Paritair Comité voor het gas- en elektriciteitsbedrijf

Collectieve arbeidsovereenkomst van 30 november 2006

TIC-materiaal

Hoofdstuk I - Toepassingsgebied en algemene begrippen

Artikel 1. Deze coUectieve arbeidsovereenkomst, is deze coUectieve arbeidsovereenkomst van toepassing op de werkgevers die onder de bevoegdheid van het Paritair Comité voor het gas- en elektriciteitsbedrijf ressorteren en op de werknemers die zij tewerkstellen.

Onder "werknemers" wordt verstaan: de mannelijke en vrouwelijke werknemers aangeworven met een overeenkomst voor bepaalde of onbepaalde duur, voltijds of deeltijds.

Hoofdstuk II - Doel

Art. 2. Deze coUectieve arbeidsovereenkomst wordt gesloten met het oog op het reglementeren van het gebruik van technologisch materiaal voor informatie en communicatie genaamd TIC-materiaal, ter beschikking gesteld door de ondernemingen van de sector gas en elektriciteit, overeenkomstig coUectieve arbeidsovereenkomst nr. 81 van 26 april 2002, gesloten in de Nationale Arbeidsraad, tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische online communicatiegegevens.

Deze coUectieve arbeidsovereenkomst doet evenmin afbreuk aan de in de ondernemingen bestaande regels en praktijken wat de uitoefening van de vakbondsactiviteiten betreft.

Commission paritaire de l'industrie du gaz et de l'électricité

Convention collective de travail du 30 novembre 2006

Matériel TIC

Chapitre premier - Champ d'application et notions générales

Article 1er. la présente convention collective de travail s'applique aux employeurs qui ressortissent à la compétence de la Commission paritaire de l'industrie du gaz et de l'électricité et aux travailleurs qu'ils occupent.

Par « travailleurs » on entend : les travailleurs masculins et féminins engagés sous contrat à durée déterminée ou indéterminée, à temps plein ou à temps partiel.

Chapitre II - But

Art. 2. La présente convention collective du travail est conclue en vue de réglementer l'utilisation du matériel de technologie de l'information et de la communication dénommé matériel TIC mis à disposition dans les entreprises du secteur du gaz et de l'électricité, conformément à la convention collective de travail n°81 du 26 avril 2002, conclue au sein du Conseil national du travail, relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau.

La présente ne porte pas préjudice aux règles et pratiques existant dans les entreprises en ce qui concerne l'exercice des activités syndicales.

De uitoefening van de syndicale activiteiten omvat onder andere het verzenden van e-mails aan de aangesloten leden in de onderneming en het raadplegen van internet sites waarvan de toegang niet verboden is door de onderneming.

L'exercice des activités syndicales comprend entre autres l'envoi d'e-mails aux affiliés dans l'entreprise et la consultation de sites Internet dont l'accès n'est pas interdit par l'entreprise.

Hoofdstuk III - Specifieke noties

Chapitre III - Notions spécifiques

Principe

Art. 3. Deze collectieve arbeidsovereenkomst heeft tot doel het grondrecht van de werknemers op de eerbiediging van hun persoonlijke levenssfeer in het kader van de dienstbetrekkingen te waarborgen door, rekening houdend met de behoeften voor een goede werking van de ondememing, te bepalen voor welke doeleinden en onder welke proportionaliteits- en transparantievoorwaarden een controle op de elektronische onlinecommunicatiegegevens kan worden geïnstalleerd en volgens welke regels de individualisering van deze gegevens is toegestaan.

Principe

Art. 3. La présente convention collective de travail a pour but de garantir le respect du droit fondamental des travailleurs au respect de leur vie privée dans la relation de travail, en définissant, compte tenu des nécessités d'un bon fonctionnement de l'entreprise, pour quelles finalités et à quelles conditions de proportionnalité et de transparence un contrôle des données de communication électroniques en réseau peut être installé et les modalités dans lesquelles l'individualisation de ces données est autorisée.

Definities

Art. 4. Voor de toepassing van deze collectieve arbeidsovereenkomst wordt verstaan onder:

- "gebruikers": de werknemers die gebruik maken van technologisch materiaal voor informatie en communicatie;
- "gebruik voor privé-doeleinden": elk gebruik dat voor persoonlijke behoeften wordt gemaakt door de gebruiker of voor een derde persoon of voor de uitvoering van een andere taak dan voor beroepsdoeleinden wordt uitgevoerd;
- "gebruik voor beroepsdoeleinden": elk gebruik dat wordt gemaakt voor de uitvoering van de arbeidsovereenkomst;

Définitions

Art. 4. Pour l'application de la présente convention de travail il faut entendre par:

- « utilisateurs »: les travailleurs qui utilisent du matériel de technologie de l'information et de la communication;
- « usage à des fins privées » : toute utilisation effectuée pour les besoins personnels de l'utilisateur ou pour une tierce personne ou pour l'exécution d'un travail autre que celui exécuté à des fins professionnelles;
- « usage à des fins professionnelles » : toute utilisation effectuée en vue de l'exécution du contrat de travail;

- "syndicale activiteiten": elke activiteit zoals beschreven in de collectieve arbeidsovereenkomst van 2 maart 1989 houdende het statuut van de syndicale afvaardigingen der personeelsleden van de gas- en elektriciteitsbedrijven;

- "technologisch materiaal voor informatie en communicatie - TIC-materiaal": elk hardwarematerieel, alle software, alle netwerken. Het gaat daarbij onder meer (maar niet uitsluitend) om informaticamateriaal, netwerken, servers, internetverbindingen, pc's (laptops en desktops), pda, smartcards, software en besturingssystemen, world wide web browsing, het e-mail systeem, het internet en extranet van de ondernemingen, gsm;

- "gegevens": alle gegevens opgeslagen, behandeld of overgebracht via de netwerken van de onderneming.

- « activités syndicales » : toute activité telle que définie dans la convention collective de travail du 2 mars 1989 organisant le statut des délégations syndicales des agents statutaires barémisés de l'industrie du gaz et de l'électricité;

- « matériel de technologie de l'information et de la communication - matériel TIC » : tout équipement hardware, software, réseaux. Il s'agit entre autres (mais de manière non exhaustive) de l'équipement informatique, des réseaux, les serveurs, des connections internet, les PC (laptops et desktops), des pda, des smartcards, du software et les systèmes d'exploitation, du world wide web browsing (navigation), du système d'e-mails, de l'intranet et extranet des entreprises, des gsm;

- « données » : toutes les données stockées, traitées ou transmises via le réseau de l'entreprise.

Hoofdstuk IV - Gebruik van TIC-materiaal

Art. 5. TIC-materiaal dat ter beschikking wordt gesteld van de gebruikers zijnde de eigendom, in de brede zin van het begrip, ook geleased materiaal, van de onderneming.

Het persoonlijk TIC-materiaal is onderworpen aan dezelfde gebruiksregels als het TIC-materiaal van de werkgever vanaf het ogenblik dat het aangesloten is op het netwerk van de onderneming.

Art. 6. TIC-materiaal mag alleen gebruikt wordt voor beroepsdoeleinden. De gebruikers dienen als een goede huisvader met de hen ter beschikking gestelde middelen om te gaan.

Chapitre IV - Utilisation du matériel TIC

Art. 5. Le matériel TIC mis à la disposition des utilisateurs est la propriété au sens large de la notion, y compris le matériel en leasing de l'entreprise.

