5401/01/NL/Def
WP 55

Werkdocument over de controle op elektronische communicatie op het werk

Goedgekeurd op 29 mei 2002

Opmerking:

* nationale hoofdstukken kunnen in overleg met nationale delegaties nog worden gewijzigd

De Groep is opgericht op grond van artikel 29 van Richtlijn 95/46/EG. Zij is het onafhankelijke EU-adviesorgaan inzake gegevensbescherming en de persoonlijke levenssfeer. De taken van de Groep zijn omschreven in artikel 30 van Richtlijn 95/46/EG en in artikel 14 van Richtlijn 97/66/EG. Het secretariaat wordt verzorgd door:

Europese Commissie, DG Interne markt, Directoraat A (Werking en effect van de interne markt - Coördinatie - Gegevensbescherming) B-1049 Brussel - België - Kamer: C100-6/136

Website: www.europa.eu.int/comm/privacy

DE GROEP VOOR DE BESCHERMING VAN PERSONEN IN VERBAND MET DE VERWERKING VAN PERSOONSGEGEVENS

Opgericht bij Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995[1],

Gelet op artikel 29 en artikel 30, lid 1, onder a), en lid 3, van deze richtlijn,

Gelet op haar reglement en met name op de artikelen 12 en 14 daarvan,

heeft het volgende werkdocument goedgekeurd:

[1] PB L 281 van 23.11.1995, blz. 31, beschikbaar op:

http://europa.eu.int/comm/internal_market/en/dataprot/index.htm.

Werkdocument van de Groep artikel 29[2] over de controle op elektronische communicatie op het werk

Ontwerp-samenvatting

Dit werkdocument is een aanvulling op advies 8/2001 over de verwerking van persoonsgegevens in het kader van de arbeidsverhouding[3] en draagt bij aan de uniforme toepassing van de nationale maatregelen die uit hoofde van de gegevensbeschermingsrichtlijn 95/46/EG[4] zijn goedgekeurd. Het document doet geen afbreuk aan de toepassing van nationale wetgeving op gebieden die met gegevensbescherming verband houden.

De Groep artikel 29 heeft een subgroep opgericht met als taak dit vraagstuk te bestuderen[5] en heeft een **uitvoerig document** goedgekeurd dat op internet op het volgende adres te vinden is[6]:

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

---

[2] De Groep artikel 29 is een adviesorgaan dat is samengesteld uit vertegenwoordigers van de gegevensbeschermingsautoriteiten van de lidstaten, onafhankelijk optreedt en onder meer als taak heeft elk vraagstuk betreffende de toepassing van de nationale maatregelen die op grond van de Richtlijn gegevensbescherming zijn goedgekeurd, te onderzoeken teneinde bij te dragen tot de uniforme toepassing van deze maatregelen.

[3] Advies goedgekeurd op 13 september 2001 en beschikbaar op het volgende internetadres:

http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48en.pdf. Dit advies bevat een grondige analyse van de toepassing van de bepalingen van de gegevensbeschermingsrichtlijn (en met name van de artikelen 6, 7 en 8) op de verwerking van persoonsgegevens in het kader van een arbeidsverhouding.

[4] Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens. PB nr. L 281 van 23.11.1995, blz. 31

[5] De volgende toezichthoudende autoriteiten hebben bijgedragen tot de werkzaamheden van deze subgroep: AT, BE, DE, ES, FR, IR, IT, NL, UK.

[6] Het document bevat een overzicht van de relevantste wetgeving op het gebied van gegevensbescherming in de lidstaten die enig effect heeft op de activiteiten in verband met controle op elektronische communicatie op het werk.

De Groep artikel 29 heeft zich in dit werkdocument beziggehouden met het vraagstuk van de controle op elektronische communicatie op het werk, met andere woorden, de controle die de werkgever uitoefent op het gebruik van e-mail en internet door zijn personeel.

In het licht van de jurisprudentie van het *Europees Hof voor de rechten van de mens* over artikel 8 van het *Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden* en van andere belangrijke internationale teksten en de bepalingen van Richtlijn 95/46/EG geeft dit document, mede aan de hand van concrete voorbeelden, inzicht in hetgeen onder aanvaardbare controlerende activiteiten en de limieten van het toezicht op werknemers door de werkgever wordt verstaan. Het is best mogelijk dat in sommige lidstaten de wetgeving in strengere beschermingsnormen voorziet dan die welke in dit werkdocument worden beschreven.

Werknemers geven hun recht op privacy en gegevensbescherming niet op telkens ze 's ochtends door de deur van hun werkplek stappen. Zij verwachten terecht een bepaalde mate van privacy op het werk aangezien ze een groot deel van hun relaties met andere mensen op de werkplek ontwikkelen. Dit recht moet echter in een normale verhouding staan tot andere gerechtvaardigde rechten en belangen van de werkgever, met name het recht van de werkgever om tot op zekere hoogte op een efficiënte manier leiding te geven aan zijn bedrijf, en, in de eerste plaats, het recht om zichzelf te beschermen tegen eventuele schade die activiteiten van werknemers kunnen veroorzaken. Deze rechten en belangen vormen gegronde redenen om passende maatregelen te nemen om het recht van de werknemer op privacy te beperken. Het duidelijkste voorbeeld hiervan vormen die gevallen waarin de werkgever het slachtoffer is van een misdrijf van de werknemer.

Om verschillende rechten en belangen met elkaar in evenwicht te houden moet met een aantal beginselen rekening worden gehouden, met name met evenredigheid. Alleen het feit dat een controlerende activiteit geschikt is om de belangen van de werkgever te dienen, zou niet voldoende zijn om het binnendringen in de persoonlijke levenssfeer van de werknemer te rechtvaardigen. Voordat een dergelijke activiteit op de werkplek wordt uitgevoerd moet zij een aantal tests ondergaan die in dit werkdocument uitvoerig zullen worden besproken.

Hoe deze beoordeling eruitziet, kan worden samengevat in de volgende vragen:

a) is de controlerende activiteit transparant voor de werknemers?

b) is zij noodzakelijk? Kan de werkgever niet dezelfde resultaten bereiken met traditionele controlemethoden?

c) Is de voorgestelde verwerking van persoonsgegevens voor de werknemers redelijk?

d) Staat zij in verhouding tot de zorgen die zij tracht weg te nemen?

In dit document wordt vooral aandacht besteed aan de praktische toepassing van deze beginselen en wordt informatie gegeven over de minimuminhoud van het beleid van ondernemingen inzake het gebruik van e-mail en internet, dat de werknemers en werkgevers als basis kunnen nemen voor de verdere uitwerking van een beleid

(waarbij rekening wordt gehouden met de typische kenmerken van een bepaalde onderneming, de grootte ervan en de nationale wetgeving op gebieden die verband houden met gegevensbescherming).

Wat het gebruik van internet voor privé-doeleinden betreft, is de Groep artikel 29 van mening dat **preventie belangrijker is dan opsporing**, m.a.w., dat het belang van de werkgever beter gediend is met het voorkomen dan met het opsporen van misbruik van internet. In dit verband zijn technologische oplossingen zeer nuttig. En algemeen verbod op het persoonlijk gebruik van internet voor werknemers lijkt niet redelijk en staat niet in verhouding tot de mate waarin internet werknemers in hun dagelijkse leven kan bijstaan.

De Groep vindt het van essentieel belang dat de werkgever de werknemer op de hoogte brengt van (i) de aanwezigheid, het gebruik en het doel van opsporingsvoorzieningen en/of apparatuur die in verbinding met zijn werkstation in gebruik zijn en van (ii) elk geconstateerd misbruik van elektronische communicatie (e-mail of internet), tenzij geheim toezicht[7] om belangrijke redenen moet worden voortgezet, hetgeen normaal niet het geval is. Met behulp van speciale software kan direct informatie worden verstrekt, zoals waarschuwende windows die verschijnen en de werknemer erop wijzen dat het systeem ongeautoriseerd gebruik van het netwerk heeft ontdekt en/of stappen heeft ondernomen om dit te voorkomen.

