemingsraad is in dit kader onvoldoende. De werknemers moeten individueel worden voorgelicht. In geval van e-mail- en internetcontrole is het moment van inloggen hiervoor het aangewezen tijdstip.

De werknemer heeft het recht op inzage in de gegevens (artikel 35). Hij kan verder de werkgever verzoeken de gegevens aan te vullen, te verbeteren, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift worden verwerkt (artikel 36). Tenslotte kan de werknemer tegen de verwerking van zijn persoonsgegevens verzet aantekenen in verband met zijn bijzondere persoonlijke omstandigheden (artikel 40).

Melden of niet?

Een verantwoordelijke is verplicht om de verwerking van persoonsgegevens te melden bij het College Bescherming Persoonsgegevens (CBP) voor hij begint met de verwerking. De melding geeft inzicht in de doeleinden van de verwerking, de personen van wie de gegevens worden verwerkt, de soorten gegevens, de ontvangers en de beveiliging van de gegevens.

Veel voorkomende verwerkingen waarvan de inbreuk op de persoonlijke levenssfeer onwaarschijnlijk is, zijn door het Vrijstellingsbesluit van de meldingsverplichting vrijgesteld. Het Vrijstellingsbesluit bevat een aantal vrijstellingen voor het verwerken van persoonsgegevens in verband met het gebruik van computers en computernetwerken. Deze vrijstellingen gelden met name voor de

normale systeemcontrole (performance), controle op autorisaties en de (externe) beveiliging van het systeem tegen virussen en dergelijke. In de definitieve tekst van het Vrijstellingsbesluit valt controle op het gebruik van e-mail en internet ook onder de vrijstelling en hoeft, mits voldaan aan de vereisten van het vrijstellingsbesluit (waaronder de instemming van de ondernemingsraad), niet te worden gemeld.

Een nieuw element in de WBP is dat het CBP een onderzoek moet instellen voorafgaand aan een verwerking, indien de verantwoordelijke voornemens is gegevens vast te leggen op grond van eigen waarneming zonder de betrokken daarvan op de hoogte te stellen (artikel 31, lid 1 onder b, WBP). Bij de melding dient de verantwoordelijke dit aan te geven (artikel 32, lid 1 WBP). Voor de verantwoordelijke in organisatie of bedrijf betekent dit dat de vrijstelling van de melding voor het systeem van controle van werknemers vervalt als hiermee ook heimelijk gegevens van personen vast worden gelegd. De verplichting tot melding aan het CBP met het oog op het instellen van een voorgaand onderzoek is niet van toepassing op een bedrijf of organisatie waarin de controle van het personeel op een transparante manier gebeurt. Hiervan is in elk geval sprake, indien de vuistregels uit dit rapport in acht zijn genomen. Het feit dat een bepaalde wijze van controleren door middel van heimelijk monitoring plaats vindt, is dus op zich geen reden tot melding indien deze wijze van controleren kenbaar is gemaakt in het bedrijf of de organisatie en de ondernemingsraad hiermee heeft ingestemd.

Meer informatie over het Vrijstellingsbesluit en de meldingen is te vinden op de internetsite van het CBP (zie www.cbpweb.nl).

Juridisch kader **3.5 Telecommunicatiewet**

Hoewel het aanbieden van e-mail- en internetvoorzieningen via eigen servers wel onder het begrip telecommunicatie valt, is de telecommunicatiewet niet van toepassing op werkgevers die hun werknemers deze diensten aanbieden. Alleen als de diensten ook beschikbaar zijn voor het publiek, ligt dit anders.

Juridisch kader **3.6 Uitspraken van de Registratiekamer**

Ook de Registratiekamer, de voorganger van het CBP, heeft enkele malen uitspraken gedaan over controle op e-mail en internetgebruik. De uitspraken zijn gebaseerd op de Wet persoonsregistraties (WPR), de voorloper van de WBP.

In een zaak van de gemeente Zwolle was de beveiliging van het e-mailsysteem uitgevallen. Daardoor kon e-mail die als 'privé' gelabeld was en onder normale omstandigheden niet leesbaar was voor derden, door anderen worden geopend. De gemeente stond een bescheiden privé-gebruik toe. Uit de inhoud van deze mail bleek dat er kwetsende opmerkingen werden gemaakt over enkele medewerkers. Dit werd gemeld aan het management, dat daarop besloot tot een onderzoek naar alle berichten.

De Registratiekamer oordeelde dat de gemeente Zwolle door het laten vervallen van de beveiligingen waardoor door derden kennis kon worden genomen van de berichten, in strijd had gehandeld met artikel 8 WPR (beveiligingsplicht). Het onderzoek naar alle berichten was naar het oordeel van de Registratiekamer in strijd met artikel 6, eerste lid, WPR (verenigbaar gebruik).

"De zorg van een goed werkgever brengt met zich mee dat de vertrouwelijkheid van berichten met een meer persoonlijke, niet zakelijke inhoud wordt gerespecteerd. Dit betekent dat de gemeente alleen gebruik mag maken van niet voor

zakelijke doeleinden bewaarde elektronische berichten, indien een gewichtig bedrijfsbelang daartoe zou dwingen en voor zover dat gebruik in juiste verhouding staat tot het nagestreefde doel terwijl dit doel niet op een minder ingrijpende wijze kan worden bereikt. De mogelijke aanwezigheid van berichten met een onoirbare inhoud is op zichzelf geen voldoende rechtvaardiging voor een inbreuk op artikel 8 EVRM, door de in de folders opgeslagen berichten aan een inhoudelijk onderzoek te onderwerpen. Daarbij moet tevens in aanmerking worden genomen dat er onvoldoende aanleiding was om alle onderzochte personen bij voorbaat als 'verdacht' aan te merken."
(Registratiekamer, 23 december 1997, 97\178.04)

In een zaak van een politiekorps werden via het bedrijfsnetwerk berichten uitgewisseld die met name vrouwelijke politieambtenaren als intimiderend en ongewenst beschouwden. Er was in casu geen sprake van eigen postbussen van medewerkers, maar van een centrale opslag. Er waren geen gebruiksregels opgesteld. De medewerkers gebruikten het systeem ook voor berichten van meer persoonlijke aard. De Registratiekamer oordeelde dat "de zorg van een goed werkgever met zich mee brengt dat het meer persoonlijke, niet zakelijke berichtenverkeer gerespecteerd wordt. Dit geldt temeer als die berichten van de aanduiding 'privé', 'persoonlijk' of 'vertrouwelijk' zijn voorzien. Het betreft hier privacy-aanspraken van werknemers die door de werkgever in beginsel dienen te worden gerespecteerd".

De Registratiekamer merkte op dat ook ter discussie staat of e-mail onder de bescherming van artikel 13 Grondwet (het brief- en telefoongeheim) staat en dat wetsvoorstellen aanhangig waren die e-mail onder de bescherming van dit artikel moesten brengen.

"Uit het voorgaande in samenhang beschouwd vloeit naar het oordeel van de Registratiekamer voort dat ten aanzien van e-mailverkeer ook in de verhouding werkgever/werknemer de privacybescherming voorop dient te staan. Inbreuken daarop dienen in concrete situaties in overeenstemming te zijn met de beginselen van proportionaliteit en subsidiariteit."

Het onderzoek naar de intimiderende berichten kon plaatsvinden met inachtneming van de gegeven randvoorwaarden. (Registratiekamer, 14 oktober 1997, 97\0578.01)

In een latere zaak vroeg de ondernemingsraad van een computerbedrijf de Registratiekamer om een oordeel over de nieuwe 'worldwide corporate policy' van het bedrijf ten aanzien van e-mail en voice-mail. Daarin werd gesteld dat de werkgever inzage kan eisen in de e-mail- en voice-mailberichten 'for any purpose' en dat werknemers 'no reasonable expectation of privacy' hebben. Dit laatste vloeide voort uit het feit dat het gebruik van het e-mailsysteem slechts was toegestaan voor zakelijk verkeer. Privé-gebruik was slechts incidenteel toegestaan. De Registratiekamer oordeelde dat het voorbehoud van de werkgever om voor 'any purpose' e-mailberichten te openen, te gebruiken, te kopiëren of te verspreiden op grond van de WPR niet is toegestaan. De werkgever zal een redelijk belang moeten kunnen aantonen voor de aanleg van de persoonsregistratie. "Een persoonsregistratie mag gelet op artikel 4 WPR slechts worden aangelegd voor een bepaald doel waartoe het belang van de houder redelijkerwijs aanleiding geeft. Dit geldt ook voor een persoonsregistratie die het resultaat is van het gebruik van e-mail. Het doel van deze persoonsregistratie mag niet in strijd zijn met de wet, de openbare orde of de goede zeden en moet bij de aanleg van de registratie vast staan. Artikel 4 dwingt de houder dus tot specificatie van de doelstelling. Van enige specificatie van het doel van deze persoonsregistratie is volgens de policy geen sprake."

