AVIS N° 21 / 2006 du 12 juillet 2006

N. Réf. : SA2 / A / 2006 / 017

OBJET : Avis relatif au code de déontologie concernant l'utilisation des moyens informatiques et le traitement électronique de données au sein du Service public fédéral Economie, PME, Classes moyennes et Energie.

La Commission de la protection de la vie privée ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, en particulier l'article 29 ;

Vu la demande d'avis introduite le 11 mai 2006 par le Ministre de l'Economie, des PME, des Classes moyennes et de l'Energie ;

Vu le rapport de Monsieur Mertens de Wilmars;

Emet, le 12 juillet 2006, l'avis suivant :

I. OBJET DE LA DEMANDE

Le Ministre de l'Economie, des PME, des Classes moyennes et de l'Energie demande à la Commission d'émettre un avis à propos du code de déontologie relatif à l'utilisation des moyens informatiques et au traitement électronique de données au sein du Service public fédéral Economie, PME, Classes moyennes et Energie (ci-après le « SPF Economie »).

II. DISCUSSION GENERALE

---

1. Le code de déontologie tend à fournir aux collaborateurs du SPF Economie « *des directives explicites quant à la façon dont ils doivent et peuvent se servir des moyens informatiques et des informations mis à leur disposition* » en vue de l'accomplissement de leur travail. Il s'agit par ailleurs, via ces directives, de « *sensibiliser tous les collaborateurs à la problématique importante de la sécurité et de la protection des systèmes et des données* » du SPF Economie.

2. Le code comprend notamment un catalogue de directives et de recommandations concrètes ayant trait à la propriété et à la gestion du matériel, à la protection des données, à l'identification des utilisateurs et à la politique en matière de mots de passe, à l'utilisation de la messagerie électronique et d'Internet, à la protection du lieu de travail, à la journalisation (« *logging* »), à « l'auditing » et aux sanctions – ainsi qu'un résumé de ces directives et recommandations.

3. La Commission souhaite souligner que l'on ne peut bien entendu qu'applaudir à l'initiative consistant à consigner dans un code les règles de conduite que doivent respecter les membres du personnel du SPF Economie si leur employeur met à leur disposition des équipements de communication numérique : en effet, conformément à l'article 9 de la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après la « LVP »), les membres du personnel en question doivent savoir ce qui est permis ou défendu en matière d'utilisation d'Internet et du courrier électronique sur le lieu de travail, et être au fait des restrictions et limites imposées dans le cadre de l'usage toléré, de même qu'ils doivent être informés de l'existence et des modalités d'un contrôle exercé à ce sujet par l'employeur.

4. La Commission souligne en outre qu'elle s'est déjà exprimée à diverses reprises au sujet du contrôle des communications électroniques sur le lieu de travail ou, pour le dire en d'autres termes, au sujet du contrôle exercé par l'employeur sur l'utilisation par son personnel de la messagerie électronique et d'Internet.[1]

5. Le « Groupe 29 », organe consultatif indépendant regroupant des représentants des autorités chargées de la protection des données au sein des divers Etats membres de l'UE, s'est lui aussi déjà penché sur cette problématique, dans son document de travail *concernant la surveillance des communications électroniques sur le lieu de travail* du 29 mai 2002.[2]

---

[1] Notamment dans l'avis de portée générale émis d'initiative le 3 avril 2000 relativement à *la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail* et ensuite, pour ne citer que ces exemples, dans l'avis d'initiative du 8 octobre 2001 *concernant la proposition de loi 2-891/1 du 29 août 2001 visant à réglementer l'utilisation des moyens de télécommunication sur le lieu de travail*, l'avis (émis suite à une plainte) du 27 février 2003 relatif au *contrôle par l'employeur des données de communication de l'un de ses employés*, l'avis du 18 décembre 2003 sur le *code de bonne conduite à l'intention des membres du personnel du Ministère de la Communauté flamande* et l'avis du 9 novembre 2005 *relatif à un projet d'arrêté du Gouvernement de la Communauté française relatif au code de bonne conduite des usagers des systèmes informatiques, du courrier électronique et d'Internet au sein des services du Gouvernement de la Communauté française, et des organismes d'intérêt public relevant du comité de secteur XVII.* Ces avis peuvent être consultés sur le site Web de la Commission : www.privacycommission.be.

[2] Cf. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_fr.pdf

III. DISCUSSION CONCRETE

----

6. Dans les lignes qui suivent, la Commission traitera uniquement des dispositions du code nécessitant à ses yeux certains commentaires. Pour ce faire, on respectera la table des matières du code telle qu'elle apparaît dans le résumé.

7. La Commission se focalisera principalement sur « l'auditing », c'est-à-dire sur le contrôle exercé par le SPF Economie, en sa qualité d'employeur, sur l'utilisation d'Internet et de la messagerie électronique par les membres de son personnel. De fait, des données à caractère personnel concernant ces derniers seront traitées à l'occasion de tels contrôles (surveillance électronique) et il y a donc lieu d'appliquer la LVP.