Werkgevers zouden kunnen overwegen om werknemers twee e-mailaccounts te geven:

a) een voor professioneel gebruik, waarbij controle binnen de in dit document aangegeven limieten mogelijk is,

b) en een voor privé-doeleinden (of toestemming voor het gebruik van webmail) die alleen in uitzonderlijke gevallen zou worden beveiligd en op misbruik zou worden gecontroleerd.

De Groep artikel 29 heeft op gebieden die verband houden met gegevensbescherming verschillen tussen de nationale wetgevingen geconstateerd, hoofdzakelijk met betrekking tot toegestane afwijkingen van het fundamentele recht op geheimhouding van correspondentie en de reikwijdte en het effect van in cao's vastgelegde werknemersvertegenwoordiging en medezeggenschap. De Groep artikel 29 heeft echter geen verschillen gevonden tussen de nationale wetgevingen op het gebied van gegevensbescherming die een gemeenschappelijke benadering in de weg zouden kunnen staan en heeft derhalve dit werkdocument uitgebracht dat in de periode 2002-2003 zal worden herzien in het licht van de ervaring en de verdere ontwikkelingen op dit gebied.

[7] Gevallen van verantwoord geheim toezicht zouden hier een goed voorbeeld vormen.

1. CONTROLE OP HET WERK. EEN UITDAGING VOOR DE SAMENLEVING

De controle van werknemers krijgt momenteel veel aandacht in de media en vormt het onderwerp van een publiek debat in de Gemeenschap. Door het toenemend gebruik van e-mail op het werk in de Gemeenschap zijn zowel werkgevers als werknemers zich steeds meer bewust geworden van het gevaar van aantasting van de privacy op de werkplek.

Als we het over controle hebben moeten we steeds voor ogen houden dat werknemers weliswaar het recht hebben op een bepaalde mate van privacy op het werk maar dat dit recht moet worden afgewogen tegen het recht van de werkgever om het functioneren van zijn bedrijf in de gaten te houden en om zichzelf te verdedigen tegen acties van werknemers die zijn rechtmatige belangen kunnen schaden, bv. in het licht van de aansprakelijkheid van de werkgever voor de acties van zijn werknemers.

Terwijl de nieuwe technologieën een positieve ontwikkeling vormen in de middelen die de werkgevers ter beschikking staan, bestaat het gevaar dat elektronische controlemiddelen op zodanige wijze worden gebruikt dat zij de fundamentele rechten en vrijheden van werknemers aantasten. Wij mogen niet vergeten dat de opkomst van de informatietechnologie geen afbreuk mag doen aan de rechten van de werknemers, ongeacht of zij on line of off line werken.

Voorts moet erop worden gewezen dat de arbeidsomstandigheden zodanig zijn geëvolueerd dat het steeds moeilijker wordt om een duidelijke lijn te trekken tussen werkuren en privéleven. Aangezien het “thuiswerken” zich steeds meer ontwikkelt, gaan talrijke werknemers thuis verder met hun werk waarbij zij gebruikmaken van de computerinfrastructuur die al dan niet door de werkgever voor dit doel is bezorgd.

De menselijke waardigheid van een werknemer staat boven elke andere overweging. Bij de bestudering van dit vraagstuk moeten we dit goed voor ogen houden en rekening houden met de negatieve gevolgen die dergelijke acties op de kwaliteit van de arbeidsverhoudingen en van het werk zelf kunnen hebben.

In het licht van al deze factoren is het dan ook niet verrassend dat dit vraagstuk bovenaan de agenda van het publieke debat staat en moet er dringend werk gemaakt worden van een uniforme interpretatie van de bepalingen van Richtlijn 95/46/EG en de nationale regelgeving waarin deze richtlijn wordt omgezet, rekening houdende met de recente jurisprudentie van het *Europees Hof voor de rechten van de mens*.

De Groep achtte het dan ook nuttig om de volgende informatie en werkdocumenten aan de publieke en particuliere sector te bezorgen. In dit werkdocument komen alle activiteiten aan bod die te maken hebben met controle op elektronische communicatie op het werk, zowel real-timetoezicht als toegang tot opgeslagen gegevens.

2. INTERNATIONALE RECHTSINSTRUMENTEN

2.1 ARTIKELEN 8 EN 10 VAN HET EUROPEES VERDRAG TOT BESCHERMING VAN DE RECHTEN VAN DE MENS EN DE FUNDAMENTELE VRIJHEDEN

Artikel 8

1. Eenieder heeft recht op respect voor zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie.

2. Geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen

Artikel 10

1. Eenieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of te verstrekken, zonder inmenging van enig openbaar gezag en ongeacht grenzen. Dit artikel belet Staten niet radio-omroep-, bioscoop- of televisieondernemingen te onderwerpen aan een systeem van vergunningen

2. Daar de uitoefening van deze vrijheden plichten en verantwoordelijkheden met zich brengt, kan zij worden onderworpen aan bepaalde formaliteiten, voorwaarden, beperkingen of sancties, die bij de wet zijn voorzien en die in een democratische samenleving noodzakelijk zijn in het belang van de nationale veiligheid, territoriale integriteit of openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden, de bescherming van de goede naam of de rechten van anderen, om de verspreiding van vertrouwelijke mededelingen te voorkomen of om het gezag en de onpartijdigheid van de rechterlijke macht te waarborgen

Alle lidstaten en de Europese Unie zijn gebonden aan de bepalingen van het *Europees verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden*. Deze rechten zijn gewoonlijk verticaal uitgeoefend (het individu tegenover de overheid) en momenteel wordt van gedachten gewisseld over de mate waarin zij horizontaal kunnen worden uitgeoefend (tussen individuen). Het staat echter vast dat deze rechten in het algemeen bestaan.

De Groep is derhalve van oordeel dat het voor een uniforme toepassing van de nationale maatregelen die uit hoofde van Richtlijn 95/46/EG zijn goedgekeurd noodzakelijk is de aandacht te vestigen op de belangrijkste beginselen van de huidige jurisprudentie van het *Europees Hof voor de rechten van de mens* m.b.t. deze bepalingen en met name m.b.t. de geheimhouding van correspondentie.

Het Hof heeft in zijn arresten duidelijk gemaakt dat de bescherming van het privéleven waarvan sprake is in artikel 8, het beroepsleven van een werknemer niet uitsluit en niet beperkt is tot het leven thuis.

De zaak **Niemitz v. Duitsland** ging over het doorzoeken van het kantoor van de klager door een publieke autoriteit. De overheid voerde aan dat artikel 8 geen bescherming biedt tegen het doorzoeken van iemands kantoor aangezien het Verdrag een duidelijk onderscheid maakt tussen enerzijds het privéleven en thuis en anderzijds het beroepsleven en de ruimte waarin dit plaatsvindt.

Het Hof wees dit standpunt af met het volgende argument:

"Respect voor het privéleven houdt tot op zekere hoogte ook het recht in om betrekkingen met andere mensen te ontwikkelen. ***Er is voorts geen enkele reden om aan te nemen waarom het begrip "privéleven" geen professionele of zakelijke activiteiten zou omvatten****, aangezien de meeste mensen het grootste deel van hun betrekkingen met de buitenwereld, of misschien zelfs allemaal, tijdens hun dagelijkse beroepsbezigheden ontwikkelen. Voor dit standpunt spreekt ook nog het feit - en de Commissie heeft hier terecht op gewezen - dat niet altijd duidelijk kan worden vastgesteld welke activiteiten van een persoon nu deel uitmaken van het beroeps-of zakelijke leven en welke niet".*[8]
In de zaak **Halford v. het Verenigd Koninkrijk** besloot het Hof dat het afluisteren van de telefoongesprekken van een werknemer op het werk in strijd is met artikel 8 van het Verdrag. Interessant hierbij is te weten dat mevrouw Halford twee telefoons had, waarvan één voor privégebruik. Er was geen enkele beperking op het gebruik van deze toestellen en er was tot dan nog geen enkele instructie gegeven.
Mevrouw Halford voerde aan dat het afluisteren van haar telefoongesprekken een schending was van artikel 8 van het Verdrag. De overheid was van oordeel dat de telefoongesprekken die mevrouw Halford vanaf haar werkplek voerde, niet voor de bescherming van artikel 8 in aanmerking konden komen omdat zij geen enkele redelijke verwachting van privacy met betrekking tot deze gesprekken kon hebben gehad. Tijdens de zitting voor het Hof betoogde de advocaat van de overheid dat een werkgever in principe telefoongesprekken die een werknemer voert met toestellen die door de werkgever ter beschikking zijn gesteld, mag controleren zonder de werknemer eerst hiervan op de hoogte te brengen.

