KONINKRIJK BELGIE

COMMISSIE VOOR DE BESCHERMING VAN DE PERSOONLIJKE LEVENSSFEER

Brussel,

Adres : Hoogstraat, 139, B-1000 Brussel
Tel.: +32(0)2/213.85.40 E-mail : commission@privacycommission.be
Fax.: +32(0)2/213.85.65 http://www.privacycommission.be

ADVIES Nr 21 / 2006 van 12 juli 2006

O. Ref. : SA2 / A / 2006 / 17

BETREFT : Advies met betrekking tot de deontologische code van de Federale Overheidsdienst Economie, KMO, Middenstand & Energie voor het gebruik van informaticamiddelen en elektronische gegevensverwerking.

De Commissie voor de bescherming van de persoonlijke levenssfeer;

Gelet op de wet van 8 december 1992 betreffende de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, inzonderheid art. 29;

Gelet op de adviesaanvraag vanwege de Minister van Economie, KMO, Middenstand & Energie van 11 mei 2006;

Gelet op het verslag van de heer Mertens de Wilmars;

Brengt op 12 juli 2006 het volgende advies uit:

I. VOORWERP VAN DE AANVRAAG

Door de Minister van Economie, KMO, Middenstand & Energie is aan de Commissie gevraagd een advies uit te brengen over de deontologische code van de Federale Overheidsdienst Economie, KMO, Middenstand & Energie (hierna FOD Economie) voor het gebruik van informaticamiddelen en elektronische gegevensverwerking.

II. ALGEMENE BESPREKING

---

1. De deontologische code strekt ertoe de medewerkers van de FOD Economie duidelijke richtlijnen te geven over hoe zij moeten en mogen omgaan met de informaticamiddelen en de informatie die hen voor de uitoefening van hun job ter beschikking worden gesteld. Daarnaast is het de bedoeling alle medewerkers via deze richtlijnen te sensibiliseren voor de belangrijke problematiek van beveiliging en bescherming van de systemen en gegevens van de FOD Economie.

2. Het bevat meer bepaald een opsomming van concrete richtlijnen en aanbevelingen, inclusief een samenvatting ervan, welke handelen over eigendom en beheer van materiaal, bescherming van gegevens, gebruikersidentificatie en paswoordbeleid, gebruik ven email, gebruik van internet, beveiliging van de werkplaats, logging, auditing en sancties.

3. De Commissie wenst te onderstrepen dat het initiatief zelf van een code met gedragsregels waaraan de personeelsleden van de FOD Economie zich moeten houden, indien hen door hun werkgever digitale communicatievoorzieningen ter beschikking worden gesteld, uiteraard alleen maar kan toegejuicht worden: die personeelsleden moeten, overeenkomstig artikel 9 van de wet van 8 december 1992 *betreffende de bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens* (hierna WVP), inderdaad weten wat inzake gebruik van internet en e-mail op de werkplek toegelaten is, wat de beperkingen en grenzen zijn aan het toegelaten gebruik en wat verboden is, evenals betreffende het bestaan en de modaliteiten van een patronale controle op dat gebruik.

4. De Commissie wijst er voorts op dat zij zich reeds verschillende malen heeft uitgesproken over 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 personeel1..

5. Ook de Groep 29, het onafhankelijk EU-adviesorgaan dat is samengesteld uit vertegenwoordigers van de gegevensbeschermingsautoriteiten van de lidstaten, waaronder België, heeft zich reeds gebogen over de problematiek die voorligt in haar werkdocument van 29 mei 2002 *over de controle op elektronische communicatie op het werk*[2].

---

[1] Met name in het algemeen advies uit eigen beweging van 3 april 2000 *betreffende het toezicht door de werkgever op het gebruik van het informaticasysteem op de werkplaats*, en nadien bijvoorbeeld in het advies uit eigen beweging *betreffende het voorstel van wet 2-891/1 van 29 augustus 2001 betreffende het reglementeren van het gebruik van telecommunicatiemiddelen op de werkplaats* van 8 oktober 2001, het advies (op klacht) van 27 februari 2003 *inzake de controle door de werkgever van de communicatiegegevens van een van zijn werknemers*, het advies *over de gedragscode voor de personeelsleden van het Ministerie van de Vlaamse Gemeenschap* van 18 december 2003 en het advies van 16 september 2005 *met betrekking tot een ontwerpbesluit van de Regering van de Franse Gemeenschap houdende de gedragscode voor gebruikers van informaticasystemen, e-mail en internet binnen de diensten van de Regering van de Franse Gemeenschap, en de instellingen van openbaar nut die onder het Comité van Sector XVII ressorteren.* Deze adviezen kunnen geraadpleegd worden op de website van de Commissie: www.privacycommission.be.

[2] Te vinden op http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_nl.pdf

III. CONCRETE BESPREKING

---

6. Hierna wordt enkel ingegaan op bepalingen uit de gedragscode waarvan de Commissie van oordeel is dat ze een zekere toelichting behoeven. Daarbij wordt de inhoudsopgave van de code zoals ze voorkomt in de samenvatting, aangehouden.

