Internet op het werk en privacy

CAO nr. 81 tot bescherming van de persoonlijke levenssfeer ten opzichte van de controle op de elektronische on-linecommunicatiegegevens

Hannelore Dekeyser
Onderzoeker
Interdisciplinair Centrum voor Recht en Informatica
Faculteit Rechtsgeleerdheid
KU Leuven
Tiensestraat 41
3000 Leuven
Tel.: 016-32 54 70
Fax: 016-32 54 38
e-mail: hannelore.dekeyser@law.kuleuven.ac.be

ARTIKEL

De sociale partners sloten op 26 april 2002 een collectieve arbeidsovereenkomst over de controle van het gebruik van internet en e-mail op het werk en de bescherming van de persoonlijke levenssfeer van de werknemers. De CAO werd algemeen verbindend verklaard bij koninklijk besluit op 12 juni 2002, waardoor de regeling bindend werd voor de hele private sector.

WAAROM WAS ER BEHOEFTE AAN DEZE CAO?

Een veel gehoord argument uit de hoek van de werkgevers is dat moderne communicatiemiddelen zoals e-mail en internet de werknemers uitnodigen tot misbruik. Volgens hen ontstaat daarom een grotere behoefte aan controle. Moderne communicatietechnologieën maken ook een erg efficiënte controle mogelijk: elke handeling van de gebruiker wordt minutieus geregistreerd en bewaard. De verleiding om van deze controlemogelijkheid gebruik te maken is voor de werkgever dus erg groot. Maar wat technisch mogelijk is, is daarom nog niet wettelijk toegelaten. Om uit te zoeken hoever een werkgever mag gaan, hebben de sociale partners uitgezocht welke wettelijke regels relevant zijn wanneer een werkgever wil controleren waarvoor zijn werknemers e-mail en internet zoal gebruiken. Zij kwamen tot de vaststelling dat twee belangrijke principes een rol spelen: enerzijds het recht op privacy en anderzijds het werkgeversgezag.

Het *recht op privacy* is het fundamentele recht van elke mens om vrij relaties met anderen aan te knopen zonder bemoeienis van buitenaf. Het Europees Hof voor de Rechten van de Mens bevestigde al herhaalde malen dat dit recht ook geldt op het werk[1]. Dat is immers de plaats bij uitstek waar mensen contact met anderen leggen. Hoe fundamenteel dit recht is, blijkt uit de hoeveelheid wetteksten die errond bestaat. De voornaamste bepalingen zijn art. 8 van het Europees Verdrag voor de Rechten van de Mens, art. 7 van het Handvest van de Grondrechten van de Europese Unie, art. 22 en 29 van de Belgische Grondwet, de privacywet[2] en de strafwetsbepalingen ter bescherming van het telecommunicatiegeheim [3].

Het *werkgeversgezag* is een basisbeginsel van ons arbeidsrecht. De werkgever draagt de eindverantwoordelijkheid en het financiële risico voor zijn onderneming. In ruil voor een loon werken de werknemers onder 'gezag, leiding en toezicht' van de werkgever. Binnen bepaalde perken mag de werkgever dus controleren waar zijn personeel mee bezig is.

Deze beide principes staan op het eerste gezicht diametraal tegenover elkaar. Noch het recht op privacy, noch het werkgeversgezag is echter

een absoluut recht en in de praktijk moet telkens een evenwicht gevonden worden.

Hoe dit evenwicht bereikt kan worden blijkt onder meer uit de privacywet. Deze wet legt strenge spelregels op aan iedereen die persoonlijke gegevens wil verwerken – en dat is wat de werkgever wil doen – maar laat het toch toe. Een nog strengere privacyregel vormt de strafrechtelijke bescherming van het telecommunicatiegeheim. Wie elektronische communicatie van een ander onderschept, is strafbaar. Afluisteren mag uitzonderlijk toch als dat gebeurt binnen een strafrechtelijk onderzoek, om het netwerk te onderhouden, met de toestemming van alle betrokkenen of wanneer de wet het oplegt of toelaat[4]. Deze laatste uitzondering wijst erop dat andere belangen voorrang kunnen krijgen op het telecommunicatiegeheim. Veel rechters schijnen ervan uit te gaan dat de arbeidssituatie zo'n ander belang is – 'schijnen' want in de meeste vonnissen wordt er over deze problematiek met geen woord gerept. De juridische situatie is dus allesbehalve helder. De sociale partners wilden een regeling uitwerken die de tegengestelde regels verzoent en zo de rechtsonzekerheid voor zowel werkgevers als werknemers wegneemt. CAO nr. 81 is het resultaat.

