

Het Emailgeheim op de werkplek

Over de toelaatbaarheid van inbreuken op het communicatiegeheim van de werknemer in het digitale tijdperk

mr L.F. Asscher en mr drs W.A.M. Steenbruggen*

Inleiding

De verhouding tussen werknemer en werkgever bij Internetgebruik is een *hot issue*. Mag de ‘baas’ zomaar meelezen? Weten “ze” precies waar ik heen gesurft ben? Er bestaat nogal wat onduidelijkheid over de toelaatbaarheid van controle van email- en internetverkeer door de werkgever.

In dit artikel onderzoeken wij of en onder welke voorwaarden de werkgever de bevoegdheid heeft kennis te nemen van de inhoud van de door zijn werknemers verzonden email. Is een procedure denkbaar waarbij privacybelangen van de werknemer gerespecteerd worden? De eerste vraag is wat de juridische betekenis van het grondrecht op bescherming van de persoonlijke levenssfeer op de werkplek is. Hoewel grondrechten in de eerste plaats als bescherming tegen de overheid bedoeld zijn, wordt algemeen aangenomen dat de werknemer ook niet rechteloos is tegenover de werkgever. Door sommigen is wel gepleit voor directe werking van grondrechten in de arbeidsverhouding in verband met de gezagsverhouding tussen werkgever en werknemer. In ieder geval gelden de grondrechten via de open normen van het civiele recht.

De tweede vraag is of emailverkeer op dezelfde manier gecontroleerd mag worden als bijvoorbeeld telefoonverkeer. Hieronder volgt eerst een beschrijving van de bescherming van het emailgeheim als onderdeel van het privacyrecht. Vervolgens gaan wij in op de status van privacy op de werkplek. Tenslotte komen wij tot enige aanbevelingen.

Emailprivacy: een grondrecht

Het recht op privacy is neergelegd in de Grondwet, in verdragen en in lagere wettelijke regelingen.

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. In *Klass* bepaalde het EHRM dat ook telefoonverkeer onder de bescherming van artikel 8 valt. Het Hof kiest daarbij niet voor een extensieve interpretatie van het begrip correspondentie maar voor een combinatie van privé-leven en correspondentie.¹ In *Malone* gaf het Hof aan dat ook *metering records* en in het bijzonder het gekozen telefoonnummer integraal deel uitmaken van de beschermde communicatie.²

* mr L.F. Asscher en mr drs W.A.M. Steenbruggen zijn als projectonderzoeker verbonden aan het Instituut voor Informatierecht, Universiteit van Amsterdam

¹ J.A. Hofman, *Vertrouwelijke communicatie. Een rechtsvergelijkende studie over de geheimhouding van communicatie in grondrechtelijk perspectief naar internationaal, Nederlands en Duits recht*, Zwolle; W.E.J. Tjeenk Willink 1995, p. 70-72; EHRM 6 september 1978 (*Klass*); R.A. Lawson en H.G. Schermers, *Leading cases of the European Court of Human Rights*, Nijmegen: Ars Aequi Libri e.a. 1997, p. 66-67.

² EHRM 2 augustus 1984 (*Malone*), NJ 1988, 534; Hofman 1995, p. 70-71; A.J. Nieuwenhuis, ‘Vertrouwde en virtuele bescherming’, *NJCM-Bulletin* 4, 1998, p. 429..

Over nieuwere communicatiemiddelen zijn nog geen uitspraken. Over het algemeen wordt echter aangenomen dat het EHRM te zijner tijd door een verdragsdynamische interpretatie ook email onder artikel 8 zal brengen.³

In *Niemitz*⁴ bepaalde het EHRM dat werknemers een gerechtvaardigd belang hebben 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. Artikel 8 EVRM beschermt het individu niet alleen tegen inbreuken door de overheid, maar tegen inbreuken door particulieren, zoals werkgevers. In *Halford* maakt het Hof duidelijk dat ook telefoongesprekken, gevoerd met een zakelijk toestel, of onder een zakelijk nummer, onder de bescherming van artikel 8 vallen.⁵ 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 standaardcontrole van de telefoons van het politiebureau. Uit het bewijs dat in de rechtszaak was overlegd, kon worden afgeleid dat de werkgever waarschijnlijk de gesprekken die via de speciale telefoon waren gevoerd, 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. Het enkele bekend zijn van de mogelijkheid tot meeluisteren of opnemen rechtvaardigt op zichzelf het gebruik daarvan evenwel niet. Kenbaarheid van de (mogelijkheid tot) controle is niet meer dan een basisvoorwaarde voor de rechtmatigheid ervan.

In de zaak *Edamse Bijstandsmoeder*⁶ heeft de Hoge Raad in 1987 expliciet erkend dat het recht op eerbiediging van de persoonlijke levenssfeer indirecte horizontale werking heeft. Hierin heeft de Hoge Raad ten aanzien van art. 8 EVRM aangenomen dat het ook werking heeft tussen burgers onderling. Aangenomen mag derhalve worden dat dit ook voor het in art. 8 EVRM opgesloten emailgeheim zal gelden.

In Nederland beschermt artikel 13 Grondwet het brief- telefoon- en telegraafgeheim. De meningen verschillen over de vraag of een extensieve interpretatie van artikel 13 Grondwet ook email onder het bestaande artikel kan brengen. Als dat al zou kunnen, is nog onduidelijk of email dan onder het eerste lid (briefgeheim) of het tweede lid (telefoon -en telegraafgeheim) zou moeten vallen. Dat maakt wel wat uit, aangezien het beschermingsregime in het eerste lid sterker is dan dat in het tweede.

De vraag of email onder het briefgeheim valt, kwam al in 1997 aan de orde in een kamervraag aan toenmalig minister van Justitie Sorgdrager.⁷ Zij antwoordde ontkennend en gaf zo het startsein van een constitutionele discussie die sindsdien voortduurt.

Qua techniek lijkt email het meest op de telegraaf. Email wordt namelijk pakketgeschakeld via het *store and forward*-principe naar de plaats van bestemming gestuurd. Het bericht wordt opgedeeld in verscheidene pakketjes die vervolgens naar de plaats van bestemming worden gerouteerd.⁸ Elk van deze pakketjes kan daarbij een andere route volgen. De bij telegrafie gebruikte transporttechniek heet *message switching*. Daarbij wordt een bericht eerst omgezet

³ Zie bijvoorbeeld al Hofman 1995, p.71-72. Zie ook H.H. de Vries, 'Vertrouwelijkheid van e-mail in arbeidsverhoudingen', p. 116-117. In H.W.K Kaspersen & C. Stuurman, *Juridische aspecten van e-mail*, Deventer: Kluwer 2001, p. 111-139.

⁴ EHRM 16 december 1992 (*Niemitz*), NJ 1993, 400

⁵ EHRM 25 juni 1997 (*Halford*), NJ 1998, 506.