7. De Commissie zal zich voornamelijk focussen op de auditing, dus de controle door de FOD Economie in zijn hoedanigheid van werkgever op het gebruik van internet en email van zijn personeelsleden. Immers, ter gelegenheid van dergelijke controles (elektronisch toezicht) zullen persoonsgegevens van personeelsleden worden verwerkt, en dient de WVP dus nageleefd te worden.

Inleiding

8. Uit de inleiding bij de code blijkt dat elk personeelslid een exemplaar van de code ontvangt en tekent voor ontvangt ervan, als voorwaarde om toegang te krijgen tot de verschillende informatie-systemen van de FOD Economie. Ingeval van vragen of onduidelijkheden over de code kunnen de personeelsleden terecht bij een helpdesk.

9. De Commissie merkt dienaangaande op dat tekenen voor ontvangst niet gelijkstaat met het verkrijgen van de toestemming van de personeelsleden, inzonderheid voor wat betreft de verwerking van hun persoongegevens voor bepaalde controlemaatregelen zoals omschreven in de deontologische code. Een dergelijke toestemming dringt zich in principe evenwel op, gelet op de toepasselijkheid van de communicatiewetgeving (zie infra).

10. Tenzij men aanneemt dat een akkoord van de vertegenwoordigers van de personeelsleden kan doorgaan als een toestemming van de betrokkenen zelf, zal dergelijk akkoord minstens kunnen bijdragen tot een verhoogde transparantie van de beoogde controle, tot een beter evenwicht tussen de rechten van de personeelsleden en de werkgever en tot de vrije aard van de instemming van het individuele personeelslid.

11. Aangezien de code, indien nodig, zal herzien en bijgewerkt worden, dienen eventuele wijzigingen ook voor kennisname en akkoord door elk personeelslid ondertekend te worden. De Commissie stelt voor dat de aanvrager bij de herziening van de deontologische code ingaat op nog niet behandelde aspecten, zoals bijvoorbeeld de noodzaak van een voorafgaande uitdrukkelijke autorisatie voor alle verwerkingen op persoonsgegevens, het beheer van de risico's die deze gegevens lopen, bewaring van bewijzen van inbreuken die een strafrechtelijk karakter zouden kunnen hebben. De mogelijkheid bestaat om zich hiervoor te laten leiden door de referentiemaatregelen die op de site van de Commissie beschikbaar zijn (www.privacycommission.be, rubriek publicaties) of door andere erkende bronnen die op een meer algemene manier gericht zijn op de beveiliging van informatie.

Eigendom en beheer van materiaal

"*Alle hard- en software die de FOD Economie ter beschikking stelt van zijn medewerkers voor de uitoefening van hun job, blijft eigendom van de FOD en mag enkel voor beroepsdoeleinden worden gebruikt, dat wil zeggen binnen het kader van de aan de FOD Economie toegewezen taken*".

12. Deze bepaling van de code moet worden gewijzigd, want in te absolute bewoordingen gesteld geworden. Aangezien verderop in de code het gebruik van de patronale informaticamiddelen in hoofde van personeelsleden voor privé-doeleinden niet wordt verboden (bijvoorbeeld het gebruik van de harde schijf van de pc en het gebruik van internet en emailfunctionaliteiten), wordt deze bepaling niet alleen best in die zin genuanceerd door toevoeging van de woorden "in principe"

tussen de woorden “mag” en “enkel”, maar wordt bovendien reeds hier best expliciet vermeld dat een zeker privégebruik toegelaten is.

Bescherming van gegevens

“*In het kader van de taken van de FOD Economie wordt vertrouwelijke informatie betreffende burgers en ondernemingen verzameld en behandeld. Toegang tot dergelijke informatie is strikt beperkt en het is verboden deze informatie zonder toelating door te geven aan derden, binnen of buiten de FOD Economie. In het algemeen mag een medewerker informatie waartoe hij in het kader van zijn functie toegang heeft gekregen niet openbaar maken, tenzij hij hiervoor de toelating heeft gekregen van de verantwoordelijke beheerder van deze informatie of van zijn eigen hiërarchische chef. Dit geldt niet voor gegevens die reeds publiek beschikbaar zijn via andere kanalen*“.

13. De toelating van de verantwoordelijke beheerder van de informatie of van de hiërarchische chef van het personeelslid volstaat niet. De openbaarmaking, dus de mededeling aan derden waarvan sprake, moet, om toelaatbaar te zijn, een grondslag vinden, hetzij in de toestemming van de persoon op wie de gegevens betrekking hebben, hetzij gebaseerd zijn op een noodzakelijkheidseis in de zin van artikel 5 b tot en met f WVP, of, in voorkomend geval, in de zin van de §§2 van de artikelen 6 tot en met 8 WVP.

“*Met uitzondering van de persoonlijke mails in de persoonlijke mailboxen, is alle informatie op de computersystemen van de FOD Economie eigendom van de FOD, medewerkers kunnen hiervoor dus geen recht op privacy inroepen* (…)”.