Het gebruik van de persoonsregistratie moet daarmee verenigbaar zijn. Ook de stelling dat de werknemer 'no reasonable expectation of privacy' heeft, is niet houdbaar. (Registratiekamer, 24 juni 1999, 99\0141.01)

Kort daarna stelde de Registratiekamer een ambtshalve onderzoek in naar een bedrijf dat was overgegaan tot het monitoren van het bedrijfsnetwerk. Het ging om een onderzoek naar overtreding van de bedrijfsvoorschriften door enkele medewerkers. Het bedrijfsbeleid stelde dat het netwerk voornamelijk was bedoeld voor zakelijke doeleinden, maar dat privé-gebruik - mits tot een minimum beperkt en met toestemming van de chef - was toegestaan. Tevens werden bepaalde vormen van gebruik uitdrukkelijk verboden, waaronder "online gokken, het versturen van kettingbrieven, pornografisch materiaal of discriminerende of seksueel intimiderende opmerkingen". Het bedrijf hield zich het recht voor om alle mailberichten en internetgebruik te onderzoeken zonder de betrokken medewerker daarvan op de hoogte te stellen. Dit beleid was voor de medewerkers toegankelijk via een verwijzing op het openingsscherm.

Het bedrijf was overgegaan tot een intern onderzoek na een klacht van een medewerker van een zustermaatschappij die een e-mailbericht met pornografisch materiaal had ontvangen dat niet voor hem bestemd was. Daarop heeft het bedrijf de mailboxen geopend van de medewerkers die bij deze zaak betrokken waren. Alleen de berichten waarvan niet kon worden uitgesloten dat zij vrij waren van verboden materiaal, werden geopend. Voorts was het onderzoek beperkt in de tijd.

De Registratiekamer oordeelde dat de beperkte omvang van het onderzoek en de wijze waarop het had plaatsgevonden behoorlijk en zorgvuldig was. Wel plaatste de Registratiekamer enkele kanttekeningen bij het opgestelde beleid.

"Afhankelijk van de momenten en de wijze waarop deze toestemming van de chef in de praktijk moet worden verkregen, miskent deze voorwaarde dat de werknemer ook in de arbeidssituatie een zekere mate van privacy toekomt, hetgeen door de rechter ook als zodanig wordt erkend. Onder dit recht op privacy mag naar het oordeel van de Registratiekamer ook een beperkt gebruik van communicatiemiddelen zonder voorafgaande toestemming van de directe chef worden gerekend."

En voorts

"De bevoegdheid die het bedrijf zich in het algemeen toekent om al het netwerkverkeer te controleren zonder de werknemer daarvan op de hoogte te stellen, is naar het oordeel van de Registratiekamer in zijn algemeenheid te ruim geformuleerd om de hiermee gepaard gaande inbreuk op de bescherming van de persoonlijke levenssfeer te rechtvaardigen. Een nadere omschrijving van de gevallen waarin van dit recht gebruik wordt gemaakt en de werkwijze die hierbij wordt gevolgd wordt dan ook aanbevolen." (Registratiekamer, 27 december 1999, 99\0927.02)

Conclusie

Hoewel de bovenstaande uitspraken onder de WPR hebben plaats gevonden, is de strekking van de argumentatie nog steeds geldig. Het CBP, en voorheen de Registratiekamer, gebruikt als uitgangspunt de privacy van werknemers ten aanzien van het gebruik van e-mail en internet. "De zorg van een goed werkgever brengt met zich mee dat de vertrouwelijkheid van berichten met een meer persoonlijke, niet zakelijke inhoud, wordt gerespecteerd." Bij een inbreuk op deze privacy van de werknemer is een duidelijke rechtvaardiging noodzakelijk. De begrippen proportionaliteit en subsidiariteit spelen daarbij een belangrijke rol.

Juridisch kader 3.7 Uitspraken van de rechter

De rechter heeft zich in een aantal zaken ook uitgesproken over controle bij het gebruik van e-mail en internet. Ter illustratie wordt hier een aantal zaken beschreven.

In de uitspraak van de Kantonrechter te Utrecht wordt erkend dat de werknemer in relatie tot de werkgever aanspraak kan doen op de eerbiediging van zijn persoonlijke levenssfeer. De Kantonrechter oordeelde dat de werkgever geen privé-correspondentie, in de vorm van e-mailberichten, mag aanvoeren als bewijs tegen de werknemer. De uitspraak luidde;

“Dat analoog aan Artikel 13 van onze Grondwet, het briefgeheim zich ook uitstrekt tot de met een persoonlijke brief vergelijkbare communicatievormen zoals in casu de betreffende e-mails. Daaraan doet niet af dat voor de verzending van zijn privé-correspondentie gebruik is gemaakt van de E-mail aansluiting van de werkgever. De aard van de correspondentie verandert immers niet zonder meer door de wijze van verzending. Voorts kan niet worden geoordeeld dat door gebruik te maken van de e-mail aansluiting van de werkgever het vertrouwelijke karakter van de e-mails is prijs gegeven. (Kantonrechter Utrecht, 16 september 1998, NJ-kort 1998, nr. 83).

Voor het Kantongerecht Almelo speelde een zaak waarin de werkgever voorwaardelijk ontbinding vorderde van de arbeidsovereenkomst met een werknemer die op staande voet was ontslagen nadat was geconstateerd dat hij zonder toestemming van de werkgever een internetaansluiting had aangelegd en bepaalde sites had bezocht. De werknemer stelde dat de werkgever inbreuk had gemaakt op zijn privacy door onder meer kennelijk het wachtwoord te kraken en de e-mail te openen. Hij eiste een vergoeding op basis van een hoge correctiefactor. De rechter oordeelde onder meer dat

“bij een onderzoek naar misbruik van het internet door de werkgever niet valt te ontkomen aan een onderzoek naar het persoonlijk gebruik dat van het internet is gemaakt. De werkgever treft derhalve geen verwijt.”

De arbeidsovereenkomst werd ontbonden zonder toekenning van een vergoeding. (Kantonrechter Almelo, 30 september 1999, Praktijkids 1999, 5365).

In een zaak die speelde voor de Kantonrechter Haarlem, ging het om een werknemer die in strijd met de bedrijfsrichtlijnen tijdens werkuren pornografisch materiaal per e-mail had verzonden aan privé-relaties. De werkgever vroeg ontbinding van de arbeidsovereenkomst. De rechter oordeelde dat

“... in het huidige tijdsgewricht is aanvaard dat er een zekere 'privétisering' van de werkplek optreedt. Dat heeft tot gevolg dat ook een werkgever binnen zekere grenzen heeft te aanvaarden dat er onder werktijd privé-contacten worden onderhouden. Een werkgever behoort de privacy van die contacten te waarborgen”.

De rechter liet derhalve de inhoud van het e-mailverkeer met derden buiten beschouwing. Dit lag anders voor de attachments bij de e-mailberichten met afbeeldingen van pornografische aard. De rechter oordeelde dat de werknemer had moeten begrijpen dat het bedrijfsnetwerk niet bedoeld was voor dit soort gebruik. Omdat het de werkgever volgens de rechter vrij stond om haar netwerk te onderzoeken op dit soort gebruik, achtte de rechter het verkregen en ter zitting aangevoerde bewijsmateriaal niet onrechtmatig. Daarnaast speelden ook andere feiten. De rechter ontbond de arbeidsovereenkomst zonder vergoeding. (Kantonrechter Haarlem, 16 juni 2000, Jurisprudentie Arbeidsrecht 2000, 170).

Niet veel later deed de Kantonrechter te Utrecht uitspraak in een zaak waarin een werkgever de ontbinding verzocht van de arbeidsovereenkomst met een oudere werknemer die dagelijks meer dan een uur erotische sites op internet bezocht via het computersysteem van het bedrijf. De rechter oordeelde dat het ontslag de werknemer onevenredig hard zou treffen en weigerde de arbeidsovereenkomst op die grond te ontbinden. Daarbij nam hij in aanmerking dat de werkgever op dat moment geen gedragscode voor het gebruik van e-mail en internet op het werk had en dat de werkgever de werknemer niet eerst had gewaarschuwd. (Kantonrechter Utrecht, 13 juli 2000, JAR 2000, 199).

Bij de uitspraak van de Kantonrechter te Apeldoorn speelt de aanwezigheid van een gedragscode eveneens een rol. De werkgever gaf aan dat werknemers gewaarschuwd waren dat het gebruik van het net op niet-zakelijke wijze niet werd getolereerd. Ook was de werkgever bezig met een gedragscode. De Kantonrechter constateerde dat deze code niet consequent werd nageleefd binnen de onderneming. Maar ook al zou dat wel zo zijn, is ontbinding wegens dringende reden niet proportioneel. (Kantonrechter Apeldoorn, 6 september 2000, JAR 2000, 212).

In het geval van een werknemer die door het bezoeken van sekssites op internet de telefoonrekening van de werkgever zeer hoog had laten oplopen, oordeelde de Kantonrechter dat ontbinding van de arbeidsovereenkomst zonder vergoeding gerechtvaardigd was. (Kantonrechter Hilversum, 6 september 2000, JAR 2000, 216).

De Kantonrechter te Utrecht ging over tot ontbinding van een arbeidsovereenkomst wegens dringende reden bij een werknemer die een e-mail met "smakeloze" plaatjes had verstuurd. Alhoewel er geen gedragscode was en niet was vast komen te staan dat de algemene waarschuwingsmail ter zake was ontvangen, was de Kantonrechter toch van oordeel dat het beleid van de werkgever op dit onderdeel de werknemer voldoende bekend was. (Kantonrechter Utrecht, 20 november 2000, JAR 2001, 7).