Le matériel TIC personnel est soumis aux mêmes règles d'utilisation que le matériel TIC de l'employeur une fois connecté au réseau de l'entreprise.

Art. 6. Le matériel TIC ne peut être utilisé qu'à des fins professionnelles. Les utilisateurs doivent se servir des moyens mis à leur disposition en bons pères de famille.

Art. 7. Onverminderd het vorige artikel, beslissen de ondernemingen, overeenkomstig hoofdstuk 10, of de gebruikers gebruik mogen maken van TIC-materiaal voor privé-doeleinden alsook voor de modaliteiten van dit gebruik.

Art. 7. Sans préjudice de l'article précédent, les entreprises déterminent, conformément au chapitre 10, si elles autorisent les Utilisateurs à utiliser le matériel TIC à des fins privées ainsi que les modalités de cette utilisation.

Art. 8. De gebruiker dient bij het gebruik van TIC-materiaal steeds de intellectuele eigendomsrechten van derden na te leven, inclusief die van de onderneming. Meer specifiek zijn de teksten, beelden of geluiden ontvangen in een e-mail of gevonden op het internet meestal beschermd door auteursrechten. Bijgevolg is het formeel verboden om deze onder welke vorm dan ook te reproduceren zonder voorafgaandelijk akkoord van de onderneming.

Art. 8. L'utilisateur est tenu de respecter les droits de propriété intellectuelle des tiers, en ce compris ceux de l'entreprise, lors de l'utilisation du matériel TIC. Plus particulièrement, les textes, images ou sons reçus dans un message électronique ou trouvés sur l'internet sont généralement susceptibles d'être protégés par les droits d'auteur et sont donc formellement interdits de reproduction sous quelque forme que ce soit sans accord préalable de l'entreprise.

Hoofdstuk V - Vertrouwelijkheid en beveiliging van gegevens

Chapitre V - Confidentialité et sécurité des données

Art. 9. De ondernemingen stellen, overeenkomstig hoofdstuk IX, de beschikkingen op die de toegang tot hun informaticasysteem regelen.

Art. 9. Les entreprises établissent, conformément au chapitre IX, les dispositions réglementant l'accès à leur système informatique.

Art. 10. Onverminderd het vorige artikel, is het de gebruikers strikt verboden om opzettelijk de werking te belemmeren of een poging tot belemmering te doen van de systemen geïmplementeerd om de gegevensbeveiliging te waarborgen (onder meer anti-virussystemen) of om de zwakke punten van deze beveiligingssystemen te identificeren of te exploiteren en/of de beveiligde gegevens te ontcijferen.

Art. 10. Sans préjudice de l'article précédent, il est strictement interdit aux utilisateurs d'entraver ou de tenter d'entraver volontairement le fonctionnement des systèmes mis en place en vue de garantir la sécurité des données (notamment les systèmes anti-virus), d'identifier ou d'exploiter les points faibles desdits systèmes de sécurité et/ou de décrypter des données sécurisées.

Elke gebruiker dient zo snel mogelijk met de dienst informatica of met personen aangeduid door de onderneming contact op te nemen bij elk probleem en/of elke situatie waarvan hij, rekening houdend met zijn vaardigheden, vermoedt dat deze de beveiliging van de systemen en/of netwerken van de onderneming zouden aantasten of kunnen aantasten, zoals een virus.

Tout utilisateur doit contacter le plus rapidement possible le service informatique ou les personnes désignées par l'entreprise de tout problème et/ou toute circonstance qu'il suspecte, compte tenu de ses aptitudes, d'être une atteinte ou un risque d'atteinte à la sécurité des systèmes et/ou réseaux de l'entreprise, tel un virus.

Art. 11. Het is de gebruikers strikt verboden (een poging te doen om) binnen te dringen in het informaticasysteem van de onderneming met het oog op het wijzigen of wissen van gegevens. Het is ook niet toegestaan om via enig technologisch middel het mogelijke gebruik van gegevens in het systeem of de correcte werking van het systeem te wijzigen. In dat verband is het de gebruikers strikt verboden opzettelijk een programma te installeren of te laten installeren dat bestemd is om het systeem schade te berokkenen. Dat geldt onder meer voor elke vernietiging of poging tot vernietiging van dossiers en informaticaprogramma's op computers van de onderneming of op andere computers (via het internet), welk middel daartoe ook gebruikt wordt. Het gaat daarbij onder meer (maar blijft daartoe niet beperkt) om virussen, Trojaanse paarden, e-mailbommen en/of elk ander informaticadossier of -programma met schadelijk effect, enz.

Art.11. Il est strictement interdit aux utilisateurs (de tenter) de s'introduire dans le système informatique de l'entreprise dans le but de modifier ou d'effacer des données. Il est également interdit de modifier par tout moyen technologique l'utilisation possible de données dans le système ou le fonctionnement correct du système. A cet égard, il est notamment strictement interdit aux utilisateurs de volontairement installer ou de faire installer un programme destiné à causer un dommage. Il en est entre autres ainsi de toute destruction ou tentative de destruction de dossiers ou de programmes informatiques sur les ordinateurs de l'entreprise ou sur d'autres ordinateurs (via Internet), quel que soit le moyen utilisé, en ce compris et de manière non limitative, les virus, chevaux de Troie, bombes e-mail et/ou tout autre dossier ou programme informatique destructeur, etc.

Het is de gebruiker ook strikt verboden de oorsprong van e-mails te vervalsen of de systemen te wijzigen die gebruikt worden om de bron van e-mails te identificeren en/of de oorsprong ervan te verbergen.

Il est également strictement interdit aux utilisateurs de falsifier l'origine des e-mails ou de transformer les systèmes utilisés en vue d'identifier la source des e-mails et/ou de cacher l'origine de ceux-ci.

Art. 12. Om de beveiliging en de integriteit van de gegevens te bewaren mogen gebruikers bij voorbeeld enkel de websites, niet verboden door de onderneming, bezoeken en dienen ze, rekening houdend met hun vaardigheden, verplicht te controleren of de ontvangen e-mails afkomstig zijn van betrouwbare bronnen. Ook bij het downloaden van elk type programma, bij het bezoeken van internetsites, enz. dienen gebruikers extra alert te zijn om geen verdachte software te installeren, zoals sniffers, virussen, ...

Art. 12. En vue de préserver la sécurité et l'intégrité des données, les utilisateurs peuvent, à titre d'exemple, uniquement visiter des sites internet dont l'accès n'est pas interdit par l'entreprise et doivent impérativement, compte tenu de leurs aptitudes, vérifier que les E-mails reçus émanent de sources dignes de confiance. De la même manière, en cas de téléchargement de programmes, de quelque nature que ce soit, de visite de sites Internet, etc., les utilisateurs doivent tout particulièrement être attentifs à ne pas installer de software suspect tels des sniffers, des virus, ...

De verzender van een e-mailbericht is verantwoordelijk voor de inhoud ervan. Het is de gebruiker daarom formeel verboden e-mailberichten te versturen waarvan de inhoud een onwettig karakter zou hebben en/of zou indruisen tegen het fatsoen en de goede zeden, onder meer obsceen, racistisch, xenofoob, discriminerend, ...

L'expéditeur d'un message électronique est responsable du contenu de celui-ci. Il est dès lors formellement interdit à l'utilisateur d'envoyer des messages électroniques dont le contenu aurait un caractère illégitime et/ou contraire aux convenances et aux bonnes mœurs, notamment obscène, raciste, xénophobe, discriminatoire, ...

