# La surveillance des communications électroniques des employés

Boulanger, Marie-Helene; Louveaux, Sophie; Lacoste, Anne-Christine

*Published in:*
Revue Ubiquité - Droit des Technologies de l'Information

*Publication date:*
2003

*Document Version*
le PDF de l'éditeur

# La surveillance des communications électroniques des employés

*Marie-Hélène Boulanger,*
*Anne-Christine Lacoste et Sophie Louveaux*[1]

## 1 *Introduction*

La question de la surveillance des communications électroniques des employés est un sujet délicat. Ces dernières années, elle a acquis un retentissement certain du fait du nombre croissant d'employés connectés à Internet sur leur lieu de travail.

Alors que par le passé, l'employeur n'envisageait pas de prendre connaissance des notes de ses employés, de crainte sans aucun doute d'y trouver des pattes de mouches illisibles, les nouvelles technologies ont accru la facilité d'accès et, partant, l'attrait pour les informations propres aux employés individuels.

Les développements technologiques ne constituent pas pour autant une justification en soi de l'accroissement de la surveillance des employés sans que ne soit menée une réflexion supplémentaire, réflexion englobant la question de la protection des données personnelles et du secret des communications.

Nul ne contestera qu'il peut exister dans certains cas des raisons peu discutables pour un employeur de procéder à l'interception de communications, par exemple dans le secteur bancaire, à titre de preuve des ordres de bourse passés en salle de marché. La question devient toutefois plus sensible lorsque l'employeur désire surveiller les communications des employés afin de garantir l'intégrité de son système de communications, de vérifier leurs activités, ou encore pour contrôler le contenu des informations que ceux-ci reçoivent ou transmettent.

Quelles sont les limites acceptables du contrôle de l'employeur et quels sont les droits que peut faire valoir un employé ? L'employeur peut-il fonder la surveillance des communications de ses employés sur une interdiction de tout usage privé des moyens de communication mis à leur ? Doit-on admettre que, d'une certaine façon, l'employeur se substitue aux autorités publiques chargées d'assurer le respect des lois et se charge lui-même de la « police » de ses réseaux ? Quel rôle doit jouer dans le débat le fait que le matériel soit mis à disposition des employés par l'employeur, qui en est en principe le propriétaire ? La notion de propriété du matériel est-elle pertinente alors que le respect de droits fondamentaux peut être en cause ?

Sans prétendre répondre à l'ensemble des questions difficiles soulevées

1. Marie-Hélène Boulanger et Anne-Christine Lacoste sont juristes ; Sophie Louveaux est consultante chez e-consult. Les auteurs n'expriment dans le présent article que leur opinion strictement personnelle.

par la surveillance des communications des employés sur leur lieu de travail, le présent article entend retracer les éléments de base du contexte de droit international (2), évoquer de brefs éléments de droit comparé (3) pour centrer le propos sur la question des dispositions applicables en droit belge, et en particulier la convention collective de travail récemment adoptée (4).

## 2 Le cadre juridique européen et international

### 1. La Charte des droits fondamentaux de l'Union européenne et la Convention européenne des droits de l'homme[2]

La correspondance, qu'elle soit électronique ou non, bénéficie de la protection offerte par les textes internationaux de protection des droits fondamentaux. On souligne l'importance de l'article 8 de la Convention européenne des droits de l'homme tout comme des articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne[3] qui se réfère, quant à elle, explicitement à la protection des communications. La Cour de Justice des Communautés Européennes a, pour sa part, reconnu que le droit à la vie privée vis-à-vis des autorités publiques fait partie des droits fondamentaux dont elle assure le respect[4].

L'article 8, § 2, de la Convention européenne des droits de l'homme autorise certaines exceptions au droit protégé, tout comme l'article 52 (3) de la Charte des droits fondamentaux de l'Union européenne[5]. La Cour européenne des droits de l'homme a eu à se prononcer à diverses reprises sur des questions mettant en cause la protection du droit à la vie privée des individus sur leur lieu de travail. Les affaires les plus connues dans ce contexte sont Niemitz et Halford. Dans l'affaire Niemitz[6], la Cour a jugé que la notion de vie privée ne pouvait être limitée à un « cercle intime où chacun peut mener sa vie personnelle à sa guise » et écarter le monde extérieur. Pour la Cour, le respect de la vie privée doit englober « dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables ». La Cour se refuse par conséquent à exclure les activités professionnelles ou commerciales du concept de vie privée,