⁶ HR 19 januari 1987, NJ 1987, 928, m.nt. E.A. Alkema (*Edamse bijstandsmoeder*).

⁷ *Aanhangsel Handelingen II* 1995/96, nr. 1370; L.F. Asscher, 'Email een ansichtkaart?', *Mediaforum* 1997-7/8, p. 103.

⁸ Vgl. Tom Standage, *The Victorian Internet: the remarkable story of the telegraph and the nineteenth century's online pioneers*, New York: Walker and company, 1998.

in elektronische pulsen die vervolgens naar een tussenstation worden verzonden. Daar wordt het bericht ontvangen, opgeslagen en vervolgens naar het volgende station verzonden. Dit wordt herhaald totdat het bericht op de plaats van bestemming is aangekomen. Gezien de overeenkomsten in de transporttechniek zou email wellicht met een extensieve interpretatie onder het telefoon –en telegraafgeheim gebracht kunnen worden. Echter, de techniekafhankelijkheid van artikel 13 en de verschillende gradaties van bescherming, daarbij de uitspraak van de minister in aanmerking genomen, zorgen ervoor dat voor de bescherming van email niet veel van het huidige grondwetsartikel te verwachten valt.

Het kabinet kwam later in 1997 met een voorstel tot wijziging van artikel 13 Grondwet waarin email wel beschermd zou zijn. Als voorwaarde voor bescherming gold dan wel dat de emailberichten versleuteld moesten zijn. Dit voorstel werd dusdanig kritisch ontvangen dat het moest worden ingetrokken. Voordat dat gebeurde was het voorstel door de Tweede Kamer al grondig geamendeerd. Een staatscommissie werd vervolgens verzocht advies uit te brengen over de gehele problematiek van ‘grondrechten in het digitale tijdperk’. Deze commissie Franken bracht in 2000 advies uit dat (althans op het punt van artikel 13) grotendeels werd gevolgd door het kabinet.

In de voorstellen van het kabinet wordt het briefgeheim vervangen door een recht op vertrouwelijke communicatie. Uit de toelichting blijkt dat email daar in beginsel ook onder valt.⁹ Daarnaast bevat het voorstel een opdracht aan de wetgever om er voor te zorgen dat het recht op vertrouwelijke communicatie ook in horizontale verhoudingen wordt gegarandeerd. “Met de commissie is het kabinet van oordeel dat er behoefte bestaat aan een sterkere doorwerking van het communicatiegrondrecht in de verhoudingen tussen burgers onderling.”¹⁰ Het kabinet geeft echter niet aan hoe die zorg moet worden ingevuld.

Desgevraagd antwoordde het kabinet aan de Tweede Kamer dat ‘uit de arbeidsverhouding voortvloeit dat een werknemer bepaalde aanspraken op bijvoorbeeld respect voor zijn persoonlijke levenssfeer en zijn recht op vertrouwelijke communicatie, opgeeft in een arbeidsrelatie. Een werknemer levert deze aanspraken echter niet volledig in. Ook tijdens werktijd moet een werknemer relaties met anderen kunnen onderhouden, onder meer door communicatie zonder inmenging door de werkgever.’¹¹ Dit werkt het kabinet niet verder uit. Belangrijk is echter wel dat het kabinet hier expliciet erkent dat een werknemer ook op de werkplek een recht heeft privé te communiceren, zij het dat dit recht beperkt kan worden. Dit is zoals we gezien hebben in overeenstemming met de jurisprudentie van het EVRM.

Wel merkt het kabinet nog op dat ‘controlemaatregelen door de werkgever met betrekking tot emailgebruik van werknemers [...] overigens alleen wederrechtelijk in de zin van deze bepalingen [zijn] wanneer sprake is van kennelijk misbruik van de controlemiddelen door de werkgever.’

Uit de jurisprudentie ten aanzien van art. 8 EVRM en de discussie omtrent een nieuw artikel 13 Grondwet kunnen twee voor dit artikel belangrijke uitgangspunten gedestilleerd worden.

Het eerste uitgangspunt is dat een werknemer een recht heeft in beperkte mate gebruik te maken van de communicatiefaciliteiten op de werkplek. Een tweede uitgangspunt is dat email in de nabije toekomst aanspraak kan maken op grondwettelijke en verdragsrechtelijke bescherming. Een vraag die vervolgens beantwoord moet worden is hoe het emailgeheim in verhoudingen tussen burgers onderling zijn werking doet gelden. We zullen dus moeten nagaan of email door wettelijke regelingen beschermd wordt of dat de genoemde fundamentele rechten doorwerken

⁹ Het voert te ver hier de precieze implicaties van de objectomschrijving van het voorgestelde artikel 13 Grondwet te beschrijven. Zie daarvoor: L.F. Asscher, ‘Trojaans hobbelpaard’, *Mediaforum* 2000-7/8, p. 228-233; E.J. Dommering, ‘De nieuwe Nederlandse Constitutie en de informatietechnologie’, *Computerrecht* 2000-4, p. 177-185; F. Kuitenbrouwer, ‘Hoe sterk zijn de digitale grondrechten’, *Computerrecht* 2000-4, p. 172-176; J.M. De Meij, ‘grondrechten in het digitale tijdperk’, *NJCM-Bulletin* 2001-3, p. 274-294.

¹⁰ *Kamerstukken II*, 27460, nr 1, p. 29.

¹¹ *Kamerstukken II*, 27460, nr 2, p. 50-51.

in de verhouding tussen werknemer en werkgever. Pas bij een bevestigend antwoord op één van beide vragen zal onderzocht kunnen worden in hoeverre het emailgeheim een belemmering vormt voor controle door de werkgever.

Dat grondrechten in verhoudingen tussen burgers onderling kunnen doorwerken, is door de Grondwetgever expliciet erkend. De regering introduceerde bij de Grondwetwijziging van 1983 een glijdende schaal met verschillende gradaties van horizontale werking, variërend van directe horizontale werking tot een opdracht aan de wetgever of overheid om een nader geformuleerd belang ook in particuliere verhoudingen te verwezenlijken.¹² In hoeverre individuele grondrechten in verhoudingen tussen burgers onderling doorwerken, gaf zij echter niet aan.