14. Deze bepaling is nogal absoluut gesteld en laat uitschijnen dat, behoudens het voorbehoud ten aanzien van persoonlijke mails in de persoonlijke mailboxen, de FOD Economie onvoorwaardelijk toegang zou hebben tot bijvoorbeeld de gegevens op de pc van een personeelslid of op de mailserver, aangezien hij eigenaar is van de pc of de server. Er lijkt daarbij onvoldoende rekening te zijn gehouden met de toepasselijke bepalingen van de communicatiewetgeving en het Strafwetboek, welke verder meer uitgebreid aan bod komen onder de titels “gebruik van email”, “gebruik van internet” en “logging en auditing”. Zo zou de werkgever uit hoofde van die wetgeving bijvoorbeeld geen kennis mogen nemen van de inhoud van ingaande en uitgaande e-mails van de mailserver en de e-mails opvragen die zich reeds op de e-mailserver bevinden. Zo ook zou de werkgever een email waar uit de subjectline blijkt dat ze vertrouwelijk is en bestemd voor een bepaald personeelslid die in een gemeenschappelijke mailbox van de FOD Economie binnenkomt en onder zich houdt, strafbaar kunnen zijn onder artikel 314 bis § 2 , lid 2 van het Strafwetboek.

15. De bepaling lijkt zelfs in strijd met één van de daaropvolgende bepalingen in de code, met name “*ICT neemt geen back-up kopieën van de bestanden die gebruikers bewaren op de harde schijven van hun PC. Op deze schijven mogen dan ook alleen bestanden voor eigen, individueel gebruik worden bewaard* (…)”.

16. Aangezien op deze schijven alleen bestanden voor eigen individueel gebruik mogen worden bewaard door het personeelslid, moet aangenomen worden dat de werkgever dergelijke bestanden niet mag openen zonder de toestemming van de betrokkene en moet het voorbehoud welke de code formuleert inzake de toegang tot persoonlijke mails in persoonlijke mailboxen ook spelen voor de persoonsgegevens op de harde schijf van de pc.

Gebruikersidentificatie en paswoordbeleid.

“*Userids en paswoorden zijn strikt persoonlijk en mogen niet worden doorgegeven of bewaard op een plaats waar ze makkelijk gevonden kunnen worden. Gebruikers die vermoeden dat anderen hun paswoord kennen, moeten het onmiddellijk wijzigen. Elke medewerker is verantwoordelijk voor het gebruik dat van de informaticamiddelen wordt gemaakt op naam van een aan hem toegewezen identiteit (userid). Het is strikt verboden om, op welke wijze dan ook, paswoorden van andere medewerkers te proberen achterhalen, of om deze te gebruiken indien men ze bij toeval kent*”.

17. Op de eigenlijke bepaling heeft de Commissie geen commentaar.

18. De Commissie wenst wel bijkomend op te merken dat niet voor alle toepassingen het gebruik van een login en een paswoord zou kunnen volstaan. Het gebruik van bepaalde toepassingen en vooral de toegang tot de infrastructuur van de FOD Economie via het internet vereist sterkere middelen van authentificatie, zoals bijvoorbeeld het gebruik van een elektronische kaart met een authentificatiecertificaat dat kan worden gebruikt mits ingave van een pincode. De identificatie- en authentificatiemiddelen zouden met andere woorden aangepast moeten zijn aan de eisen van beveiliging die worden gesteld in functie van de aard van de toepassing en de toegangskanalen.

"*Het is strikt verboden om, op welke wijze dan ook, paswoorden van andere medewerkers te proberen achterhalen, of om deze te gebruiken indien men ze bij toeval kent*".

19. De Commissie wenst dat dienaangaande een specifieke bepaling wordt toegevoegd aan de code voor de systeem- en netwerkbeheerders, die immers ook personeelsleden zijn van de FOD Economie en voor wie de bedoelde handelingen kunnen/moeten worden gesteld in de uitoefening van hun werkzaamheden, met name de goede werking van het netwerk na te gaan en de goede uitvoering van een elektronische communicatiedienst te garanderen (zie artikel 125 §1, 2° van de wet van 13 juni 2005).

<u>Gebruik van het internet</u>

"*De toegang tot het Internet wordt aangeboden als hulpmiddel voor de uitoefening van de functie. Gebruik voor privé-doeleinden is slechts toegelaten in beperkte mate en mits met de nodige voorzichtigheid gehanteerd. In elk geval mag het persoonlijk gebruik geen problemen veroorzaken voor het professioneel gebruik*".

20. Daarmee komt de code tegemoet aan hetgeen de Commissie, onder verwijzing naar rechtspraak van het Europees Hof voor de Rechten van de Mens, stelde in haar advies van 3 april 2000[3] : aangezien de werkvloer de uitgelezen plaats is om contacten te onderhouden met collega's, en zelfs met buitenstaanders, moeten werkgevers een zekere tolerantie vertonen ten aanzien van privé-communicatie die door hun personeelsleden wordt gevoerd met hun communicatiemiddelen.

21. Wat ter zake redelijk is of niet zou nader geconcretiseerd kunnen worden in de code, bijvoorbeeld internetgebruik voor private doeleinden is enkel tijdens de werkpauze mogelijk.