WAT ZEGT CAO NR. 81?

Inleiding

In de eerste artikelen schetst de CAO de problematiek die hij wil oplossen: de controle op het gebruik van telecommunicatiemiddelen [5] in het bedrijf met inachtneming van het grondrecht op privacy van de werknemers. De CAO regelt niet wie toegang moet krijgen tot deze communicatiemiddelen. Die beslissing blijft voorbehouden aan de werkgever. Zoals gebruikelijk krijgen gunstigere regelingen die afgesproken worden op ondernemingsniveau of in paritaire comités voorrang op de regels van de CAO.

Een definitie van het begrip telecommunicatiemiddelen, of 'elektronische on-linecommunicatiemiddelen' in de terminologie van de CAO, geven de sociale partners niet. Zij wijzen er enkel op dat het begrip erg ruim begrepen moet worden. In de praktijk gaat het om elke vorm van communicatie waarbij gegevens via een elektronisch netwerk uitgewisseld worden, zoals telefoon, e-mail en internet. De inhoud van de harde schijf of van een netwerkpartitie van een werknemer valt niet onder dit begrip. Eén beperking is er toch: enkel gegevens uitgewisseld in het kader van de dienstbetrekking mogen gecontroleerd worden. Volgens sommigen betekent dit dat enkel communicatie met een professionele inhoud gecontroleerd mag worden, maar dit criterium is in de praktijk ontoepasbaar. De bits die over het netwerk gestuurd worden zien er allemaal hetzelfde uit, alleen professionele bits controleren is dus onmogelijk. 'In het kader van de dienstbetrekking' herinnert de werkgever eraan dat hij enkel mag controleren voor zover zijn werkgeversgezag reikt. Hierover kunnen bijvoorbeeld vragen rijzen wanneer werknemers ook van thuis uit werken.

Voorwaarden voor de installatie van een controlesysteem

De werkgever moet drie principes respecteren: transparantie, finaliteit en proportionaliteit. Niet toevallig zijn dat de drie basisprincipes uit de privacywet, die in de CAO concreet worden toepast op de arbeidssituatie.

• *Finaliteit*

Een werkgever die een controlesysteem wil invoeren moet allereerst vastleggen wat hij daarmee precies wil bereiken. Voordat het controlesysteem geïnstalleerd wordt, moeten deze doelstellingen immers aan het personeel uitgelegd worden. De CAO geeft ter inspiratie drie categorieën van doelstellingen waarvan de sociale partners menen dat ze controle legitimeren. Daarnaast is er nog een restcategorie.

Een eerste categorie is het voorkomen van 'ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of die de waardigheid van een andere persoon kunnen schaden' [6]. In de commentaar bij dit artikel wordt het voorbeeld gegeven van een werknemer die computers kraakt om andermans e-mail te lezen of om de bestanden van de personeelsdienst te lezen. De werkgever mag de toegangsbevoegdheid van zijn werknemer beperken tot bepaalde delen van het informaticasysteem en hij moet dat doen om persoonsgegevens van zijn personeel en/of klanten te beschermen. Daarom is het ook logisch dat de werkgever mag controleren of iedereen zich aan de regels houdt. Een werknemer die uit pure nieuwsgierigheid zijn toegangsprivileges overschrijdt, is overigens niet strafbaar, in tegenstelling tot hackers buiten het bedrijf. De wetgever vindt dat in deze gevallen interne sancties gepaster zijn. Enkel wanneer de werknemer een bedrieglijk doel nastreeft of het opzet heeft om te schaden, pleegt hij een misdrijf.