De glijdende schaal komt voort uit de definitie die de regering met betrekking tot horizontale werking hanteert. Van horizontale werking is sprake in alle gevallen waarin grondrechten rechtens relevant zijn. Verhey komt tot de conclusie dat de glijdende schaal in de praktijk niet zo functioneert. In plaats daarvan kan men een driedeling in de jurisprudentie constateren: uitspraken waarin directe werking wordt aangenomen, die waarin sprake is van indirecte werking en tenslotte uitspraken waarin van doorwerking van grondrechten op het eerste gezicht niets blijkt, maar waarin het grondrechtelijk gezichtspunt impliciet wel een rol speelt in de privaatrechtelijke rechtsvinding.¹³ Directe werking betekent dat grondrechten op dezelfde manier in horizontale verhoudingen doorwerken als in verticale verhoudingen. Over het algemeen wordt deze vorm afgewezen, onder meer omdat beperkingen op het grondrecht herleidbaar tot de grondwettelijke bijzondere beperkingsclausules moeten zijn, nu bij de grondwetsherziening de leer van de algemene beperkingen is afgewezen.¹⁴ Sinds 1983 blijkt dat wetgever en rechter ongeschreven beperkingen aanvaarden of hun toevlucht zoeken in een restrictieve interpretatie. In plaats van strikte toepassing van het grondwettelijke systeem wordt steeds meer een belangenafweging *in concreto* toegepast.¹⁵ Daarmee ontwikkelt de grondrechtelijke beperkingsmethodiek zich in de richting van een noodzakelijkheidstoetsing à la het EVRM.¹⁶ Zet deze ontwikkeling door, dan ontvalt bovengenoemd argument tegen directe horizontale werking alle grond.

Ook voor het emailgeheim zal dus in beginsel horizontale werking kunnen worden aangenomen. Wanneer wettelijke regelingen voldoende bescherming aan het emailgeheim bieden, zal doorwerking van het emailgeheim echter minder noodzakelijk zijn. Zijn er in het arbeidsrecht echter specifieke wettelijke regelingen te vinden waarop de werknemer zich kan beroepen ter bescherming van zijn privacy-aanspraken tijdens werktijd? Dat is de vraag die we in de volgende paragrafen willen beantwoorden. Het eerst komen voor bespreking in aanmerking de wettelijke regeling van de arbeidsovereenkomst en de Wet op de ondernemingsraden. In hoeverre bieden deze de werknemer bescherming?

Arbeidsrechtelijke regelingen

In boek 7 titel 10 BW wordt de arbeidsovereenkomst geregeld. Een bepaling die de privacy van de werknemer op de werkvloer beschermt, komt daarin niet voor. Wel is een algemene instructiebevoegdheid van de werkgever opgenomen. 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, aldus art. 7: 660 BW. Op basis hiervan mag hij in beginsel ook het gebruik van email en Internet reguleren en controleren. Deze

¹² *Aanhangsel Handelingen II* 1975/1976, nr. 3. Zie ook J.A. Hofman 1995, p. 131.

¹³ L.F.M. Verhey, *Horizontale werking van grondrechten, in het bijzonder van het recht op privacy*, Zwolle: W.E.J. Tjeenk Willink 1992, p. 180 e.v.

¹⁴ Verhey, p. 155.

¹⁵ Verhey, p. 28.

¹⁶ Zie ook F.H. Kistenkas, 'Naar een grondrechtelijke evenredigheidstoets', *Gemeentestem* 1991, nr. 6925, p. 377 e.v.

bevoegdheid kan echter niet ongelimiteerd zijn. Dat verdraagt zich niet met de hierboven door ons geschetste uitgangspunten. Het recht op privacy en het communicatiegeheim zullen aan deze werknemersbevoegdheid grenzen stellen.

De ondernemer heeft op grond van art. 27 lid 1 sub k en l WOR toestemming van de ondernemingsraad nodig voor een voorgenomen besluit tot vaststelling, wijziging of intrekking van regelingen ten aanzien van registratie van en omgang met persoonsgegevens en regelingen ten aanzien van personeelsvolgsystemen. Onder personeelsvolgsystemen verstaat de wet *voorzieningen die gericht zijn op of geschikt zijn voor waarneming van of controle op aanwezigheid, gedrag, prestaties van de in de onderneming werkzame personen; een en ander voorzover betrekking hebbende op alle of een groep van de in onderneming werkzame personen*. Ook een intranet is geschikt voor registratie en observatie van het personeel en als zodanig een personeelsvolgsysteem. Als een dergelijk systeem eenmaal met toestemming van de ondernemingsraad is ingevoerd, houdt de inspraak van de OR op. Dit artikel ziet niet op het gebruik van de met behulp van het systeem verkregen gegevens. Veel waarborgen voor de privacy of het communicatiegeheim biedt het artikel dus niet. Overigens bindt de instemming van de ondernemingsraad de individuele werknemers niet.

Voorts kan nog gewezen worden op art. 25 lid 1 k WOR dat de ondernemer verplicht de ondernemingsraad tijdig om advies te vragen in aangelegenheden die belangrijke technologische vernieuwingen impliceren.

Een arbeidsrechtelijke regeling die op een adequate manier de privacy-aanspraken van de werknemer beschermt, is er op dit moment dus niet. Wellicht bieden algemene wettelijke regelingen de werknemer soelaas.

Algemene wettelijke regelingen

De bescherming van de privacy en het communicatiegeheim bij computergebruik is uitgewerkt in het Wetboek van Strafrecht.¹⁷ Als deze artikelen al van toepassing zijn op de maatregelen die een werkgever neemt ter controle van email -en internetgebruik van werknemers, geldt dat de controle door de werkgever niet wederrechtelijk is, aangezien hij de gerechtigde tot de aansluiting is. Dit is alleen anders wanneer sprake is van kennelijk misbruik van de controlemiddelen door de werkgever.

De informatiele privacy wordt beschermd in de Wet Bescherming Persoonsgegevens, die op 1 september 2001 in werking is getreden. Gegevens met betrekking tot email -en internetgebruik van de werknemers zijn in veel gevallen te kwalificeren als persoonsgegevens. Immers, ze zijn meestal tot de persoon herleidbaar. Artikel 7 WBP bepaalt dat het verzamelen van dergelijke gegevens uitsluitend is toegestaan ten behoeve van een welbepaald uitdrukkelijk omschreven en gerechtvaardigd doel. Emailgebruik leidt tot een verzameling persoonsgegevens, aangezien deze gegevens gedurende enige tijd zullen worden bewaard. In de praktijk komt art. 7 Wbp erop neer, dat de werkgever vooraf doel en omvang van een controle zal moeten vaststellen. Bovendien moet de controle proportioneel zijn.¹⁸

In de artikelen 33 en 34 WBP is een informatieplicht opgenomen die vereist dat de werkgever zijn werknemers, zowel individueel als collectief, van de controle op de hoogte stelt. Een dergelijke kennisgeving zou bijvoorbeeld op het moment van inloggen op het bedrijfsnetwerk kunnen plaatsvinden.¹⁹ Daarnaast heeft de werknemer het recht de over hem verzamelde

¹⁷ Zie bijvoorbeeld artikel 138a: computervredebreuk, artikel 139b: aftappen / opnemen van gegevensoverdracht, artikel 139c: aftappen / opnemen van gegevensoverdracht via telecommunicatienetwerk, artikel 350a: ontoegankelijk maken computergegevens