"*Enkel ICT kan bepalen via welke wegen gebruikers toegang hebben tot het Internet* (…)".

22. De Commissie wenst dienaangaande op te merken dat het niet enkel aan ICT kan zijn om zulks te bepalen, aangezien uiteindelijk ICT zelf de instructies van de hiërarchie ter zake dient toe te passen, doch waaromtrent zij eventueel wel een voorafgaand advies heeft uitgebracht.

"(…). *Onder meer volgende types web sites of services worden op dit moment afgesloten: chat en instant messaging sites, web based mail service sites, file sharing netwerken, file transfer services,....".*

23. De Commissie wenst dienaangaande op te merken dat er toepassingen zijn die "file transfer" zouden vereisen, en voor wie deze 'verboden' toepassingen niettemin noodzakelijk zijn in de uitoefening van hun professionele werkzaamheden bij de FOD Economie. Om die reden moet, om elk misverstand ter zake te vermijden, het woord "afgesloten" aangevuld worden als volgt: "in het kader van het privégebruik".

[3] Advies van de Commissie uit eigen beweging van 3 april 2000 *betreffende het toezicht door de werkgever op het gebruik van het informaticasysteem op de werkplaats*.

Gebruik van email

"*E-mail staat in principe ter beschikking van iedere medewerker die toegang heeft tot het netwerk. Op vraag van de hiërarchisch verantwoordelijken, via de Information Manager, kan deze toegang voor bepaalde medewerkers beperkt worden*".

24. Allicht wordt hiermee bedoeld dat de werkgever de toegang kan beperken voor bepaalde categorieën van medewerkers, bijvoorbeeld voor de categorieën van medewerkers voor wie die uitrusting niet echt nodig is voor het verrichten van de overeengekomen prestaties. Men kan echter moeilijk binnen eenzelfde categorie, bepaalde personen a priori uitsluiten en anderen niet van een dergelijke toegang, tenzij als modaliteit van sanctie in het kader van het tuchtrecht.

"*De toegang tot e-mail wordt aangeboden als hulpmiddel voor de uitoefening van de functie. Gebruik voor privé-doeleinden is toegelaten in beperkte mate en mits op verantwoorde wijze gebruikt en niet storend voor het professioneel gebruik*".

25. Ook hier zou een algemeen verbod op het persoonlijk gebruik van internet voor werknemers niet redelijk zijn en niet in verhouding staan tot de mate waarin internet werknemers in hun dagelijkse leven kan bijstaan[4].

26. Ook hier zou wat ter zake redelijk is of niet nader geconcretiseerd kunnen worden in de code, bijvoorbeeld een maximale mailgrootte introduceren voor niet-professioneel gebruik.

"*De FOD Economie respecteert de vertrouwelijkheid van de persoonlijke elektronische post, tenzij in die gevallen waar de wet expliciet dit geheim opheft of ondergeschikt acht aan andere overwegingen*".

27. Er wordt niet verduidelijkt over welke wet het wel zou gaan en in welke gevallen die wet dan expliciet dit geheim opheft of ondergeschikt acht aan andere overwegingen.

28. Vermoedelijk viseert de deontologische code artikel 125 van de wet van 13 juni 2005 *betreffende de elektronische communicatie*, welke de uitzonderingen weergeeft op het principe van de vertrouwelijkheid van de communicatie gewaarborgd door artikel 124 van dezelfde wet en de artikelen 259bis en 314bis van het Strafwetboek. Volgens voornoemde wet van 13 juni 2005 is dat onder meer het geval indien daartoe toestemming werd verkregen van alle andere, direct of indirect betrokken personen (artikel 124 in fine), of wanneer de wet het stellen van de bedoelde handelingen toestaat of oplegt of wanneer de bedoelde handelingen worden gesteld met als enig doel de goede werking van het netwerk na te gaan en de goede uitvoering van een elektronische communicatiedienst te garanderen (artikel 125 § 1, 1° en 2°).

Beveiliging van de werkplaats

"(…).*De Windows PCs van de FOD Economie bieden de mogelijkheid om zichzelf automatisch te vergrendelen na een bepaalde periode (bvb. 10 minuten) van inactiviteit. Het wordt aangeraden dit te activeren*".

29. De Commissie wenst dienaangaande op te merken dat het beter zou zijn dat deze mogelijkheid onmiddellijk zou worden geactiveerd op het moment van de installatie van de pc, met daaraan verbonden het verbod in hoofde van de gebruiker om deze functionaliteit naderhand te desactiveren.

30. De (overige) bepalingen in de deontologische code onder deze hoofding zijn een concretisering van hetgeen wettelijk vereist is onder artikel 16 § 4 WVP: om de veiligheid van de persoonsgegevens van hun klanten te waarborgen moeten personeelsleden van de FOD Economie de gepaste technische en organisatorische maatregelen treffen die nodig zijn voor de

[4] Zie het werkdocument van de Groep 29, p. 25.

bescherming van die gegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies, evenals tegen de wijziging van of de toegang tot, en iedere andere niet toegelaten verwerking met betrekking tot die persoonsgegevens.