In het bijzonder is het verboden:

- e-mailberichten te verspreiden die een nadelige invloed kunnen hebben op de goede reputatie van de ondernemingen van de sector of van een of meerdere gebruikers, klanten of derden. Het gaat daarbij onder meer om berichten rond ras, nationaliteit, afkomst, geslacht, seksuele geaardheid, leeftijd, handicap, godsdienst, filosofie van personen of een groep personen;

- kettingberichten te versturen of te forwarden;

- spam, te weten, overbodige of niet gewenste e-mailberichten en/of mailings naar verschillende distributielijsten, individuen of organisaties massaal te verspreiden;

- opzettelijk virussen of andere storende of destructieve programma's te verspreiden;

- expliciet seksueel en/of obsceen beeldmateriaal of berichten door te sturen en/of op aanvraag te ontvangen en/of op te slaan;

- meer algemeen is elk gebruik van e-mail verboden dat indruist tegen het normaal gedrag van een goede huisvader.

Plus particulièrement, sont interdits:

- la dispersion de messages électroniques avec effet défavorable à la bonne réputation des entreprises du secteur ou de l'un ou plusieurs de ses utilisateurs, clients ou tiers, notamment des messages concernant la race, la nationalité, l'origine, le sexe, le comportement sexuel, l'âge, le handicap, la religion, la philosophie de personnes ou de groupes de personnes ;

- l'envoi ou le ré acheminement de messages en chaîne;

- spam, à savoir la distribution en masse de messages électroniques superflus ou non sollicités et/ou les mailings vers différentes listes de distribution, individus ou organisations;

- la dispersion intentionnelle de virus ou autres programmes perturbateurs ou destructifs;

- la transmission et/ou la réception sur demande et/ou la sauvegarde d'images ou de messages explicitement sexuels ou obscènes;

- de manière générale, toute utilisation du courrier électronique contraire à un comportement normal de bon père de famille.

Hoofdstuk VI - Controle

Regels voor globale controle van elektronische communicatie

Art.13. De ondernemingen houden zich het recht voor een globale controle (algemene, niet-individuele controle op het voltallige personeel) en permanente controle uit te oefenen. Deze globale controle wordt uitgeoefend om de rechten en vrijheden van anderen te beschermen of om daden waarvoor de ondernemingen aansprakelijk kunnen worden gesteld, te voorkomen, te onderzoeken en/of op te sporen, zoals onder meer het schenden van de intellectuele eigendomsrechten.

Chapitre VI - Contrôle

Modalités du contrôle global des communications électroniques

Art.13. Les entreprises ont le droit d'exercer un contrôle global (contrôle généralisé et non individualisé s'appliquant à l'ensemble du personnel) et permanent. Le contrôle global est exercé en vue de protéger les droits et libertés d'autrui ou en vue de prévenir, rechercher et/ou détecter des actes susceptibles d'engager la responsabilité des entreprises, tels que, entre autres, la violation des droits de propriété intellectuelle

Art. 14. De controle wordt uitgeoefend door de dienst informatica met de volgende doelstellingen:

1° het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die tegenstrijdig zijn met de goede zeden of de waardigheid van een ander persoon kunnen schaden, bijvoorbeeld computer kraken, niet toegestane vergaring van elektronische persoonsgegevens (persoonlijke administratieve en financiële gegevens, medische gegevens,...), raadplegen van sites met pornografisch of pedofiel karakter of sites die aanzetten tot discriminatie, segregatie, haat of geweld tegenover een groep, een gemeenschap of zijn leden omwille van hun ras, kleur, voorouders, godsdienst, nationale of etnische afkomst

2° de bescherming van de economische, handels- en financiële belangen van de onderneming die vertrouwelijk zijn alsook het tegengaan van ermee in strijd zijnde praktijken, bijvoorbeeld denigrerende reclame, zoals bepaald door de wet op de handelspraktijken, verspreiding van documenten en bestanden en schending van het bedrijfsgeheim, inclusief onderzoek en ontwikkeling, fabricageprocessen en alle vertrouwelijke gegevens;

3° de veiligheid en/of de goede technische werking van de informatica netwerksystemen van de onderneming, met inbegrip van de controle op de kosten die ermee gepaard gaan alsook de fysieke bescherming van de installaties van de onderneming, bijvoorbeeld gebruik van bandbreedte op het netwerk;

4° het te goeder trouw naleven van de in de onderneming geldende beginselen en regels voor het gebruik van onlinetechnologieën.

Regels voor individuele controle van elektronische communicatie

Art. 15. De werkgever omschrijft duidelijk en expliciet de doelstelling(en) van de controle. Als een onderneming bij een globale controle, anomalieën vaststelt of vermoedt, kunnen zich twee hypothesen voordoen:

Art. 14. Le contrôle est exercé par le service informatique dans le cadre des finalités suivantes :

1° la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui, par exemple le piratage informatique, la prise de connaissance non autorisée de données électroniques relatives aux personnes (données administratives et financières personnelles, données médicales...), la consultation de sites à caractère pornographique ou pédophile ou de sites incitant à la discrimination, à la ségrégation, à la haine ou à la violence à l'égard d'un groupe, d'une communauté ou de leurs membres, en raison de la race, de la couleur, de l'ascendance, de la religion ou de l'origine nationale ou ethnique de ceux-ci;

2° la protection des intérêts économiques, commerciaux et financiers des entreprises auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires, par exemple la publicité dénigrante, telle que définie dans la loi sur les pratiques du commerce, la divulgation de documents et fichiers et la violation du secret des affaires y compris la recherche et le développement, les processus de fabrication et toutes données confidentielles;

3° la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations des entreprises, par exemple la consommation de bande passante sur le réseau;

4° le respect de bonne foi des principes et règles d'utilisation des technologies de l'information, tels que fixés dans l'entreprise.

Modalités d'individualisation du contrôle des communications électroniques

Art. 15. L'employeur définit clairement et de manière explicite la ou les finalités du contrôle. Si, à l'occasion d'un contrôle global, une entreprise constate ou suspecte des anomalies, deux hypothèses doivent être distinguées :

1° Directe individualisering

In deze hypothese wil men de anomalieën onderzoeken die opgespoord werden in het kader van de globale controledoelstellingen zoals bepaald in artikel. 14, 1°,2° en 3°, met name:

- het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die strijdig zijn met de goede zeden of de waardigheid van een andere persoon kunnen schaden;
- de bescherming van de economische, commerciële en financiële belangen van de ondernemingen die een vertrouwelijk zijn karakter hebben alsook de strijd tegen praktijken die ertegen indruisen;
- de beveiliging en/of optimale technische werking van de IT netwerksystemen van de ondernemingen, inclusief controle van de daarmee gepaard gaande kosten en de fysieke bescherming van de ondernemingsinstallaties.

In deze gevallen kunnen de ondernemingen zonder enige andere procedure opteren voor een individuele controle waarmee de identiteit van de persoon (personen) kan opgespoord worden (in het verleden) die verantwoordelijk is (zijn) voor de anomalie.