Het Hof was echter van oordeel dat *"de jurisprudentie duidelijk aantoont dat op telefoongesprekken die in het gebouw van een bedrijf of thuis worden gevoerd de begrippen van "privéleven" en "correspondentie", in de zin van artikel 8, lid 1 van toepassing zijn (…).*

Er is geen enkel bewijs dat mevrouw Halford, als gebruiker van het interne telecommunicatiesysteem, van tevoren is gewaarschuwd dat telefoongesprekken die op dat systeem worden gevoerd, kunnen worden afgeluisterd. Daarom heeft zijn volgens het Hof een redelijke verwachting van privacy voor deze gesprekken gehad ..."[9]

Het begrip "correspondentie" omvat niet alleen brieven op papier maar ook andere vormen van elektronische communicatie die op de werkplek worden ontvangen of

---

[8] 23 November 1992, Series A n° 251/B, par. 29;

[9] 27 mei 1997

verstuurd, zoals telefoongesprekken die een bedrijfsgebouw worden gemaakt of ontvangen, of e-mails die met de kantoorcomputers worden ontvangen of verstuurd.

Volgens sommigen betekent deze uitspraak ook (ofschoon dit niet duidelijk in het arrest is geformuleerd) dat een werknemer die van tevoren door een werkgever is gewaarschuwd dat zijn communicaties kunnen worden gecontroleerd, elke verwachting van privacy kan verliezen en controle geen schending van artikel 8 van het Verdrag kan zijn. De Groep is van oordeel dat het van tevoren waarschuwen van een werknemer niet voldoende is om een inbreuk op het gegevensbeschermingsrecht te verantwoorden.

In het algemeen kunnen op grond van de jurisprudentie over artikel 8 van het *Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden* drie beginselen worden geformuleerd:

a) werknemers hebben een redelijke verwachting van privacy op de werkplek die niet teniet wordt gedaan door het feit dat zij gebruikmaken van communicatie-apparatuur of andere ondernemingsfaciliteiten van de werkgever.

   Het verstrekken van duidelijke informatie door de werkgever aan de werknemer kan de redelijke verwachting van privacy van de werknemers echter beperken;

b) het algemene beginsel van geheimhouding van correspondentie heeft betrekking op communicaties op de werkplek. Het is aannemelijk dat hieronder ook e-mailberichten en de meegestuurde bestanden vallen;

c) respect voor het privéleven houdt tot op zekere hoogte ook het recht in om betrekkingen met andere mensen te ontwikkelen. Het feit dat deze betrekkingen voor een groot deel op de werkplek plaatsvinden, vormt een beperking van de aanvaardbare behoefte van de werkgever aan controlemaatregelen.

Artikel 10 is eveneens belangrijk omdat het de vrijheid van meningsuiting en de vrijheid om inlichtingen of denkbeelden te ontvangen of te verstrekken, zonder inmenging van enig openbaar gezag regelt. Het ziet ernaar uit dat het Hof in zijn overwegingen in de bovenvermelde zaak Niemitz v. Duitsland met dit artikel rekening heeft gehouden. Zoals het Hof aanstipte ontwikkelen mensen een groot deel van hun betrekkingen met de buitenwereld op hun werk en een daarom zou hun recht op vrijheid van meningsuiting beslist een belangrijke rol in dit verband spelen.

2.2 VERDRAG TER BESCHERMING VAN DE MENS BIJ DE AUTOMATISCHE VERWERKING VAN PERSOONSGEGEVENS (VERDRAG NR. 108)

Het Verdrag werd op 28 januari 1981 ter ondertekening aangeboden en was het eerste wettelijk bindende internationale instrument op het gebied van gegevensbescherming. De partijen bij dit verdrag moeten in hun nationale wetgeving de nodige maatregelen nemen om de beginselen uit het verdrag toe te passen, teneinde ervoor te zorgen dat op hun

grondgebied de fundamentele mensenrechten van alle personen met betrekking tot de verwerking van persoonsgegevens worden geëerbiedigd.[10]

Andere belangrijke documenten in verband met Verdrag 108 zijn:

Aanbeveling (89) 2 van de Raad van Europa betreffende de bescherming van persoonsgegevens bij de arbeid. [11]

Aanbeveling (97) 5 van de Raad van Europa betreffende de bescherming van medische gegevens.[12]

Aanbeveling (86) 1 van de Raad van Europa betreffende de bescherming van persoonsgegevens bij de sociale zekerheid. [13]

Aanbeveling (95) 4 van de Raad van Europa inzake de bescherming van persoonsgegevens op het terrein van de telecommunicatiediensten, en met name met betrekking tot telefoondiensten.

2.3. HET HANDVEST VAN DE GRONDRECHTEN VAN DE EUROPESE UNIE

Artikel 7 ***Eerbiediging van het privéleven en het familie- en gezinsleven***

Eenieder heeft recht op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie.

Artikel 8 ***Bescherming van persoonsgegevens***

1. Eenieder heeft recht op bescherming van de hem betreffende persoonsgegevens.

2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.

3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels.

Het *Handvest van de grondrechten van de Europese Unie* lijkt dezelfde hoofdlijnen te volgen als het EVRM en het begrip geheimhouding van correspondentie is uitgebreid tot "geheimhouding van communicaties", met de bedoeling elektronische communicatie dezelfde bescherming te geven als die welke aan traditionele post is toegekend.

---

[10] Zie ook Aanbeveling No. R (89) 2 van de Raad van Europa betreffende de bescherming van persoonsgegevens bij de arbeid : http://cm.coe.int/ta/rec/1989/89r2.htm

[11] http://cm.coe.int/ta/rec/1989/89r2.htm

[12] http://cm.coe.int/ta/rec/1997/97r5.html

[13] http://www.legal.coe.int/dataprotection/Default.asp?fd=rec&fn=R(86)1E.htm

Bovendien vormt artikel 8, door gegevensbescherming vanuit een heel andere hoek te bekijken, een aanvulling op de bescherming die door artikel 7 wordt toegekend. Dit resultaat is met name belangrijk voor het vraagstuk van de controle op e-mail.

2.4. INTERNATIONAAL ARBEIDSBUREAU (ILO)

De Gedragscode van het Internationaal Arbeidsbureau met betrekking tot de bescherming van persoonsgegevens van werknemers (1997)

"5. Algemene beginselen

5.1. Persoonsgegevens moeten rechtmatig en eerlijk worden verwerkt, en alleen om redenen die direct relevant zijn voor het werk van de werknemer.

5.2. Persoonsgegevens mogen in principe alleen gebruikt worden voor de doeleinden waarvoor ze oorspronkelijk zijn verzameld.

5.3. Indien persoonsgegevens moeten verwerkt worden voor andere doeleinden dan die waarvoor zij werden verzameld, dient de werkgever ervoor te zorgen dat zij niet gebruikt worden op een manier die indruist tegen het oorspronkelijke doel en dient hij de nodige maatregelen te nemen om elk misverstand dat door een verandering van de context wordt veroorzaakt, te voorkomen.

5.4. Persoonsgegevens verzameld in verband met technische of organisatorische maatregelen die genomen zijn voor de beveiliging en het correct functioneren van geautomatiseerde informatiesystemen, mogen niet worden gebruikt om het gedrag van werknemers te controleren.

5.5. Beslissingen ten aanzien van een werknemer mogen niet uitsluitend gebaseerd worden op de geautomatiseerde verwerking van de persoonsgegevens van de desbetreffende werknemer.

5.6. Persoonsgegevens verzameld tijdens het elektronisch toezicht mogen niet de enige criteria zijn om de prestaties van een werknemer te beoordelen (…)

6.14.

(1) Indien werknemers worden gecontroleerd moeten zij van tevoren zijn geïnformeerd over de redenen voor de controle, de controleperioden, de methoden en technieken en de gegevens die worden verzameld, en de werkgever dient het binnendringen in de persoonlijke levenssfeer van de werknemers zullen zoveel mogelijk te beperken.