Ook de Kantonrechter te Emmen gaat over tot ontbinding van een arbeidsovereenkomst na buitensporig e-mailgebruik van desbetreffende werknemer. "Het had werknemer ook zonder verbod of regeling duidelijk moeten zijn dat zijn gedragingen niet getolereerd konden worden. [...] Tenslotte geldt dat het recht op privacy op de werkplek afgewogen moet worden tegen het recht van een onderwijsinstelling niet met seksactiviteiten in verband te worden gebracht. Bij een afweging van belangen prevaleert dit laatste recht." (Kantonrechter Emmen, 29 november 2000, JAR 2001, 4).

Een politieambtenaar is bij de Rechtbank Rotterdam in beroep gegaan tegen het besluit van haar werkgever om tegen haar een disciplinair onderzoek in te stellen naar aanleiding van een vermoeden van buitenproportioneel oneigenlijk e-mailgebruik. Hierbij zijn haar e-mailberichten ingezien. De vrouw doet daarbij een beroep op haar privacy. De rechtbank concludeert dat er een zorgvuldige afweging van belangen heeft plaats gevonden. De politieambtenaar kan zich niet verschuilen achter het feit dat er geen e-mail en internetregeling is. (Rechtbank Rotterdam, 29 maart 2001, ELRO-nr: AB0812).

De Amsterdamse rechtbank weigerde een ontbinding van de arbeidsovereenkomst na het verzenden van e-mailberichten met "Clintoniaanse" woordgebruik. Het ging om een beperkt aantal mails: "...het volledig verbieden van elke niet-zakelijke communicatie valt moeilijk te verbieden. Ook al is dat in een gedragscode vast gelegd." (Kantonrechter Amsterdam, 26 april 2001, JAR 2001, 101). Drie werknemers van DSM vochten bij de Kantonrechter in Sittard hun ontslag

op staande voet aan. Dit naar aanleiding van een grote hoeveelheid pornografische e-mails op de harde schijf van de bedrijfscomputer. De kantonrechter stelt dat de werknemers behoorden en konden weten dat de bedrijfsapparatuur niet voor privé-doeleinden mocht worden gebruikt. De gedragingen van de betreffende werknemers rechtvaardigden echter niet een ontslag op staande voet. Maar op basis van verstoorde arbeidsverhoudingen wordt het contract wel ontbonden. (Kantonrechter Sittard, beschikking d.d. 3 december 2001, zaak no. 101435)

Conclusie

Het is niet makkelijk om algemene lijnen uit deze jurisprudentie te halen. Wel laten de hierboven beschreven uitspraken zien dat bij ontslag (op staande voet) vanwege e-mail of internetmisbruik, onafhankelijk of er nu wel of geen gedragscode is, dit ontslag in de meeste gevallen gerechtvaardigd wordt geacht.

Er is een duidelijke uitspraak gedaan over de huidige “privetisering” van de werkplek. Dat houdt in dat een bepaalde mate van niet-zakelijk e-mail- en internetgebruik onder werktijd niet verboden kan worden.

De aanwezigheid van een gedragscode wordt in de meeste uitspraken wel mee gewogen als relevante factor. Het is voor werkgevers dan ook veiliger om een duidelijk beleid te hebben. Echter de afwezigheid van een dergelijk beleid is nog geen rechtvaardiging voor de handelwijze van betrokken werknemers. Want ook zonder expliciete gedragscode kunnen werknemers weten wat wel of niet acceptabel is.

Vuistregels voor controle



Dit hoofdstuk geeft vuistregels voor het gebruik van e-mail en internet op de werkplek en de controle hier op. De vuistregels sluiten aan bij wettelijke regels vanuit het privacyrecht en het arbeidsrecht en bij algemene noties met betrekking tot personeelsvolgsystemen. Vertrekpunt zijn algemene regels die gelden voor personeelsvolgsystemen in het algemeen en de controle op het gebruik van het bedrijfsnetwerk. Vervolgens komen de specifieke regels aan bod voor de controle op e-mailgebruik waarbij met name de bescherming van de inhoud van het bericht centraal staat. Daarnaast zijn er regels die specifiek zijn toegesneden op de controle van internet. Waar nodig zal aangegeven worden op welke vorm van internet de regel met name betrekking heeft.

Vuistregels voor **Algemeen**

Als men nadenkt over het fenomeen e-mail en internet op de werkplek, dan komt men al snel tot de conclusie dat het gaat om nieuwe technologieën die tegemoet komen aan oude behoeften en doeleinden. Meestal kan hieraan ook op een andere, minder snelle wijze tegemoet worden gekomen. Als men op deze wijze over de problematiek nadenkt, zal men snel tot de conclusie komen dat er in wezen niet zo veel verandert door de introductie van deze technologieën op de werkplek.

Aan de andere kant is de impact van systematische controle op het gedrag van werknemers bij het gebruik van computers groot, hetgeen ook blijkt uit de bepalingen die hieromtrent in de Arbeidsomstandighedenregelgeving zijn opgenomen. De werkgever zal bij de vormgeving van zijn beleid uit moeten gaan van de loyaliteit van zijn werknemers. Permanente controle op werkprocessen draagt niet bij tot een sfeer van wederzijds vertrouwen.

4.1 Behandel zaken online op dezelfde manier als off line

Werknemers doen hun taken op een bepaalde manier. Zij kunnen daar vaak verschillende methoden voor gebruiken. Als men iets wil mededelen aan een ander, kan men naar die ander toe gaan voor een persoonlijk gesprek, men kan dit ook telefonisch doen, een brief schrijven of een fax versturen. Sinds enige tijd kan men hetzelfde bericht ook e-mailen. Ook het gebruik van internet kan vergeleken worden met andere vormen van omgang met bijvoorbeeld informatie. Men kan achter een bureau de krant lezen, maar ook op internet. Een werknemer kan even langs het reisbureau gaan, maar hij kan ook online informatie krijgen. Men kan een bestand op diskette versturen, maar ook via FTP of e-mail.

In het algemeen dient de werkgever er bij de vaststelling van zijn beleid rekening mee te houden dat de werknemer alternatieve wegen kan bewandelen om hetzelfde doel te bereiken. Het verbieden van een privé-mail zal in het algemeen onredelijk zijn als men een privé-telefoontje wel toestaat (waarbij men overigens kan bedenken dat de operationele kosten van telefoneren hoger zijn dan van e-mailen). Zo geldt dit ook voor andere zaken. Het beleid voor online gedrag moet dus in overeenstemming zijn met het beleid voor off line gedrag.

4.2 Stel heldere regels op met de instemming van de ondernemingsraad

De regels voor het gedrag van werknemers moeten helder en eenduidig zijn. Bepaal wat in de organisatie is verboden of wat is toegestaan, op welke manier de gegevens worden verzameld en gebruikt, wie geautoriseerd is om de gegevens te gebruiken en onder welke omstandigheden, hoelang de gegevens worden bewaard en wat de sancties zijn op overtreding van de regels.

Volgens artikel 27 WOR is de instemming van de ondernemingsraad vereist, omdat controle op e-mail- en internetgedrag als personeelsvolgsysteem moet worden geduid en loggingen van (vaste) IP-adressen en andere gegevens als het verwerken van persoonsgegevens gelden.

4.3 Publiceer de regels op een voor de werknemer toegankelijke wijze

De regels moeten helder gecommuniceerd worden naar de werknemers. De werknemer moet weten wat is toegestaan of is verboden, dat controle mogelijk is, op welke wijze dat geschiedt en wat de consequenties zijn van zijn handelen. Op betrekkelijk eenvoudige wijze kunnen de regels tijdens het opstarten van het systeem of van het programma worden gepresenteerd op het beeldscherm van de werknemer. Op deze wijze wordt gegarandeerd dat de werknemer zich van de regels bewust is.

4.4 Stel vast in hoeverre privé-gebruik van de faciliteiten is toegestaan

Een werkgever is bevoegd om regels te stellen omtrent de mate waarin privé-gebruik van e-mail en internet is toegelaten. In het algemeen zal een beperkte vorm van privé-gebruik worden toegestaan evenals bij telefoneren gebruikelijk is. In zijn algemeenheid is een totaal verbod op privé-gebruik van e-mail en internet niet aanvaardbaar. Alleen bij communicatiefaciliteiten met een specifieke doelstelling, kan het privé-gebruik verboden worden. De werknemer moet dan wel andere communicatiemogelijkheden ter beschikking hebben. Overigens zou ook bij een algeheel verbod op privé-gebruik de werkgever nog niet het recht hebben om continue het gebruik te controleren. Dit zou immers een ingrijpende en niet-evenredige inmenging in het functioneren van de werknemers betekenen. Continue controle wordt door de Arbeidsomstandighedenwetgeving dan ook met reden als schadelijk gezien voor de gezondheid en het welzijn van de werknemer en zal in het algemeen ook niet kunnen worden gekwalificeerd als goed werkgeverschap.

4.5 Maak verboden gebruik zoveel mogelijk softwarematig onmogelijk

Het is raadzaam om het verboden gebruik in te bouwen in de software die binnen de organisatie wordt gebruikt om te e-mailen of te internetten. In veel gevallen zal dat kunnen door 'content-filtering' (het scannen van berichten of bestanden op verboden woorden of extensies), door het afsluiten van websites of nieuwsgroepen, het stoppen van de doorgifte, enzovoorts. Hierdoor is overtreding van het beleid feitelijk vrijwel onmogelijk en is er geen grond meer voor een continue of actieve controle en logging op het gebruik van de faciliteiten.