Préambule

8. Il ressort de l'introduction du code que chaque membre du personnel recevra un exemplaire de celui-ci et devra impérativement en accuser réception, via l'apposition de sa signature, pour avoir accès aux différents systèmes d'information du SPF Economie. Les agents pourront adresser à un service d'assistance (« *help-desk* ») leurs éventuelles questions et demandes d'éclaircissements.

9. A cet égard, la Commission fait remarquer qu'obtenir une signature pour réception n'équivaut pas à obtenir le consentement des membres du personnel, notamment en ce qui concerne le traitement de leurs données à caractère personnel dans le cadre de certaines mesures de contrôle décrites dans le code de déontologie. Toutefois, compte tenu du fait que la législation relative aux communications est applicable (cf. infra), un tel consentement est en principe requis.

10. A moins d'admettre qu'un accord des représentants des membres du personnel peut faire figure de consentement des intéressés eux-mêmes, un tel accord pourra au moins contribuer à une transparence accrue du contrôle envisagé, à un meilleur équilibre entre les droits des membres du personnel et de l'employeur et à la liberté du consentement du membre du personnel individuel.

11. Le cas échéant, le code sera revu et remanié. Dès lors, il faudra également demander à chaque agent une signature pour prise de connaissance et accord si des modifications y sont apportées. La Commission suggère que, lors de la révision du Code de déontologie, le demandeur y aborde des aspects non encore traités, tels que par exemple la nécessité des autorisations explicites préalables pour tout traitements sur des données à caractère personnel, la gestion des risques encourus par ces données, la préservation des preuves pour les infractions pouvant avoir un caractère judiciaire. Pour ce faire, il est possible de s'inspirer des mesures de références disponibles sur le site de la Commission (www.privacycommission.be , rubrique publications) ou des autres sources reconnues adressant de manière plus générale la sécurité de l'information.

Propriété et gestion du matériel

« *Tout le matériel et le logiciel que le SPF Economie met à la disposition de ses collaborateurs dans l'exercice de leur fonction, reste la propriété du SPF et ne peut être utilisé qu'à des fins professionnelles, c'est-à-dire dans le cadre des tâches attribuées au SPF Economie*. »

12. Cette disposition du code doit être modifiée, parce que formulée en des termes trop absolus. En effet, l'utilisation à des fins privées, par les membres du personnel, des moyens informatiques de l'employeur (par exemple l'utilisation du disque dur du PC, d'Internet et des fonctionnalités e-mail) n'est pas prohibée dans la suite du code. Par conséquent, il est non seulement préférable de nuancer en ce sens cette disposition en insérant « en principe » entre

les mots « peut » et « être », mais il vaut de surcroît mieux signaler explicitement dès ce stade qu'un certain usage privé est toléré.

Protection des données

« *Dans le cadre des tâches du SPF Economie, des informations confidentielles concernant les citoyens et les entreprises sont réunies et traitées. L'accès à de telles informations est strictement limité et il est interdit de transmettre, sans en avoir la permission, ces informations à des tiers, que ce soit à l'intérieur ou à l'extérieur du SPF Economie. En général, un collaborateur ne peut pas de diffuser des informations auxquelles il a obtenu accès dans l'exercice de sa fonction, à moins d'en avoir obtenu la permission du gestionnaire responsable de cette information ou de son propre chef hiérarchique. Ceci ne s'applique pas aux données que sont déjà rendues publiques via d'autres canaux.* »

13. La permission du « gestionnaire responsable de l'information » ou du supérieur hiérarchique de l'agent ne suffit pas. Pour être admissible, la publicité – et donc la communication à des tiers dont il est ici question – doit trouver son fondement légal dans le consentement de la personne concernée par les données ou être justifiée par une des nécessités impératives définies dans l'article 5, b) à f) inclus, de la LVP, ou, le cas échéant, dans le § 2 des articles 6, 7 et 8 de la LVP.

« *A l'exception des mails personnels dans les mailbox privés, toute information présente sur les systèmes informatiques du SPF Economie est la propriété du SPF. Les collaborateurs ne peuvent donc pas invoquer le droit à la vie privée pour les fichiers ou données stockés par le SPF. Les droits d'accès aux données sont uniquement attribués par les responsables désignés pour ces données qui suivent des procédures établies à cette fin*. »