(2) Geheime controle is alleen toegestaan:

a) indien de geheime controle niet strijdig is met de nationale wetgeving of

b) indien er gegronde redenen zijn om aan te nemen dat er sprake is van criminele activiteiten of ander ernstig wangedrag

(3) Permanente controle is alleen toegestaan als dit vereist is voor de gezondheid en veiligheid of voor de bescherming van eigendom (...)

12.2. Werknemersorganisaties dienen, in overeenstemming met de nationale wetgeving en de gebruiken, te worden geïnformeerd en geraadpleegd:

a) over de invoering of wijziging van geautomatiseerde systemen die persoonsgegevens van werknemers verwerken,

b) voordat wordt overgegaan tot het elektronisch controleren van het gedrag van werknemers op de werkplek

c) over het doel, de inhoud en de toepassing en interpretatie van vragenlijsten en tests betreffende de persoonsgegevens van de werknemers"

3. CONTROLE OP ELEKTRONISCHE COMMUNICATIE OP HET WERK VOLGENS RICHTLIJN 95/46/EG

Dit werkdocument is gebaseerd op de toepassing van de beginselen in Richtlijn 95/46/EG op het aan de orde zijnde vraagstuk, waarbij rekening wordt gehouden met artikel 8 van het *Europees Verdrag voor de bescherming van de rechten van de mens en de fundamentele vrijheden*, waarin staats dat eenieder recht heeft op respect voor zijn correspondentie en zijn privéleven.

De werkgever beschikt over talrijke vormen van toezicht op de werkplek en elk middel heeft zijn eigen problemen. In dit werkdocument worden twee vormen van toezicht behandeld waarop dezelfde beginselen van toepassing zijn; controle op e-mail en toezicht op de toegang tot internet.

Uitgangspunt is de bevestiging van het standpunt dat in Advies 8/2001 is geformuleerd, namelijk dat Richtlijn 95/46/EG van toepassing is op de verwerking van persoonsgegevens in een arbeidsverhouding zoals in elke andere context.[14] Naast de algemene Richtlijn 95/46/EG kan ook Richtlijn 97/66/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector van belang zijn. Deze richtlijn gaat dieper in en vormt een aanvulling op Richtlijn 95/46/EG m.b.t. de verwerking van persoonsgegevens in de telecommunicatiesector. Controle op elektronische communicatie, waaronder e-mail en internettoegang, door de werkgevers, valt niet alleen onder Richtlijn 95/46/EG maar waarschijnlijk ook onder Richtlijn 97/66/EG die momenteel wordt aangepast in het kader van een herziening van de communautaire regelgeving op het gebied van telecommunicatie. In de situaties waarin deze richtlijn van toepassing is, kunnen artikel 5 (vertrouwelijk karakter van de oproepen) en artikel 6 (verkeers- en rekeninggegevens) een heel belangrijke rol spelen.

3.1 ALGEMENE BEGINSELEN VAN TOEPASSING OP CONTROLE OP E-MAIL EN INTERNET

De volgende beginselen inzake gegevensbescherming zijn afgeleid van Richtlijn 95/46/EG en zouden moeten worden nageleefd bij de verwerking van persoonsgegevens die bij dergelijke controle plaatsvindt. Naleving van alle hiernavolgende beginselen is noodzakelijk, willen wij dat controle rechtmatig en verantwoord plaatsvindt.

3.1.1. NOODZAKELIJKHEID

Dit beginsel houdt in dat de werkgever moet nagaan of elke vorm van controle echt noodzakelijk is voor het specifieke doel, voordat hij daadwerkelijk tot een dergelijke controle overgaat. Traditionele methoden voor toezicht die minder ingrijpen in de persoonlijke levenssfeer van personen, moeten in overweging worden genomen en indien mogelijk worden toegepast voordat wordt overgegaan tot de controle van elektronische communicaties.

Alleen in uitzonderlijke omstandigheden zou het controleren van de e-mail of het internetgebruik van werknemers als noodzakelijk mogen worden beschouwd. De e-mail

[14] http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48en.pdf.

van een werknemer zou bijvoorbeeld mogen worden gecontroleerd indien dit noodzakelijk is om de bevestiging of het bewijs voor sommige acties van deze werknemer te verkrijgen. Tot dergelijke acties behoren criminele activiteiten van de werknemer, voorzover de werkgever hier zijn eigen belangen moet verdedigen, bijvoorbeeld wanneer hij indirect aansprakelijk is voor de acties van de werknemer. Deze activiteiten omvatten ook het opsporen van virussen en in het algemeen elke activiteit die door de werkgever wordt uitgevoerd om de veiligheid van het systeem te garanderen.

Het openen van de e-mail van een werknemer kan ook noodzakelijk zijn om andere redenen dan het controleren, bv. om correspondentie van een afwezige werknemer (bv. ziekte of vakantie) bij te houden die niet op een andere manier kan worden bijgehouden (bv. door automatisch beantwoorden of automatisch doorsturen).

Het noodzakelijkheidbeginsel houdt ook in dat een werkgever gegevens niet langer mag bewaren dan noodzakelijk is voor het specifieke doel van de controlerende activiteit.

3.1.2. DOELGERICHTHEID

Dit beginsel houdt in dat gegevens moeten worden verzameld voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en niet verder mogen worden verwerkt op een wijze die onverenigbaar is met die doeleinden. In deze context betekent het "verenigbaarheids"-beginsel dat, indien de verwerking van gegevens verantwoord is vanwege de veiligheid van het systeem, deze gegevens niet voor andere doeleinden zoals voor de controle van het gedrag van de werknemer mogen worden verwerkt.

3.1.3. TRANSPARANTIE

Dit beginsel betekent dat een werkgever over zijn activiteiten duidelijk en open moet zijn. Dit betekent dat geen geheime e-mailcontrole door werkgevers is toegestaan, behalve in de gevallen waarin een wetgeving in de lidstaat overeenkomstig artikel 13 van de richtlijn voorziet.[15] Dit is meestal het geval wanneer bepaalde criminele activiteiten aan het licht zijn gekomen (waarbij bewijs moet worden verzameld en de wetten en procedures van de lidstaten moeten worden nageleefd) of in die gevallen waarin de nationale wetgevingen, die in de noodzakelijke garanties voorzien, de werkgever toestaat stappen te ondernemen om overtredingen op de werkplek op te sporen.

Voorts kunnen in dit beginsel twee aspecten worden onderscheiden:

3.1.3.1. DE VERPLICHTING OM DE BETROKKENE INFORMATIE TE VERSTREKKEN

Dit is misschien het meest relevante voorbeeld van het transparantiebeginsel in de praktijk. Het betekent dat de werkgever aan zijn werknemers op een duidelijke en nauwkeurige manier zijn beleid inzake de controle op e-mail en internet moet uitleggen.

---

[15] Artikel 13 geeft de lidstaten de mogelijkheid wettelijke maatregelen te nemen ter beperking van de reikwijdte van de rechten en plichten waarin bepaalde artikelen van de richtlijn voorzien indien dit noodzakelijk is ter vrijwaring van belangrijke publieke belangen zoals de veiligheid van de Staat of het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten, of de bescherming van de betrokkene of van de rechten en vrijheden van anderen.

Werknemers moeten volledige informatie krijgen over de specifieke omstandigheden waarin een dergelijke uitzonderlijke maatregel verantwoord is en over de reikwijdte en omvang van de controle. Deze informatie moet omvatten:

1. Het e-mail/internetbeleid van het bedrijf waarbij gedetailleerd wordt aangegeven in hoeverre de communicatievoorzieningen van het bedrijf voor de persoonlijke communicatie van werknemers mogen worden gebruikt (bv. met beperkingen op tijdstip en duur).

2. De redenen waarom en doeleinden waarvoor eventuele controle wordt uitgevoerd. Wanneer de werkgever het gebruik van de communicatievoorzieningen van het bedrijf voor particulier gebruik heeft toegestaan, dan mogen deze privé communicaties onder zeer beperkte omstandigheden worden gecontroleerd, bijvoorbeeld om de veiligheid van het informatiesysteem te garanderen (virus checking).