2° Indirecte individualisering mits naleving van een voorafgaande informatiefase.

a) Principe

In deze hypothese wil men anomalieën onderzoeken die opgespoord werden in het kader van de globale controle of naleving van de principes en regels inzake het gebruik van informatietechnologieën vastgelegd binnen de ondernemingen.

b) Voorafgaande informatieprocedure

Voor die anomalieën gebeurt de individuele controle als volgt:

1° Individualisation directe

Dans cette hypothèse, on vise des anomalies détectées dans le cadre des finalités de contrôle global tel que prévue à l'article 14, 1°,2° et 3°, à savoir :

- la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui;
- la protection des intérêts économiques, commerciaux et financiers des entreprises auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires;
- la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau des entreprises, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations des entreprises.

Dans ces cas, les entreprises peuvent opter sans autre forme de procédure pour un contrôle individualisé permettant de retracer (pour le passé) l'identité de la (ou des) personne(s) responsable(s) de l'anomalie.

2° Individualisation indirecte moyennant le respect d'une phase préalable d'information.

a) Principe

Dans cette hypothèse, on vise des anomalies qui sont détectées dans le cadre de la finalité du respect de bonne foi des principes et règles d'utilisation des technologies de l'information fixée dans les entreprises.

b) Procédure préalable d'information

Pour ces anomalies, le contrôle individuel se fait comme suit :

Wanneer men een afwijking vaststelt in het kader van de globale controle of naleving van de principes zoals bepaald in artikel 14, 4°, van deze collectieve arbeidsovereenkomst, zullen alle gebruikers op de hoogte worden gesteld van deze afwijking. Ze zullen bovendien verwittigd worden van het feit dat de onderneming kan overgaan tot een individuele controle van de gegevens, wanneer een nieuwe afwijking van dezelfde aard wordt vastgesteld, dit om de identiteit van de persoon (personen) verantwoordelijk voor de afwijking op te sporen.

Lorsque l'on constate une anomalie dans le cadre du contrôle global du respect des principes tels que prévues à l'article de la présente note 14, 4°, de la présente convention collective de travail, l'ensemble des utilisateurs seront mis au courant de l'existence de l'anomalie et seront avertis du fait que l'entreprise pourra procéder à une individualisation des données lorsqu'une nouvelle anomalie de même nature sera constatée, afin de retracer l'identité de la (ou des) personne(s) responsable(s) de l'anomalie.

3° Indien de onderneming van mening is dat de persoon verantwoordelijk voor een afwijking dient bestraft te worden, zal de verantwoordelijke in de hiërarchie en/of human ressources hem/haar uitnodigen voor een gesprek. Dit gesprek zal voorafgaan aan elke beslissing van de onderneming die de gebruiker als individu kan treffen. De gebruiker kan zich steeds laten bijstaan door een syndicaal afgevaardigde van zijn keuze overeenkomstig het syndicale statuut.

3° Si l'entreprise estime qu'il y a lieu de sanctionner l'utilisateur responsable d'une anomalie, le responsable hiérarchique et/ou les ressources humaines invitera ce dernier à un entretien. Cet entretien sera préalable à toute décision de l'entreprise susceptible d'affecter individuellement l'utilisateur. L'utilisateur peut toujours se faire assister d'un délégué syndical de son choix conformément au statut syndical.

Art. 16. Bovendien worden de geïnstalleerde controlesystemen regelmatig geëvalueerd, naar gelang het geval in de ondernemingsraad, het comité voor preventie en bescherming op het werk of met de vakbondsafvaardiging, met het oog op voorstellen om ze aan te passen aan de technologische ontwikkelingen.

Art. 16. Une évaluation des systèmes de contrôle installés est en outre réalisée régulièrement, selon le cas, au sein du conseil d'entreprise, du comité pour la prévention et la protection au travail ou avec la délégation syndicale de manière à faire des propositions en vue de les revoir en fonction des développements technologiques.

Hoofdstuk VII - Privé-leven en bewaring van persoonlijke gegevens

Chapitre VII - Vie privée et conservation des données personnelles

Art. 17. De gebruiker aanvaardt dat gegevens met persoonlijke karakter die op hem/haar betrekking hebben, behandeld of verzameld en bewaard worden om systemen te implementeren en om te controleren of het gebruik ervan overeenstemt met de doelstellingen die in deze collectieve arbeidsovereenkomst werden vastgelegd.

Art. 17. L'utilisateur accepte que des données à caractère personnel le concernant soient traitées, collectées et conservées en vue de la mise en œuvre des systèmes et de la vérification de leur utilisation conformément aux finalités fixées par la présente convention collective de travail.

De behandelde gegevens zijn onder meer internet-adressen van bezochte websites, de duur en frequentie van de bezoeken, de omvang van e-mails, het adres van de bestemmeling van de e-mail met naleving van de principes inzake de doelstellingen, de proportionaliteit en de transparantie voorzien door de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, bekendgemaakt in het Belgisch Staatsblad van 18 maart 1993.

Les données traitées incluent les adresses internet des sites visités, la durée et la fréquence des visites, la taille des e-mails, l'adresse du destinataire de l'e-mail dans le respect des principes de finalités, de proportionnalité et de transparence prévus par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, publiée au Moniteur Belge du 18 mars 1993.

Een controle kan uitgevoerd worden op de gegevens bewaard vanaf de inwerkingtreding van deze collectieve arbeidsovereenkomst.

Un contrôle peut être effectué sur les données conservées à partir de la date d'entrée en vigueur de la présente convention collective de travail.

Gegevens met persoonlijk karakter kunnen slechts bewaard worden gedurende een periode nodig voor de realisatie van de doelstellingen nagestreefd door deze collectieve arbeidsovereenkomst.

Les données à caractère personnel ne peuvent être conservées que pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités poursuivies par la présente convention collective de travail.

Art. 18. De gebruiker heeft het recht op toegang tot deze gegevens met persoonlijke karakter en kan ze laten verbeteren, in overeenstemming met de procedures bepaald in de voornoemde wet van 8 december 1992 en de bijhorende uitvoeringsbesluiten.

Art. 18. L'utilisateur a un droit d'accès à ces données à caractère personnel et peut les faire corriger, conformément aux procédures arrêtées par la loi du 8 décembre 1992, précitée, et à ses arrêtés d'exécution.

De gebruiker die wenst te weten welke informatie er omtrent zijn persoon werd verzameld in het kader van een globale en/of individuele controle, kan daartoe een schriftelijk verzoek richten tot de bevoegde dienst aangewezen door de ondernemingen.

L'utilisateur qui souhaite savoir quelles informations ont été rassemblées à son propos dans le cadre d'un contrôle global et/ou individuel, peut adresser à cet effet une demande écrite au service compétent désigné par les entreprises.

Hoofdstuk VIII - Sancties

Chapitre VIII - Sanctions

Art. 19. Bij vaststelling van een inbreuk op deze collectieve arbeidsovereenkomst of van de interne reglementen van de ondernemingen, zullen deze een van de sancties kunnen toepassen voorzien door hun arbeidsreglement(en).

Art. 19. En cas de constatation d'une infraction à la présente convention collective de travail ou des règlements internes des entreprises, celles-ci pourront appliquer une des sanctions prévues par leur(s) règlement(s) de travail.

Hoofdstuk IX - Lokale akkoorden

Art. 20. Deze collectieve arbeidsovereenkomst kan op nuttige wijze vervolledigd worden door een ondernemingscollectieve arbeidsovereenkomst of een lokaal paritair akkoord.

Chapitre IX - Accords locaux

Art. 20. La présente convention collective de travail peut être utilement complétée par une convention collective de travail d'entreprise ou un accord paritaire local.

Hoofdstuk X - Geldigheidsduur

Art. 21. Deze collectieve arbeidsovereenkomst wordt gesloten voor onbepaalde duur en heeft uitwerking met ingang van 1 juni 2006.

