

**AVIS N° 10 / 2000 du 3 avril 2000.**

*N. Réf. : 10 / IP / 2000 / 017*

**OBJET : Avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail.**

---

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 le rapport du Président;

Emet d'initiative, le 3 avril 2000, l'avis suivant:

Le présent avis fait suite à l'augmentation constante du nombre de questions posées à la Commission relativement à la surveillance par l'employeur de l'utilisation du courrier électronique et d'Internet par les employés.

L'origine des questions posées à la Commission est particulièrement large : celles-ci sont formulées par des personnes en leur la qualité d'employeur ou d'employé, appartenant au secteur public comme au secteur privé.

## I. TEXTES JURIDIQUES APPLICABLES

L'étendue et les conditions du contrôle que la loi permet à l'employeur d'effectuer doivent se baser sur plusieurs textes:

### 1. Textes juridiques de base

#### - l'article 22 de la Constitution :

*« Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit. »*

#### - l'article 8 de la Convention européenne de Sauvegarde des droits de l'homme et des libertés fondamentales, Rome, 4 novembre 1950 :

*« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.  
2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »*

#### - la Recommandation n° R (89) 2 du Comité des Ministres du Conseil de l'Europe aux Etats membres sur la protection des données à caractère personnel utilisées a des fins d'emploi, adoptée par le Comité des Ministres le 18 janvier 1989 :

*« 3. Information et consultation des employés  
3.1. Conformément aux législations et pratiques nationales et, le cas échéant, aux conventions collectives, les employeurs devraient informer ou consulter leurs employés ou les représentants de ceux-ci préalablement à l'introduction ou à la modification de systèmes automatisés pour la collecte et l'utilisation de données à caractère personnel concernant les employés.  
Ce principe s'applique également à l'introduction ou à la modification de procédés techniques destinés à contrôler les mouvements ou la productivité des employés.  
3.2. L'accord des employés ou de leurs représentants devrait être recherché avant l'introduction ou la modification de tels systèmes ou procédés lorsque la procédure de consultation mentionnée au paragraphe 3.1 révèle une possibilité d'atteinte au droit au respect de la vie privée et de la dignité humaine des employés, à moins que d'autres garanties appropriées ne soient prévues par la législation ou la pratique nationales. »<sup>1</sup>*

---

<sup>1</sup> Il n'est pas fait mention dans cet avis de l'article 314bis du Code pénal. Celui-ci prévoit une interdiction pour toute personne de prendre connaissance, pendant leur transmission, du contenu des télécommunications à laquelle elle ne prend pas part. La consultation par un employeur de données relatives à des courriers électroniques qui sont stockées sur le disque dur de l'employé ou sur un fichier géré par la personne chargée du contrôle est souvent considérée comme

## 2. Textes normatifs spécifiques

- **Les articles 4 et 5 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<sup>2</sup>** précisent les conditions que doit respecter tout maître de fichier lors de la collecte et du traitement de telles données;

*« Art. 4. § 1er . Les données à caractère personnel doivent être :*

*1 ° traitées loyalement et licitement;*

*2 ° collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables. (...);*

*3 ° adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement; (...)*

*5 ° conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement. (...)*

*Art. 5. Le traitement de données à caractère personnel ne peut être effectué que dans l'un des cas suivants :*

*a) lorsque la personne concernée a indubitablement donné son consentement;*

*b) lorsqu'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci; (...)*

*f) lorsqu'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le tiers auquel les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui peut prétendre à une protection au titre de la présente loi.*

*(...) »*

- **L'article 109 ter D de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques**, qui régit les conditions dans lesquelles un tiers peut prendre connaissance de données transmises par voie de télécommunications.

*« Sous réserve de l'autorisation de toutes les autres personnes directement ou indirectement concernées par l'information, l'identification ou les données visées ci-après, il est interdit à quiconque, qu'il agisse personnellement ou par l'entremise d'un tiers :*

*1° de prendre frauduleusement connaissance de l'existence de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature transmis par voie de télécommunications, en provenance d'autres personnes et destinées à celles-ci [modifié par l'article 13, § 2, 1° de la loi du 30 juin 1994] ;*

*2° de transformer ou de supprimer frauduleusement par n'importe quel procédé technique l'information visée au 1° ou d'identifier les autres personnes ;*

*3° de prendre connaissance intentionnellement de données en matière de télécommunications, relatives à une autre personne ;*

*4° de révéler ou de faire usage quelconque de l'information, de l'identification et des données obtenues intentionnellement ou non, et visées aux 1°, 2°, 3°, de les modifier ou de les annuler. »*

---

étant effectuée après la transmission de la communication, et ne tombe donc pas dans cette hypothèse sous le coup de l'article 314bis.