3. De details van de controlemaatregelen, d.i. wie? wat? hoe? wanneer?

4. Informatie over handhavingsprocedures waarin wordt uiteengezet hoe en wanneer werknemers op de hoogte zullen worden gebracht van overtredingen van intern beleid en de mogelijkheid krijgen om tegen dergelijke claims tegen hen te reageren.

De Groep vindt het vanuit praktisch oogpunt wenselijk dat de werkgever de werknemer onmiddellijk op de hoogte brengt van elk geconstateerd misbruik van elektronische communicatie, tenzij geheim toezicht[16] om belangrijke redenen moet worden voortgezet, hetgeen normaal niet het geval is. Met behulp van speciale software kan direct informatie worden verstrekt, zoals waarschuwende windows die verschijnen en de werknemer erop wijzen dat het systeem ongeautoriseerd gebruik van het netwerk heeft ontdekt. Heel wat misverstanden zouden op die manier kunnen worden voorkomen.

Nog een voorbeeld van het transparantiebeginsel is de praktijk waarbij werkgevers werknemersvertegenwoordigers informeren en/of raadplegen voordat beleidsmaatregelen worden ingevoerd waarmee de werknemer te maken heeft. Er zij op gewezen dat beslissingen over de controle van werknemers, zoals het toezicht op de elektronische communicaties van de werknemers, onder de onlangs goedgekeurde Richtlijn 2002/14/EG vallen, op voorwaarde dat de desbetreffende onderneming binnen het toepassingsgebied van de richtlijn valt. Met name voorziet de richtlijn in de verplichting om informatie te verstrekken aan of overleg te voeren met werknemers m.b.t. beslissingen die tot ingrijpende wijzigingen kunnen leiden in de werkorganisatie of in de contractuele relaties. In nationale wetgeving of cao's kunnen regelingen zijn uitgewerkt die voor de werknemers nog gunstiger zijn.

Collectieve arbeidsovereenkomsten kunnen niet alleen de werkgever ertoe verplichten de werknemersvertegenwoordigers te informeren en te raadplegen voordat controlesystemen worden ingevoerd, maar kunnen de invoering ervan

[16] Gevallen van verantwoord geheim toezicht zouden hier een goed voorbeeld vormen.

afhankelijk maken van de voorafgaande toestemming van de werknemersvertegenwoordigers.

In collectieve overeenkomsten kan ook worden vastgelegd in hoeverre werknemers gebruik kunnen maken van internet en e-mail en op welke manier dit gebruik kan worden gecontroleerd.

3.1.3.2. DE VERPLICHTING OM DE TOEZICHTHOUDENDE AUTORITEITEN OP DE HOOGTE TE BRENGEN VOORDAT WORDT OVERGEGAAN TOT EEN OF MEER VOLLEDIG OF GEDEELTELIJK GEAUTOMATISEERDE VERWERKINGEN VAN GEGEVENS

Dit is een andere manier om voor transparantie te zorgen aangezien werknemers, wanneer de werkgever de persoonsgegevens van zijn werknemers verwerkt, altijd in de gegevensbeschermingregisters kunnen nagaan om welke categorieën gegevens het gaat, met welk doel en voor wie de verwerking plaatsvindt.

3.1.3.3. RECHT VAN TOEGANG

Een werknemer, alsmede ieder individu als bedoeld in de richtlijn[17], heeft een recht van toegang tot zijn persoonsgegevens die door zijn werkgever worden verwerkt en kan waar nodig eisen dat gegevens die niet beantwoorden aan de bepalingen van de richtlijn, met name omdat ze onvolledig of onjuist zijn, worden gecorrigeerd, gewist of afgeschermd.

Toegang tot de bestanden van de werkgever, vrijelijk en zonder beperking, met redelijke tussenpozen en zonder bovenmatige vertraging of kosten, is een efficiënt instrument waarvan iedere werknemer afzonderlijk gebruik kan maken om ervoor te zorgen dat de controlerende activiteiten op de werkplek voor de werknemers

---

[17] Artikel 12: de lidstaten waarborgen elke betrokkene het recht van de voor de verwerking verantwoordelijke te verkrijgen:

a) vrijelijk en zonder beperking, met redelijke tussenpozen en zonder bovenmatige vertraging of kosten:

- uitsluitsel omtrent het al dan niet bestaan van verwerkingen van hem betreffende gegevens, alsmede ten minste informatie over de doeleinden van deze verwerkingen, de categorieën gegevens waarop deze verwerkingen betrekking hebben en de ontvangers of categorieën ontvangers aan wie de gegevens worden verstrekt;

- verstrekking, in begrijpelijke vorm, van de gegevens die zijn verwerkt, alsmede de beschikbare informatie over de oorsprong van de gegevens;

- mededeling van de logica die ten grondslag ligt aan de automatische verwerking van hem betreffende gegevens, in elk geval als het gaat om de geautomatiseerde besluiten als bedoeld in artikel 15, lid 1;

b) naar gelang van het geval, de rectificatie, de uitwissing of de afscherming van de gegevens waarvan de verwerking niet overeenstemt met de bepalingen van deze richtlijn, met name op grond van het onvolledige of onjuiste karakter van de gegevens;

c) kennisgeving aan derden aan wie de gegevens zijn verstrekt, van elke rectificatie, uitwissing of afscherming, uitgevoerd overeenkomstig punt b), tenzij zulks onmogelijk blijkt of onevenredig veel moeite kost.

rechtmatig en eerlijk verlopen. In uitzonderlijke omstandigheden kan de toegang tot de bestanden van de werkgever problematisch zijn, bv. als het gaat om de zogenaamde beoordelingsgegevens.

De Groep heeft hierover reeds een standpunt ingenomen[18] en kan in de toekomst nog meer adviezen geven op grond van de opgedane ervaring.

3.1.4. RECHTMATIGHEID

Dit beginsel betekent dat elke gegevensverwerking slechts kan plaatsvinden als zij een rechtmatig doel heeft, als bedoeld in art. 7 van de richtlijn en de nationale wetgeving die de richtlijn omzet. Art. 7 (f) van de richtlijn is, wat dit beginsel betreft, heel belangrijk, omdat daarin wordt gezegd dat het verwerken van de gegevens van werknemers overeenkomstig Richtlijn 95/46/EG pas mogelijk is als de verwerking noodzakelijk is voor de behartiging van het rechtmatige belang van de werkgever en als geen afbreuk wordt gedaan aan de fundamentele rechten van de werknemers.

De noodzaak voor de werkgever om zijn bedrijf te beschermen, bijvoorbeeld om te voorkomen dat vertrouwelijke informatie aan een concurrent wordt doorgegeven, kan een dergelijk rechtmatig belang zijn.

De verwerking van gevoelige gegevens is in dit verband bijzonder problematisch, aangezien artikel 8 van de richtlijn geen belangenafweging mogelijk maakt in de zin van artikel 7 (f) van de richtlijn. In lid 2, sub b) van artikel 8 heeft men het echter over “de verwerking die noodzakelijk is met het oog op de uitvoering van de verplichtingen en de rechten van de voor de verwerking verantwoordelijke inzake arbeidsrecht, voorzover zulks is toegestaan bij de nationale wetgeving en deze adequate garanties biedt”.

Het verwerken van gevoelige gegevens in verbinding met controlerende activiteiten is een moeilijk vraagstuk dat niet alleen in het kader van een arbeidsverhouding van belang is. Het is een algemeen vraagstuk waarover de Groep in de toekomst nog advies zal uitbrengen.

Tenzij nationale wetgeving hierin speciaal voorziet en ook passende garanties biedt, vinden controlerende activiteiten die direct bedoeld zijn om gevoelige gegevens van werknemers te verwerken geen rechtmatigheid in de bepalingen van richtlijn 95/46/EG en zijn derhalve niet aanvaardbaar. Het voorkomen of bemoeilijken van controlerende activiteiten (die in talrijke gevallen niet alleen rechtmatig zijn maar ook wenselijk, bijvoorbeeld om de veiligheid van het systeem te waarborgen), alleen vanwege het feit dat het verwerken van sommige gevoelige gegevens onvermijdbaar kan zijn, is evenmin acceptabel.