Deze collectieve arbeidsovereenkomst kan, mits het naleven van een opzegtermijn van 6 maanden, door één van de ondertekenende partijen, geheel of gedeeltelijk, worden opgezegd bij aangetekende brief, gericht aan de voorzitter van het Paritair Comité voor het gas- en elektriciteitsbedrijf.

Chapitre X - Durée de validité

Art. 21. La présente convention collective de travail est conclue pour une durée indéterminée et produit ses effets le 1er juin 2006.

La présente convention collective de travail peut être dénoncée, en tout ou en partie, par l'une des parties, moyennant le respect d'un délai de préavis de 6 mois, par lettre recommandée adressée au président de la Commission paritaire de l'industrie du gaz et de l'électricité.

Bijlage 1 bij de collectieve arbeidsovereenkomst van 30 november 2006, gesloten in het Paritair Comité voor het gas- en elektriciteitsbedrijf, betreffende het TIC-materiaal

-

Toepassingsmodaliteiten

van artikel 2, 3de lid :

In het kader van de collectieve informatie met een algemeen karakter, door de vakbonden verspreid via e-mails, zullen de HR-vertegenwoordigers van de onderneming ter informatie in kopie gezet worden.

Met algemeen karakter bedoelt men documenten die de vakbonden normaal aan de uithangborden van de vakbonden zouden opgehangen hebben, verdeeld in vergaderingen of verdeeld in kantoren, kleedkamers, werkplaatsen, ...

Met "collectieve informatie" bedoelt men documenten bestemd voor het geheel van de aangeslotenen in een onderneming, een TBE, een departement/BU, ...

Bij het verzenden van e-mails zullen de syndicale mandatarissen ervoor zorgen dat geen verwarring bestaat tussen hun syndicaal mandaat en hun beroepsactiviteiten.

Bijvoorbeeld zij zullen ervoor zorgen dat hun syndicale handtekening op een beroepsmail niet wordt gebruikt en vice-versa, noch een syndicaal onderwerp in "subject" op een beroepsmail te vermelden en vice-versa.

Annexe 1 à la convention collective de travail du 30 novembre 2006, conclue au sein de la Commission paritaire de l'industrie du gaz et de l'électricité, relative au matériel TIC

-

Modalités d'applications

de l'article 2, 3ème alinéa :

Dans le cadre de l'information collective à caractère général, faite par les organisations syndicales via les e-mails, les responsables RH de l'entreprise seront mis en copie pour information.

On entend par caractère général des documents que les organisations syndicales auraient normalement affiché aux valves syndicales, distribué dans des assemblées ou distribué dans les bureaux; les vestiaire, ateliers, ...

On entend par "information collective"des documents destinés à l'ensemble des affilié dans une entreprise, une UTE, un département/BU, ...

Lors de l'envoi d'e-mails, les mandataires syndicaux veilleront à ne créer aucune confusion entre leur mandat syndical et leurs activités professionnelles.

Par exemple, ils veilleront à ne pas utiliser leur signature syndicale dans un mail professionnel et vice-versa, ni à mettre en "subject" un sujet syndical dans un mail professionnel et vice-versa.

van artikel 6 :

Dit artikel doet geen afbreuk aan de bestaande afspraken terzake in de ondernemingen op datum van de ondertekening van deze overeenkomst.

van artikel 7 :

De ondernemingen zijn ertoe gehouden alles in het werk te stellen om de nodige filters te installeren en "user policies" op te stellen zodat de Gebruikers enkel toegang hebben tot het "TIC"-materiaal dat voor hen bestemd en toegankelijk is.

van artikel 11, 2de lid :

Het verbergen van de oorsprong van de e-mail wil niet zeggen dat, in het geval van een overdracht/forwarding van de inhoud van de e-mail, de naam van de oorspronkelijke verzender niet mag verwijderd worden.

de l'article 6 :

Cet article ne porte pas préjudice aux accords existants en la matière dans les entreprises à la date de signature de la présente convention.

de l'article 7 :

Les entreprises sont tenues de mettre tout en œuvre pour installer les filtres nécessaires et créer des "user policies" afin que les Utilisateurs n'aient accès qu'au matériel (TIC" qui leur est destiné et accessible.

de l'article 11, 2ème alinéa :

Cacher l'origine d'e-mails ne veut pas dire que dans le cas d'un transfert/forwarding du contenu d'un e-mail, le nom de l'expéditeur d'origine ne peut pas être effacé.

*Bijlage 2 bij de collectieve arbeidsovereenkomst van 30 november 2006, gesloten in het Paritair Comité voor het gas- en elektriciteitsbedrijf, betrejfende het **TIC-materiaal***

Advies van 20 oktober 2006 van de Commissie voor de Berekening van de Persoonlijke levenssfeer betreffende het protocol van **overeenkomst "TIC"-Materiaal** van 1 juni 2006 - Wet Verwerking Persoonsgegevens (privacywet)[1]

Algemeen

Alvorens in te gaan op de grond van de zaak past het enkele voorafgaande **opmerkingen** te **formuleren.**

Er bestaat voor de gehele private sector reeds een **duidelijke** regelgeving hoe de tegengestelde belangen (de bescherming van de persoonlijke levenssfeer in hoofde van de **werknemers** enerzijds en de wettigheid van een zeker toezicht van de werkgever op het gebruik van de werkinstrumenten anderzijds) kunnen verzoend worden en dat is de CAO 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,** gesloten in de Nationale Arbeidsraad en algemeen verbindend verklaard bij Koninklijk besluit van 12 juni 2002. Deze CAO nr. 81 is ook van toepassing op de werkgevers die vallen onder het paritair comité voor het gas- en elektriciteitsbedrijf. Waar CAO nr. 81 juist het kluwen van regels probeert te ontwarren - de problematiek van werkgeverscontrole op email en internetgebruik wordt immers beheerst door een samenloop van bepalingen uit diverse wetgevingen - zou zich met de CAO in wording echter een nieuwe **normering,** weliswaar met beperkt toepassingsgebied ratione personae, toevoegen aan het reeds bestaand **"wettelijk"** arsenaal.

Het verslag[2] dat CAO nr. 81 voorafgaat voorziet dat de basisnormen van CAO nr. 81 op sector- **en/of ondernemingsniveau** kunnen worden verduidelijkt, aangevuld en/of aangepast rekening houdend met de specifieke situatie.

Vooreerst vraagt de Commissie zich af of de "specifieke situatie" waarvan sprake in het verslag bij CAO nr. 81 zich **wel stelt om** voor de sector gas- en elektriciteit de basisnormen van CAO nr. 81 te verduidelijken, aan te vullen en/of aan te passen. Het verdient aanbeveling deze te **vermelden.**

[1] De wet van 8 december 1992 **tot** bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens.

[2] Vermoedelijk vonden de stellers van onderhavige protocolovereenkomst een aanknopingspunt voor hun werkzaamheden in bedoeld verslag.

Ten tweede, wat de eventuele aanpassing ervan betreft, mag, ingevolge artikelen 9, 10 en 51 van de wet van 5 december 1968 betreffende de collectieve arbeidsovereenkomsten en de paritaire comités, een overeenkomst gesloten in een paritair comité niet in strijd komen met een in de Nationale Arbeidsraad gesloten en bij KB algemeen verbindend verklaard interprofessioneel akkoord, noch met de hogere rechtsnormen die hier in het geding zijn, zoals de privacywet, de wet van 13 juni 2005 betreffende de elektronische communicatie en de artikelen 259bis en 314bis van het Strafwetboek.