<sup>2</sup> Ci-après, la loi du 8 décembre 1992 telle que modifiée par la loi du 11 décembre 1998, M.B., 3février 1999.

- **L'article 6 de la loi du 8 avril 1965 instituant les règlements de travail**<sup>3</sup>:

*« Le règlement de travail doit indiquer (...):*

*5° les droits et obligations du personnel de surveillance ».*

On souligne que c'est conformément à cet article qu'a été adoptée la Convention collective de travail n° 68 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail, rendue obligatoire par arrêté royal le 20 septembre 1998<sup>4</sup>.

- **L'article 2, § 1<sup>er</sup> de la Convention collective de travail n° 39 du 13 décembre 1983 concernant l'information et la concertation sur les conséquences sociales de l'introduction des nouvelles technologies :**

*« Lorsque l'employeur a décidé d'un investissement dans une nouvelle technologie et lorsque celui-ci a des conséquences collectives importantes en ce qui concerne l'emploi, l'organisation du travail ou les conditions de travail, il est tenu, au plus tard trois mois avant l'implantation de la nouvelle technologie, d'une part de fournir une information écrite sur la nature de la nouvelle technologie, sur les facteurs qui justifient son introduction ainsi que sur la nature des conséquences sociales qu'elle entraîne et d'autre part, de procéder à une concertation avec les représentants des travailleurs sur les conséquences sociales de l'introduction de la nouvelle technologie. »*

## **II. APPLICATION DES DISPOSITIONS JURIDIQUES DANS LE CADRE DE LA RELATION DE TRAVAIL**

Le contexte des conditions de travail présente des caractéristiques spécifiques. Celles-ci ont été décrites par la Cour européenne des droits de l'Homme. Ainsi dans l'affaire Niemitz c. Allemagne: *« Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables.*

*Il paraît, en outre, n'y avoir aucune raison de principe de considérer cette manière de comprendre la notion de "vie privée" comme excluant les activités professionnelles ou commerciales: après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur. Un fait, souligné par la Commission, le confirme: dans les occupations de quelqu'un, on ne peut pas toujours démêler ce qui relève du domaine professionnel de ce qui en sort. »*<sup>5</sup>

La relation qui unit employeur et employé présente à cet égard un caractère partiel : l'autorité de l'employeur ne peut s'exercer sur la totalité des aspects de la personnalité et des activités de l'employé.

---

<sup>3</sup> Cette loi règle l'obligation de négociation avec les employés dans le secteur privé.

<sup>4</sup> La jurisprudence a consacré cette exigence d'un dialogue avec les représentants des employés dans l'hypothèse de prise de mesures visant à contrôler le rendement de ces derniers : *« De ondernemingsraad heeft o.a. als taak advies uit te brengen en alle suggesties en bezwaren te kennen te geven over alle maatregelen die de arbeidsorganisatie, de arbeidsvoorwaarden en het rendement van de onderneming zouden kunnen wijzigen (art. 15, a Wet 20 September 1948 houdende organisatie van het bedrijfsleven) (...). »* Arbeidsrechtbank Brugge, Tweede Kamer, Openbare terechtzitting van 4 September 1998.

<sup>5</sup> 23 novembre 1992, Série A n°251/B, par. 30 .

Voyez également Affaire Halford c. Royaume-Uni du 27 mai 1997, Recueil 1997-III, par. 44. *« Pour la Cour, il ressort clairement de sa jurisprudence que les appels téléphoniques émanant de locaux professionnels, tout comme ceux provenant du domicile, peuvent se trouver compris dans les notions de "vie privée" et de "correspondance" visées à l'article 8 par. 1 (art. 8-1) (voir l'arrêt Klass et autres c. Allemagne du 6 septembre 1978, série A n° 28, p. 21, par. 41., l'arrêt Malone c. Royaume-Uni du 2 août 1984, série A n° 82, p. 30, par. 64, l'arrêt Huvig c. France du 24 avril 1990, série A n° 176-B, p. 4. »*

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.