14. Cette disposition est formulée de manière passablement absolue et laisse entendre qu'à l'exception de la restriction ayant trait aux courriels personnels enregistrés dans les boîtes aux lettres électroniques privées, le SPF Economie aurait par exemple inconditionnellement accès aux données stockées sur le PC d'un agent ou sur le serveur de messagerie (« e-mail server »). Il semble qu'il ne soit pas suffisamment tenu compte à ce propos des dispositions de la législation relative aux communications et du Code pénal applicables en la matière – dispositions qui seront abordées de manière plus détaillée ultérieurement, dans les rubriques « utilisation de l'e-mail », « utilisation de l'Internet » et « logging et auditing ». Ainsi, la législation précitée interdit par exemple à l'employeur de prendre connaissance du contenu des courriels entrant et sortant, ou d'ouvrir ceux se trouvant déjà sur le serveur. De même, l'employeur qui détiendrait un courriel entrant dans une boîte aux lettres électronique commune du SPF Economie et dont la ligne objet fait apparaître qu'il s'agit d'un message confidentiel destiné à un agent bien précis tomberait sous le coup de l'article 314 bis, §2, 2ème alinéa, du Code pénal.

15. La disposition semble même aller à l'encontre d'une des dispositions suivantes du code, selon laquelle : « *L'ICT ne prend pas de copies de sauvegarde des fichiers que les utilisateurs conservent sur les disques durs de leur PC. Dès lors ils ne peuvent sauvegarder sur ces disques que des fichiers personnels* (…) ».

16. Puisqu'il est uniquement permis d'enregistrer sur ces disques des fichiers destinés à un usage personnel, il convient d'admettre que l'employeur n'a pas le droit d'ouvrir de tels fichiers sans le consentement de l'intéressé et, par voie de conséquence, que la restriction formulée dans le code quant à l'accès aux courriels personnels enregistrés dans une boîte aux lettres électronique privée joue également pour les données à caractère personnel stockées sur le disque dur du PC.

Identification des utilisateurs et politique en matière de mots de passe

« *Les userids et les mots de passe sont strictement personnels et ne peuvent pas être transmis à des tiers ou conservés en un lieu où ils peuvent facilement être retrouvés. Les utilisateurs qui soupçonnent que d'autres personnes connaissent leur mot de passe doivent le modifier immédiatement. Chaque collaborateur est responsable de l'usage qui est fait des moyens informatiques au nom d'une identité (userid) qui lui est attribuée. Il est strictement défendu d'essayer, de quelque façon que ce soit, de découvrir les mots de passe d'autres collaborateurs ou de les utiliser si on les a découverts par hasard.* »

17. La disposition proprement dite ne suscite aucun commentaire de la part de la Commission.

18. Celle-ci souhaite toutefois faire remarquer, à titre subsidiaire, que l'utilisation d'une ouverture de session (« login ») et d'un mot de passe ne suffit pas pour toutes les applications. L'emploi de certaines applications et surtout l'accès via Internet à l'infrastructure du SPF Economie requièrent des moyens d'authentification plus « pointus », tels que le recours à une carte électronique avec certificat d'authentification utilisable moyennant l'introduction d'un « code PIN ». En d'autres termes, les moyens d'identification et d'authentification devraient être adaptés aux normes de sécurité établies en fonction de la nature de l'application et des canaux d'accès.

« *Il est strictement défendu d'essayer, de quelque façon que ce soit, de découvrir les mots de passe d'autres collaborateurs ou de les utiliser si on les a découverts par hasard.* »

19. La Commission souhaite qu'une disposition spécifique soit ajoutée à ce propos dans le code, à l'intention des administrateurs de système et de réseau, qui font en effet également partie du personnel du SPF Economie et qui peuvent/doivent accomplir les actes visés dans le cadre de l'exécution de leurs activités, à savoir « *vérifier le bon fonctionnement du réseau et* (…) *assurer la bonne exécution d'un service de communications électroniques* » (cf. article 125, § 1, 2°, de la loi du 13 juin 2005).

Utilisation de l'Internet

« *L'accès à l'Internet est offert comme outil dans l'exercice de la fonction. L'utilisation à des fins personnelles est uniquement autorisée dans une mesure limitée et à condition de respecter les règles de sécurité. L'utilisation* [dans un but] *personnel ne peut en aucun cas occasionner des problèmes pour l'utilisation professionnelle*. »

20. En cela, le code se conforme à ce que la Commission affirmait dans son avis du 3 avril 2000, par référence à la jurisprudence de la Cour européenne des Droits de l'Homme[3] : le lieu de travail étant le lieu le plus propice pour entretenir des contacts avec des collègues et même avec des personnes extérieures, les employeurs doivent faire preuve d'une certaine tolérance quant aux communications privées passées par les membres de leur personnel à l'aide de leurs moyens de communication.

21. Le code pourrait indiquer plus concrètement ce qu'il convient en l'occurrence de considérer comme raisonnable, par exemple en stipulant qu'Internet ne peut être utilisé à des fins privées que durant la pause.

« *L'ICT seul décide de quelle façon et par quelles voies les utilisateurs ont accès à l'Internet* (…) ».