Ten derde, wat de eventuele verduidelijking of aanvulling ervan betreft, heeft de Commissie, na lezing van de protocolovereenkomst, niet de indruk dat deze de basisnormen van CAO nr. 81 verduidelijkt of aanvult, althans niet in die mate dat zij het juridisch bestaansrecht van deze toekomstige CAO voor de werkgevers en werknemers die vallen onder het paritair comité voor het gas- en elektriciteitsbedrijf zou verantwoorden. De Commissie durft zelfs te gewagen van het tegendeel omdat een zeer belangrijk principe uit CAO nr. 81, met name de verplichting tot collectieve en individuele informatie over de mogelijkheid van controle, niet meer terug te vinden is in de protocolovereenkomst.

Ten vierde bestaat er een controverse onder rechtsgeleerden over de juridische waarde van CAO nr. 81 zelf[3]. Daarom is het niet evident om, enerzijds, CAO nr. 81 als uitgangspunt te nemen (cfr. artikel 2 van de protocolovereenkomst : doel is het reglementeren van het gebruik van technologisch materiaal voor informatie en Communicatie ter beschikking gesteld door de ondernemingen van de sector overeenkomstig CAO nr. 81, eigen cursivering) en anderzijds deze CAO nr. 81 gedeeltelijk te "herschrijven" (onder andere door gebruikmaking van een andere terminologie, het expliciteren van rechten die niet in de CAO 81 zelf staan, zoals het recht van toegang en verbetering en het niet voorzien van procedures die de werkgever bij de installatie van het controlesysteem in acht moet nemen met betrekking tot de voorlichting van de werknemers, in tegenstelling tot CAO nr. 81).

Concreet

Wat volgt is een bespreking van een aantal voor de Commissie relevante artikelen van de protocolovereenkomst.

[3] Zonder volledig te willen zijn gaat het om twijfels in het licht van artikel 22 Grondwet (anders dan artikel 8 EVRM vereist artikel 22 Grondwet een wet in de formele zin van het woord voor privacybeperkingen), of nog, twijfels in het licht van het strafrechtelijk beschermd telecommunicatiegeheim (controle van inhoud van communicatie en bestaan van communicatiegegevens door een niet-deelnemer is in principe niet toegelaten behoudens de toestemming van bij de communicatie betrokken personen, cfr. Artikel 124 van de wet elektronische communicatie en de artikelen 259bis en 314bis van het Strafwetboek). Anderzijds moet vastgesteld worden dat CAO nr. 81 in een bijzonder ingewikkelde en delicate materie een evenwicht heeft willen vinden tussen de conflicterende belangen die op het spel staan en CAO nr. 81 minstens op praktisch vlak zijn nut reeds heeft bewezen of kan bewijzen, ook al zijn er wat juridische problemen.

Artikel 5 van de protocolovereenkomst

Het betreft een kopie van artikel 1, § 1, CAO nr. 81, waarnaar trouwens expliciet wordt verwezen. Het is, net zoals bij CAO nr. 81, het basisartikel uit de protocolovereenkomst en waarin wordt verwezen naar 3 grote principes uit de WVP : de werkgever kan enkel controles verrichten op elektronische on-linecommunicatiegegevens wanneer de beginselen van finaliteit, proportionaliteit en transparantie worden nageleefd.

Ondanks de bewoordingen van artikel 5 van de protocolovereenkomst, moet vastgesteld worden dat, wat betreft het transparantiebeginsel, de protocolovereenkomst niet voorziet in enige procedure die de werkgever bij de installatie van het controlesysteem in acht moet nemen met betrekking tot de voorlichting van de werknemers, in tegenstelling tot CAO nr. 81 (zie ook supra).

Artikelen 8 en 9 van de protocolovereenkomst

Volgens deze artikelen mag het technologisch materiaal voor informatie en communicatie enkel gebruikt worden voor de uitvoering van de arbeidsovereenkomst, tenzij de werkgever beslist dat zijn werknemers ervan gebruik mogen maken voor privédoeleinden.

De protocolovereenkomst, net zoals CAO 81, regelt dus niet de toegang en het gebruik van de elektronische communicatiemogelijkheden op het werk zelf. Dit behoort tot het beslissingsdomein van de werkgever.

De ondernemer heeft weliswaar het recht te bepalen dat er enkel beroepsmatig gebruik mag zijn, maar zelfs in dat geval zal privégebruik voor dwingende reden aanvaardbaar zijn. De Commissie, onder verwijzing naar rechtspraak van het Europees Hof voor de Rechten van de Mens, stelde eerder dat aangezien de werkvloer de uitgelezen plaats is om contacten te onderhouden met collega's, en zelfs met buitenstaanders, werkgevers een zekere tolerantie moeten vertonen ten aanzien van privé-communicatie die door hun personeelsleden wordt gevoerd met hun communicatiemiddelen[4].

[4] EHRM, arrest van 16 december 1992 (zaak Niemitz), Serie A, vol. 251 B.

Artikelen 15 tot en met 17bis van de protocolovereenkomst

Deze artikelen uit de protocolovereenkomst bevestigen de getrapte, proportionele aanpak, zoals die bleek uit het advies van de Commissie van 3 april 2000 en CAO nr. 81 : in een eerste fase worden enkel globale gegevens verzameld op grond waarvan het niet mogelijk is individuele werknemers te identificeren (artikel 15 protocolovereenkomst). Wanneer een anomalie wordt vastgesteld in het kader van die algemene, niet individuele controle op het voltallige personeel, wordt vervolgens in een tweede fase overgegaan tot identificatie van de voor de anomalie verantwoordelijke werknemer (artikel 17 protocolovereenkomst).

Net zoals CAO nr. 81 gaat de protocolovereenkomst ervan uit dat controle op de telecommunicatiegegevens en het toeschrijven ervan aan fysieke personen mogelijk is onder bepaalde voorwaarden, al zijn er wat terminologische verschillen met de bewoordingen van CAO nr. 81.

Controle op telecomgegevens is slechts voor vier doeleinden geoorloofd : (1) het voorkomen van ongeoorloofde of lasterlijke feiten, feiten die tegenstrijdig zijn met de goede zeden of de waardigheid van een ander persoon kunnen schaden, (2) de bescherming van de economische, handels- en financiële belangen van de onderneming die vertrouwelijk zijn alsook het tegengaan van ermee in strijd zijnde praktijken, (3) de veiligheid en/of de goede technische werking van de IT netwerksystemen van de onderneming, met inbegrip van de controle op de kosten die ermee gepaard gaan alsook de fysieke bescherming van de installaties van de onderneming en (4) het te goeder trouw naleven van de in de onderneming geldende beginselen en regels voor het gebruik van onlinetechnologieën (artikel 16 protocolovereenkomst).

Ook de regelmatige evaluatie van geïnstalleerde controlesystemen werd ingeschreven in de protocolovereenkomst (artikel 17bis protocolovereenkomst).

Niet aanwezig in de protocolovereenkomst, en nochtans cruciaal als voorwaarde voor de controle op telecomgegevens in CAO nr. 81, is de verplichte voorafgaande collectieve en individuele informatie welke de werkgever bij het invoeren van de controle in acht moet nemen.