¹⁸ Vgl. art. 8 sub f WBP; Zie meer uitvoerig over de betekenis van de Wbp voor emailgebruik op de werkplek H.H. de Vries 2001, p. 127-132

¹⁹ Zie J.H.J. Terstegge, *Goed werken in netwerken. Regels voor controle op e-mail- en internetgebruik door werknemers*, Registratiekamer 2000.

gegevens in te zien en te corrigeren. De werkgever is bovendien verplicht de verwerking van persoonsgegevens te melden bij het College Bescherming Persoonsgegevens, indien hij van plan is de inhoud van email te gaan controleren.²⁰

De Wbp is een kaderwet: de wettelijke bepalingen zijn algemeen omschreven. Omdat zij niet steeds concrete gedragsvoorschriften bevatten, maar een belangenafweging op grond van bepaalde criteria voorschrijven, zal de werkgever, als verantwoordelijke voor de gegevensverwerking, deze in het concrete geval moeten maken. Tot een adequate belangenafweging zal hij echter niet in staat zijn, wanneer het hem aan het benodigde inzicht in de materie ontbreekt.

Tenslotte is de Telecommunicatiewet van belang als lagere regeling waarin het emailgeheim beschermd wordt. In artikel 18.13 Tw wordt aanbieders verplicht ook in horizontale verhoudingen het emailgeheim te respecteren. Dit artikel geldt echter alleen voor aanbieders van openbare telecommunicatiediensten en –netwerken.

Algemene wettelijke regelingen bieden zoals is gebleken de werknemer in de praktijk slechts een beperkte bescherming. De Wbp kan daarin verandering brengen, de werkgever moet immers in het kader van de Wbp nagaan of zijn belang bij controle een beperking van het emailgeheim rechtvaardigt. In dat verband is het belangrijk na te gaan of het emailgeheim doorwerkt in de arbeidsovereenkomst.

Horizontale werking van het emailgeheim

In de arbeidsrechtelijke literatuur wordt gepleit voor betere waarborgen ten aanzien van de grondwettelijke vrijheden van de werknemer.²¹ De reden is dat de verhouding van de werknemer tot de werkgever verticaal getint is.²² De werknemer is in sterke mate afhankelijk van de werkgever, zowel in financieel-economisch als in sociaal opzicht. Daarnaast heeft de werkgever een instructiebevoegdheid ten opzichte van de werknemer. Een gezagsverhouding is immers bepalend voor het bestaan van een arbeidsovereenkomst.²³ Verhulp pleit mede daarom voor directe werking van grondrechten in het arbeidsrecht.²⁴

De werknemer kan in de uitoefening van zijn grondwettelijke vrijheden op verschillende wijzen beperkt worden. Allereerst kan de werkgever de uitoefening eenzijdig beperken door bijvoorbeeld gegevens uit de persoonlijke levenssfeer van de werknemer te registreren. Ook kan uitoefening van een grondrecht beperkt worden doordat een werknemer daarmee instemt. Ten aanzien van het laatste moet echter de nodige terughoudendheid betracht worden. De werknemer zal in veel gevallen immers niet in staat zijn vooraf geheel te overzien hoever een grondrechtsbeperking kan gaan.

Wij gaan ervan uit dat het recht op privacy en het communicatiegeheim in elk geval indirect tussen burgers onderling werken, doordat zij zich in de open normen van het privaatrecht als af te wegen belangen manifesteren. Op grond van art. 3:12 BW moet de rechter bij uitleg van de open normen van het BW teruggrijpen op algemeen erkende rechtsbeginselen.²⁵ Grondrechten vormen een directe uitdrukking van dergelijke rechtsbeginselen en dienen als zodanig zwaar te wegen in een rechterlijke belangenafweging. Bij de rechterlijke oordeelsvorming kunnen de aard van het grondrecht, de aard van de rechtsbetrekking en de evenredigheidstoets een rol

²⁰ De werkgever moet ook rekening houden met artikel 18.13 Telecommunicatiewet, indien de dienst ook aan het publiek wordt aangeboden, bijvoorbeeld in geval van een ISP.

²¹ E. Verhulp, *Grondrechten in het arbeidsrecht*, Deventer: Kluwer 1999, p. 61-64; P.F. van der Heijden, *Grondrechten in de onderneming*, Deventer: Kluwer 1988; G.A.I. Schuijt, *Werkers van het woord: media en arbeidsverhoudingen in de journalistiek*, Deventer: Kluwer 1987.

²² Zie ook A-G Mok in zijn noot bij HR 30 maart 1984, NJ 1985, 350 (*Venhorst/Inan*)

²³ P.F. van der Heijden, 'De definitie van de arbeidsovereenkomst in art. 610boek 7 NBW', P.F. van der Heijden (red.), I.P. Asscher-Vonk, M.M. Olbers, T. van Peijpe, *De arbeidsovereenkomst in het NBW*, Deventer: Kluwer 1991, p. 41-56.

²⁴ E. Verhulp, *Vrijheid van meningsuiting van werknemers en ambtenaren*, Den Haag: Sdu 1996, p. 31-32.

²⁵ HR 8 april 1994, NJ 1994, 704 (*Agfa/Schoolderman*).

spelen. De aard van het grondrecht is van belang voor de doorwerking. Het ene grondrecht leent zich nu eenmaal beter voor doorwerking in een civielrechtelijke verhouding dan het andere.²⁶ Ten aanzien van het brief-, telefoon- en telegraafgeheim en dus ook het emailgeheim als daarvan afgeleide vorm kan worden aangenomen dat het ook in de relatie werkgever-werknemer kan worden toegepast. Van oudsher ziet het geheim op privé-communicatie *die ter transport aan een derde wordt toevertrouwd*. Vroeger was dat het Staatsbedrijf der PTT, tegenwoordig zijn dat particuliere partijen. De ratio van het grondrecht blijft echter onverminderd geldig.

De aard van de rechtsbetrekking is mede van belang om te bepalen of de beperking van het grondrecht geoorloofd is. De werknemer dient rekening te houden met de gerechtvaardigde belangen van de werkgever en vice versa. In de evenredigheidstoets komt de belangenafweging tot uitdrukking. Beperkingen moeten geschikt zijn om een bepaald doel te bereiken, proportioneel zijn en mogen niet verder gaan dan strikt noodzakelijk is. Dit geldt ook voor beperkingen op het emailgeheim.

Goed werkgeverschap

In boek 7 titel 10 BW is een aantal open normen te vinden. Het ontslagrecht kent bijvoorbeeld beëindiging van de arbeidsovereenkomst wegens een dringende reden. Een andere open norm is het goed werkgeverschap van art. 7: 611 BW. De werkgever en de werknemer zijn over en weer verplicht zich als een goed werkgever en een goed werknemer te gedragen.