3.1.5. EVENREDIGHEID

Dit beginsel houdt in dat persoonsgegevens die voor controle worden bewaard of gebruikt, toereikend, ter zake dienend en niet bovenmatig moeten zijn voor het doel waarvoor de controle wordt gerechtvaardigd. Het beleid van het bedrijf op dit gebied zou op maat gesneden moeten zijn, overeenkomstig het type gevaar en de mate waarin het bedrijf hiermee wordt geconfronteerd.

---

[18] Zie Aanbeveling 1/2001 over beoordelingsgegevens betreffende werknemers

Een algemene controle van de e-mails en het internetgebruik van alle medewerkers is volgens het evenredigheidbeginsel dan ook uit den boze, tenzij het noodzakelijk is om de veiligheid van het systeem te garanderen. Indien het vastgestelde doel op een minder indringerige manier kan worden bereikt, moeten de werkgever deze mogelijkheid in overweging nemen (bv., hij moeten systemen vermijden die automatisch en continu controleren).

Het controleren van een e-mails zou, zo mogelijk, geen betrekking mogen hebben op de inhoud van de communicaties, maar alleen op het gegevensverkeer en het tijdstip, indien dit voldoende is om de bezorgdheid van de werkgevers weg te nemen. Indien toegang tot de inhoud van het bericht toch noodzakelijk is, dient ook rekening te worden gehouden met de privacy van de degenen die buiten de organisatie eveneens het bericht ontvangen. De werkgever kan bijvoorbeeld niet te rekenen op instemming van degenen die buiten de organisatie e-mails naar zijn werknemers sturen. De werkgever moet redelijke inspanningen leveren om de personen buiten de organisatie op de hoogte brengen van het bestaan van controlerende activiteiten, aangezien deze ook van invloed zijn op die personen van buiten de organisatie. Er zouden bijvoorbeeld waarschuwende berichten over het bestaan van de controlesystemen kunnen worden toegevoegd aan alle uitgaande berichten van de organisatie.

De technologie geeft de werkgever voldoende mogelijkheden om het gebruik van e-mail door zijn werknemers te beoordelen, door bv. het aantal verstuurde of ontvangen mails te controleren, of het formaat van de attachments, en daarom is het openen van de mails zelf niet nodig. Technologie kan verder worden gebruikt om ervoor te zorgen dat de maatregelen die een werkgever neemt om de internettoegang die hij aan zijn werknemers verleent te vrijwaren van misbruik, evenredig zijn door blokkerende voorzieningen te gebruiken in plaats van controlerende. [19]
Systemen voor de verwerking van elektronische communicaties moeten zodanig worden ontworpen dat de hoeveelheid verwerkte persoonsgegevens tot een strikt minimum wordt beperkt[20].

Wat het vraagstuk van evenredigheid betreft, zij erop gewezen dat cao- onderhandelingen zeer nuttig kunnen zijn om te besluiten welke acties in verhouding staan tot welke gevaren waarmee de werkgever wordt geconfronteerd. Werkgevers en werknemers kunnen op die manier tot overeenstemming komen over de manier waarop met beider belangen rekening kan worden gehouden.

---

[19] Wat dit gebruik van de technologie betreft, zijn er in de praktijk al talrijke voorbeelden voorhanden.

internet: sommige bedrijven gebruiken software die zodanig kan worden geconfigureerd dat elke verbinding met bepaalde categorieën websites wordt geblokkeerd. De werkgever kan na de aanvaarde lijst van door zijn werknemers bekeken websites te hebben geraadpleegd, besluiten om aan de lijst van reeds geblokkeerde websites andere toe te voegen (na zijn werknemers ervan op de hoogte te hebben gebracht dat een verbinding met een dergelijke site wordt geblokkeerd, behalve indien de noodzaak van een verbinding met deze site door een werknemer wordt aangetoond).

E-mail: andere bedrijven maken gebruik van een automatische doorstuurvoorziening naar een aparte server voor alle e-mails die een bepaalde omvang overschrijden. De ontvanger voor wie e-mail is bestemd, wordt automatisch geïnformeerd dat een verdachte e-mail naar die server is gestuurd en daar kan worden ingekeken.

[20] Ontwerp-richtlijn 97/66, considerans 30

3.1.6. NAUWKEURIGHEID EN BEWARING VAN GEGEVENS

Volgens dit beginsel moeten gegevens die rechtmatig door een werkgever zijn opgeslagen (na zich ervan vergewist te hebben dat alle andere in dit hoofdstuk uiteengezette beginselen zijn nageleefd) en die verband houden met het e-mailadres van de werknemers of hun gebruik van internet, nauwkeurig en bijgewerkt zijn en mogen zij niet langer dan noodzakelijk worden bewaard. Werkgevers moeten aangeven hoe lang e-mails in hun centrale servers, afhankelijk van de behoeften van het bedrijf, worden bewaard. Een bewaarperiode van de langer dan drie maanden kan moeilijk worden verantwoord.

3.1.7. BEVEILIGING

De werkgever moet op het werk passende technische en organisatorische maatregelen ten uitvoer leggen om te garanderen dat de persoonsgegevens van zijn werknemers veilig worden bewaard. Dit omvat ook het recht van de werkgever om zijn systeem tegen virussen te beschermen en kan leiden tot het automatisch scannen van e-mails en verkeersgegevens van het netwerk.

De Groep is van mening dat, gezien het belang van een veilig systeem, het automatisch openen van e-mails niet als een schending van het privacyrecht van de werknemers mag worden beschouwd, op voorwaarde dat passende garanties voorhanden zijn. Werkgevers kunnen thans beschikken over technologieën die hun veiligheidsbelangen dienen zonder dat de privacyrechten van de werknemers worden geschonden.

In dit verband wijst de Groep artikel 29 op de rol van de systeembeheerder, een werknemer die uit het oogpunt van de gegevensbescherming grote verantwoordelijkheden heeft. Het is van kapitaal belang dat de systeembeheerder en iedereen die toegang heeft tot de persoonsgegevens van de werknemers tijdens de controle, zich aan het beroepsgeheim houden m.b.t. de vertrouwelijke informatie waartoe zij toegang hebben.

4. CONTROLE OP E-MAIL

4.1. DE GEHEIMHOUDING VAN CORRESPONDENTIE

Zoals eerder een dit document reeds is aangegeven is de Groep van mening dat on line en off line situaties niet verschillend mogen worden behandeld en e-mail moet als zodanig dezelfde bescherming van fundamentele rechten krijgen als traditionele brieven[21]. De jurisprudentie van het *Europees Hof voor de rechten van de mens* geeft richtsnoeren voor de toepassing van het principe van geheimhouding van correspondentie in een democratische samenleving. De lidstaten interpreteren dit beginsel echter enigszins verschillend, vooral wat de toepassing ervan betreft op communicaties op het werk, zowel m.b.t. de inhoud als tot het gegevensverkeer. Dit heeft voor de gegevensbescherming belangrijke consequenties, vooral wanneer moet worden vastgesteld in welke mate het controleren van de e-mail van werknemers gerechtvaardigd is.

De Groep artikel 29 is van mening dat de begrippen "privéleven" en "correspondentie" in de zin van artikel 8, lid 1, van het Europees Verdrag, van toepassing zijn op elektronische communicaties die in de gebouwen van een bedrijf tot stand worden gebracht. Er is hier weinig ruimte voor interpretatie aangezien er over dit vraagstuk reeds een duidelijke uitspraak van het Hof is geweest, namelijk in de hierboven vermelde zaak **Halford v. het Verenigd Koninkrijk.**

Het enige punt waar nog ruimte voor interpretatie lijkt te zijn, is de vraag in welke mate afwijkingen van of beperkingen op dit principe mogelijk zijn, met name wanneer het wordt afgewogen tegen de rechten en vrijheden van anderen die op een soortgelijke manier door het Verdrag worden beschermd (bv. de rechtmatige belangen van de werkgever). **Het huren en bezitten van de gebruikte elektronische middelen laat geheimhouding van communicaties en correspondentie, zoals vastgelegd in fundamentele wettelijke beginselen en grondwetten, onverlet.**

De Groep artikel 29 zou er niettemin nogmaals op willen wijzen dat dit geen specifiek probleem is voor de verwerking van persoonsgegevens in een arbeidsverhouding, maar een algemeen probleem dat zijn oorsprong vindt in het feit dat wetten en voorschriften betreffende gegevensbescherming niet theoretisch kunnen worden toegepast. Rechten in verband met gegevensbescherming moeten op verschillende wettelijke systemen kunnen worden toegepast, met andere wetten die voorzien in andere rechten en verplichtingen voor personen (bv. arbeidswetgeving). De Groep artikel 29 is er niettemin van overtuigd dat de oplossingen die in dit werkdocument worden voorgesteld nuttig kunnen zijn

---

[21] In een van de eerste aanbevelingen van de Groep, Aanbeveling 3/97 "Anonimiteit op internet" staat reeds dat on en off line situaties op dezelfde manier moeten worden behandeld.