31. De personeelsleden van de verantwoordelijke voor de verwerking hebben er, waar mogelijk, baat bij eenzelfde ingesteldheid en zorgvuldigheidsplicht aan te nemen met betrekking tot de eigen persoonsgegevens voorhanden op de werkplek (bv. evaluatiegegevens, weddenfiches, …) en deze dus voldoende af te schermen van derden, zelfs binnen de instelling.

Logging en Auditing

"De FOD Economie houdt informatie en logbestanden bij over het gebruik van diensten en toepassingen op de verschillende netwerksystemen en centrale servers. Deze informatie is niet bedoeld ter controle van de activiteiten van individuele medewerkers, maar zal enkel gebruikt worden om de goede werking van de informatica-infrastructuur te controleren en beter te kunnen reageren bij problemen. Bij vastgestelde problemen of incidenten kan de FOD Economie beslissen meer gericht te gaan loggen of controleren. Eventueel betrokken medewerkers en hun verantwoordelijken zullen hierover voorafgaandelijk worden ingelicht. Elke medewerker dient nochtans te beseffen dat het principe van de bescherming van het privé-leven niet mag misbruikt worden om ongestraft ongeoorloofde feiten te plegen, en dat de wet toelaat om, zelfs zonder verwittiging, individuele controles uit te oefenen om op te treden tegen flagrant onwettige daden, die een onmiddellijke actie vereisen en de veiligheid en de goede werking van het IT-netwerksysteem te beschermen".

32. Het betreft allicht de belangrijkste bepaling uit de code, althans uit het oogpunt van wat de Commissie aanbelangt en met name de bescherming van de persoonlijke levensfeer van de werknemers die moet worden gewaarborgd ten opzichte van dergelijke controle, terwijl net op dit punt, de code nogal bondig en zelfs beknot is. Het is immers niet duidelijk hoe de FOD Economie de code in realiteit zal handhaven, met andere woorden op welke (procedurele) wijze het samenstel van waarborgen, neergelegd in onder andere de WVP, in de praktijk door de FOD Economie zal worden aangeboden en geëerbiedigd, ten einde hun recht op bescherming van de privacy bij de controle veilig te stellen.

33. Hoewel de bepaling op zich geen commentaar behoeft, profiteert de Commissie ervan om een aantal, in haar ogen, nuttige en noodzakelijke richtsnoeren ter zake in herinnering te brengen.

34. De FOD economie zou zich ter zake kunnen inspireren op de mogelijkheid van een geleidelijke en voorwaardelijke controle op elektronische communicatiegegevens die de werknemer verstuurt of ontvangt via het bedrijfsnetwerk, zoals uitgewerkt in de Collectieve arbeidsovereenkomst nr. 81 van 26 april 2002 *tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische on-linecommunicatiegegevens*, algemeen verbindend verklaard bij Koninklijk besluit van 12 juni 2002.

35. Anderzijds kan de FOD Economie als werkgever de toelaatbaarheid van de controle op internet en e-mail gebruik van zijn personeelsleden moeilijk steunen louter op de deontologische code die voorligt.

36. Deze code kan weliswaar doorgaan als een verschijningsvorm van wat onder artikel 9 WVP vereist is aan voorafgaande informatie naar de personeelsleden toe, maar niet als een toelaatbaarheidsgrond voor de controle als dusdanig. Dergelijke controle grijpt immers in op het communicatiegeheim, een verschijningsvorm van communicatieve privacy, beschermd door de communicatiewetgeving, welke ook speelt in arbeidsverhoudingen. Onder die communicatiewetgeving is zowel de controle van de inhoud van de communicatie als de controle van de omringende kenmerken van communicatie (verkeersgegevens), behoudens wanneer de toestemming werd verkregen van de bij de communicatie betrokken personen, in principe verboden. Een limitatief aantal wettelijke excepties zijn weliswaar voorzien, dewelke echter restrictief zullen moeten worden geïnterpreteerd. Een controle die echter niet op voldoende wijze

kan terugvallen op één van die strafuitsluitingsgronden, valt onder het strafrechtelijk verbodsregime van de communicatiewetgeving.

37. Zo zijn de bepalingen van artikel 124 van de reeds vernoemde wet van 13 juni 2005 en de artikelen 259bis en 314bis van het Strafwetboek onder meer niet van toepassing wanneer de bedoelde handelingen worden gesteld met als enig doel de goede werking van het netwerk na te gaan en de goede uitvoering van een elektronische communicatiedienst te garanderen (artikel 125 §1, 2° van de wet van 13 juni 2005).

38. Het is echter zeer de vraag of deze bepaling kan worden gebruikt door een werkgever die het telecommunicatieverkeer van zijn werknemers wil controleren. Dit bleek reeds uit de voorbereidende werkzaamheden bij de oude wet van 21 maart 1991 *betreffende de hervorming van sommige economische overheidsbedrijven*.