Art. 7: 611 BW beslaat de meest uiteenlopende verplichtingen van de werkgever, van minimale tot uiterst zwaarwichtige, zoals het eerbiedigen van de grondrechten van zijn werknemers.²⁷ Indirecte werking werd door de rechter in een aantal gevallen gehonoreerd. Een voorbeeld biedt de zaak *Agfa/Schoonderman*.²⁸ In deze zaak ging het om een oproepkracht die op uurloonbasis betaald werd en al jarenlang bijna de volledige werktijd voor Agfa gewerkt had. Zij vond dat ze er recht op had op dezelfde manier behandeld te worden als het personeel in vaste dienst. Agfa voerde in cassatie aan dat het gelijkheidsbeginsel zoals neergelegd in art. 1 Gw niet horizontaal werkte. De Hoge Raad oordeelde dat dit middel niet tot cassatie kon leiden, omdat de Rechtbank slechts het algemene rechtsbeginsel dat gelijke arbeid in gelijke omstandigheden op gelijke wijze moet worden beloond, in aanmerking heeft genomen. Hiertoe was de Rechtbank op grond van art. 3: 12 BW zelfs verplicht, aldus de Hoge Raad.

Ten aanzien van het recht op privacy kan gewezen worden op de *Koma*-zaak.²⁹ Het bedrijf Koma had camera's laten monteren die praktisch het hele bedrijf konden gadeslaan. Deze observatie had tot doel om bij technische problemen direct in te kunnen grijpen en ook om de kwaliteit van eindproducten te bewaken. Later in de procedure werd als reden voor de camerabewaking aangevoerd dat af en toe een productieoverzicht beschikbaar zou komen. De rechter overwoog dat een belang van de werkgever dat duidelijk opwoog tegen dat van de werknemers bij bescherming van hun persoonlijke levenssfeer niet aanwezig was. In hoger beroep kwam het Hof Den Bosch tot hetzelfde resultaat.³⁰ Het Hof toetste echter niet aan het recht op privacy, maar enkel aan het goed werkgeverschap.

Grondrechten kunnen dus via het goed werkgeverschap doorwerken in het arbeidsrecht. Dat is ook in de jurisprudentie erkend. Inmiddels zijn ook een aantal zaken met betrekking tot email- en internetgebruik op de werkplek gepubliceerd. We zullen deze hieronder bespreken om na te gaan in hoeverre het emailgeheim in rechte wordt gerespecteerd.

²⁶ Verhey, p. 174.

²⁷ M.A.C. de Wit, *Het goed werkgeverschap als intermediair van normen in het arbeidsrecht*, (diss.) Tilburg 1999, p. 137.

²⁸ HR 8 april 1994, *NJ* 1994, 704.

²⁹ Pres. Rb. Roermond 12 september 1985, *KG* 1985, 299.

³⁰ Hof Den Bosch 2 juli 1986, *NJ* 1987, 451 (*Koma*).

Jurisprudentie

Een interessante uitspraak is *KLM/Reinders*.³¹ Werknemer Reinders had privé-email vanaf zijn werk verstuurd waaronder ook pornografische email. Daarnaast had hij 06-lijnen gebeld en daarbij een 06-blokkade omzeild. KLM verzoekt ontbinding van de arbeidsovereenkomst. Reinders stelt dat de bewijsgaring onrechtmatig was, omdat zijn bureau was doorzocht, terwijl hij er niet was, zijn computer gekraakt en een als privé gelabelde diskette gelezen. De Kantonrechter overweegt dat een zekere privétesering in de huidige tijd op de werkplek plaatsvindt. Een werkgever heeft daarom binnen zekere grenzen te aanvaarden dat onder werktijd privé-contacten worden onderhouden, waarvan hij de privacy dient te waarborgen. Dat ligt anders bij afbeeldingen van gewelddadige en pornografische aard, die de werknemer met zijn email meestuurt. De werknemer had moeten begrijpen dat een bedrijfsnetwerk daarvoor niet is bedoeld. Op dit soort gebruik mag de werkgever zijn netwerk onderzoeken. Dit geldt ook voor onderzoek naar het onrechtmatig gebruik van telefoon en fax door een uitdraai van de eigen gegevens te maken.

In deze zaak wordt expliciet erkend dat de werkgever tot op zekere hoogte het recht op privacy van de werknemer dient te respecteren. Ietwat vreemd is wel dat de kantonrechter stelt dat de privacy niet geldt voor afbeeldingen met pornografische of gewelddadige inhoud. Dat bij pornografische email controle wellicht toelaatbaar is, wil niet zeggen dat deze controle geen beperking van het recht op privacy is. Over het communicatiegeheim zegt de rechter niets.

In een Amsterdamse zaak werd ontbinding geweigerd na het verzenden en ontvangen van pornografische emails. Het ging om een klein aantal emails die de werknemer uitwisselde met zijn collega annex minnares. De werkgever kon niet elk privé-gebruik van email verbieden.³² Ook de Rechtbank Rotterdam sprak zich uit over emailmisbruik.³³ Naar aanleiding van klachten over seksuele intimidatie binnen het politiekorps was een intern onderzoek ingesteld. Daaruit kwam naar voren dat van email in dat kader misbruik was gemaakt. Dit lekte uit en in televisieprogramma *Barend & Witteman* werden emails van betrokkene in de openbaarheid gebracht. Naar aanleiding hiervan rees het vermoeden dat betrokkene zich ook in de niet reeds openbare email schuldig had gemaakt aan buitensporig seksistisch, deels pornografisch getint emailgebruik. Na weigering van betrokkene inzage in haar email te geven, gaf de korpschef toestemming de email te openen. De rechtbank was van oordeel dat onder de gegeven omstandigheden de korpschef gerechtigd was tot deze inbreuk.

Hoewel grondrechten in het ambtenarenrecht anders, namelijk verticaal, werken dan in het arbeidsovereenkomstenrecht, biedt deze zaak interessante aanknopingspunten. In tegenstelling tot in *KLM/Reinders* wordt hier wel een rechtstreeks beroep gedaan op art. 10, 13 Gw en art. 8 EVRM. De Rechtbank overweegt dat er sprake is van een discussie omtrent de status van email onder art. 13 Gw, maar is van mening dat wat daarvan ook zij, in dit geval de Grondwet de beperking toelaat, aangezien art. 13 lid 1 Gw beperkingen in de gevallen bij wet bepaald toelaat.³⁴ De rechtbank is blijkbaar van mening dat bepalingen in de Ambtenarenwet in casu een afdoende wettelijke basis bieden. Zij geeft echter niet aan welke bepalingen dat zouden moeten zijn, noch onderkent zij dat in art. 13 lid 1 en 2 ook nog andere eisen aan beperkingen op het geheim gesteld worden. Wel toetst de rechtbank de beperking uitvoerig aan subsidiariteit en proportionaliteit. Daarin speelt onder meer een rol dat de reeds openbaar gemaakte berichten seksistisch en pornografisch getint waren, dat de integriteit van de politie in het geding is, en dat niet volstaan had kunnen worden met een lichter middel. Je kunt je

³¹ Ktg. Haarlem 16 juni 2000, *JAR* 2000-170, p. 948-950 (*KLM/Reinders*).