Een tweede voorbeeld bij deze categorie is het surfen naar pornografische, pedofiele en xenofobe websites. De strafrechtelijke aspecten buiten beschouwing gelaten, zal dergelijk gebruik van het internet zelden binnen de taakomschrijving van de werknemer vallen. De omschrijving die de CAO gebruikt is erg vaag. Uiteraard zal er weinig discussie zijn wanneer een werknemer een pornosite uitbaat op het werk, racistische e-mails verspreidt en dergelijke. Maar wat zijn feiten die de waardigheid van een andere persoon kunnen schaden? Volstaan de vele min of meer pikante foto's die doorgestuurd worden op het werk? Welke moppen kunnen door de beugel

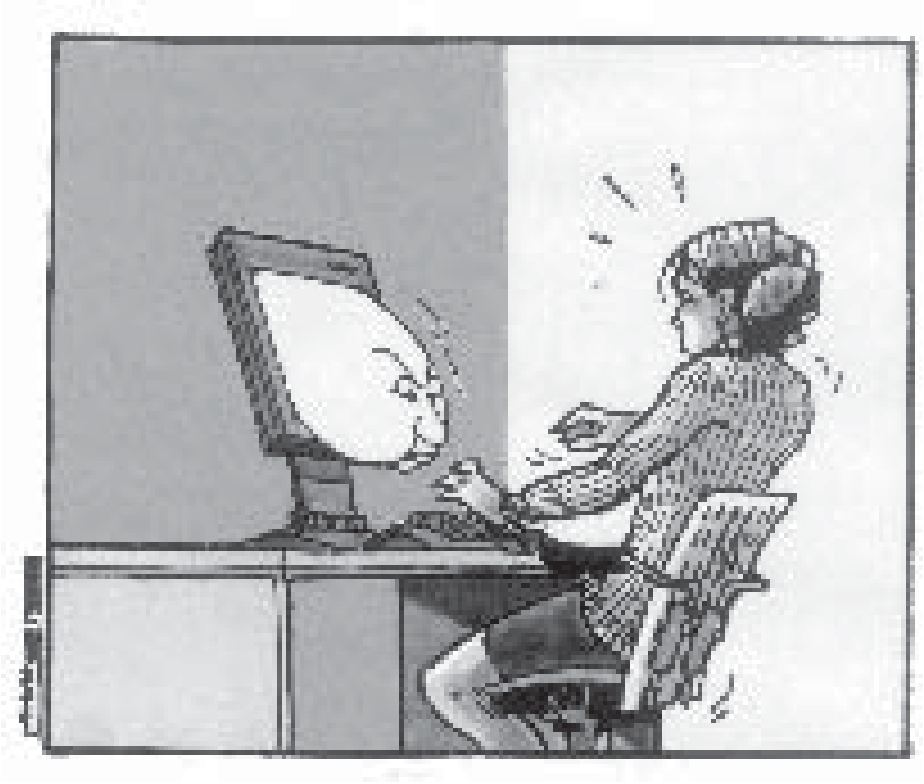
en welke niet? Tenzij er sprake is van pesten, worden zulke gevallen beter niet behandeld onder de categorie ongeoorloofde feiten, gezien de zware gevolgen die eraan vasthangen, maar onder een andere categorie.

Een volgende categorie behelst de bescherming van de economische, handels- en financiële belangen voor zover die vertrouwelijk zijn[7]. De werkgever moet ervoor zorgen dat de werknemers weten of op zijn minst kunnen achterhalen welke gegevens vertrouwelijk zijn. Vervolgens geeft hij best richtlijnen over hoe werknemers met zulke gegevens moeten omgaan. Ten slotte kan hij dan controleren of de werknemers zich hieraan houden.

De derde doelstelling omvat het garanderen van de veiligheid en/of de goede technische werking van het informaticasysteem van het bedrijf, met inbegrip van de controle op de daarmee verbonden kosten en de fysieke bescherming van de installaties van de onderneming[8]. De werkgever mag alle e-mail laten controleren op de aanwezigheid van virussen en mag ook verhinderen dat werknemers inbellen op dure betaallijnen. De 'fysieke bescherming van de installaties van de onderneming' doelt waarschijnlijk op de schade die (interne) hackers kunnen toebrengen door de elektronische besturingssystemen te beschadigen of in de war te sturen.

Ten slotte voorziet de CAO een restcategorie die alle overige controledoelstellingen kan omvatten, namelijk het te goeder trouw naleven van de in de onderneming geldende regels voor het gebruik van on-linetechnologieën[9]. Uiteraard moet het nog steeds gaan om legitieme controledoelstellingen, dit wil zeggen: doelstellingen waarvan men de noodzaak in een arbeidssituatie kan verdedigen.