Ook is het mogelijk om toepassingen volledig af te sluiten door de daarvoor benodigde software zelf niet aan te bieden. Internet kent veel verschijningsvormen met ieder zijn eigen toepassingsmogelijkheden en gebruiksoftware. Als een werkgever bijvoorbeeld niet wenst dat zijn werknemers tijd besteden aan chatten, zal hij geen chat-programma ter beschikking moeten stellen. Verder zal hij het gebruik ervan ook moeten verbieden om te voorkomen dat werknemers deze software zelf meenemen. Een beoordeling van voor- en nadelen van toepassingsmogelijkheden en ter beschikking gestelde programma's is noodzakelijk.

4.6 Anonimiseer rapportages en gebruiksstatistieken

Als het gebruikelijk is om het management rapportages en gebruiksstatistieken van het e-mail- en internetgebruik van de werknemers te verstrekken, is het doorgaans niet noodzakelijk om dat op persoonsniveau te doen. De gegevens in de rapportages en statistieken zullen dus meestal ontdaan kunnen worden van hun identificerende kenmerken. Alleen als er concrete bedenkingen bestaan tegen een bepaalde werknemer, is rapportage op persoonsniveau noodzakelijk en dan ook toegestaan.

4.7 Houdt rekening met de back-ups van het systeem

Als men zorgvuldig met informatiesystemen omgaat, zal men regelmatig back-ups van de systemen maken om in geval van nood eenvoudig terug te kunnen keren naar een werkend systeem. Dit betekent dat van loggingen en andere gegevens over het e-mail- en internetgedrag van werknemers een back-up wordt gemaakt. De werkgever moet zich ervan bewust zijn dat onzorgvuldig of onbevoegd gebruik van deze back-ups even schadelijk kan zijn voor de persoonlijke levenssfeer van de werknemer als onzorgvuldig of onbevoegd gebruik van het actuele systeem. Back-ups dienen derhalve op een veilige plaats bewaard te worden.

Nadat gegevens zijn aangepast zal zo snel mogelijk een nieuwe back-up gemaakt moeten worden en moeten oude versies worden vernietigd, zodat de gegevens niet na een eventuele terugplaatsing van een back-up nogmaals moeten worden aangepast.

4.8 Garandeer de integriteit van de systeembeheerder

De systeembeheerder heeft uit hoofde van zijn functie via een speciale username/password-combinatie toegang tot alle gegevens in het computernetwerk. Dit maakt de functie van de systeembeheerder tot een functie die met de nodige waarborgen moet worden omgeven.

Allereerst moet de systeembeheerder zich ervan bewust zijn dat hij gegevens die hij tijdens zijn werk tegenkomt, niet zonder meer openbaar maakt. Hij heeft dus een soort vertrouwensfunctie. Het opleggen van een geheimhoudingsplicht aan de systeembeheerder is vereist (zie ook artikel 12, lid 2 WBP). De systeembeheerder is uiteraard in beginsel niet bevoegd tot het lezen van documenten of e-mail of het real-time meekijken met het internetgebruik van de werknemers zonder dat daar een bijzondere aanleiding toe is.

De systeembeheerder moet tegenover het management een zekere onafhankelijkheid hebben. Een systeembeheerder moet zich als ondergeschikte medewerker niet in een positie gebracht voelen waarin hij opdrachten van het management niet op basis van zijn professionaliteit en de hierboven beschreven regels kan uitvoeren. Er moet dus een heldere procedure bestaan die antwoord geeft op de vraag wie in welke gevallen de systeembeheerder opdracht kan geven om bepaalde zaken op het netwerk nader te controleren of daarover informatie te verschaffen.

4.9 Bespreek geconstateerd gedrag zo spoedig mogelijk met betrokkene

Werknemers van wie geconstateerd is dat zij zich niet aan de regels van het bedrijfsbeleid houden, dienen zo spoedig mogelijk op hun gedrag te worden aangesproken. Een zekere tijd voor dossieropbouw is toegestaan indien de omstandigheden daartoe aanleiding geven.

4.10 Biedt inzage in de gegevens

Indien de werknemers de mogelijkheid wordt geboden om de loggegevens van het netwerk- en internetgebruik in te kunnen zien, zal dit het wantrouwen in de geautomatiseerde controle voor een groot deel kunnen wegnemen. Zij kunnen immers zelf zien wat de werkgever van hen vastlegt. Dit betekent dat de loggegevens in begrijpelijke vorm moeten worden weergegeven en met enige regelmaat moeten worden ververst.

4.11 Evalueer periodiek de regels

Regels verouderen omdat de organisatie, de omgeving waarin zij verkeert en de technische mogelijkheden wijzigen. Het is dan ook zaak periodiek de regels te evalueren zodat tijdig bijstelling kan plaatsvinden.

Vuistregels voor **E-mail en internet**

Controle van e-mail is op zichzelf niet verboden. De werkgever is bevoegd om op basis van zijn gezagsbevoegdheid voorwaarden te stellen aan het gebruik van e-mail-faciliteiten of bepaalde soorten gebruik te verbieden. De werkgever zal wel de doeleinden moeten bepalen waarvoor hij controle noodzakelijk acht. De maatregelen moeten in een redelijke verhouding staan tot de belangen van de werknemer. Via e-mail zal de werknemer immers niet alleen zakelijk communiceren, maar in sommige gevallen ook privé-zaken afhandelen. Eveneens zal de werknemer de ruimte moeten worden gelaten om zijn werkzaamheden naar eigen inzicht te verrichten zonder dat zijn baas voortdurend over zijn schouder meekijkt. Continue controle op e-mail – met name op de inhoud ervan – doet daaraan afbreuk.

Op grond van de belangenafweging moet de werkgever vervolgens het minst vergaande middel kiezen. In het algemeen dient de werkgever rekening te houden met het recht op vertrouwelijke communicatie van zijn werknemers.

Evenals controle op e-mail is controle op het internetgebruik van werknemers toegestaan. Met name is de werkgever bevoegd om op basis van zijn gezagsbevoegdheid voorwaarden te stellen aan het gebruik (bijv. tijd en plaats) of bepaalde soorten gebruik te verbieden. Ook hier geldt dat de genomen maatregelen in een redelijke verhouding moeten staan tot de belangen van werknemer en dat de gebruikte middelen niet een verdergaande inbreuk mogen maken op die belangen dan strikt noodzakelijk is.

Gelet op het voorgaande is het verstandig om bij de vormgeving van het beleid rekening te houden met de volgende vuistregels:

4.12 Probeer zakelijke en privé-mail te scheiden en ontzie privé-mail zoveel mogelijk

Het is vanuit het oogpunt van de bescherming van de persoonlijke levenssfeer van de werknemers wenselijk om de zakelijke mail van de privé-mail te scheiden. Dit kan bijvoorbeeld door de werknemer twee mailadressen aan te bieden, waarvan er één zakelijk en één privé is. De werknemer kan de mogelijkheid worden geboden om de mailbox met privé-mail met een password te beveiligen. Zakelijke e-mail kan dan bij afwezigheid van de werknemer door anderen worden geopend zonder gevaar voor inbreuk op de privacy van de werknemer. Ook kan een werkwijze zijn om bij de onderwerpsaanduiding aan te geven dat het een privé-mail betreft.

Indien scheiding tussen zakelijke en privé-mail niet mogelijk blijkt, dient de werkgever er rekening mee te houden dat er privé-berichten worden ontvangen en verstuurd. Bij controle dient met name de inhoud van de e-mailberichten te worden ontzien. Dit ligt anders als de werkgever gewichtige redenen heeft om

van het bericht kennis te nemen. Ook voor controle van verstuurde privé-mail moet de werkgever een gewichtige reden kunnen aantonen.

4.13 Beperk de controle tot het vooraf geformuleerde doel; voorzie in controlemechanismen die op de doeleinden zijn toegesneden

Een werkgever kan meerdere redenen hebben om e-mail of internetgebruik te willen controleren. Deze doeleinden stellen voorwaarden en beperkingen aan de omvang en de wijze van controle. Veel voorkomende doeleinden zijn:

Begeleiding en/of individuele beoordelingen

In het kader van begeleiding of individuele beoordeling van werknemers kan controle op de inhoud van de zakelijke e-mail aan de orde zijn. Dit moet dan wel rechtstreeks verband houden met diens taken. Zo kan een helpdesk-medewerker tot wiens taak het behoort om per e-mail met klanten te communiceren aan een steekproefsgewijze inhoudelijke controle onderworpen worden. In deze situatie is het wenselijk om de mogelijkheid van controle vast te leggen in de arbeidsovereenkomst. De berichten moeten zo spoedig mogelijk worden geëvalueerd. Indien dit is gebeurd, is er geen noodzaak om het bericht nog langer te bewaren.

Bij het internetgebruik zal het doeleinde begeleiding en individuele beoordeling in de meeste organisaties geen rol spelen. Voor zover dat wel het geval is (bijvoorbeeld in geval van documentalist die externe bronnen of online vakliteratuur moeten raadplegen), dienen de regels voor controle op e-mail overeenkomstig te worden toegepast.

Vastleggen van bewijs en/of archief

Vaak is een kopie van e-mail gewenst vanwege de behoefte aan bewijs van zakelijke transacties of dossiervorming. Op dit punt zullen de procedures die gelden voor het archiveren van berichten op papier doorgaans van overeenkomstige toepassing zijn.