De voorwaarden tot individualisering van de telecommunicatiegegevens (het leggen van een band tussen de gegevens en een werknemer) voorzien, net zoals in CAO nr. 81, een indirecte en directe procedure.

Een directe procedure van individualisering is van toepassing op de controles uitgevoerd ter bestrijding van onrechtmatig gedrag, de bescherming van de bedrijfsgegevens en de veiligheid van het net.

De directe individualisering is toegestaan zonder verder bijkomende verplichtingen. De verplichte voorafgaande collectieve en individuele informatie bij het invoeren van de controle in de onverdachte periode volstaat.

Een indirecte procedure van individualisering is van toepassing op controles op de naleving van de interne afspraken van het gebruik van het netwerk (zoals het verbod om overdreven veel e-mails voor privé-zaken te verzenden). In dat geval mag de werkgever de verantwoordelijke voor de bedoelde onregelmatigheid in eerste instantie niet identificeren. Het is pas nadat werknemers herinnerd worden aan het bestaan van de overtreden regel (alarmbelprocedure) en zich opnieuw een onregelmatigheid van dezelfde aard heeft voorgedaan dat identificatie mogelijk is. Vooraleer de geïdentificeerde werknemer verantwoordelijk kan worden gesteld, moet hij worden gehoord, zodat hij zijn gedrag kan verantwoorden. Men kan zich de vraag stellen of dit laatste niet ook van toepassing zou moeten zijn bij de directe procedure van individualisering.

Artikelen 18 en 19 van de protocolovereenkomst

Inhoudelijk vergen deze artikelen weinig commentaar, maar op redactioneel gebied kunnen de volgende opmerkingen worden genoteerd.

Artikelen 18 en 19 spreken nu eens van "persoonlijke gegevens", dan weer van "gegevens van persoonlijke aard", een andere keer van "gegevens met persoonlijk karakter". Er wordt in artikel 18 ook verwezen naar de WVP, terwijl de titulatuur van deze wet verkeerdelijk wordt weergegeven. Artikel 19 spreekt van uitvoeringsbesluiten bij de WVP, terwijl er maar één besluit ter zake werd genomen en met name het koninklijk besluit van 13 februari 2001. Een terminologische opfrissing is zeker aangewezen.

Artikel 19 van de protocolovereenkomst bevestigt het recht van artikel 10 en 12 WVP. Dit is een pluspunt in vergelijking met CAO nr. 81, aangezien dit recht slecht wordt vernoemd in het verslag dat CAO nr. 81 voorafgaat en niet in de tekst van CAO nr. 81 zelf.

Conclusie

Uit onderhavige analyse moet blijken dat de Commissie alvast voorbehoud maakt ten aanzien van de noodzaak van bedoelde CAO in voorbereiding.

Indien de noodzaak van dergelijke CAO zich niettemin zou aandienen, herinnert de Commissie eraan dat hierin de procedure moet worden voorzien die de werkgever bij de installatie van het controlesysteem in acht moet nemen met betrekking tot de voorlichting van de werknemers.

Annexe 2 à la convention collective de travail du 30 novembre 2006, conclue au sein de la Commission paritaire de l'industrie du gaz et de l'électricité, relative au matériel TIC

-

Avis du 20 octobre 2000 de la Commission pour la protection de la vie privée relatif au protocole de convention matériel "TIC" du 1er juin 2006 - Loi sur le traitement des données personnelles (loi sur la protection de la vie privée)[1].

GENERALITES

Avant de traiter le fond de l'affaire, il convient de formuler quelques remarques préalables.

I. Pour l'ensemble du secteur privé, il existe déjà une réglementation claire précisant la manière de concilier des intérêts divergents (protection de la vie privée des travailleurs d'une part et légitimité d'un certain contrôle de l'employeur sur l'utilisation des instruments de travail, d'autre part), à savoir la convention collective de travail n° 81 du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau, conclue au sein du Conseil national du travail et rendue obligatoire par arrêté royal du 12 juin 2002. Cette convention collective de travail n° 81 est également applicable aux employeurs ressortissant à la Commission paritaire de l'industrie du gaz et de l'électricité. Alors que la convention collective de travail n° 81 tente précisément de démêler l'enchevêtrement de règles - la problématique du contrôle patronal sur le courrier électronique et l'utilisation d'internet est en effet régie par un ensemble de dispositions issues de différentes législations - la convention collective de travail en préparation ne ferait qu'ajouter une nouvelle norme, bien que le champ d'application en serait restreint ratione personae, à l'arsenal "juridique" existant.

II. Le rapport[2] qui précède la convention collective de travail n° 81 prévoit que les normes de base de la convention collective de travail n° 81 peuvent être précisées, complétées et/ou au niveau du secteur et/ou de l'entreprise, compte tenu de la situation spécifique.

Tout d'abord, la Commission se demande si la "situation spécifique" dont il est question dans le rapport à la convention collective de travail n° 81 se pose effectivement pour envisager une précision, un complément ou une adaptation des normes de base de la convention collective de travail n° 81 dans le secteur du gaz et de l'électricité. Il convient de le mentionner.

[1] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.
[2] Les rédacteurs du protocole de convention y trouveront probablement du point d'ancrage pour leurs travaux.

Deuxièmement, en ce qui concerne une éventuelle adaptation, une convention conclue au sein d'un organe paritaire ne peut, conformément aux articles 9, 10 et 51 de la loi du 5 décembre 1968 sur les conventions collectives de travail et les commissions paritaires, être contraire à un accord interprofessionnel conclu au sein du Conseil national du travail et rendu obligatoire par arrêté royal, ni à des normes juridiques de niveau supérieur mentionnées en l'espèce, notamment la loi sur la protection de la vie privée, la loi du 12 juin 2005 relative aux communications électroniques ainsi que les articles 259bis et 314bis du Code pénal.

Troisièmement, en ce qui concerne une explication ou un complément éventuel, la commission n'a pas l'impression, après lecture du protocole de convention, que ce dernier explique ou complète les normes de base de la convention collective de travail n° 81, du moins pas dans la mesure où il justifierait le droit d'existence juridique de cette future convention collective de travail pour les employeurs et les travailleurs ressortissant à la Commission paritaire de l'industrie du gaz et de l'électricité. La commission peut mener poser le contraire parce que un principe très important de la convention collective de travail n° 81, à savoir l'obligation d'une information collective et individuelle sur la possibilité de contrôle, ne se retrouve plus dans le protocole de convention.

Quatrièmement, il existe une controverse quant entre juristes quant à la valeur juridique de la convention collective de travail n° 81 en elle-même[3]. C'est pourquoi il n'est pas évident, d'une part, de prendre la convention collective de travail n° 81 comme point de départ (cf. article 2 du protocole de convention : l'objectif est de réglementer l'utilisation du matériel technologique par les entreprises du secteur conformément à la convention collective de travail n° 81, mise en italique propre) et, d'autre part, de "réécrire" partiellement cette convention collective de travail n° 81 (entre autres par le biais de l'utilisation d'une part terminologie, l'explicitation de droits qui ne figurent même pas dans la convention collective de travail 81 elle-même, tels que le droit d'accès et de rectification ainsi que l'absence de mention de procédures que l'employeur doit respecter lors de l'installation du système de contrôle, portant notamment sur l'information aux travailleurs, contrairement à la convention collective de travail n° 81).

CONCRETEMENT

Ce qui suit est une discussion d'une série d'articles du protocole de convention, pertinents pour la commission.