³² Werknemer ontkende overigens zijn relatie met de betreffende collega in 'Clintoniaanse' bewoordingen, aldus de kantonrechter Amsterdam 26 april 2001, *JAR* 2001-101.

³³ Rb. Rotterdam 29 maart 2001, ELRONr. AB0812.

³⁴ De rechtbank overweegt dat 'de wetgever een ontwerp van wet [heeft] aanhangig gemaakt (Wet bescherming persoonsgegevens (sic!)) waarin wordt beoogd de bescherming van art. 13 Gw voor wat betreft het brief-, telefoon –en telegraafgeheim, te vervangen door een techniekonafhankelijk geformuleerd grondrecht om vertrouwelijk te communiceren.)

daarbij wel afvragen of de werkgever nog een belang had bij controle, nu reeds uit de openbare email gebleken was dat de werknemer zich schuldig gemaakt had aan ontoelaatbaar emailgebruik.

In de jurisprudentie lijkt een trend waarneembaar dat wanneer het gaat om het constateren van strafbare feiten gepleegd door werknemers, en als de mogelijkheid van controle (vooraf) kenbaar is, controle niet onredelijk wordt geacht.³⁵ Permanente controle zal slechts bij hoge uitzondering toegestaan zijn. Zo oordeelde het Hof Den Bosch in het eerder besproken *Koma*-arrest dat het permanent controleren van werknemers door middel van een gesloten TV-circuit in de werkruimte uit het oogpunt van normale menselijke bejegening - behoudens gevallen van duidelijke noodzaak - niet aanvaardbaar is.

In beginsel is het afluisteren van de telefoon niet toegestaan, tenzij het gaat om het beoordelen van het functioneren van de desbetreffende werknemer.³⁶ Het afluisteren zal eerder mogen plaatsvinden als de taak van werknemer bestaat uit het plegen van telefoontjes. Voor email geldt in beginsel hetzelfde. De werknemer dient (vooraf) op de hoogte te worden gesteld van een controle. Een permanente registratie van gesprekken ter beoordeling van de werkprestaties is in elk geval niet toegestaan.³⁷

Goed werken in netwerken

In de jurisprudentie over emailprivacy op de werkplek wordt opvallend genoeg het recht op privacy in veel gevallen niet expliciet als af te wegen belang genoemd. Voor het communicatiegeheim geldt dit nog sterker. Rechters zijn blijkbaar nog relatief onbekend met het emailgeheim. De rechterlijke erkenning van het feit dat sprake is van privétesering van de werkplek en de daaruit getrokken consequentie dat de werkgever de plicht heeft een beperkte mate van privé-gebruik van email te respecteren en zelfs te waarborgen, moet als positief gezien worden. Duidelijk is echter dat met betrekking tot de reikwijdte van het emailgeheim op de werkplek nog onduidelijkheid bestaat. Onder welke omstandigheden mag de werkgever nu de emails van zijn werknemers controleren? Deze vraag heeft de Registratiekamer in zijn rapport 'Goed werken in netwerken' geprobeerd te beantwoorden. In dit rapport is een aantal vuistregels voor een zorgvuldig beleid met betrekking tot Internet en emailgebruik opgenomen.³⁸ Dat controle van computergebruik een bedreiging voor de privacy van de werknemer betekent, erkent de Registratiekamer uitdrukkelijk. Een aantal legitieme werkgeversbelangen kan echter controle vereisen. Deze controle moet volgens de Registratiekamer voldoende kenbaar zijn voor de werknemer en aan eisen van proportionaliteit en subsidiariteit voldoen. Wij zullen hieronder weergeven tot welke conclusies en aanbevelingen de Registratiekamer op grond van bovengenoemde uitgangspunten komt. In beginsel dient de werkgever onder raadpleging van de OR heldere en eenduidige gedragsregels op te stellen en te publiceren, zodat de werknemer weet of en welk privé-gebruik toegestaan is. Bij een controle op verboden gebruik verdienen softwarematige maatregelen de voorkeur. Deze vereisen geen actieve of continue controle en zijn derhalve minder belastend dan permanente monitoring. Een softwarematige aanpak zal vooral ten behoeve van systeem –en netwerkbeveiliging toegepast kunnen worden. Echter, ook om het

³⁵ Ktg. Schiedam 8 juli 1997, *JAR* 1997, 189; Verhulp 1999, p. 154.

³⁶ Verhulp 1999, p. 156.

³⁷ Pres. Rb. Amsterdam 14 december 1989, *KG* 1990, 33 (*Distrivox*).

³⁸ Registratiekamer, Goed werken in netwerken – Regels voor controle op email en internetgebruik van werknemers. Internet: http://www.registratiekamer.nl/bis/top_1_5_35_18.html. Hier dient ook gewezen te worden op de initiatieven van respectievelijk VNO-NCW en de FNV. Beide organisaties hebben een modelgedragscode voor internet- en emailgebruik opgesteld. VNO-NCW, Surfen op de werkplek. Een modelgedragscode voor internet –en emailgebruik, maart 2001. Internet: <http://www.vno-ncw.nl/map4/brochure.html?code=58>; FNV, Voorbeeldprotocol 'Privacy bij internet –en emailgebruik. Internet: <http://www.bondgenoten.fnv.nl/start/fbg/site-mz/vb-prtel.htm>.

uitlekken van bedrijfsgeheimen tegen te gaan en negatieve publiciteit te voorkomen heeft automatische *content-filtering* de voorkeur van de Registratiekamer. Emails die bepaalde woorden bevatten die op een ongewenste inhoud duiden, kunnen opzij gezet worden, zodat de werkgever er later kennis van kan nemen. Content-filtering kan feitelijk echter vrij gemakkelijk omzeild worden. Daarom heeft de werkgever naar de mening van de Registratiekamer het recht na een gerezen verdenking steekproefsgewijs de inhoud van email controleren.

Als aan de hand van de verkregen gegevens algemene rapportages worden opgesteld, dienen deze gegevens volgens de Registratiekamer zoveel mogelijk geanonimiseerd te worden. Een uitzondering kan gemaakt worden als tegen een werknemer een concrete verdenking bestaat. Als blijkt dat werknemers zich niet aan de regels houden, moeten zij zo spoedig mogelijk op hun gedrag te worden aangesproken. De Registratiekamer overweegt dat de werkgever zich zoveel mogelijk dient te onthouden van het inzien van privé-mail. Hij zal niet *alle* privé-email mogen controleren. Alleen als er een gewichtige reden is, zal hij kennis mogen nemen van een specifiek bericht.