Systeem- en netwerkbeveiliging

Vanuit beveiligingsoogpunt is het wenselijk om e-mail te controleren. Het kan dan gaan om het tegengaan van systeemaanvallen door virussen, trojans of andere schadelijke programma's. Bij deze controle verdient een geheel geautomatiseerde controle van de inkomende berichten en de bijlagen de voorkeur. Indien een besmet bericht gevonden wordt, kan dit op een aparte locatie worden bewaard voor nader onderzoek en eventuele herstelwerkzaamheden. Uiteraard wordt hierbij geen onderscheid gemaakt in zakelijke en privé-mail.

Vanuit beveiligingsoogpunt is het ook wenselijk om internetgebruik te controleren. Het kan dan gaan om het tegengaan van systeemaanvallen door virussen, trojans of andere schadelijke programma's. Voor dit doel verdient een geheel geautomatiseerde controle van de inkomende content de voorkeur, mits de controle tot dit doel beperkt blijft. Indien het voor de inhoud van de functie van de medewerkers niet noodzakelijk is dat zij steeds toegang hebben tot internet, kan dit doel eenvoudig bereikt worden door de toegang aan te bieden op aparte computers die niet aan het interne netwerk zijn verbonden.

Beschermen van bedrijfsgeheimen

Een werkgever die zich tegen het uitlekken van bedrijfsgeheimen wil wapenen, zou de inhoud van de uitgaande berichten en de bijlagen kunnen controleren. Het controleren van e-mail zal echter slechts een beperkt middel zijn, vanwege de andere (en vaak betere) mogelijkheden die daarvoor aan te wenden zijn.

Indien e-mailcontrole hiervoor toch wordt ingezet, heeft geautomatiseerde controle middels content-filtering de voorkeur. Een verdacht bericht kan apart worden gezet voor nader onderzoek. Onderscheid tussen privé- en zakelijke mail is niet van belang.

NB. In dit verband is het van belang zich te realiseren dat het voor de gebruiker eenvoudig is om deze controle te omzeilen (zie ook de opmerkingen in paragraaf 2.3).

Controle op het uitlekken van bedrijfsgeheimen via het internet zal moeten geschieden door middel van content-filtering. Dit is niet geschikt voor alle vormen van internetgebruik. Een organisatie die het internetgebruik van de werknemers met het oog hierop wil controleren, doet er dus verstandig aan aandacht te besteden aan de verscheidenheid van internet en bepaalde vormen (met name daar waar uploading mogelijk is, zoals FTP en Chat) wellicht geheel te verbieden. Bedenk wel dat in dat geval ook het onderhoud van websites niet meer mogelijk is. Overigens kleeft het risico van uitlekken van bedrijfsgeheimen ook aan het verzenden van e-mail.

Voorkomen van negatieve publiciteit

Werknemers kunnen via e-mail de goede naam van een organisatie behoorlijk aantasten. Het plegen van strafbare feiten, seksuele intimidatie of discriminerende uitingen geschiedt immers onder gebruikmaking van het e-mailadres van de organisatie. Ook hier verdient het de voorkeur om controle geheel geautomatiseerd te laten plaatsvinden middels content-filtering. Verdachte berichten – zowel inkomende als uitgaande – dienen zo mogelijk (geautomatiseerd) te worden teruggestuurd aan de afzender, waardoor vastlegging van de inhoud van het bericht niet nodig is. Slechts indien sprake is van herhaaldelijke pogingen van een medewerker om dergelijke berichten te versturen, kan de werkgever deze uitnodigen om het een en ander toe te lichten (zie paragraaf 4.9).

Indien men gebruik maakt van internetdiensten via een ISP, is dit doel betrekkelijk eenvoudig te bereiken door de naam van de organisatie uit alle internetverkeer te verwijderen. In veel programma's wordt men geacht gebruikersgegevens (naam, organisatienaam, e-mailadres, reply-adres) in te vullen. Deze gebruikersgegevens worden bij het internetgebruik steeds meegezonden. Door deze gegevens achterwege te laten, wordt veel negatieve publiciteit voorkomen omdat de gebruiker of de organisatie bij de beheerder van de website dan onbekend is. Ook kan gebruik worden gemaakt van een proxyserver bij een betrouwbare serviceprovider. Uiteraard vormt dit geen vrijbrief voor werknemers om zich te misdragen op het internet. Steekproefsgewijze controle is mogelijk.

Het voorgaande geldt niet voor internetverkeer via vaste IP-adressen. Deze zijn immers altijd herleidbaar op een organisatie. In dat geval kan een werkgever internetverkeer van de werknemer controleren. Dit zal hij echter slechts steekproefsgewijs kunnen doen.

Tegengaan van seksuele intimidatie

Via e-mail kan eenvoudig seksuele intimidatie worden gepleegd. Zowel de inhoud van het bericht als de bijlagen kunnen seksueel intimiderend zijn. Ook is het niet ingewikkeld om de afzender van een bericht te maskeren.

Een werkgever die het beleid hiervoor wil handhaven, kan inkomende berichten onderwerpen aan een geautomatiseerde controle. Zo kan de tekst gescand worden

op verboden woorden en kunnen bijlagen nader bekeken worden, als daar gezien de situatie aanleiding voor is. Verdachte berichten dienen (geautomatiseerd) te worden teruggestuurd aan de afzender.

Het tegengaan van seksuele intimidatie via internet (bijvoorbeeld in Chatsessies) is lastig. Bepaalde vormen zijn volstrekt ongeschikt om te controleren met het oog op dit doel. In dit kader past een meer repressieve benadering middels een klachtenprocedure.

Controle op naleving van afspraken over verboden gebruik

Een goed beleid voorziet in heldere regels over het gebruik van e-mail en internet die op een toegankelijke manier aan de werknemers kenbaar zijn gemaakt. Veel werkgevers zullen de behoefte hebben om bepaalde soorten gebruik te verbieden. Het zal dan gaan om gokken, het versturen van kettingsbrieven, het bekijken of verspreiden van pornografisch materiaal, het doen van discriminerende of seksueel intimiderende uitingen of het downloaden of versturen van illegale software of omvangrijke bestanden die veel beslag leggen op de beschikbare capaciteit.

Een werkgever kan de behoefte hebben om te controleren of deze regels ook worden nageleefd. Dit doel rechtvaardigt echter niet een continue controle en de daarmee gepaard gaande verregaande inbreuk op de persoonlijke levenssfeer van de werknemer. In de regel zal de controle op naleving van de afspraken slechts steekproefsgewijs mogen geschieden. Indien echter een werknemer of een groep werknemers ervan worden verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaatsvinden.

Kosten- en capaciteitsbeheersing

Uiteraard kost het versturen van e-mail geld en legt het beslag op de beschikbare capaciteit van het netwerk. Het kostenaspect is met name aan de orde als de e-mailverbinding via de telefoon verloopt. De tijd die het kost om de mail te versturen, is gerelateerd aan de hoeveelheid berichten en de omvang ervan. Dit vertaalt zich in het aantal telefoontikken en dus in de hoogte van de telefoonrekening. Door vastlegging van de verkeersgegevens kan de medewerker worden aangesproken op zijn mailgedrag. Kennisneming van de inhoud van de mail is voor dit doel niet noodzakelijk.

Ook voor capaciteitsbeheersing is controle op inhoud niet noodzakelijk. De controle zal voor dit doel beperkt kunnen blijven tot gegevens over tijd, hoeveelheid, omvang, en dergelijke. Uiteraard kost het gebruik van internet geld. Dit is met name het geval als er alleen via de telefoon verbinding is met internet. Dit vertaalt zich in het aantal telefoontikken en dus in de hoogte van de telefoonrekening. Door vastlegging van de verkeersgegevens kan de medewerker worden aangesproken op zijn internetgedrag. Kennisneming van de inhoud van het internetgebruik is voor dit doel niet noodzakelijk.

4.14 Voer de controles op naleving zo beperkt mogelijk uit (maatwerk)

Indien er aanwijzingen zijn dat werknemers de regels overtreden ten aanzien van het e-mailgebruik, is vaak gedurende kortere of langere tijd gerichte controle wenselijk. Hierbij moet de omvang van de controle zo beperkt mogelijk worden gehouden. Maatwerk is derhalve vereist. Eerst dient een selectie te worden gemaakt in verdachte en niet-verdachte werknemers. Vervolgens kunnen van de verdachte werknemers de onderschepte berichten worden gescreend op een verdachte afzender of bestemming, een verdacht onderwerp, verboden woorden in de inhoud of verboden extensies van de bijlage. Berichten waarvan aannemelijk is dat het regulier verkeer betreft of waartegen ook overigens geen bedenkingen

bestaan, mogen niet worden geopend. Uiteindelijk blijven alleen berichten over die afkomstig zijn van of gericht zijn aan een verdachte werknemer waarvan het onderwerp, woorden in de inhoud of de extensie van de bijlage aanleiding vormen voor een nader onderzoek. Deze berichten kunnen worden geopend. De overige berichten worden vernietigd (kopieën) of alsnog doorgezonden (originale berichten).