De werkgever kan opleggen dat elke e-mail van een exoneratieclausule voorzien wordt of op een uniforme wijze ondertekend wordt. Hij kan opleggen dat van een automatische afwezigheidsboodschap gebruikgemaakt moet worden of dat e-mail automatisch naar een vervanger gestuurd wordt bij geplande afwezigheid. Encryptie van berichten kan verboden of juist opgelegd worden. Het is erg moeilijk om een voorbeeld te vinden van een controledoelstelling die absoluut niet verdedigbaar is in een arbeidssituatie, wat aantoont hoe ver deze CAO gaat in het toelaten van controles. Zo kan gediscussieerd worden over controles op het voorkomen van emoticons[10], grof taalgebruik, taalfouten..., zeker in communicatie met klanten. Het lijkt erop dat alleen pietluttigheden aan de controlebevoegdheid van de werkgever ontsnappen, bijvoorbeeld of de werknemers in hun emoticons een 'neus' gebruiken of niet. Op dit punt gaat de CAO uit de bocht. De werkgever zorgt best dat de controles die hij uitvoert een gegronde reden hebben.



Een vergelijking met de controles die nodig worden geacht in de traditionele papieren omgeving kan hierbij erg verhelderend zijn.

• *Proportionaliteit*

Zodra de werkgever vastgelegd heeft waarom hij controles wil doorvoeren, moet hij uittekenen hoe hij dat wil doen. Ook het controlesysteem moet immers haarfijn uitgelegd worden aan het personeel. Als leidraad geldt dat controles in principe geen enkele inmenging in de persoonlijke levenssfeer van de werknemer tot gevolg mogen hebben. Als er toch een inmenging is, moet die tot het minimum beperkt blijven. Erg mooi als beginsel, maar hoe werkt dat in de praktijk? De CAO geeft enkele wenken, al blijven er nog heel wat vragen onopgelost.

Voor een goed begrip van de regels die de CAO oplegt, moet het onderscheid gemaakt worden tussen de gegevens die om technische reden nu eenmaal door het informaticasysteem

geregistreerd worden en de gegevens die voor controledoeleinden verzameld worden. De CAO regelt niet wat het informaticasysteem mag registreren, enkel in welke mate deze gegevens hergebruikt mogen worden voor controledoeleinden. Enkel die gegevens die strikt noodzakelijk zijn voor de controle mogen uit het systeem gehaald worden. Bijvoorbeeld wanneer het e-mailadres van de geadresseerde volstaat om te weten of een e-mail privé is of professioneel, hoeft het onderwerp niet meer bekeken te worden; wanneer het bestandstype volstaat moet de inhoud niet bekeken worden.

Vanuit de bezorgdheid om elke inmenging in de privacy van de werknemers te beperken, schrijft de CAO voor dat controles in eerste instantie anoniem en globaal moeten gebeuren aan de hand van statistische gegevens. Zo kan men een lijst opstellen van alle bezochte websites, voor alle personeel gezamenlijk of voor een afdeling. Ook statistische gegevens over e-mail kunnen nuttig zijn, onder meer het aantal e-mailberichten, hun grootte en het bestandstype van de bijlagen. In de commentaar bij de CAO suggereren de sociale partners dat deze statistieken per werkpost opgesteld mogen worden. Wanneer een werkpost aan één bepaalde werknemer is toegewezen, rijst toch de vraag of de anonimiteit voldoende gewaarborgd is.

Deze strikte vereiste van anonimiteit is niet van toepassing op één categorie gegevens: de communicatiegegevens waarvan het beroepsmatige karakter door de werknemer niet in twijfel wordt getrokken. Deze bepaling zal het meeste nut hebben voor e-mail. Om van deze uitzondering gebruik te maken moet de werkgever een systeem invoeren waarbij de werknemer bij het versturen of ontvangen van e-mail onmiddellijk aangeeft of het professionele of privé e-mail is[11]. De werkgever mag dan zonder enige vorm van procedure de professionele e-mail inkijken. Dat kan van groot belang zijn om de goede werking van de onderneming te waarborgen, bijvoorbeeld wanneer een medewerker plots wegvalt.

Uit de anonieme controles kan blijken dat iemand de gebruiksregels overtreedt. In dat geval zal de werkgever willen overgaan tot individuele controles, waarover verder meer. Bij de voorbereiding van de installatie van het controlesysteem tekent de werkgever het best een concreet scenario uit voor het precieze verloop van zowel de anonieme als de individuele controles: wie voert deze controles uit, wat zijn de prerogatieven van het toezichthoudend personeel, hoe verloopt de verdere communicatie met het personeel over de correcte naleving van de gebruiksregels?