Voor beoordeling en begeleiding van individuele werknemers kan volgens de Registratiekamer controle van de inhoud van zakelijke email rechtens toegestaan zijn. Zij stelt dan wel als voorwaarde dat er een rechtstreeks verband met de taken van de werknemer moet bestaan.

De Registratiekamer acht controle van de inhoud niet toegestaan wanneer zij slechts dient om de kosten van communicatiefaciliteiten te beperken. Kennisname van de verkeersgegevens is immers voldoende om de werknemer op zijn gedrag aan te spreken, zo stelt zij.

In elk geval moet volgens de Registratiekamer de omvang van de controle zo beperkt mogelijk worden gehouden qua tijdsduur, frequentie en de gecontroleerde personen. Het emailgebruik van geprivilegieerden zoals bedrijfsartsen en OR-leden mag überhaupt niet inhoudelijk gecontroleerd worden.

Een ander belangrijk punt dat de Registratiekamer aanroert, is de positie van de systeembeheerder. Daarover stelt zij dat de positie van systeembeheerder met de nodige waarborgen omgeven moet worden, aangezien hij in beginsel toegang heeft tot alle gegevens in het computernetwerk. Dat betekent dat de systeembeheerder een bepaalde mate van onafhankelijkheid tegenover het management moet hebben, omdat hij in zekere zin een vertrouwensfunctie bekleedt.

Het rapport biedt een aantal geschikte aanknopingspunten en aanbevelingen. Wel had de Registratiekamer ons inziens meer duidelijkheid kunnen creëren met betrekking tot *wanneer* welke vorm van controle toegestaan is.

Analyse van emailcontrole

Er zijn aanwijzingen dat de jurisprudentie en afspraken over telefoongebruik op de werkplek niet een op een kunnen worden vertaald naar het gebruik van email. De verschillen tussen email en telefonie op de werkplek zitten enerzijds in de andere functionaliteit van email en anderzijds in de andere (grotere) mogelijkheden tot controle.

Email wordt anders gebruikt dan telefonie. Het kostenargument gaat niet of nauwelijks op. Tenzij er buitengewoon veel verkeer wordt gegenereerd, kan niet worden gezegd dat het voor de werkgever duurder is als zijn werknemer af en toe een privé-mailtje verstuurt. De werknemer heeft er recht op in beperkte mate van de emailfaciliteit gebruik te maken voor privé-doeleinden. Dit vormt een onderdeel van het recht van de werknemer relaties met anderen te onderhouden.³⁹

Email is technisch veel gemakkelijker te controleren dan telefonie. Bij telefonie zijn er in beginsel twee mogelijkheden voor controle. De werkgever kan de verkeersgegevens controleren of hij kan een gesprek afluisteren. Bij email zijn er veel meer

³⁹ Zie ook hierboven, en EHRM 16 december 1992 (*Niemitz*), NJ 1993, 400.

controle mogelijkheden. Naast het feit dat emailgebruik sporen achterlaat in de computer van verzender en ontvanger, kan email ook nog eens vrij gemakkelijk onderschept worden wanneer een boodschap via een bedrijfsintern netwerk wordt verstuurd. Vaak is een dergelijk netwerk slechts op een punt met het Internet verbonden en dient het verkeer een *firewall* te passeren alvorens het echt de digitale snelweg opdraait. Op dat punt kan in beginsel, voorzover geen gebruik wordt gemaakt van encryptie, al het op IP/TCP gebaseerde verkeer worden opgevangen en doorgelicht. Email kan onderzocht worden op het gebruik van bepaalde woorden of andere inhoudselementen. Dit maakt dat controle op emailgebruik in beginsel voor de privacy bedreigender is dan controle van telefonie. Gezien deze grotere bedreiging zou wellicht een sterkere bescherming van email ten opzichte van telefonie op zijn plaats zijn. Naar huidig recht is dit echter niet het geval.

De voornaamste argumenten voor controle op emailgebruik zijn het voorkomen van schade aan het bedrijf en het controleren van de productiviteit van een werknemer.

Bij schade aan het bedrijf kan worden gedacht aan het verzenden van beledigende mailtjes of het ophalen en doorsturen van pornografische post. Daarbij moet wel worden opgemerkt dat de schade veroorzaakt door pornografische mail door de werkgever zal moeten worden aangetoond. De in de jurisprudentie heersende trend dat indien er sprake is van porno, het ontslag zonder meer gerechtvaardigd is, steunt o.i. niet op een juiste interpretatie van het recht. Voorkomen van schade kan een gerechtvaardigde inbreuk op het communicatiegeheim van de werknemer opleveren. Dat laat onverlet dat proportionaliteit en subsidiariteit voorop moeten blijven staan.

Een ander voorbeeld van schade die het bedrijf kan worden berokkend via email is de verspreiding van bedrijfsgeheimen. Controle van email is alleen rechtmatig op die grond indien er een sterke verdenking bestaat van een dergelijke vorm van misbruik.

Anders dan bij telefonie is het voor veel werknemers gebruikelijk hetzelfde adres te voeren als werk- en als privé-emailadres. Dat betekent dat het ontvangen van privé-email niet altijd een misbruikelement in zich heeft. Gaat het om het controleren van de arbeidsproductiviteit van een werknemer, dan is het controleren van diens email, een betrekkelijk zwaar middel dat enkel bij zware verdenking mag worden ingezet. Overigens is niet ondenkbaar dat wanneer (in de toekomst) het opstellen en verzenden van email een hoofdbestanddeel van de taak van de werknemer is, de werkgever in beginsel een gerechtvaardigd belang heeft steekproefsgewijs de inhoud van emails te controleren. Dit dient echter wel zoveel mogelijk te gebeuren na voorafgaande notificatie van de werknemer.

Indien de werkgever voldoende aanleiding heeft de email van de werknemer te controleren, staan hem verschillende niveaus van controle ten dienst. Zo kan hij de hoeveelheid capaciteit bekijken die zijn werknemer verstuurt en downloadt. Pas als die controle wijst op onregelmatig gebruik kan hij verder gaan. Daarnaast kan hij filteren op gebruik van bepaalde woorden in de subject line, kan hij de inhoud van de mails zelf filteren op gebruik van bepaalde woorden en kan hij de verzonden attachments controleren. De meest ingrijpende vorm van controle is het inzien van de door zijn werknemer verstuurd en ontvangen emails. Het inzien van de inhoud komt dus pas als allerlaatste controlemiddel in aanmerking.