22. Sur ce point, la Commission souhaite faire observer qu'en la matière, la décision ne peut revenir à l'ICT seul, puisqu'en définitive, celui-ci doit lui-même appliquer les instructions de la hiérarchie – même s'il a le cas échéant émis un avis préalable à ce propos.

[3] Avis d'initiative *relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail* émis par la Commission le 3 avril 2000.

« (…) *Entres autres l'accès aux types de sites web ou de services suivants est actuellement condamné : chat et instant messaging sites, web based mail services sites, réseaux file sharing, file transfer services,...* »

23. A cet égard, la Commission désire faire remarquer que certains membres du personnel pourraient être obligés, dans l'exercice de leurs activités professionnelles au sein du SPF Economie, d'avoir recours à des applications susceptibles de requérir des transferts de fichiers (« file transfer »). Dès lors, pour éviter tout malentendu à ce sujet, il y a lieu de compléter le texte de cette phrase comme suit : « *est actuellement condamné* **dans le cadre de l'utilisation à des fins privées** ».

Utilisation de l'e-mail

« *L'utilisation d'e-mail est en principe à la disposition de chaque collaborateur qui a accès au réseau. A la demande des responsables hiérarchiques, via l'Information Manager, cet accès peut être limité pour certains collaborateurs*.»

24. On veut très probablement dire par là que l'employeur peut restreindre l'accès pour certaines catégories de collaborateurs, par exemple celles qui n'ont pas véritablement besoin de cet équipement pour accomplir les prestations convenues. Toutefois, au sein d'une même catégorie, on peut difficilement refuser a priori un tel accès à certaines personnes et l'accorder à d'autres, à moins que ce ne soit en guise de sanction disciplinaire.

« *L'accès à l'e-mail est offert comme outil dans l'exercice de la fonction. L'utilisation à des fins personnelles est uniquement autorisée dans une mesure limitée et à condition de respecter les règles de sécurité, et sans entraver l'utilisation professionnelle.* »

25. Dans ce cas également, interdire toute utilisation à des fins privées de la messagerie électronique serait déraisonnable et hors de proportion avec l'apport que celle-ci peut représenter dans la vie quotidienne des travailleurs. [4]

26. Ici aussi, on pourrait indiquer plus concrètement dans le code ce qu'il y a en l'occurrence lieu de considérer comme raisonnable, par exemple en définissant une taille maximale pour les courriels envoyés ou reçus à titre privé.

« *Le SPF Economie respecte la confidentialité du courrier électronique personnel, sauf dans les cas où la loi abolit explicitement cette confidentialité ou la subordonne à d'autres considérations*. »

27. On ne précise pas de quelle loi il s'agit et quels sont les cas dans lesquels elle abolit explicitement cette confidentialité ou la subordonne à d'autres considérations.

28. Le code de déontologie vise sans doute l'article 125 de la loi du 13 juin 2005 *relative aux communications électroniques*, dans lequel sont énumérées les exceptions au principe de confidentialité des communications, un principe garanti par l'article 124 de cette même loi et les articles 259bis et 314bis du Code pénal. Selon la loi du 13 juin 2005, de telles exceptions sont notamment possibles à condition d'obtenir à cet effet le consentement de toutes les personnes directement ou indirectement concernées (article 124), lorsque la loi permet ou impose l'accomplissement des actes visés ou bien encore lorsque les actes visés sont accomplis « *dans le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de communications électroniques* » (article 125, § 1, 1° et 2°).

[4] Voir le document de travail du Groupe 29 cité plus haut, p.25.

Protection du lieu de travail

« (…) *Les PC Windows du SPF Economie disposent d'une possibilité d'autoverrouillage après une période déterminée (p.ex. 10 minutes) d'inactivité. Il est conseillé d'activer cette option*. »

29. A cet égard, la Commission fait observer qu'il serait préférable d'activer d'office cette fonctionnalité lors de l'installation du PC, et d'interdire simultanément à l'utilisateur de la désactiver par la suite.

30. Les (autres) dispositions du code déontologique reprises sous cette rubrique visent à concrétiser les exigences formulées à l'article 16, § 4, de la LVP : pour garantir la sécurité des données à caractère personnel des « clients » du SPF Economie, les agents de celui-ci doivent « *prendre les mesures techniques et organisationnelles requises pour protéger les données* [en question] *contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé de* [ces] *données à caractère personnel* ».

31. Les membres du personnel du responsable du traitement ont tout intérêt, chaque fois que cela est possible, à faire preuve de la même prévoyance et de la même vigilance en ce qui concerne leurs propres données à caractère personnel accessibles sur le lieu de travail (fiches d'évaluation ou de traitement, …) et à protéger convenablement celles-ci contre [les agissements non autorisés] de tiers, y compris au sein de l'institution.