Les instruments de négociation et de concertation entre employeurs et employés élaborés dans le cadre du droit social ont précisément pour objectif de tempérer les conséquences de cette relation inégalitaire.

Il convient de souligner que la détermination de ce qui est admissible ou non sur le lieu de travail peut dépendre de différents facteurs, notamment du contexte de travail, de la nature des responsabilités de l'employeur et de l'employé et de la nature du travail à proprement parler.

C'est ainsi au cas par cas et au sein de l'entreprise ou du service concerné que cette question devra être abordée, afin que soit trouvé, conjointement par l'employeur et les employés ou leurs représentants, un équilibre entre la légitimité d'un certain contrôle par l'employeur de l'utilisation des outils de travail d'une part, et la protection de la vie privée de l'employé d'autre part. Les engagements pris sur cette base devront dès lors être respectés par les différentes parties.

Afin de respecter les droits des deux parties en cause, cet équilibre devrait être atteint dans le respect des dispositions juridiques susmentionnées (notamment des conditions strictes qui sont posées par l'article 109 *ter* D de la loi du 21 mars 1991). Les principes suivants explicitent les modalités d'application de ces dispositions juridiques.

## **1. Transparence**

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<sup>6</sup>) ;
- 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.

### a. En ce qui concerne le secteur privé

La transparence des méthodes de contrôle envisagées devra passer par une concertation avec les employés et leurs représentants au sein des organes de dialogue de l'entreprise ou des services concernés, ainsi que le prévoient par exemple la loi du 8 avril 1965 instituant les règlements de travail et la Recommandation n° R (89) 2 du Conseil de l'Europe sur la protection des données à caractère personnel utilisées à des fins d'emploi.

---

<sup>6</sup> Le détail de l'information visée à l'alinéa 2 doit être communiqué à l'ensemble des employés, de façon générale et préalable à la mise en place du système de contrôle, afin que ceux-ci sachent précisément sur quoi porteront les contrôles. Ceci n'implique pas, par exemple, que la date précise d'un contrôle soit préalablement communiquée à la personne concernée, ce qui aurait pour effet de priver ledit contrôle de toute efficacité.

## b. En ce qui concerne le secteur public

Si les dispositions de la Recommandation R (89) du Conseil s'appliquent indifféremment au secteur public et au secteur privé, les modalités concrètes du dialogue n'ont pas été reprises dans un texte normatif tel que celui qui prévoit, pour le secteur privé, la discussion des principes de surveillance dans le cadre du règlement de travail.

C'est donc un instrument équivalent au sein de la fonction publique qui devra être utilisé dans le cadre de ce dialogue.

La loi du 19 décembre 1974 organisant les relations entre les autorités publiques et les syndicats des agents relevant de ces autorités, et en particulier l'article 2 de celle-ci, prévoit à cet égard les procédures de concertation ou de négociation avec les organisations syndicales concernées. Ces procédures peuvent varier selon les services concernés<sup>7</sup>.

A titre d'exemple, certains ministères soumettent au comité de concertation les mesures prises en matière de vidéo-surveillance dans les locaux de travail.

## **2. Proportionnalité et nécessité**

Tout contrôle devrait être ponctuel et justifié par des indices laissant suspecter une utilisation abusive des outils de travail. Un contrôle général et *a priori* de l'ensemble des données de télécommunications de même qu'un enregistrement systématique de l'ensemble de ces données apparaît disproportionné par rapport à l'objectif poursuivi.

Il est en outre peu conforme à la dignité humaine – et pas nécessairement productif – de faire travailler des employés sous une surveillance constante<sup>8</sup>.

La Commission rappelle que, de même que pour toute autre collecte de données, les données de télécommunications visées ne peuvent être collectées que pour la finalité de contrôle précisée, et ne peuvent être utilisées à des fins différentes.

En ce qui concerne plus précisément la nature des données sujettes à contrôle, seules les données nécessaires à ce dernier peuvent être collectées. Dans la majeure partie des cas, la prise de connaissance du contenu des informations n'est pas nécessaire à l'exercice du contrôle.

On opère ici une distinction entre le contrôle du courrier électronique envoyé ou reçu par les employés, et le contrôle des données de trafic relatives à la consultation d'Internet.