Zie http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48en.pdf.

In het werkdocument van de Task Force Internet, het belangrijkste document dat door de Groep over privacy op internet is goedgekeurd, wordt in hoofdstuk 3,op bladzijde 21 nadrukkelijk op dit idee gewezen:

Zie http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48en.pdf.

wanneer deze moeilijke afweging van verschillende belangen op de juiste manier wordt uitgevoerd.

4.2. RECHTVAARDIGING OP GROND VAN RICHTLIJN 95/46/EG

E-mails bevatten persoonsgegevens waarop de bepalingen van Richtlijn 95/46/EG van toepassing zijn en daarom moeten werkgevers aanvaardbare redenen hebben om deze gegevens te verwerken. Zoals reeds uitvoerig in Advies 8/2001 is uiteengezet, moeten werknemers volledig geïnformeerd zijn en vrijelijk hun toestemming kunnen geven en mogen werkgevers deze toestemming niet gebruiken als een algemeen middel om de verwerking te rechtvaardigen.

De meest aanvaardbare rechtvaardiging voor controle van e-mail staat in artikel 7 (f) van de richtlijn, namelijk wanneer de verwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van de voor de verwerking verantwoordelijke of van de derde(n) aan wie de gegevens worden verstrekt. Voordat de toepassing van deze bepaling op de punten die hier aan de orde zijn wordt geanalyseerd, moet er op gewezen worden dat dergelijke rechtvaardiging de fundamentele rechten en vrijheden van de werknemer niet te niet kan doen. Dit omvat ook het fundamentele recht op geheimhouding van correspondentie.

De Groep heeft reeds het standpunt ingenomen dat[22]

"wanneer een werkgever als noodzakelijk en onvermijdbaar gevolg van de arbeidsverhouding persoonsgegevens moet verwerken, het misleidend is indien hij deze verwerking door middel van toestemming tracht te wettigen. Zich baseren op toestemming moet worden beperkt tot gevallen waarin de werknemer een echte vrije keuze heeft en nadien de mogelijkheid heeft om de toestemming zonder nadeel in te trekken."

Aangezien e-mails zowel persoonsgegevens van de afzender als van de ontvanger bevatten en werkgevers meestal alleen de toestemming van een van deze partijen zonder grote moeilijkheden kunnen krijgen (tenzij de e-mails correspondentie tussen medewerkers onderling omvatten) is de mogelijkheid om het controleren van e-mails op basis van toestemming te rechtvaardigen, zeer beperkt. Soortgelijke overwegingen gelden ook voor artikel 7 (b) van de richtlijn, aangezien een van de partijen nooit een overeenkomst zou hebben met de voor de gegevens verantwoordelijke in de zin van deze bepaling, bv. om de mail te controleren.

Het verdient aanbeveling er hier op te wijzen dat wanneer een werknemer een e-mailadres voor persoonlijk gebruik heeft gekregen of toegang tot een webmailadres, het openen van e-mail in dit adres door de werkgever (afgezien van het scannen van virussen) alleen kan worden verantwoord onder zeer beperkte omstandigheden[23] en onder normale

---

[22] Zie alinea in het kader op bladzijde 23 van advies 8/2001.

[23] Tot dergelijke acties behoren criminele activiteiten van de werknemer, voorzover de werkgever hier zijn eigen belangen moet verdedigen, bijvoorbeeld wanneer hij aansprakelijk is voor de acties van de werknemer, of wanneer hij het slachtoffer is van de criminele activiteit.

omstandigheden niet op basis van artikel 7 (f) omdat het niet tot de rechtmatige belangen van de werkgever behoort toegang tot dergelijke gegevens te hebben. Hier prevaleert het fundamentele recht op geheimhouding van correspondentie.

Daarom kan op de vraag in hoeverre artikel 7 (f) de controle van e-mail toestaat alleen geval per geval een antwoord worden gegeven, op basis van de in hoofdstuk 3. 2. uiteengezette fundamentele principes. Zoals in hoofdstuk 3.1.4 (rechtmatigheid) reeds is aangegeven, moet bij het maken van deze afweging terdege rekening worden gehouden met de privacy van degenen die zich buiten de organisatie bevinden maar toch door de controle worden beïnvloed.

4.3 AANBEVOLEN MINIMUMINFORMATIE DIE HET BEDRIJF AAN ZIJN WERKNEMERS MOET VERSTREKKEN

Bij de uitstippeling van hun beleid dienen werkgevers zich te houden aan de principes die in hoofdstuk 3.1.3 onder het algemene Transparantiebeginsel[24] zijn uiteengezet, in het licht van de behoeften en de omvang van de organisatie.

In verband met e-mail moeten met name de volgende punten worden opgehelderd;

a) Heeft een werknemer het recht op een e-mailadres voor persoonlijk gebruik, of is het gebruik van webmailadressen tijdens het werk toegestaan, of is de werkgever voorstander van het gebruik door werknemers van een privé webmailadres om over e-mailadres voor persoonlijk gebruik te beschikken (zie hoofdstuk 4.4).

b) De afspraken die met werknemers worden gemaakt om toegang tot de inhoud van e-mail te hebben, bijvoorbeeld wanneer de werknemer onverwacht afwezig is, en het specifieke doel van deze toegang.

c) Wanneer een backupkopie van e-mailberichten wordt gemaakt, de bewaarperiode hiervan.

d) Informatie over het tijdstip waarop e-mails definitief op de server worden gewist.

e) Beveiliging

24

1. Het e-mail/internetbeleid van het bedrijf waarbij gedetailleerd wordt aangegeven in hoeverre de communicatievoorzieningen van het bedrijf voor de persoonlijke communicatie van werknemers mogen worden gebruikt (bv. met beperkingen op tijdstip en duur).

2. De redenen waarom en doeleinden waarvoor eventuele controle worden uitgevoerd. Wanneer de werkgever het gebruik van de communicatievoorzieningen van het bedrijf voor particulier gebruik heeft toegestaan, dan mogen deze privé communicaties onder zeer beperkte omstandigheden worden gecontroleerd, bijvoorbeeld om de veiligheid van het informatiesysteem te garanderen (virus checking).

3. De details van de controlemaatregelen, d.i. wie? wat? hoe? wanneer?

4. Informatie over handhavingsprocedures waarin wordt uiteengezet hoe en wanneer werknemers op de hoogte zullen worden gebracht van overtredingen van intern beleid en de mogelijkheid krijgen om tegen dergelijke claims tegen hen te reageren.

f) De participatie van de werknemersvertegenwoordiging bij het uitstippelen van het beleid.

Het spreekt vanzelf dat werkgevers de plicht hebben dit beleid continu aan te passen aan de technologische ontwikkelingen en de standpunten van de werknemers.

4.4 WEBMAIL[25]

De Groep is van mening dat een dergelijk beleid waarbij werknemers gebruik kunnen maken van een privé-adres of van webmail kan bijdragen tot een praktische oplossing voor het probleem dat hier aan de orde is. Een dergelijke document opgesteld door de werkgever zou het onderscheid tussen e-mail voor professioneel gebruik en e-mail voor particulier gebruik verduidelijken en zou het gevaar dat werkgevers binnendringen in de persoonlijke levenssfeer van hun werknemers beperken. Voorts zou dit voor de werkgever geen of slechts minimale extra kosten met zich brengen.