Logging et auditing

« *Le SPF Economie enregistre des informations et des fichiers "log" concernant l'utilisation des services et des applications sur les différents systèmes informatiques et les serveurs centraux. Cette information n'est nullement destinée à contrôler les activités des collaborateurs individuels, mais ne sera en principe utilisée que pour vérifier le bon fonctionnement de l'infrastructure informatique et pour pouvoir réagir plus efficacement en cas de problèmes. Lorsque des problèmes ou des incidents sont constatés, le SPF Economie peut décider d'effectuer des loggings ou des contrôles plus ciblés. Les collaborateurs et leurs responsables éventuellement impliqués en seront informés préalablement. Tout collaborateur doit toutefois se rendre compte qu'on ne peut pas abuser du principe de la protection de la vie privée pour commettre impunément des actions illicites, et que la loi permet d'effectuer des contrôles individuels, même sans avertissement,* (…) *pour intervenir contre des actions manifestement illicites, pour lesquelles une réponse immédiate est nécessaire* [et] *pour protéger la sécurité et le bon fonctionnement du système de réseau IT*. »

32. Le code s'avère passablement laconique et même sommaire quant à ce point précis, alors qu'il s'agit à n'en pas douter de sa disposition la plus importante – du moins si on l'examine au regard des compétences de la Commission, et notamment du point de vue des garanties dont les travailleurs doivent avoir l'assurance de bénéficier quant à la protection de leur vie privée dans le cadre de pareil contrôle. En effet, on n'explique pas clairement comment le SPF Economie veillera concrètement au respect du code ou, pour le dire autrement, quelle(s) procédure(s) il appliquera afin d'offrir et de respecter dans les faits l'ensemble des garanties consignées - entres autres - dans la LVP et visant à protéger la vie privée des travailleurs lors du contrôle.

33. Quoique la disposition en elle-même ne nécessite aucun commentaire, la Commission profite de l'occasion pour rappeler un certain nombre de directives qu'il est à ses yeux utile et nécessaire de suivre en la matière.

34. Dans ce domaine, le SPF Economie pourrait s'inspirer de 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*, rendue obligatoire par l'arrêté royal du 12 juin 2002, qui traite en détail de la possibilité [et des modalités] d'un contrôle progressif et

conditionnel des communications électroniques envoyées ou reçues par le travailleur via le réseau de l'entreprise.

35. D'autre part, en tant qu'employeur, le SPF Economie peut difficilement fonder l'admissibilité du contrôle de l'utilisation d'Internet et de la messagerie électronique par ses agents sur le seul code de déontologie ici examiné.

36. Celui-ci peut être considéré comme une manière de fournir au personnel l'information préalable exigée à l'article 9 de la LVP, mais pas comme un motif d'admissibilité du contrôle en tant que tel. En effet, pareil contrôle implique une atteinte au secret des communications, qui est une manifestation de la dimension communicationnelle du droit à la vie privée et est protégé par la législation sur les communications – laquelle joue également dans les relations de travail. En vertu de cette législation, une interdiction de principe pèse aussi bien sur le contrôle du contenu des communications que sur celui des données de trafic se rapportant à celles-ci, à moins d'avoir obtenu au préalable le consentement des personnes concernées par les communications. Un nombre limité d'exceptions légales est certes prévu, mais il faudra les interpréter de manière restrictive. Tout contrôle pour la justification duquel une de ces causes exclusives de peine ne peut être invoquée de manière suffisamment probante est interdit sous peine d'encourir les sanctions pénales prévues par la législation relative aux communications.

37. Les dispositions de l'article 124 de la loi, déjà citée, du 13 juin 2005 et les articles 259bis et 314bis du Code pénal ne sont pas applicables « *lorsque les actes visés sont accomplis dans le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de communications électroniques* » (article 125, §1, 2°, de la loi du 13 juin 2005).

38. Il est toutefois douteux que cette disposition puisse être utilisée par un employeur souhaitant contrôler les télécommunications de ses salariés. Ceci ressortait déjà des travaux préparatoires de l'ancienne loi du 21 mars 1991 *portant réforme de certaines entreprises publiques économiques*.

39. La Commission rappelle également avoir émis la considération suivante dans son avis du 9 novembre 2005 : « *En ce qui concerne la collecte de données de communication, et notamment d'éventuels loggings, la Commission rappelle par ailleurs que le principe de confidentialité des données de télécommunication s'applique sans préjudice de la nécessaire adoption de mesures de sécurité techniques et organisationnelles telles que prévues à l'article 16 de la loi, destinées à sécuriser l'accès aux réseaux et à assurer de façon globale la protection des données à caractère personnel. L'enregistrement de loggings dans cette perspective est admissible et même souhaitable, mais il doit être effectué dans une perspective de protection des données, sans détournement de finalité et réutilisation à des fins de contrôle permanent des employés*. »

40. La Commission a admis, eu égard aux responsabilités et obligations spécifiques incombant à l'employeur en vertu de la loi du 4 août 1996 *relative au bien-être des travailleurs lors de l'exécution de leur travail*, qu'il lui était par exemple permis, si le contenu d'un courriel – consulté avec l'autorisation de son destinataire – pouvait être assimilé à du harcèlement moral ou sexuel, ou à une autre forme de comportement agressif, d'utiliser les données journalisées pour retrouver le poste de travail à partir duquel le message en question avait été envoyé (cf. avis du 18 décembre 2003).