• *Transparantie*

Zodra de werkgever vastgelegd heeft waarom hij controles wil uitvoeren en hoe hij dat wil aanpakken, moet hij zijn personeel hierover informeren. Hij doet dat in principe voordat het controlesysteem in gebruik genomen wordt.

Eerst moeten de werknemers collectief geïnformeerd worden. Afhankelijk van de situatie van de onderneming moet de ondernemingsraad op de hoogte gebracht worden, of het comité voor preventie en bescherming op het werk, de vakbondsafvaardiging en desnoods de werknemers zelf.

De collectieve informatie behandelt alle aspecten van de controle, waaronder het controlebeleid en de prerogatieven van de werkgever en het toezichthoudend personeel, de doelstellingen, het feit of persoonsgegevens al dan niet bewaard worden, de plaats en de duur van bewaring en het al dan niet permanente karakter van de controle[12].

Vervolgens moeten de werknemers individueel geïnformeerd worden over het controlesysteem. Inhoudelijk moet de collectieve informatie hernomen worden en aangevuld met richtlijnen over het gebruik van de instrumenten die de werknemer ter beschikking krijgt en in het bijzonder over de rechten en plichten van de werknemer bij het gebruik van telecommunicatiemiddelen. Ook moeten de straffen bepaald in het arbeidsreglement herhaald worden. De informatie moet effectief, begrijpelijk en bijgewerkt zijn. De werkgever mag kiezen in welke vorm hij deze informatie meedeelt: binnen algemene instructies, door vermelding in het arbeidsreglement, door vermelding in de individuele arbeidsovereenkomst of door instructies bij ieder gebruik van de instrumenten. Omdat controle op het gebruik van e-mail en internet zo'n gevoelig punt is, gebruikt de werkgever best verschillende middelen tegelijk, zodat elke werknemer redelijkerwijze moet weten dat er een controlesysteem bestaat en waar hij de details erover kan lezen.

Al deze informatie moet de werknemers in staat stellen de dialoog aan te gaan met hun werkgever over het controlesysteem. Daarom vereist de CAO dat het geïnstalleerde controlesysteem regelmatig geëvalueerd wordt, naargelang van het geval in de ondernemingsraad, het comité voor preventie en bescherming op het werk of met de vakbondsafvaardiging. Technische ontwikkelingen die een minder ingrijpend controlemechanisme mogelijk maken, kunnen dan besproken worden.

Voorwaarden voor de uitvoering van controles

Naast de vele voorwaarden die opgelegd worden voor de installatie van het controlesysteem, regelt de CAO ook enkele aspecten rond het uitvoeren van de controles. De basisprincipes ‘finaliteit’, ’proportionaliteit’ en ‘transparantie’ blijven een centrale rol spelen.

Over het verloop van de anonieme en globale controle zegt de CAO niet veel. De sociale partners gingen er blijkbaar vanuit dat dit geen probleem zou vormen. Het onderzoek naar het gedrag van een individuele werknemer wordt wel aan bepaalde regels onderworpen.

• *Finaliteit*

Elke controle, zowel anoniem als individueel, mag slechts gebeuren met één van de doelstellingen die de werkgever heeft opgegeven aan zijn werknemers, zoals hoger uitgelegd.

Gegevens verzameld over een individuele werknemer verder gebruiken voor een ander doel is niet verboden, zolang het nieuwe doel verenigbaar is met het oorspronkelijke doel. De werkgever moet daarenboven alle nodige maatregelen nemen om interpretatiefouten te vermijden. Zo zou de werkgever het tijdstip kunnen nagaan waarop de werknemer e-mail verstuurd en ontvangen heeft om daaruit zijn arbeidstijd af te leiden. Elke e-mail bevat immers de datum en het uur van verzenden of ontvangst. In de praktijk is deze vermelding slechts betrouwbaar als de interne klok van de versturende e-mailserver juist ingesteld is. Bovendien kan e-mail ook automatisch verstuurd worden op een later tijdstip. Ten slotte is dit nieuwe doel – de arbeidstijd controleren – moeilijk te verzoenen met de oorspronkelijke doelstellingen uit de CAO, namelijk het controleren van misbruik.