[3] Sans être exhaustif, il s'agit en fait de doutes émis à la lumière de l'article 22 de la Constitution (au contraire de l'article 8 de la CEDH, l'article 22 de la Constitution requiert une loi dans le sens formel du terme pour des restrictions à la vie privée) ou encore de doutes émis à la lumière du secret des télécommunications protégé pénalement (le contrôle du contenu des communications et connaissance de données de communication par un non-participants ne sont en principe pas autorisés sauf autorisation des personnes prenant part à la communication, cf. article 124 de la loi relative aux communications électroniques et les articles 259bis et 314bis du Code pénal). D'autre part, il faut constater que la convention collective de travail n° 81 a souhaité trouver un équilibre, dans une matière particulièrement complexe et délicate, entre des intérêts conflictuels; elle a d'ailleurs déjà démontré son importance dans la pratique, même s'il existe quelques problèmes juridiques.

Article 5 du protocole de convention

Il s'agit d'une copie de l'articleler, § 1er de la convention collective de travail n° 81, dont la référence est d'ailleurs explicite. Comme pour la convention collective de travail n° 81, il s'agit de l'article de base du protocole de convention, qui se réfère à 3 grands principes de la loi sur la protection de la vie privée : l'employeur ne peut effectuer des contrôles sur des données de communications électroniques que lorsque les principes de finalité, proportionnalité et transparence sont respectés.

Malgré les termes de l'article 5 du protocole de convention, force est de constater qu'en ce qui concerne le principe de transparence, le protocole de convention ne prévoit aucune procédure devant être respectée par l'employeur lors de l'installation du système de contrôle, portant notamment sur l'information aux travailleurs, contrairement à la convention collective de travail n° 81 (voir aussi supra).

Articles 8 et 9 du protocole de convention

Selon ces articles, le matériel technologique destiné à l'information et la communication ne peut être utilisé que pour l'exécution du contrat de travail à moins que l'employeur ne décide que ses travailleurs peuvent également l'utiliser à des fins privées.

Le protocole de convention, tout comme la convention collective de travail 81, ne règle donc pas l'accès et l'utilisation des possibilités de communication électroniques au travail même. Cela relève d'une décision de l'employeur.

L'employeur a toutefois le droit de décider que l'utilisation est limitée à des fins professionnelles mais, même dans ce cas, l'usage privé pour des raisons impérieuses sera acceptable. En référence à la jurisprudence de la Cour européenne des Droits de l'Homme, la Commission a posé précédemment que le lieu de travail étant l'endroit privilégié pour entretenir des contacts avec les collègues et même avec des personnes de l'extérieur, les employeurs devaient faire preuve d'une certaine tolérance à l'égard des communications privées que leur personnel entretient avec leurs moyens de communication[4].

[4] CEDH, arrêt du 16 décembre 1992 (affaire Niemitz), Serie A, vol. 251 B.

Articles 15 et 17bis inclus du protocole de convention

Ces articles du protocole de convention confirment l'approche par paliers et proportionnelle visée par l'avis de la Commission du 3 avril 2000 et al convention collective de travail n° 81 : dans une première phase, seules des données globales sont collectées sur la base desquelles il n'est pas possible d'identifier des travailleurs individuels (article 15 du protocole de convention). Lorsqu'une anomalie est constatée dans le cadre de ce contrôle général non individuel sur l'ensemble du personnel, il est ensuite, dans une deuxième phase, procédé à l'identification du travailleur responsable de l'anomalie (article 17 du protocole de convention).

Tout comme la convention collective de travail n° 81, le protocole de convention part du principe que le contrôle des données de télécommunications et son attribution à des personnes physiques est possible sous certaines conditions, même si des différences terminologiques sont à noter par rapport à la convention collective de travail n° 81.

Le contrôle des données télécoms est uniquement licite pour 4 objectifs : (1) la prévention de faits illicites, diffamatoires, contraires aux bonnes mœurs ou pouvant nuire à la dignité d'une autre personne, (2) la protection des intérêts économiques, commerciaux et financiers confidentiels de l'entreprise ainsi que la lutte contre des pratiques contraires à ces intérêts, (3) la sécurité et/ou le bon fonctionnement technique de systèmes de réseau **IT** de l'entreprise, en ce compris le contrôle des coûts y liés ainsi que la protection physique des installations de l'entreprise et (4) le respect de bonne foi des principes et règles en vigueur dans l'entreprise en matière d'utilisation des technologies en ligne (article 16 du protocole de convention).

L'évaluation régulière des systèmes de contrôle installés a également été inscrit dans le protocole de convention (article 17bis du protocole de convention).

Par contre, une disposition n'est pas présente dans le protocole de convention alors qu'elle est cruciale pour le contrôle des données télécoms dans la convention collective de travail n° 81, à savoir celle qui concerne l'obligation d'information individuelle et collective préalable que l'employeur doit respecter lors de l'instauration du contrôle.

Les conditions d'individualisation des données télécoms (le lien entre les données et un travailleur) prévoit, tout comme la convention collective de travail n° 81, une procédure directe et indirecte.

Une procédure directe d'individualisation s'applique aux contrôles effectués pour lutter contre des comportements impropres, pour protéger les données et l'entreprise et garantir la sécurité du réseau.

L'individualisation directe est autorisée sans autre obligation supplémentaire. L'obligation d'information individuelle et collective préalable lors de l'instauration du contrôle suffit.

Une procédure indirecte d'individualisation s'applique aux contrôles effectués en vue de vérifier le respect es accords internes concernant l'utilisation du réseau (comme l'interdiction d'envoyer trop de courriers électroniques à des fins privées). Dans ce cas, l'employeur ne peut pas identifier, dans un premier temps, la personne responsable de l'irrégularité. Ce n'est qu'après rappel de la règle enfreinte aux travailleurs (procédure de la sonnette d'alarme) et constat de la même irrégularité que l'identification est possible. Avant que le travailleur identifié ne soit déclaré responsable, il doit être entendu afin de pouvoir se justifier. On peut se poser la question de savoir si cette mesure ne devrait pas aussi s'appliquer en cas de procédure directe d'individualisation.

Articles 18 et 19 du protocole de convention

Ces articles nécessitent peu de commentaires quant à leur contenu mais, au niveau rédactionnel, les observations suivantes peuvent être formulées.

Les articles 18 et 19 parlent de "données personnelles" puis de "données de nature personnel" puis encore de "données à caractère personnel". A l'article 18, on note une référence à la loi sur la protection de la vie privée alors que l'intitulé de cette loi est erroné. L'article 19 parle d'arrêtés d'exécution de la loi sur la protection de la vie privée alors qu'un seul arrêté a été pris en la matière, à savoir l'arrêté royal du 13 février 2001. Un rafraîchissement terminologique est donc recommandé.

L'article 19 du protocole de convention confirme le droit visé aux articles 10 et 12 de la loi sur la protection de la vie privée. C'est un avantage par rapport à la convention collective de travail n° 81 vu que ce droit est nommé de manière erronée dans le rapport précédant la convention collective de travail n° 81 et n'est pas mentionné dans le texte de cette convention collective de travail.

CONCLUSION

Cette analyse démontre que la Commission émet des réserves quant à la nécessité de la convention collective de travail en préparation.

Néanmoins, si la nécessité d'une telle convention collective de travail se présentait, la Commission entend rappeler que cette convention collective de travail doit prévoir la procédure que l'employeur doit respecter lors de d'information du contrôle, en matière d'information des travailleurs.