41. La Commission attire l'attention des auteurs du code sur quelques éléments susceptibles de les aider à trouver le juste équilibre entre la protection de la vie privée des membres du personnel et la légitimité d'un certain contrôle par l'employeur de l'utilisation des outils de travail – bien que la plupart des éléments en question figurent déjà dans l'avis de portée générale émis par la Commission en [avril] 2000.

42. La surveillance électronique des travailleurs ne peut pas être assimilée sans plus à une forme « moderne » d'exercice de l'autorité. La Commission considérait déjà ce qui suit dans son avis du [3 avril] 2000 : « *La relation de travail qui unit employeur et employé est par ailleurs caractérisée par un rapport de force déséquilibré. On ajoute que les outils de contrôle qui s'offrent aujourd'hui à l'employeur présentent des possibilités techniques particulièrement intrusives par rapport aux moyens disponibles antérieurement*. ». De son côté, le Groupe 29 faisait observer « [qu']*avec l'avènement des technologies de l'information, il* [était] *vital que les salariés bénéficient des mêmes droits, qu'ils travaillent en ligne ou hors ligne* » et que « [l'employeur] *devrait envisager sérieusement des méthodes traditionnelles de supervision, impliquant une intrusion moindre dans la vie privée des salariés, et, le cas échéant, les mettre en oeuvre avant de s'engager dans une forme quelconque de surveillance des communications électroniques* ».[5]

43. Considérés en eux-mêmes, le rapport d'autorité et le fait d'être propriétaire des équipements de communication ne constituent pas une base légale suffisante pour porter atteinte au secret des communications, qui est une des facettes du droit fondamental au respect de la vie privée.

44. Le Groupe 29 a considéré, exactement comme la Commission l'avait fait dans son avis du [3 avril] 2000, que : « *Dans la mesure du possible, la prévention devrait l'emporter sur la détection. En d'autres termes, il est davantage dans l'intérêt de l'employeur de prévenir l'utilisation abusive de l'Internet par des moyens techniques plutôt que de consacrer des ressources à sa détection. Dans la limite de ce qui est raisonnablement possible, la politique de l'entreprise concernant l'Intemet devrait s'appuyer sur des outils techniques visant à limiter l'accès plutôt que sur des dispositifs de contrôle des comportements, par exemple par des systèmes verrouillant l'accès â certains sites ou générant des avertissements automatiques*. »[6]

45. A supposer qu'un contrôle s'avère néanmoins nécessaire, on peut ensuite renvoyer à l'approche par paliers telle qu'elle ressort de l'avis émis par la Commission le 3 avril 2000 et, pour ne citer que cet exemple, de la CCT n° 81 évoquée plus haut.

Dans une première phase, seule la collecte de données globales est autorisée, sans identification immédiate des personnes concernées par les flux de données.

La seconde phase du contrôle, à savoir l'individualisation des données de télécommunications visées – en d'autres termes leur mise en relation avec un membre du personnel déterminé – ne pourra intervenir qu'après qu'un contrôle statistique de l'utilisation de l'infrastructure numérique de l'employeur aura débouché sur la constatation d'anomalies telles qu'une durée de consultation d'Internet anormalement longue, la présence d'adresses de sites suspects, la fréquence élevée, le grand nombre ou la taille des courriels, le type de pièce jointe à ceux-ci, … Dans la CCT, une distinction supplémentaire est faite entre « l'individualisation directe » et « l'individualisation indirecte ». La procédure directe est applicable dans le cadre du contrôle visant à lutter contre les comportements illicites et à protéger les intérêts de l'entreprise ainsi que la sécurité du réseau. La procédure indirecte, qui concerne le contrôle exécuté en vue de veiller à l'application des accords conclus au sein de l'entreprise relativement à l'utilisation du réseau, n'est autorisée que moyennant le respect d'une phase préalable d'information destinée à avertir explicitement et de manière compréhensible les travailleurs de l'existence d'une anomalie et du fait qu'il sera procédé à l'individualisation des données de communication électroniques si une anomalie de même nature est à nouveau constatée.

L'accomplissement des finalités en vue desquelles le contrôle a été institué – notamment combattre l'usage abusif des moyens informatiques – ne requiert en principe pas, en particulier en ce qui concerne le contrôle de l'utilisation excessive à des fins privées, de prendre connaissance du contenu même des courriers électroniques / sites Web visités : la liste des courriels envoyés et/ou reçus ou des sites Web consultés durant une période déterminée contiendra théoriquement assez d'éléments pour dissiper les préoccupations de l'employeur à ce

[5] Voir le document de travail du Groupe 29 déjà cité, pp. 6 et 14.
[6] Voir le document de travail du Groupe 29 déjà cité, p.25.

sujet – tout comme une facture de téléphone pourrait par exemple faire apparaître des montants anormalement élevés.