39. De Commissie herinnert ook aan een overweging gemaakt in haar advies van 16 september 2005: "*Wat het verzamelen van de communicatiegegevens, en ondermeer van eventuele loggings betreft, herinnert de Commissie er overigens aan dat het beginsel van vertrouwelijkheid van de communicatiegegevens toepasselijk is, zonder afbreuk te doen aan de noodzakelijke invoering van technische en organisatorische veiligheidsmaatregelen zoals voorzien bij artikel 16 van de wet, bedoeld om de toegang tot het netwerk te beveiligen en op globale wijze de veiligheid van persoonsgegevens te verzekeren. In dit perspectief is de registratie van loggings toelaatbaar en zelf wenselijk maar moet dit wel gebeuren met het oog op de bescherming van de gegevens, zonder omleiding van de finaliteit en hergebruik voor het uitoefenen van een permanente controle op de werknemers*".

40. De Commissie aanvaardde wel, gelet op de specifieke verantwoordelijkheden en verplichtingen van de werkgever onder de wet van 4 augustus 1996 *betreffende het welzijn van de werknemers bij de uitvoering van hun werk*, om bijvoorbeeld op basis van de door de ontvanger vrijgegeven inhoud van een emailbericht dat kan worden gekwalificeerd als pesterij, ongewenst seksueel gedrag of als een andere vorm van gewelddadig gedrag en om aan de hand van de log-gegevens, het werkstation te traceren van waaruit het emailbericht werd verzonden (cfr. advies Commissie van 18 december 2003).

41. De Commissie trekt de aandacht van de opstellers van de code op enkele elementen die kunnen helpen bij het vinden van het juiste evenwicht tussen de bescherming van de persoonlijke levenssfeer in hoofde van de personeelsleden enerzijds en de wettigheid van een zeker toezicht van de werkgever op het gebruik van de werkinstrumenten anderzijds, hoewel het gros van die elementen reeds voorkomen in het algemeen advies van de Commissie van 2000.

42. Elektronisch toezicht op werknemers kan niet zonder meer gelijkgesteld worden met een 'moderne' vorm van gezagsuitoefening. De Commissie overwoog reeds in het advies van 2000 dat "*de arbeidsrelatie tussen werkgever en werknemer bovendien gekenmerkt [wordt] door een onevenwichtige machtsverhouding. We voegen hieraan toe dat de controle-instrumenten die de werkgever heden ter beschikking staan, technische mogelijkheden hebben die bijzonder indringend zijn in vergelijking met de vroeger bestaande middelen*". De Groep 29 wees er van haar kant op 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*", en dat "*traditionele methoden voor toezicht die minder ingrijpen in de persoonlijke levenssfeer van personen, in overweging [moeten] worden genomen en indien mogelijk worden toegepast voordat wordt overgegaan tot de controle van elektronische communicaties*" [5].

43. De gezagsverhouding en het eigenaarschap over de communicatievoorzieningen kunnen, op zichzelf beschouwd, niet volstaan als een voldoende wettelijke basis om te raken aan het communicatiegeheim, een facet van het grondrecht op privé-leven.

[5] Zie het werkdocument van de Groep 29, respectievelijk p. 6 en 14.

44. Net zoals de Commissie in haar advies van 2000, overwoog de Groep 29 ook dat "*in de mate van het mogelijke preventie belangrijker [moet] zijn dan opsporing. 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 het 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*" [6].

45. Indien niettemin controle noodzakelijk zou blijken kan vervolgens worden verwezen naar de getrapte aanpak, zoals die bleek uit het advies van de Commissie van 3 april 2000 en bijvoorbeeld de CAO nr. 81 waarvan hoger sprake.

In een eerste fase mogen enkel globale gegevens worden verzameld zonder dat in eerste instantie de personen worden geïdentificeerd die bij het dataverkeer betrokken zijn.

De tweede fase van de controle, met name de individualisering van de telecommunicatiegegevens, dus het toeschrijven van de geviseerde telecommunicatiegegevens aan een bepaald personeelslid, mag slechts gebeuren, nadat ter gelegenheid van een statistische controle op het gebruik van de patronale digitale infrastructuur, abnormaliteiten werden vastgesteld, bijvoorbeeld een abnormaal lange duur van de raadpleging van het internet, adressen van verdachte sites, een hoge frequentie, aantal, omvang van email, type van bijlage welke een email vergezelt,…. In de CAO wordt een bijkomend onderscheid gemaakt tussen directe en indirecte individualisering. De directe procedure is van toepassing op de controle uitgevoerd ter bestrijding van onrechtmatig gedrag, de bescherming van de bedrijfsbelangen en de veiligheid van het net. De indirecte procedure, van toepassing op de controle uitgevoerd ter naleving van de interne netwerkafspraken binnen het bedrijf, is maar toegestaan mits een voorafgaande voorlichtingsfase in acht wordt genomen welke ertoe strekt de werknemers op een duidelijke en begrijpelijke wijze in te lichten over het bestaan van de onregelmatigheid en over het feit dat de elektronische communicatiegegevens geïndividualiseerd zullen worden wanneer opnieuw een dergelijke onregelmatigheid zou worden vastgesteld.