Een extra complicatie doet zich voor bij telewerken. Wanneer de werknemer vanaf thuis inlogt en met een door de werkgever ter beschikking gestelde Internetverbinding contact houdt met de werkvloer, dient de werkgever nog meer de privacybelangen van zijn werknemer in acht te nemen.⁴⁰ De werkgever dient zich te realiseren dat ook huisgenoten van de werknemer van de dienst gebruik kunnen maken. Email van huisgenoten mag hij niet inzien.

Uit het voorgaande moge blijken dat de werkgever zich bij controle moet houden aan vereisten van subsidiariteit en proportionaliteit. Dat wil dus zeggen dat altijd de lichtste, minst

⁴⁰ Vgl. M.H.J. Limmen, : 'De telewerker: zorgende alleskunner of 24 uren werknemer?' in: "De waarde(n) van de kennissamenleving", Tilburg: PlantijnCasparie 2001, p. 50-54.

inbreukmakende vorm van controle moet worden gekozen. Daarbij dient de werkgever rekening te houden met het bijzondere karakter van emailcorrespondentie.

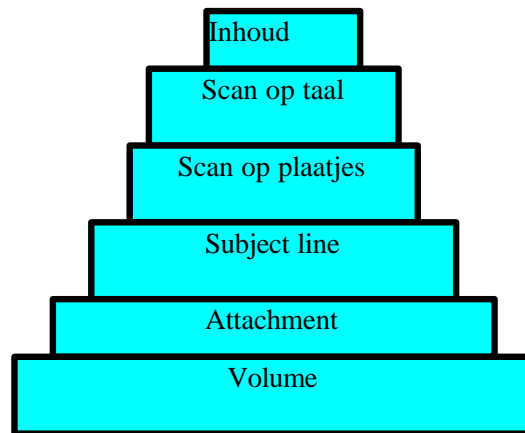
Conclusie: de privacypiramide

Het voorgaande leidt tot de conclusie dat de werkgever onder slechts omstandigheden gerechtigd is inbreuk te maken op het communicatiegeheim van de werknemer. De onderstaande eisen moeten daarbij in acht worden genomen.

Volgens vaste jurisprudentie moet de controle kenbaar zijn. Dat betekent concreet dat een gedragscode moet worden opgesteld waarin beschreven wordt welke vormen van privé-gebruik door de werkgever als ontoelaatbaar worden aangemerkt. Deze gedragscode moet aan de Ondernemingsraad ter instemming voorgelegd worden. In de gedragscode zal expliciet moeten worden vastgelegd dat de werkgever de bevoegdheid heeft bij een verdenking van ontoelaatbaar gebruik tot controle over te gaan.

Een dergelijke controle zal alleen rechtmatig zijn wanneer de eisen van proportionaliteit en subsidiariteit in acht worden genomen. De subsidiariteitseis brengt met zich mee dat in ieder geval het minst inbreukmakende middel het eerst moet worden toegepast. Voor de werkgever is het niet altijd duidelijk wat de minst inbreukmakende methode is. Juist bij email kan echter ons inziens een rangorde van de ernst van de inbreukmakende maatregel worden aangegeven. Deze uitgangspunten zouden bijvoorbeeld kunnen leiden tot de volgende piramide.

Privacypiramide



Hierboven is weergegeven hoe de verschillende controlemogelijkheden van de werkgever in ernst toenemen. Bovenstaande figuur heeft de vorm van een piramide, omdat het ons inziens mogelijk is door de verschillende trappen af te werken, de groep gecontroleerden steeds verder te verkleinen. Ons inziens is de meest eenvoudige en minst inbreukmakende controlemogelijkheid de analyse van het volume van verkeer voor alle werknemers afgezet tegen het gemiddelde volume. Als daaruit niets vreemds naar voren komt, zal het ook wel goed zitten met de individuele werknemers. Een verdergaande controle is in dat geval niet toegestaan.

Als de werkgever op basis van de analyse wel wat verdachts ontdekt, kan hij een verdergaande controle uitvoeren. Dan zou hij kunnen scannen op het voorkomen van ontoelaatbare attachments. Hij kan dan bijvoorbeeld bekijken wat voor attachments verstuurd worden. Dat is te zien aan de extensie. Word-documenten hebben bijvoorbeeld de extensie .doc, muziekbestanden .mp3, plaatjes .jpg etc.⁴¹ Op basis hiervan kan een verdenking toenemen of afnemen. Ontdekt de werkgever niets vreemds, dan houdt het hier op. Neemt de verdenking toe, dan kan hij verder gaan. Zo kunnen alle bovengenoemde trappen worden afgegaan. Op deze wijze wordt de groep gecontroleerden steeds kleiner, want de onschuldigen kunnen al vrij snel worden uitgesplitst. Bij de vierde trap kan worden gekeken of de emails zogenaamde 'vleeskleur' bevatten, een bekende methode om te kijken of er wellicht porno wordt verstuurd. Het verst gaat het inzien van emails van een individuele werknemer. Daartoe zal de werkgever pas gerechtigd zijn bij zeer ernstige verdenkingen en nadat hij de eerdere trappen reeds heeft afgewerkt. Het voordeel van dit afwegingsmechanisme is dat de inbreuk op de privacy van werknemers tot een minimum beperkt blijft. Van onschuldige werknemers kan reeds in een vroeg stadium worden vastgesteld dat zij onschuldig zijn. Deze hoeven verder niet gecontroleerd te worden. Uiteindelijk wordt alleen bij de werknemers waarop een ernstige verdenking rust, de meest vergaande controle toegepast.

Het voordeel van de hier voorgestelde piramide is, dat een controle door de werkgever sneller in overeenstemming zal zijn met het subsidiariteitsbeginsel. Natuurlijk kan de werkgever besluiten om niet de verschillende trappen af te gaan. In dat geval zal hij de subsidiariteit van de controle echter moeilijker kunnen aantonen.

Bij elke vorm van controle zal de werkgever echter moeten nagaan of de controle proportioneel is, met andere woorden of het doel waarvoor controle plaatsvindt, de concrete maatregel rechtvaardigt. Ook hier heeft de bovenstaande privacypiramide een toegevoegde waarde, omdat het de werkgever de gelegenheid biedt zich na elke trap te bezinnen en te bezien

⁴¹ Het betreft hier een niet-limitatieve opsomming.

of een verdergaande maatregel nog noodzakelijk zal zijn. Het inzien van privé-email door de werkgever zal op deze manier tot een minimum beperkt blijven. De laatste, maar zeker niet onbelangrijke eis voor de toelaatbaarheid van de controle is dat de werknemer zo spoedig mogelijk, nadat controle heeft plaatsgevonden, van de controle op de hoogte dient te worden gesteld. Immers, alleen indien de werknemer van de controle in kennis is gesteld, kan hij de rechtmatigheid daarvan (laten) beoordelen.

Volgt de werkgever de hier voorgestelde benadering, dan kan aan zijn belangen tegemoet worden gekomen, zonder dat het emailgeheim meer dan noodzakelijk wordt geschonden.