46. Le « Groupe 29 » a averti que : « *Dans leur analyse de l'utilisation de l'Internet par les salariés, les employeurs devraient éviter de tirer des conclusions hâtives, étant donné qu'il est facile de se retrouver involontairement sur certains sites du fait de réponses inattendues de moteurs de recherche, de liens hypertextuels ambigus, de bandeaux publicitaires trompeurs ou de fausses manoeuvres. Dans tous les cas, le salarié en cause doit se voir présenter tous les faits qui lui sont reprochés et disposer de tous les moyens nécessaires pour contester l'utilisation abusive alléguée par l'employeur*. »[7]

47. Pour autant que cela soit possible, l'employeur devra agir avec davantage encore de circonspection si le contrôle exercé porte sur des courriels entrants, vu que le travailleur n'en est pas l'auteur et qu'il ne s'attendait très probablement même pas à recevoir certains d'entre eux (exception faite des contrôles effectués à l'aide de moyens techniques visant par exemple à bloquer les messages d'une taille telle qu'ils sont susceptibles de provoquer un engorgement du réseau). En outre, il ne faut pas perdre de vue que les correspondants des usagers de la messagerie électronique peuvent eux aussi se prévaloir de droits en vertu de la LVP et de la législation relative aux communications.

48. La volonté des employeurs de mettre en œuvre un contrôle semble principalement motivée par le souci de lutter contre la tendance à consacrer une part excessive de son temps de travail à la navigation sur le Web à des fins privées, cette pratique entraînant une diminution correspondante de la productivité. A cela, la Commission réplique que l'employeur doit être en mesure, pour contrôler une éventuelle baisse du rendement de certains travailleurs, de recourir à d'autres méthodes que celle consistant à placer le personnel sous la surveillance constante d'un « croque-mitaine électronique ».[8]

49. Ainsi que cela a été dit auparavant, le code de déontologie, s'il ne peut pas être considéré en soi comme une cause de justification de la surveillance électronique, peut en revanche constituer une manière d'assurer la transparence requise, en confirmant clairement par écrit et en portant à la connaissance du personnel l'existence et les modalités d'un contrôle exercé par l'employeur quant à l'utilisation d'Internet et de la messagerie électronique.

50. Cependant, à y regarder de plus près, les éléments d'information contenus dans le code s'avèrent encore insuffisants. On peut se référer à ce propos à ce que la Commission indiquait dans son avis du [3 avril] 2000 :

« *Le dialogue entre employeur et employés devra permettre d'établir de façon suffisamment détaillée, conformément à l'article 9 de la loi du 8 décembre 1992, les différentes caractéristiques de la politique de contrôle de l'employeur. Celles-ci devront notamment viser :*

- *les modalités d'utilisation du courrier électronique et de l'Internet qui sont permises, tolérées ou interdites ;*
- *les finalités et modalités du contrôle de cette utilisation (nature des données collectées, étendue et circonstances des contrôles, personnes ou catégories de personnes sujettes aux procédures de contrôle ;*
- *l'existence d'un stockage des données de télécommunication et la durée de ce stockage, par exemple sur un serveur central, dans le cadre de la gestion technique du réseau, et les éventuels systèmes de cryptage existants ;*
- *les décisions pouvant être prises par l'employeur à l'endroit de l'employé sur la base du traitement des données collectées à l'occasion d'un contrôle ;*
- *le droit d'accès de l'employé aux données à caractère personnel le concernant.* »

[7] Ibidem, p.25.
[8] Voir en ce sens : Tribunal du travail de Bruxelles, 2 mai 2002.

51. Le code de déontologie du SPF Economie ne fait par exemple jamais mention des droits dont les membres du personnel peuvent se prévaloir en vertu des articles 10 à 12 de la LVP, à savoir le droit d'accès aux données à caractère personnel les concernant qui ont fait l'objet d'un enregistrement, le droit de faire rectifier les données inexactes qui les concernent et le droit d'obtenir la suppression des données qui, compte tenu des finalités du traitement, sont inexactes, ou dont l'enregistrement, la communication ou la conservation sont interdits par la loi, ou qui ont été conservées au-delà du délai raisonnable. La Commission signale que lors de la collecte de données pouvant entraîner de lourdes conséquences pour la personne concernée (par ex. des sanctions disciplinaires), il est essentiel, afin de garantir un traitement loyal à l'égard de l'intéressé, d'attirer son attention sur les droits qui lui sont reconnus en matière d'accès et de rectification. Les modalités d'exercice des droits visés aux articles 10 et 12 de la LVP sont précisées dans les articles 32 et 33 de l'arrêté royal du 13 février 2001 *portant exécution de la loi du 8 décembre 1992*.[9] La Commission souligne à ce propos que le requérant doit impérativement apporter la preuve de son identité - ceci afin d'éviter que quelqu'un ne puisse obtenir la communication, la rectification ou la suppression de données concernant une autre personne. La Commission estime que ces informations complémentaires sont susceptibles d'accroître la transparence des traitements prévus.