De uitvoering van de doelstellingen waarvoor de controle werd ingesteld, meer bepaald misbruik van de informaticamiddelen tegengaan, en dan inzonderheid wat betreft de controle op overdreven privégebruik, vereist in principe niet de kennisneming van de inhoud zelf van email/geraadpleegde website: de lijst van verstuurde en/of ontvangen e-mails of een lijst van websites die tijdens een bepaalde periode werden geraadpleegd, bevatten in principe voldoende elementen om de bezorgdheid van de werkgever op dat vlak weg te nemen, net zoals bijvoorbeeld factuurgegevens abnormaal hoge telefoonbedragen aan het licht zouden brengen.

46. De Groep 29 waarschuwde dat de werkgevers bij de beoordeling van het internetgebruik door werknemers zorgvuldig moet zijn bij het formuleren van 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*" [7].

47. Bij het uitoefenen van controle op binnenkomende email zal de werkgever, zo mogelijk, nog voorzichtiger moeten optreden, vermits de werknemer er de auteur niet van is en bepaalde mails allicht zelf niet verwachtte (met uitzondering van de controles verricht met behulp van technische middelen, die bijvoorbeeld gericht zijn op het tegenhouden van omvangrijke berichten die tot een verstopping van het netwerk zouden kunnen leiden). Bovendien mag niet vergeten worden dat ook

[6] Zie het werkdocument van de Groep 29, p. 25.
[7] Zie het werkdocument van de Groep 29, p. 25.

de correspondenten van de emailgebruikers rechten kunnen laten gelden onder de WVP en de communicatiewetgeving.

48. Vooral het overmatig spenderen van arbeidstijd aan webnagivatie voor persoonlijke doeleinden lijkt een patronale hoofdbekommernis om controle te willen implementeren, aangezien een besteding met zulk doeleinde een overeenkomstige daling van de arbeidsproduktiviteit tot gevolg heeft. Daarop replicerend komt het de Commissie voor dat de werkgever in staat moet zijn eventueel rendementsverlies van personeelsleden ook na te gaan op andere manieren dan enkel door de personeelsleden te plaatsen onder een permanente elektronische boeman[8].

49. Zoals eerder gesteld kan de deontologische code weliswaar op zich niet doorgaan als een rechtvaardigingrond om het elektronisch toezicht te legitimeren, maar wel een antwoord zijn op de nood aan transparantie door het bestaan en de modaliteiten van een patronale controle op het gebruik van internet en email schriftelijk duidelijk vast te leggen en bekend te maken aan de personeelsleden.

50. Niettemin bevat de code bij nader toezien nog onvoldoende informatie-elementen. Er kan worden verwezen naar hetgeen de Commissie stelde in het advies van 2000.

"*De dialoog tussen werkgever en werknemers zal het mogelijk moeten maken om op voldoende gedetailleerde wijze, conform artikel 9 van de wet van 8 december 1992, de verschillende bijzonderheden van het controlebeleid van de werkgever vast te leggen. Deze bijzonderheden dienen onder meer betrekking te hebben op:*

- het gebruik van de elektronische post en het internet dat wordt toegestaan, getolereerd of verboden;

- de doeleinden van de controle en de wijze waarop dit gebruik wordt gecontroleerd (aard van de verzamelde gegevens, omvang en omstandigheden van de controles, personen of categorieën van personen die onderworpen zijn aan controleprocedures;

- het feit of de telecommunicatiegegevens worden opgeslagen en de duur van opslag, bijvoorbeeld op een centrale server, in het kader van het technisch beheer van het netwerk, en de eventuele bestaande encrypteringssystemen;

- de beslissingen die de werkgever kan nemen ten aanzien van de werknemer op grond van de verwerking van de gegevens die worden verzameld naar aanleiding van een controle;

- het recht van toegang van de werknemer tot de hem betreffende persoonsgegevens".

51. Zo wordt bijvoorbeeld nergens in de deontologische code van de FOD Economie gewag gemaakt van de rechten waarover de personeelsleden beschikken krachtens de artikelen 10 tot 12 van de WVP, met name het recht op toegang tot persoonsgegevens die hen betreffen en het voorwerp uitmaakten van registratie, het recht op verbetering van onjuiste gegevens die hen betreffen en het recht op verwijdering van de gegevens die, rekening houdend met de doeleinden van de verwerking, onjuist zijn of waarvan de registratie, mededeling of bewaring wettelijk verboden zijn of waarvan de bewaring de redelijke termijn overschrijdt. De Commissie wijst er op dat bij het verzamelen van gegevens die zwaarwichtige gevolgen kunnen hebben voor de betrokkene (bv. disciplinaire sancties), het essentieel is dat de betrokkene gewezen wordt op zijn recht van toegang en verbetering, ten einde ten overstaan van hem een eerlijke verwerking te waarborgen. De uitoefening van de rechten bedoeld in de artikelen 10 en 12 van de WVP wordt verder uitgewerkt in artikel 32 en 33 van het Koninklijk besluit van 13 februari 2001 *ter uitvoering*

[8] In die zin blijkbaar arbeidsrechtbank Brussel van 2 mei 2002.

van de wet van 8 december 1992[9]. De Commissie onderstreept daarbij de noodzaak van het bewijs van de identiteit van de verzoeker. Dergelijk bewijs is nodig om te vermijden dat een persoon mededeling, verbetering of verwijdering kan bekomen van gegevens van een andere persoon. De Commissie is van oordeel dat deze bijkomende informatie de transparantie van de opgezette verwerkingen kunnen vergroten.