Met een dergelijk beleid kan de werkgever, in specifieke situaties waarbij er een ernstig vermoeden is m.b.t. het gedrag van een werknemer, nagaan in welke mate de werknemer zijn PC voor persoonlijke doeleinden gebruikt, door de tijd die hij aan webmailadressen besteedt, te registreren. Op die manier kunnen de belangen van de werkgevers worden gevrijwaard zonder dat de persoonsgegevens van de werknemers, er met name de gevoelige gegevens, worden ontsloten.

Bovendien komt een dergelijk beleid de werknemers ten goede, aangezien het zekerheid geeft m.b.t. het niveau van privacy dat zij kunnen verwachten, hetgeen in de meer complexe en onduidelijke gedragscodes zou kunnen ontbreken. Het is voorts noodzakelijk erop te wijzen dat:

a) **het feit dat het gebruik van webmail of privé-adressen is toegestaan, doet geen afbreuk aan de volledige toepassing van de andere onderdelen van dit hoofdstuk op andere e-mailadressen op de werkplek**

b) wanneer het gebruik van webmail wordt toegestaan moeten de bedrijven zich ervan bewust zijn dat dit gebruik van invloed kan zijn op de netwerken van het bedrijf, vooral m.b.t. het verspreiden van virussen.

c) werknemers moeten zich ervan bewust zijn dat servers van webmail zich soms in derde landen bevinden waar de persoonsgegevens van mensen misschien niet passend worden beschermd.

Deze overwegingen gelden voor de normale verhoudingen tussen de werkgever en werknemer. Misschien zijn er speciale regels nodig voor de communicatie van werknemers die door beroepsgeheim aan speciale verplichtingen zijn gebonden.

---

[25] Webmail is een mailsysteem op het web dat weggebaseerde e-mail van elke POP of IMAP server aanbiedt die meestal beschermd is met een gebruikersnaam en een password.

5. CONTROLE OP INTERNETTOEGANG

5.1 PRIVÉ-GEBRUIK VAN INTERNET OP HET WERK

In de eerste plaats moet erop gewezen worden dat het aan de bedrijven zelf is te beslissen of werknemers op internet mogen voor privé-gebruik en over de mate waarin dit wordt toegestaan.

Afgezien hiervan is de Groep van mening dat een algemeen verbod op persoonlijk gebruik van internet door werknemers niet praktisch en enigszins onrealistisch is, omdat op die manier de mate waarin internet werknemers in hun dagelijkse leven kan bijstaan niet af te leiden is.

5.2. BEGINSELEN IN VERBAND MET INTERNETCONTROLE

Voor de controle van de toegang van de werknemers tot internet kunnen sommige beginselen worden toegepast.

In de mate van het mogelijke moet **preventie belangrijker zijn dan opsporing**. M.a.w., het belang van de werkgever is beter gediend met het voorkomen van misbruik van internet met behulp van technische middelen dan met het besteden van middelen aan opsporing van misbruik. In de mate van een mogelijke moet een internetbeleid gebaseerd zijn op technische middelen om de toegang te beperken in plaats van op het controleren van gedrag, bv. door sommige sites te blokkeren of automatische toegangswaarschuwingen te installeren.

Het onmiddellijk waarschuwen van de werknemer dat een verdacht gebruik van internet is geïdentificeerd, is belangrijk om problemen zo klein mogelijk te houden. Indien controle echter noodzakelijk is, moet dit **in verhouding staan** tot het risico dat de werkgever loopt. In de meeste gevallen kan misbruik van internet worden opgespoord zonder dat de inhoud van de bekeken sites moet worden geanalyseerd. Bijvoorbeeld, de controle van de bestede tijd, of de controle van de meeste bezochte sites door een afdeling kunnen voldoende zijn om de werkgever de zekerheid te geven dat zijn voorzieningen niet worden misbruikt. Als uit deze algemene controle blijkt dat internet toch wordt misbruikt kan de werkgever extra controle op het desbetreffende gebied uitvoeren.

Bij de beoordeling van het internetgebruik door werknemers moeten werkgevers **zorgvuldig zijn bij het formuleren van hun conclusies**; zij moeten namelijk voor ogen houden dat websites gemakkelijk onopzettelijk door onverwachte antwoorden van zoekinstrumenten kunnen worden bezocht, dat hypertextlinks onduidelijk kunnen zijn, dat reclamebanners misleidend kunnen zijn en dat bij het intoetsen fouten kunnen worden gemaakt. In ieder geval moeten de feiten aan de werknemers worden voorgelegd en deze moeten de kans krijgen om het door de werkgever aan de kaak gestelde misbruik, te weerleggen.

5.3 AANBEVOLEN MINIMUMINHOUD VAN HET INTERNETBELEID VAN EEN BEDRIJF

1. De in hoofdstuk 3.1.3 onder het transparantiebeginsel vermelde informatie[26]

   In verband met internetgebruik moet met name met de volgende punten rekening worden gehouden;

2. De werkgever moet aan de werknemers duidelijk de voorwaarden uiteenzetten waaronder privé-gebruik van internet wordt toegestaan en het materiaal aangeven dat niet kan worden bekeken of gekopieerd. Deze voorwaarden en restricties moeten aan de werknemers worden uitgelegd.

3. Werknemers moeten informatie krijgen over de systemen die worden gebruikt om toegang tot bepaalde sites tegen te gaan en om misbruik op te sporen. De omstandigheden van de controle moeten worden gespecificeerd: bv. heeft de controle betrekking op bepaalde personen of afdelingen van het bedrijf, of wordt de inhoud van de bezochte sites door de werkgever onder bepaalde omstandigheden bekeken of geregistreerd. Voorts dient het beleid duidelijk aan te geven wat er gebeurt met gegevens die eventueel worden verzameld over personen die bepaalde sites hebben bezocht.

4. Werknemers moeten geïnformeerd worden over de taak van hun vertegenwoordigers, zowel bij de tenuitvoerlegging van dit beleid als bij het onderzoek naar vermeende overtredingen.

CONCLUSIE

De Groep heeft dit werkdocument opgesteld om een bijdrage te leveren aan de uniforme toepassing van de nationale maatregelen goedgekeurd op grond van Richtlijn 95/46/EG op het gebied van de controle op elektronische communicaties op het werk. (Zie de overzichten van de nationale wetgevingen in de bijlage bij dit document).

De Groep heeft op gebieden die verband houden met gegevensbescherming verschillen tussen de nationale wetgevingen geconstateerd, hoofdzakelijk met betrekking tot toegestane afwijkingen van het fundamentele recht op geheimhouding van correspondentie en de reikwijdte en het effect van in cao's vastgelegde werknemersvertegenwoordiging en medezeggenschap. De Groep artikel 29 wil er

---

26

1. Het e-mail/internetbeleid van het bedrijf waarbij gedetailleerd wordt aangegeven in hoeverre de communicatievoorzieningen van het bedrijf voor de persoonlijke communicatie van werknemers mogen worden gebruikt (bv. met beperkingen op tijdstip en duur).

2. De redenen waarom en doeleinden waarvoor eventuele controle worden uitgevoerd. Wanneer de werkgever het gebruik van de communicatievoorzieningen van het bedrijf voor particulier gebruik heeft toegestaan, dan mogen deze privé communicaties onder zeer beperkte omstandigheden worden gecontroleerd, bijvoorbeeld om de veiligheid van het informatiesysteem te garanderen (virus checking).

3. De details van de controlemaatregelen, d.i. wie? wat? hoe? wanneer?

4. Informatie over handhavingsprocedures waarin wordt uiteengezet hoe en wanneer werknemers op de hoogte zullen worden gebracht van overtredingen van intern beleid en de mogelijkheid krijgen om tegen dergelijke claims tegen hen te reageren.

niettemin nadruk op leggen dat verschillen tussen de nationale wetgevingen die Richtlijn 95/46/EG omzetten, geen onoverkoombaar obstakel vormen voor een gemeenschappelijke benadering die gevormd wordt door de beginselen en de goede praktijken die in dit werkdocument zijn uiteengezet.

De Subgroep voor arbeidsverhoudingen zal dit werkdocument steeds opnieuw bekijken in het licht van de ervaring en de verdere ontwikkelingen op dit gebied in de periode 2002-2003.

Gedaan te Brussel, 29 mei 2002

Voor de Groep

De voorzitter

Stefano RODOTA