• *Proportionaliteit*

Net als bij een anonieme controle, mogen bij een individuele controle slechts die gegevens verwerkt worden die strikt noodzakelijk zijn in het licht van de doelstelling. De verwerkte gegevens moeten toereikend, relevant en niet overmatig zijn. Wanneer statistische gegevens over het surfgedrag volstaan om misbruik aan te tonen, is het niet nodig verder in detail te treden. Wanneer uit het aantal en de frequentie van berichten die tussen twee personen uitgewisseld worden al blijkt dat er sprake is van misbruik, moet de inhoud van de berichten niet meer bekeken worden. De inhoud van e-mailberichten mag slechts in allerlaatste instantie ingekeken worden, nadat alle andere mogelijkheden uitgeput werden.

Om de proportionaliteit van de individuele controles te garanderen, legt de CAO een beperkt aantal procedurevoorwaarden op. Wanneer uit de anonieme en globale controles blijkt dat iemand ongeoorloofde feiten pleegt, vertrouwelijke gegevens verspreidt of het netwerk in gevaar brengt[13], mag de werkgever onmiddellijk onderzoeken wie de dader is. Deze procedure heet de directe individualisering en houdt geen bijkomende beperkingen in. In de overige gevallen waar blijkt dat iemand de bedrijfsinterne regels voor het gebruik van telecommunicatiemiddelen niet naleeft, mag de werkgever niet onmiddellijk nagaan wie hiervoor verantwoordelijk is. Eerst moeten de geldende regels opnieuw uitgelegd worden aan de werknemer(s) en moet de werkgever waarschuwen dat bij een volgende soortgelijke inbreuk de verantwoordelijke gezocht zal worden. Een werknemer die uiteindelijk verantwoordelijk wordt gesteld voor de inbreuk, moet door de werkgever gehoord worden vóór een beslissing genomen wordt over de gevolgen. Vreemd genoeg legt de CAO deze vereiste enkel op bij de indirecte procedure, toch zal de behoefte van de werknemer om zich te verdedigen even groot of nog groter zijn bij de toepassing van de directe procedure.

De regels over de indirecte individualisering roepen meteen allerlei vragen op. Moet het voltallige personeel opnieuw ingelicht worden of mag dit tot een afdeling beperkt worden? Mag een individuele werknemer gewaarschuwd worden door een vertrouwenspersoon of via een automatisch bericht? Voor hoelang geldt de waarschuwing en voor wie? Deze vragen kunnen niet zomaar in het algemeen beantwoord worden, maar moeten door een rechter geval per geval bekeken worden. De werkgever moet deze vragen in elk geval bekijken bij het installeren van het controlesysteem en er een antwoord op geven in een scenario dat hij uitwerkt. Ook de informatie die de werknemers kregen bij de installatie van het systeem is cruciaal.

• *Transparantie*

Volgens de sociale partners garanderen de procedurevoorwaarden voor de individualisering eveneens de transparantie van de controles. Deze stelling is alvast erg betwistbaar wat de directe individualisering betreft. De indirecte individualisering kan bijdragen tot meer transparantie, afhankelijk van hoe de waarschuwingsprocedure binnen het bedrijf concreet wordt uitgewerkt.

Werknemers die willen weten welke gegevens hun werkgever bijhoudt over hun individueel e-mail- en internetgebruik, kunnen zich beroepen op de privacywet. Deze wet kent iedereen een inzagerecht toe[14].

Conclusie

De sociale partners hebben uit het kluwen van rechtsregels over privacy en arbeidsrecht een coherent geheel van spelregels gedistilleerd die de relatie tussen de werkgever en zijn werknemers regelt. De CAO stelt dat de werkgever het recht heeft controle uit te oefenen op het gebruik van de telecommunicatiemiddelen die hij aan het personeel ter beschikking stelt voor de uitoefening van hun functie. Het recht op privacy van de werknemers op de werkvloer wordt gewaarborgd door drie fundamentele principes: transparantie, finaliteit en proportionaliteit.