**a. En ce qui concerne le courrier électronique**, la Commission considère que la prise de connaissance du contenu des courriers électroniques est excessive, et contraire aux dispositions légales mentionnées *supra*, de la même façon que le serait l'écoute et/ou l'enregistrement des communications téléphoniques de l'employé.

Il existe différentes solutions qui permettent de cibler les courriers suspects, tels que les logiciels qui identifient l'expédition de courriers électroniques en chaîne ou qui isolent et/ou bloquent ceux dont la taille est excessive et qui peuvent provoquer un engorgement ou un ralentissement du réseau. Ceci est le cas en particulier lorsque des images ou des fichiers exécutables sont envoyés ou reçus en annexe aux messages.

---

<sup>7</sup> Il existe ainsi plusieurs types de comités de négociation - A, B, C, D, E, selon la nature du service public : national, local, sectoriel, provincial, etc., et certains services ne sont pas soumis au statut syndical de la loi de 1974 : tel est le cas par exemple du personnel des forces armées, des agents des services extérieurs de la sûreté de l'Etat, des magistrats et des greffiers de l'ordre judiciaire (article 1<sup>er</sup>, §§ 2 et 3 de la loi du 19 décembre 1974).

<sup>8</sup> Ce principe a d'ailleurs été explicitement repris dans la convention collective de travail n° 68 conclue le 16 juin 1998 au sein du Conseil national du Travail, relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail, et rendue obligatoire par l'arrêté royal du 20 septembre 1998, M.B., 2 février 1998.

C'est ainsi sur la base d'une liste de courriers et non de leur contenu - comme sur la base d'une facture de téléphone laissant apparaître des montants anormalement élevés - que l'absence de respect des règles posées par l'employeur pourra être décelée.

La Commission ajoute que l'absence de respect desdites règles devrait être prise en considération par l'employeur au regard des courriers *envoyés* par l'employé ; elle émet toutefois des réserves quant à l'exercice du contrôle au regard des courriers *entrants*, l'employé n'étant pas l'auteur de ces derniers (à l'exception des contrôles par le biais de moyens techniques, visant par exemple le blocage des courriers entrants de grande taille qui constituent un risque d'engorgement du réseau).

**b. En ce qui concerne le contrôle des sites Internet** consultés par l'employé, les données concernées sont des données de trafic (adresse des sites consultés). Ces données constituent des données à caractère personnel à partir du moment où l'employeur est en mesure d'établir un lien entre les adresses des sites consultés et un employé particulier.

Dans cette optique, la Commission est d'avis que le contrôle doit se fonder sur des données objectives restreintes et non sur une prise de connaissance préalable et systématique du contenu de toutes les données de trafic concernant chaque employé.

L'employeur pourra à cet effet disposer par exemple d'une liste d'adresses de sites consultés de façon globale sur une certaine période, sans que soient identifiés dans un premier temps les auteurs des consultations. Il pourra sur cette base repérer une durée anormalement élevée de consultation d'Internet ou la mention d'adresses de sites suspects et prendre les mesures de contrôle appropriées. La détection de la consultation de certains sites pourrait également être effectuée de façon automatique grâce à un logiciel spécifique sur la base de mots-clés déterminés.

### **3. Durée de conservation et conditions de stockage des données**

En vertu de l'article 4 de la loi du 8 décembre 1992, les données collectées à l'occasion ou en vue des contrôles ne doivent pas être conservées plus longtemps que nécessaire à l'exercice de celui-ci.

Le stockage des données pendant une durée déterminée, par exemple sur un serveur de réseau, doit être effectué en conformité avec les dispositions de l'article 16 de la loi du 8 décembre 1992 concernant la confidentialité et la sécurité des traitements.

En particulier, l'accès à ces données ne peut être autorisé que par l'employeur et dans les conditions et pour les finalités strictes prévues pour l'exercice d'un contrôle.

Il s'agit en effet d'éviter que des données qui peuvent s'avérer confidentielles ne puissent être interceptées par des personnes extérieures à la communication<sup>9</sup> (par exemple échange de courriers électroniques entre membres d'un syndicat, documents préparatoires à une prise de position officielle d'une institution ou d'une entreprise, ou encore échange de vues confidentiel entre différentes entreprises ou autorités).

Le secrétaire

Le président

(sé)B. HAVELANGE

(sé)P. THOMAS

---

<sup>9</sup> C'est en ce sens que l'employé devrait, par exemple, être informé des possibilités de cryptage disponibles.