2. Il existe de nombreux autres textes pertinents pour la discussion. On signalera en particulier les recommandations du Conseil de l'Europe adoptées dans le sillage de la Convention n° 108 de 1981 (Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel) et les travaux du Bureau international du travail.
3. La Charte a été proclamée de manière conjointe par la Commission, le Conseil et le Parlement lors du sommet européen de Nice. Actuellement, sur la base des discussions en cours au sein de la Convention, on peut supposer que la Charte sera incorporée dans les traités de l'Union européenne. L'article 7 de la Charte assure la protection du droit à la vie privée de manière assez similaire à l'article 8 de la Convention européenne des droits de l'homme, tandis que l'article 8, plus novateur, consacre le droit fondamental à la protection des données. La Charte s'adresse aux institutions de l'Union et aux Etats membres lorsqu'ils mettent en oeuvre le droit de l'Union. Parmi les nombreux commentaires sur le sujet, voy. par exemple, P. EECKHOUT, « The EU Charter of fundamental rights and the federal question », *Common Market Law Review*, 2002, 39, pp. 945-994.
4. Voy. par exemple affaires jointes 46/87 et 227/87 (Hoechst ), *Recueil*, 1989, p. 2919.
5. L'article 52 (1) de la Charte circonscrit toutefois les possibilités de limiter les droits fondamentaux énoncés, dont l'essence doit être respectée.
6. *Niemitz c. Allemagne*, C.E.D.H., 16 décembre 1992, *J.T.T.*, 1994, p. 65, en particulier § 29.

soulignant que c'est dans « leur travail que la majorité des gens ont beaucoup, voir le maximum d'occasions de resserrer leurs liens avec le monde extérieur »[7]. A l'appui de son interprétation, la Cour évoque en particulier l'imbrication entre activités professionnelles et non professionnelles. La Cour fait également état de ce que le droit d'ingérence des Etats consacré à l'article 8, § 2, « pourrait fort bien aller plus loin pour des locaux ou activités professionnels ou commerciaux que dans d'autres cas ».

Dans l'affaire Halford[8], la Cour a jugé « que les appels téléphoniques émanant de locaux professionnels, tout comme ceux provenant du domicile, peuvent être intégrés dans les notions de "vie privée" et de "correspondance" visées à l'article 8, paragraphe 1 »[9]. Il est intéressant de souligner que la requérante, Mme Halford, avait à sa disposition deux appareils téléphoniques, dont l'un était réservé à ses communications privées. L'utilisation de ces téléphones n'était assortie d'aucune restriction et aucun conseil ne lui avait été donné à cet égard. L'arrêt s'appuie en particulier sur la circonstance que rien ne prouve que Mme Halford avait été prévenue que les appels qu'elle passait étaient susceptibles d'être interceptés. La Cour en déduit dès lors que Mme Halford pouvait raisonnablement croire au caractère privé de ses appels.

## 2. Directives européennes relatives à la protection des données

Aucune des directives communautaires relatives à la protection des données n'aborde de manière spécifique la question de la surveillance des employés dans un contexte professionnel.

La directive « protection des données » spécifique au secteur des télécommunications (97/66/CE)[10] contient en son article 5 un principe d'interdiction d'interception des télécommunications par d'autres personnes que les utilisateurs sans le consentement de ceux-ci. Elle autorise toutefois l'enregistrement, prévu par le droit national, de communications afin de fournir la preuve d'une transaction commerciale ou de tout autre communication commerciale[11]. Est ici visé en particulier l'enregistrement des opérations passées en bourse ou des commandes passées par voie électronique. Un tiers qui envoie un message sur un réseau public de télécommunication à destination d'un employé individualisé d'une compagnie bénéficie sans aucun doute de la protection offerte par la directive 97/66/CE.