De CAO veegt niet alle controverses van de baan. Ongetwijfeld zullen er hevige discussies ontstaan wanneer een werknemer als verantwoordelijke aangewezen wordt voor misbruik of overtreding van de gebruiksregels. Wie is er verantwoordelijk voor een virusbesmetting? Wat met Trojaanse paar-

den die ongewenste reclame, ook wel spam genoemd, uitsturen of die buitenstaanders toelaten illegale bestanden uit te wisselen?

Aan preventie wordt bovendien geen aandacht geschonken, terwijl er vele mogelijkheden bestaan om misbruik te voorkomen. Aan de hand van filtersoftware kan de toegang tot bepaalde websites geblokkeerd worden; instant messenging programma's, chat-programma's en ruilprogramma's kunnen afgegrendeld worden, de e-mailserver kan bepaalde bestandstypes als bijlage weigeren...

Naast de controle van misbruik zijn er nog situaties waarin de werkgever communicatiegegevens van zijn werknemers wil verwerken, bijvoorbeeld om een e-mailarchief aan te leggen. Op het eerste gezicht regelt de CAO dat niet. Toch zijn het dezelfde achterliggende principes – het recht op privacy en het werkgeversgezag – die deze situaties beheersen. Het valt te betreuren dat de sociale partners hier geen oog voor hadden. Toch zal de oplossing van de CAO op zijn minst als leidraad kunnen dienen.

Ten slotte regelt de CAO enkel de verhouding werkgever-werknemer. Vaak zullen echter ook gegevens van derden verwerkt worden, voornamelijk bij de controles op e-mail. Derden kunnen een beroep doen op de privacywet, die onverkort van toepassing blijft.

De CAO wordt om al deze redenen hevig bediscussieerd in juridische kringen. Het is aan de rechter om over deze controverses uitspraak te doen. In afwachting moeten werkgevers en werknemers zelf hun best doen om de regels op een faire manier in de praktijk om te zetten.

NOTEN

1. Met name in de zaak Niemitz (16 december 1992) en de zaak Halford (25 juni 1997)
2. Wet ter bescherming van de persoonlijke levenssfeer van 8 december 1992.
3. Art. 259bis en 314bis van het strafwetboek en art. 109terD en 109terE van de wet van 21 maart 1991 betreffende de hervorming van sommige overheidsbedrijven (Telecomwet).
4. Art. 109terE Telecomwet
5. De CAO gebruikt telkens de zelf uitgevonden term ‘elektronische on-linecommunicatiemiddelen’. In deze bijdrage wordt de term regelmatig vervangen door het begrip 'telecommunicatie', dat voorkomt in de wetteksten waarop deze CAO voortbouwt.
6. Art. 5, §1, 1° CAO nr. 81.
7. Art. 5, §1, 2° CAO nr. 81.
8. Art. 5, §1, 3° CAO nr. 81.
9. Art. 5, §1, 4° CAO nr. 81.
10. Emoticons zijn symbolen die gebruikt worden in zogenaamde 'platte' tekst om emoties uit te drukken, daartoe worden bepaalde leestekens gecombineerd die eruitzien als een gekanteld gezichtje. Het lachebekje :-) is het best gekende voorbeeld.
11. De werknemers kunnen dit werkje erg versnellen door gebruik te maken van filters die e-mail sorteren volgens zelf gespecificeerde regels.
12. Art. 9, §1 CA O nr. 81.
13. Art. 5, §1, 1°-3° CAO nr. 81.
14. Art. 10 Privacywet.

SAMENVATTING

Internet is in geen tijd ontzettend populair geworden, zowel in een professionele context als daarbuiten. Bedrijven benutten wat graag de voordelen van dit snelle communicatiemiddel, maar staan er tegelijk argwanend tegenover. Waar surfen de werknemers naartoe? Sturen ze grapjes door of leveren ze serieus werk? Met een eenvoudige ingreep in het bedrijfsnetwerk kan de werkgever elke muisklik van zijn personeel volgen. Big Brother scenario’s zijn dan niet meer veraf. Zover wilden de sociale partners het echter niet laten komen.

ABSTRACT

In no time, the Internet has become extremely popular, not only as a source of intertainment but also as a professional tool. Businesses are eager to take advantage of the many benefits this rapid means of communication provides. At the same time, they remain somewhat mistrustful. What sites do the employees visit? Are they exchanging jokes or serious documents? A relatively simple modification of the corporate network allows the employer to monitor every mouse click his employees make. Big Brother scenarios are just a small step away. However, the social partners did not allow things to go that far.