Indien er aanwijzingen zijn dat bepaalde werknemers de regels overtreden ten aanzien van het internetgebruik, is vaak gedurende kortere of langere tijd gerichte controle wenselijk. Hierbij moet de omvang van de controle zo beperkt mogelijk worden gehouden. Maatwerk is derhalve vereist. Eerst dient een selectie te worden gemaakt in verdachte en niet-verdachte werknemers of computers. Vervolgens worden van de verdachte werknemers of computers het onderschep-te verkeer gescreend op een verdachte URL, een verdacht onderwerp, verboden woorden of verboden gebruik.

4.15 Beperk de logging tot de verkeersgegevens; bewaar de loggegevens niet langer dan noodzakelijk is

Het doel van het e-mailsysteem is om de berichten zo snel en efficiënt mogelijk op hun bestemming te krijgen. Daarom kan de logging beperkt blijven tot gegevens over de afzender, de bestemming, de datum en de tijd van het bericht. Dit zijn de zogeheten 'verkeersgegevens'.

Bewaar de verkeersgegevens niet langer dan noodzakelijk is. In het Vrijstellingsbesluit is uitgegaan van een redelijke bewaartermijn van maximaal 6 maanden voor deze persoonsgegevens. Indien er bijzondere redenen zijn om de gegevens langer te bewaren dan moet dat expliciet worden gemaakt. Als er afgeweken wordt van de voorwaarden uit het Vrijstellingsbesluit dient de gegevensverwerking te worden gemeld bij het CBP (zie paragraaf 3.5)

Het is mogelijk om op een firewall het inkomende en uitgaande internetverkeer tot op een zeer gedetailleerd niveau te loggen. In beginsel kan iedere tekst, ieder plaatje en iedere up- of download afzonderlijk worden vastgelegd via loggings. De logging dient beperkt te blijven tot de gegevens die noodzakelijk zijn voor de realisering van de vooraf gestelde doelen. Met name bij privé-gebruik moet terughoudend worden omgegaan met het vastleggen van de URL op persoonsniveau. Overige loggings mogen niet plaatsvinden of dienen terstond te worden vernietigd.

Het is doorgaans niet nodig om de loggings lang te bewaren. Als standaard bewaartermijn kan dan ook maximaal 6 maanden aangehouden worden. Indien er bijzondere redenen zijn om de gegevens langer te bewaren dan moet dat expliciet kunnen worden gemaakt en worden gemeld bij het CBP. Dit kan zich bijvoorbeeld voordoen indien een werknemer ervan wordt verdacht zich niet aan de vastgestelde regels te houden.

4.16 Ontzie geprivilegieerde informatie in elektronische berichten

Evenals andere werknemers communiceren ook leden van de ondernemingsraad en bedrijfsartsen onderling met behulp van e-mail. Voor zover zij dat doen in hun hoedanigheid als OR-lid of arts is hun e-mail beschermd en mag de werkgever daar geen kennis van nemen. Dit betekent niet dat er geen controle op de veiligheid van het berichtenverkeer mag plaats vinden. De werkgever zal in zijn beleid dus rekening moeten houden met beroepsgeheim of ander recht op vertrouwelijkheid.

Samenvatting en overzicht vuistregels

5

Het gebruik van e-mail en internet in organisaties is de afgelopen jaren flink toegenomen. Meer en meer werknemers hebben via een computer op hun werkplek toegang tot het World Wide Web. Tegelijkertijd is de vrees toegenomen voor on-eigenlijk en risicovol gebruik van deze middelen. Werkgevers willen dit graag controleren, terwijl werknemers dit al snel beschouwen als een inbreuk op hun persoonlijke levenssfeer. Dit rapport is een handreiking voor werkgevers, ondernemingraden en individuele werknemers bij het formuleren van een bedrijfsbeleid ten aanzien van controle op e-mail- en internetgebruik dat recht doet aan de privacy van werknemers.

De regels uit dit rapport zijn van toepassing op alle verschijningsvormen van het internet. Zowel de oudere toepassingen als e-mail, internetsites, nieuwsgroepen en chat, als de modernere varianten zoals WAP. Elke nieuwe gebruiksvaariant heeft nieuwe mogelijkheden, maar brengt ook weer nieuwe risico's voor de werkgever en de werknemer mee. Voor de werkgever kan het gaan om de beveiliging van het netwerk, het tegengaan van 'verboden gebruik' of het beschermen van de goede naam van de organisatie. Voor de werknemer staat vaak diens privacybelang door de controle onder druk, maar ook de vrijheid van vrije meningsuiting of de vrijheid om informatie te verzamelen.

Onder werktijd geldt er voor werknemers een zekere beperking van de grondrechten. Dit betekent niet dat een werkgever bij het naleven van zijn belang (bijvoorbeeld het tegengaan van misbruik door controle van het e-mail of internetgebruik) de fundamentele vrijheden van zijn medewerkers aan de kant kan schuiven. De bescherming van de privacy op de werkplek is in een scala van wet- en regelgeving vastgelegd. Op basis van artikel 8 ERVM heeft de werknemer recht op een zekere mate van vertrouwelijke communicatie op de werkplek zonder inmenging door de werkgever. Op basis van de begrippen goed werknemerschap en goed werkgeverschap uit het Burgerlijk Wetboek moeten beide partijen zich houden aan zowel verantwoord gebruik van e-mail en internet als aan een zorgvuldig controlebeleid. De Wet op de ondernemingsraden geeft de ondernemingsraad het instemmingsrecht voor de invoering van een dergelijk beleid. Tenslotte geeft de Wet bescherming persoonsgegevens (WBP) het kader aan hoe er met persoonsgegevens over e-mail en internetgebruik omgegaan moet worden.

Op basis van het arbeidsrecht en het privacyrecht zijn vuistregels geformuleerd voor het gebruik en controle van e-mail en internet op de werkplek. Deze vuistregels zijn bedoeld als handvat voor het opstellen van een behoorlijk en zorgvuldig beleid in de arbeidsorganisatie. Om de toepasbaarheid van de vuistregels te vergroten heeft het CBP een raamregeling voor het gebruik van e-mail en internet ontwikkeld. Dit is bedoeld als instrument voor organisaties, bedrijven en ondernemingraden om de vuistregels in het eigen beleid toe te passen.

Vuistregels voor controle op gebruik van e-mail en internet

Algemene vuistregels

- 1 Behandel zaken online op dezelfde manier als off line.
- 2 Stel heldere regels op met de instemming van de ondernemingsraad.
- 3 Publiceer de regels op een voor de werknemer toegankelijke wijze.
- 4 Stel vast in hoeverre privé-gebruik van de faciliteiten is toegestaan.
- 5 Maak verboden gebruik zoveel mogelijk softwarematig onmogelijk.
- 6 Anonimiseer rapportages en gebruiksstatistieken.
- 7 Houdt rekening met de back-ups van het systeem.
- 8 Garandeer de integriteit van de systeembeheerder.

- 9 Bespreek geconstateerd gedrag zo spoedig mogelijk met betrokkene.
- 10 Biedt inzage in de gegevens.
- 11 Evalueer de regels periodiek.

Vuistregels voor e-mail en internet

- 12 Probeer zakelijke en privé-mail te scheiden en ontzie privé-mail zoveel mogelijk.
- 13 Beperk de controle tot het vooraf geformuleerde doel. Voorzie in op de doeleinden toegesneden controlemechanismen.
- 14 Voer de controles op naleving zo beperkt mogelijk uit (maatwerk).
- 15 Beperk de logging tot de verkeersgegevens. Bewaar de loggegevens niet langer dan noodzakelijk is.
- 16 Ontzie geprivilegieerde informatie van ondernemingsraadleden en bedrijfsartsen in elektronische berichten.

Bijlagen



Bijlage Deelnemerslijst expertmeeting

De expertmeeting vond plaats op woensdag 25 oktober 2000 bij Registratiekamer.

Aanwezig waren:

Compumatica Secure Systems BV
FNV
FNV Bondgenoten
Kennedy Van der Laan Advocaten

KPMG
Ministerie van Sociale Zaken
en Werkgelegenheid
Ministerie van Verkeer en Waterstaat
Singewald Consultants Group BV
Van Diepen van der Kroef Advocaten

Mw. P. van Schaijk
mr. H. van Steenbergen
Mw. drs. S. Lieon
Mw. mr.dr. H.H. de Vries
mr. D.J. Rutgers
R.C. Crouwel RA
Mw. mr.drs. S. Voortman
Mw. mr. L. Verplak
ir. A. Otte (tevens ISOC)
mr. H.J.M. Gardeniers
Mw. mr. B.A.J. Spiegler
(namens E92 Plus)

Schriftelijk hebben gereageerd:

VNO-NCW
Nederlandse Vereniging voor Personeelsbeleid

Van de Registratiekamer waren aanwezig:
mr .dr. U. van de Pol
mr. drs. J.H.J. Terstegge
drs. R. Schreijnders
Mw. S.M. Artz

Bijlage Literatuur

Asscher, L.F., en W.A.M. Steenbruggen, 'Het E-mailgeheim op de werkplek. Over de toelaatbaarheid van inbreuken op het communicatiegeheim van de werknemer in het digitale tijdperk', in: *NJB*, 2001-37, p.1787-1794.

Homan, T.C., 'Privacy, internet en e-mail op de werkplek', in: *Arbeid Integraal* 6, december 2000, p.186-192.

Vries, H. de, 'Rechtspraak over 'mailen en surfen'', in: *Privacy en informatie*, 2002, nr. 1, p. 4-9.