52. De plus, il n'est pas permis de prendre des décisions à l'encontre d'un employé sur la seule base du traitement automatisé de ses données à caractère personnel. Les données recueillies au cours de la surveillance électronique ne peuvent pas constituer les seuls critères d'appréciation des prestations d'un employé. Sur ce point, il peut être fait référence à la CCT n° 81, en vertu de laquelle l'employé tenu pour responsable d'une utilisation anormale des moyens de communication électroniques en réseau, suite à l'application de la procédure d'individualisation, sera « *invité à un entretien préalablement à l'adoption de toute décision ou évaluation susceptible de l'affecter individuellement* ». Cette procédure contradictoire permettra au travailleur « *de s'expliquer sur l'utilisation faite des moyens de communication électroniques en réseau mis à sa disposition* ».

Sanctions

53. La représentation du personnel est appelée à jouer un rôle non négligeable dans le cadre de la mise en œuvre de systèmes de surveillance électronique sur le lieu de travail.

54. Le conseil d'entreprise a pour mission d'émettre des avis et « *de formuler toutes suggestions ou objections sur toutes mesures qui pourraient modifier l'organisation du travail, les conditions de travail et le rendement de l'entreprise* » (article 15 de la loi du 20 septembre 1948 *portant organisation de l'économie*). La surveillance électronique a de toute évidence des implications quant à la politique de l'employeur. Dans le secteur de la fonction publique, les compétences du conseil d'entreprise sont exercées par les comités de négociation ou de concertation prévus par la loi du 19 décembre 1974 *organisant les relations entre les autorités publiques et les syndicats des agents relevant de ces autorités*. Dans le code, rien ne laisse transparaître que cette procédure d'information et de consultation collective aurait été respectée.

---

[9] « *Art. 32. Toute personne, justifiant de son identité, a le droit d'obtenir, dans les conditions prévues par la loi, communication de l'information visée à l'article 10 de la loi, en adressant une demande signée et datée qu'elle remet sur place ou qu'elle envoie par la poste, ou par tout moyen de télécommunication :*

** soit au responsable du traitement ou à son représentant en Belgique, ou à l'un de ses mandataires ou préposés;*

** soit au sous-traitant du traitement des données à caractère personnel qui la communique, le cas échéant, à une des personnes mentionnées ci-dessus.*

En cas de remise de la demande sur place, la personne, qui la reçoit, délivre immédiatement un accusé de réception daté et signé à l'auteur de la demande.

Art. 33. Les demandes de rectification, de suppression ou d'interdiction des données à caractère personnel, ou la communication d'une opposition, fondée sur l'article 12 de la loi, sont introduites selon la même procédure et auprès des mêmes personnes que celles mentionnées à l'article 32 du présent arrêté. »

55. Les mesures de contrôle et les sanctions y liées prévues dans le cadre de la surveillance électronique doivent être reprises dans le règlement de travail. En ce qui concerne l'établissement et la modification de celui-ci, la loi du 8 avril 1965 *instituant les règlements de travail* prévoit une procédure spécifique, qui est également applicable au SPF Economie (article 2 de ladite loi) et qui va plus loin que la simple information et consultation (des représentants) du personnel : en l'espèce, il s'agit même d'une procédure de cogestion (article 11 de la loi précitée). Il ne ressort à aucun moment du code que ces exigences auraient été satisfaites.

56. En outre, il a déjà été mentionné ci-dessus qu'un accord des représentants des membres du personnel concernant le contrôle électronique, s'il ne peut faire office de consentement des intéressés eux-mêmes, peut au moins contribuer à la liberté du consentement des membres du personnel individuels

« *En cas d'infractions graves ou répétées à ce code, l'ICT se réserve le droit de prendre des actions préventives pour protéger l'infrastructure informatique* (…) »

57. A cet égard, la Commission souhaite faire remarquer que le droit d'entreprendre de telles actions ne peut être l'apanage de l'ICT, puisqu'en définitive, celui-ci doit lui-même se conformer aux instructions données à ce sujet par la hiérarchie – même s'il a le cas échéant émis un avis préalable à ce propos.

PAR CES MOTIFS,

La Commission émet un avis favorable au sujet du code de déontologie qui lui a été soumis par le SPF Economie, à condition qu'il soit tenu compte des remarques formulées plus haut.

L'administrateur,	Le président,
(sé) Jo BARET	(sé) Michel PARISSE