52. Bovendien mogen beslissingen ten aanzien van een werknemer niet uitsluitend gebaseerd worden op de geautomatiseerde verwerking van de persoonsgegevens van de desbetreffende werknemer. Persoonsgegevens verzameld tijdens het elektronisch toezicht mogen niet de enige criteria zijn om de prestaties van een werknemer te beoordelen. Er kan ter zake worden verwezen naar de CAO nr. 81, waar de werknemer die bij toepassing van de individualiseringsprocedure verantwoordelijk wordt geacht voor een onregelmatigheid bij het gebruik van de elektronische on-linecommunicatiemiddelen, wordt uitgenodigd voor een gesprek vóór iedere beslissing of evaluatie die hem individueel kan raken; deze procedure op tegenspraak zal de werknemer in staat stellen het gebruik van de hem ter beschikking gestelde elektronische on-linecommunicatiemiddelen te rechtvaardigen.

Sancties

53. De rol van de vertegenwoordiging van het personeel is een niet onbelangrijk element bij de implementatie van systemen van elektronisch toezicht op de werkplek.

54. De ondernemingsraad heeft tot taak advies uit te brengen en alle suggesties of bezwaren te kennen te geven over alle maatregelen die de arbeidsorganisatie, de arbeidsvoorwaarden en het rendement van de onderneming zouden kunnen wijzigen (artikel 15 van de wet van 20 september 1948 *houdende organisatie van het bedrijfsleven*. Elektronisch toezicht heeft nu eenmaal implicaties op het personeelsbeleid van de werkgever. In de sector van het openbaar ambt worden de bevoegdheden van de ondernemingsraad uitgeoefend door de onderhandelings- of overlegcomités waarin wordt voorzien door de wet van 19 december 1974 *tot regeling van de betrekkingen tussen de overheid en de vakbonden van haar personeel*. Nergens blijkt uit de code dat zou zijn voldaan aan deze procedure van collectieve informatie en raadpleging.

55. De controlemaatregelen en daaraan verbonden sancties in het raam van elektronisch toezicht moeten ten slotte worden opgenomen in het arbeidsreglement. Inzake het opstellen en wijzigen ervan voorziet de wet van 8 april 1965 *tot instelling van de arbeidsreglementen* een specifieke procedure die ook van toepassing is op de FOD Economie (artikel 2 van bedoelde wet). Die procedure gaat verder dan het louter informeren en consulteren van (de vertegenwoordiging van) het personeel: het gaat hem hier zelfs over een medezeggenschapsprocedure (artikel 11 van bedoelde wet). Nergens blijkt uit de code dat hieraan zou zijn voldaan.

56. Bovendien werd er hoger al op gewezen dat een akkoord van de vertegenwoordigers van de personeelsleden betreffende het elektronisch toezicht, zoniet kan doorgaan als een toestemming van de betrokkenen zelf, dan minstens kan bijdragen tot het vrije karakter van de toestemming van de individuele personeelsleden.

---

[9] Eenieder die zijn identiteit bewijst, heeft het recht om onder de voorwaarden gesteld bij de wet kennis te krijgen van de in artikel 10 van de wet vermelde informatie, zulks op ondertekend en gedagtekend verzoek dat ter plaatse wordt overhandigd, of over de post of met een telecommunicatiemiddel wordt toegezonden :

* hetzij aan de verantwoordelijke voor de verwerking of aan zijn vertegenwoordiger in België, of aan een van de door hem gemachtigde of aangestelde personen;

* hetzij aan de verwerker van de persoonsgegevens die het in voorkomend geval aan een van voornoemde personen doorgeeft.

Indien het verzoek ter plaatse wordt overhandigd, reikt de persoon die het in ontvangst neemt aan de verzoeker onmiddellijk een gedagtekend en ondertekend ontvangbewijs uit.

De verzoeken tot verbetering, verwijdering of verbod op de aanwending van de persoonsgegevens en enig verzet gegrond op artikel 12 van de wet worden ingediend volgens dezelfde procedure en bij dezelfde personen dan die vermeld in het artikel 32 van dit besluit.

"*Bij zware of herhaalde inbreuken op deze code heeft ICT het recht om preventieve acties te nemen ter bescherming van de informatica-infrastructuur* (…)".

57. De Commissie wenst dienaangaande op te merken dat het niet (enkel) ICT kan zijn die het recht heeft om dergelijke acties te nemen, aangezien uiteindelijk ICT zelf de instructies van de hiërarchie ter zake dient toe te passen, doch waaromtrent zij eventueel wel een voorafgaand advies heeft uitgebracht.

OM DEZE REDENEN,

Brengt de Commissie een gunstig advies uit over de deontologische code van de FOD Economie welke haar werd voorgelegd, mits rekening wordt gehouden met de supra gemaakte opmerkingen.

De administrateur,	De voorzitter,
(get.) Jo BARET	(get.) Michel PARISSE