Bijlage Raamregeling

Het CBP krijgt regelmatig verzoeken van bedrijven en organisaties voor het toetsen van een e-mail- en internetregeling. Dit rapport geeft een aantal vuistregels aan de hand waarvan een organisatie het eigen beleid omtrent controle op het gebruik van e-mail en internet kan toetsen. In de onderstaande raamregeling geeft het CBP een model waarin de vuistregels verder zijn uitgewerkt. De raamregeling is besproken met betrokken partijen zoals werkgevers- en werknemersorganisaties. Deze regeling is bedoeld als hulpmiddel voor organisaties, bedrijven en ondernemingsraden om de vuistregels in het eigen beleid toe te passen.

Het CBP is van oordeel dat de concrete invulling van beleid voor het gebruik van e-mail en internet maatwerk is en daarom binnen de eigen organisatie moet plaats vinden. De raamregeling bevat daarom keuzes die door de organisatie verder ingevuld moeten worden. Waar mogelijk heeft het CBP al een aantal opties vermeld. Natuurlijk kan de regeling ook verder worden gewijzigd of aangevuld, mits een en ander gebeurt binnen het in het rapport *Goed werken in netwerken* beschreven wettelijk kader en de aanpassingen niet strijdig zijn met de WBP en de vuistregels uit dit rapport. Voor de invoering van een regeling met betrekking tot controle op het gebruik van e-mail en internet is instemming van de ondernemingsraad vereist.

De tekst van de raamregeling wordt gevolgd door een toelichting op diverse onderdelen.

Drs. S. Lieon

Raamregeling voor het gebruik van e-mail en internet

Doel van de afspraken

- 1.1. Deze regeling geeft de wijze aan waarop in de organisatie wordt omgegaan met e-mail en internetgebruik. Deze omvat gedragsregels ten aanzien van verantwoord gebruik van e-mail en internet en geeft regels over de wijze waarop controle op e-mail en internetgebruik plaats vindt.
- 1.2. De controle op persoonsgegevens bij gebruik van e-mail en internet vindt plaats met als doel:
 -
 -
 -

Algemene uitgangspunten

- 2.1 De controle op e-mail- en internetgebruik zal overeenkomstig deze afspraak uitgevoerd worden. Indien er zich situaties voordoen waarin deze regeling niet voorziet, zal conform het arbeidsrechtelijk kader en de Wet bescherming persoonsgegevens (WBP) en in overleg met de ondernemingsraad gehandeld worden.
- 2.2 Gestreefd wordt naar een goede balans tussen controle op verantwoord e-mail- en internetgebruik en bescherming van de privacy van werknemers op de werkplek.
- 2.3 Persoonsgegevens gerelateerd aan e-mail en internetgebruik worden niet langer bewaard dan noodzakelijk, met een maximum bewaartermijn van 6 maanden.
- 2.4 De werkgever treft voorzieningen voor de positie en integriteit van de systeembeheerder en/of afdeling systeembeheer en de controle daarop.

E-mailgebruik

- 3.1 Werknemers mogen
- 3.2 Het versturen van e-mailberichten moet voldoen aan de volgende voorwaarden:
 -
 -
 -
- 3.3 Het is niet toegestaan om:
 -
 -
 -

Internetgebruik

- 4.1 Werknemers mogen
- 4.2 Het is niet toegestaan om:

Controle

- 5.1 Controle op e-mail en internetgebruik vindt slechts plaats in het kader van in artikel 1.2 genoemde doelen. Deze doeleinden stellen beperkingen aan de omvang en wijze van controle:
 -
 -
 -
- 5.2 Controle vindt in beginsel plaats op het niveau van getotaliseerde gegevens die niet herleidbaar zijn tot individuele personen. Indien een werknemer of een groep werknemers ervan wordt verdacht de regels te overtreden, kan gedurende een vastgestelde (korte) periode gerichte controle plaats vinden.
- 5.3 Controle beperkt zich in principe tot verkeersgegevens van het gebruik van e-mail en internet. Alleen bij zwaarwegende redenen vindt er controle op de inhoud plaats.
- 5.4 'Verboden' e-mail- en internetgebruik wordt zo veel mogelijk softwarematig onmogelijk gemaakt. Overige controle vindt slechts steekproefsgewijs plaats.
- 5.5 Werknemers ten aanzien van wie geconstateerd is dat zij zich niet aan deze regeling houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken.
- 5.6 E-mailberichten van OR-leden, bedrijfsartsen en andere medewerkers met een vertrouwensfunctie zijn in beginsel uitgesloten van controle. Dit geldt niet voor de controle op de veiligheid van het berichtenverkeer.

Rechten van de betrokkenen

- 6.1 De werkgever informeert de werknemers voorafgaand aan de invoering van de regeling over controle op e-mail- en internetgebruik, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling (zie artikel 33 WBP).
- 6.2 De werknemer kan zich tot de werkgever wenden met het verzoek om een volledig overzicht van zijn verwerkte persoonsgegevens. Het verzoek wordt binnen 4 weken beantwoord. (zie artikel 35, WBP)
- 6.3 De werknemers kan de werkgever verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend, dan wel in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek wordt binnen 4 weken beantwoord (zie artikel 36 WBP).
- 6.4 De werknemer kan bij de werkgever verzet aantekenen tegen de verwerking van zijn persoonsgegevens in verband met bijzondere persoonlijke omstandigheden. De werkgever oordeelt binnen 4 weken na ontvangst van het verzet of dit gerechtvaardigd is. Indien de werkgever het verzet gerechtvaardigd acht, beëindigt hij terstond de verwerking (zie artikel 40 WBP).

Slotbepaling

- 7.1 De werkgever kan deze regeling met instemming van de ondernemingsraad wijzigen. Deze wijzigingen worden schriftelijk vastgelegd en voorafgaand aan de invoering aan de werknemers bekend gemaakt.
- 7.2 Deze regeling wordt jaarlijks geëvalueerd door de werkgever en de ondernemingsraad. De eerstkomende evaluatie vindt plaats voor (datum invullen).

7.3 Deze regeling is tot stand gekomen in overleg met en met instemming van de ondernemingsraad bij besluit van (datum invullen).

Toelichting op de Raamregeling

Algemeen

De invoering van de raamregeling voor het gebruik van e-mail en internet is een besluit waarvoor instemming van de ondernemingsraad nodig is (artikel 27, lid 1 onder 1, WOR). Het CBP heeft een checklist ontwikkeld die de OR een handvat biedt bij de beoordeling van een dergelijke regeling. Deze privacychecklist is te bestellen bij het CBP of te downloaden van de website (www.cbpweb.nl).

Uitleg bij 1.2

Persoonsgegevens mogen slechts voor welbepaalde, duidelijk omschreven en gerechtvaardigde doeleinden verwerkt worden. Deze doelomschrijving moet nauwkeurig en zo volledig mogelijk zijn. In overleg moet worden vastgesteld welke doeleinden voor controle van e-mail- en internetgebruik noodzakelijk zijn voor de eigen organisatie. De privacybelangen van de werknemers horen hierbij meegewogen te worden. In de onderstaande lijst worden de meest voorkomende doeleinden voor controle op e-mail- en internetgebruik opgesomd.

- begeleiding en/of individuele beoordelingen
- bewijs en archivering
- systeem- en netwerkbeveiliging
- bescherming van bedrijfsgeheimen
- voorkomen van negatieve publiciteit
- tegengaan van seksuele intimidatie
- tegengaan van “verboden gebruik”
- kosten- en capaciteitsbeheersing

Uitleg bij 2.2

Controle en gedragsregels ten aanzien van het gebruik van e-mail en internet moet niet los gezien worden van het beleid ten aanzien van andere communicatiemiddelen en controlemaatregelen in de organisatie. Het beleid voor online gedrag moet in overeenstemming zijn met het beleid voor off line gedrag. Niet de technische mogelijkheid van controle, maar de noodzaak dient de vorm en de maat hiervan te bepalen.

Uitleg bij 2.4

De systeembeheerder is als het ware de sleutel tot de persoonsgegevens gerelateerd aan het gebruik van e-mail en internet. Vanuit het oogpunt van de privacy is het belangrijk om afspraken te maken wie in welke gevallen opdracht kan geven tot de controle. Ook de geheimhoudingsplicht (artikel 12, lid 2, WBP) moet ter sprake komen in verband met de eigen integriteit van de systeembeheerder.

Uitleg bij 3.1:

In de raamregeling kunnen gedragsregels worden opgenomen over wat er in de organisatie onder verantwoord e-mailgebruik wordt verstaan. Hieronder treft u een aantal opties aan. Een totaal verbod op het versturen en ontvangen van persoonlijke e-mailberichten is niet mogelijk. Hieronder treft u een aantal opties aan.

- Werknemers mogen het e-mailsysteem gebruiken voor het ontvangen en versturen van persoonlijke e-mailberichten mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk.
- Voor het versturen en ontvangen van persoonlijke e-mailberichten verstrekt de onderneming een apart e-mailadres.
- Werknemers mogen het e-mailsysteem gebruiken voor het ontvangen en versturen van persoonlijke e-mailberichten mits dit beperkt blijft tot ... minuten per dag/week.

- Werknemers mogen het e-mailsysteem gebruiken voor het ontvangen en versturen van persoonlijke e-mailberichten mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk.
- Werknemers mogen incidenteel en kortstondig het e-mailsysteem gebruiken voor het ontvangen en versturen van persoonlijke e-mailberichten mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk.
- Werknemers mogen uitsluitend gebruik maken van het e-mailsysteem voor het ontvangen en versturen van persoonlijke e-mailberichten in situaties waar uitstel van deze communicatie niet mogelijk en onredelijk is.
- Etc.

Uitleg bij 3.2

In de raamregeling kunnen gedragsregels worden opgenomen onder welke voorwaarden verantwoord e-mailgebruik moet plaats vinden. Hieronder treft u een aantal opties aan.

- Een correcte vermelding van afzender
- Het meesturen van een disclaimer
- Duidelijke onderwerpaanduiding indien het een privé-mail betreft
- Verbod op het meesturen van attachments
- Etc.

Uitleg bij 3.3

In de raamregeling kunnen gedragsregels worden opgenomen over wat niet toegestaan is bij een verantwoord e-mailgebruik. Hieronder treft u een aantal opties aan.

- Dreigende, beledigende, seksueel getinte dan wel discriminerende berichten te versturen
- Kettingbrieven versturen
- Etc.

Uitleg bij 4.1

In deze raamregeling kunnen gedragsregels worden opgenomen over wat er in de organisatie onder verantwoord internetgebruik wordt verstaan. Hieronder treft u een aantal opties aan. Een totaal verbod op internetgebruik voor persoonlijke doeleinden is in strijd met artikel 8 EVRM niet mogelijk.

- Voor het gebruik van het internetsysteem voor persoonlijke doeleinden stelt de onderneming een aparte computer beschikbaar die zich(plaats invullen) bevindt. Het is niet toegestaan om de computer op de eigen werkplek hiervoor te gebruiken.
- Werknemers mogen het internetsysteem voor persoonlijke doeleinden te gebruiken, mits dit beperkt blijft tot ... minuten per dag/week.
- Werknemers mogen het internetsysteem voor persoonlijke doeleinden gebruiken mits niet storend voor de dagelijkse werkzaamheden en het computernetwerk.
- Werknemers mogen incidenteel en kortstondig het internetsysteem voor persoonlijke doeleinden gebruiken mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk.
- Werknemers mogen uitsluitend gebruik maken van het internetsysteem voor persoonlijke doeleinden in situaties waar uitstel van deze communicatie niet mogelijk en onredelijk is.
- Etc.

Uitleg bij 4.2

In de raamregeling kunnen gedrageregels worden opgenomen over wat niet toegestaan is bij een verantwoord internetgebruik. Hieronder treft u een aantal opties aan.

- Bewust sites bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten.
- Op internet in strijd met de wet of onethisch handelen.
- Software en applicaties downloaden.
- Etc.

Uitleg bij 5.1

Beschrijf op welke wijze de controle plaats vindt in relatie tot de geselecteerde doeleinden. Hieronder staan een aantal opties beschreven.

- In het kader van begeleiding en/of individuele beoordelingen vindt er steekproefsgewijs controle plaats van zakelijke e-mailberichten zoals overeengekomen met de individuele werknemer.
- Conform de bedrijfsregels maakt de ...(invullen: individuele medewerker / secretariaat / administratie) een kopie van de zakelijke e-mailberichten met als doel bewijs en/of archivering.
- Voor het tegengaan van virussen en andere schadelijke programma's, in het kader van systeem- en netwerkbeveiliging, wordt het e-mail en internetgebruik op geautomatiseerde wijze gecontroleerd.
- Controle op het uitlekken van bedrijfsgeheimen vindt plaats op basis van steekproefsgewijze contentfiltering. Een verdacht bericht wordt apart gezet voor nader onderzoek.
- Controle in het kader van het voorkomen van negatieve publiciteit vindt plaats op basis van contentfiltering. Verdachte berichten worden geautomatiseerd terug gestuurd naar de afzender en "verboden" sites geblokkeerd.
- Controle in het kader van het tegengaan van seksuele intimidatie vindt op geautomatiseerde wijze plaats. Verdachte berichten worden geautomatiseerd terug gestuurd naar de afzender.
- Controle in het kader van het tegengaan van 'verboden gebruik' vindt in beginsel geanonimiseerd en slechts steekproefsgewijs plaats.
- Controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot verkeersgegevens (tijd, hoeveelheid, omvang, en dergelijke).

Uitleg bij 6.2 en 6.3

Wanneer er in de onderneming reeds een klachtenregeling of klachten- cq beroepscommissie aanwezig is, kan hiernaar verwezen worden bij problemen met betrekking tot de rechten van de betrokkenen en de naleving van deze raamregeling. Dit betekent dat een werknemer aan wie bijvoorbeeld inzage in diens gegevens is geweigerd, zich hiervoor tot de klachtencommissie kan wenden, ongeacht de rechtsbescherming op grond van hoofdstuk 8 van de WBP.

Bijlage Achtergrondstudies en Verkenningen

In de serie Achtergrondstudies en verkenningen zijn verschenen:

Eijk, M.M.M. van en Helden, W.J. van, **Klant te koop, Privacyregels voor adressenhandel.** A&V 24; College bescherming persoonsgegevens, Den Haag 2001.

Blarkom, G.W. van, **Beveiliging van persoonsgegevens.** A&V 23; Registratiekamer, Den Haag 2001.

Versmissen, J.A.G., **Sleutels van vertrouwen, TTP's, digitale certificaten en privacy.** A&V 22; Registratiekamer, Den Haag 2001.

Terstegge, J.H.J., **Goed werken in netwerken, regels voor controle op e-mail en internetgebruik van werknemers.** A&V 21; Registratiekamer, Den Haag 2000.

Buitenhuis, R., Campen, N.G.M. van, Helden, W.J. van, Vries, H.H. de, **Bankverzekeraars en privacy, gegevensverwerking in financiële conglomeraten.** A&V 20; Registratiekamer, Den Haag 2000.

Helden, W.J. van, **Herkomst van de klant, privacyregels voor etnomarketing.** A&V 19; Registratiekamer, Den Haag 2000.

Wishaw, R.W.A. **De gewaardeerde klant, privacyregels voor credit scoring.** A&V 18; Registratiekamer, Den Haag 2000.

Artz, M. en Eijk, M.M.M. van, **Klant in het web. Privacywaarborgen voor internettoegang.** A&V 17; Registratiekamer, Den Haag 2000.

Zeeuw, J. de. **Informatieverstrekking. Ontheffing van de fiscale geheimhoudingsplicht in het licht van privacywetgeving.** A&V 16; Registratiekamer, Den Haag 2000.

Hes, R., Borking, J.J. en Hooghiemstra, T.F.M. **At face value. On biometrical identification and privacy.** A&V 15; Registratiekamer, Den Haag 1999.

Artz, M.J.T., **Koning Klant. Het gebruik van klantgegevens voor marketingdoeleinden.** A&V 14; Registratiekamer, Den Haag 1999.

Borking, J.J., e.a., **Intelligent software agents and privacy.** A&V 13; Registratiekamer, Den Haag 1999.

Hooghiemstra, T.F.M., **Privacy & Managed care.** A&V 12; Registratiekamer, Den Haag 1998.

Hes, R. en J. Borking, **Privacy-enhancing technologies: the path to anonymity.** A&V 11 revised edition; Registratiekamer, Den Haag 1998.

Almelo, L. van, e.a., **Gouden bergen van gegevens. Over datawarhousing, datamining en privacy.** A&V 10; Registratiekamer, Den Haag 1998.

Zandee, C., **Doelbewust volgen. Privacy-aspecten van cliëntvolgsystemen en andere vormen van gegevensuitwisseling.** A&V 9; Registratiekamer, Den Haag 1998.

Zeeuw, J. de, **Informatiegaring door de fiscus. Privacybescherming bij derdenonderzoeken.** A&V 8; Registratiekamer, Den Haag 1998.

Hulsman, B.J.P. en P.C. Ippel, **Gegeven: de Genen. Morele en juridische aspecten van het gebruik van genetische gegevens.** A&V 7; Registratiekamer, Den Haag 1996.

Gardeniers, H.J.M., **Chipcards en privacy. Regels voor een nieuw kaartspel.** A&V 6, Registratiekamer, Den Haag 1995.

Rossum, H. van e.a., **Privacy-enhancing technologies: the path to anonymity, volume I and II.** A&V 5; Registratiekamer, Den Haag 1995.

Rommelse, A.F., **Zwarte lijsten. Belangen en effecten van waarschuwingssystemen.** A&V 4; Registratiekamer, Rijswijk 1995.

Rommelse, A.F., **Ziekteverzuim en privacy. Controle door de werkgever en verplichtingen van de werknemer.** A&V 3; Registratiekamer, Rijswijk 1995.

Casteren, J.P.M. van, **Bevolkingsgegevens: Wie mag ze hebben? Verstrekking van gegevens uit de GBA aan vrije derden.** A&V 2; Registratiekamer, Rijswijk 1995 (niet meer beschikbaar).

Hulsman, B.J.P. en Ippel, P.C., **Personeelsinformatiesystemen - de Wet persoonsregistraties toegepast.** A&V 1; Registratiekamer, Rijswijk 1994 (niet meer beschikbaar).

Vrijwel alle publicaties van het CBP kunt u inzien en/of downloaden van de website www.cbpweb.nl. Voor het toezenden van gedrukte publicaties kunnen verzend- en handlingkosten in rekening worden gebracht.