7. La Commission européenne des droits de l'homme avait déjà estimé auparavant que le fait de nouer des relations avec autrui est une composante du droit au respect de la vie privée protégé au titre de l'article 8 de la Convention (Van Oosterwijk c. Belgique, rapport de la Commission de 1979).
8. *Halford c. Royaume-Uni*, C.E.D.H, arrêt du 27 mai 1997.
9. Voy. en particulier §§ 44-45 de l'arrêt.
10. Directive 97/66/CE du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications. Cette directive sera remplacée en novembre 2003 par la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques en raison de sa nécessaire adaptation aux développements technologiques. Elle détaille et complète la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
11. Il convient de souligner ici que cet enregistrement constitue un traitement au sens de la directive 95/46/CE. Le considérant 23 de la directive 2002/58/CE le confirme explicitement et en indique les conséquences : « La directive 95/46/CE est applicable en pareil cas. Les parties aux communications devraient être informées de l'enregistrement avant qu'il n'ait lieu, de la ou des raisons pour lesquelles la communication est enregistrée et de la durée du stockage de l'enregistrement. La communication enregistrée devrait être effacée dès que possible et, en tout état de cause, lors de l'expiration du délai légal de recours contre la transaction ».

Pour ce qui est de la directive générale relative à la protection des données (95/46/CE), elle contient un certain nombre de principes permettant d'établir les conditions de l'équilibre entre ficheurs et fichés. On citera essentiellement le principe de proportionnalité sur lequel repose la majorité des dispositions de ce texte. A cet égard, il est important de souligner que l'obtention du consentement du travailleur n'est pas un élément suffisant pour déroger à ce principe de proportionnalité. Toutefois, on relèvera que les différents pays européens ont des approches différentes sur le poids à donner au consentement.

Des éléments utiles pour l'interprétation de la directive 95/46/CE dans le cadre de la surveillance des communications des employés ont été apportés par le groupe de travail institué par l'article 29 de la directive 95/46/CE. Ce groupe a adopté en mai 2002 un document de travail concernant la surveillance des communications sur le lieu de travail[12]. On relèvera d'emblée que la dénomination du document se veut prudente car il ne s'agit ni d'une opinion ni d'une recommandation mais d'un simple document de travail. Conformément au mandat octroyé par les directives européennes relatives à la protection des données[13] à ce groupe, le document est censé contribuer à l'application uniforme des mesures nationales adoptées au titre de la directive relative à la protection des données. Cela étant, le groupe évoque d'emblée le fait que des législations nationales puissent être plus strictes en particulier sur la base du secret de la correspondance, et renonce de ce fait à intégrer dans son analyse la protection offerte par le secret.

On regrettera cette approche pour deux raisons. D'une part, le groupe aurait pu intégrer le secret de la correspondance dans sa démarche, sur la base des concepts de légitimité et de licéité des traitements évoqués à l'article 6 de la directive 95/46/CE. Ces concepts font partie des conditions de base applicables à tout traitement de données à caractère personnel et ils impliquent le respect de l'ensemble des normes légales applicables. Les données à caractère personnel doivent être traitées licitement pour des finalités légitimes. D'autre part, le groupe institué à l'article 29 de la directive 95/46/CE est compétent sur la base de la directive 97/66/CE relative à la protection des données dans le secteur des télécommunications qui harmonise la protection offerte en intégrant le secret de la correspondance. Or, comme nous l'avons vu, le tiers qui transmet des données sur un réseau public de télécommunication à destination d'un employé déterminé doit pouvoir bénéficier de la protection offerte par les directives relatives à la protection des données spécifiques aux télécommunications.

Pour l'essentiel, le groupe de l'article 29 fonde son analyse de l'application de la directive 95/46/CE sur une mise en balance de deux intérêts. L'employé a droit au respect de ses droits et libertés fondamentaux, et en particulier le droit à la vie privée et la liberté d'information, alors que l'employeur doit également pouvoir défendre ses intérêts et notamment protéger sa responsabilité en cas d'action illicite de la part de ses employés. Sur la base de cette prémisse, le groupe examine les conséquences de l'application de la directive 95/46/CE et en particulier la détermination de la finalité du traitement de données personnelles et leur non-réutili-

12. Document de travail concernant la surveillance des communications électroniques sur le lieu de travail adopté le 29 mai 2002.
13. Directive 95/46/CE, directive 97/66/CE et directive 2002/58/CE.

sation à des fins incompatibles[14], la proportionnalité du traitement qui implique notamment d'opter pour le moyen de contrôle le moins intrusif, les fondements de légitimité pouvant être invoqués, ainsi que la transparence qui est particulièrement importante dans le contexte d'une relation de travail et peut nécessiter un dialogue avec les travailleurs et leurs représentants. On réitérera la remarque précédemment formulée sur le peu de place laissé à l'intérêt du tiers à la relation de travail mais partie à la communication en cause. Par ailleurs, en bonne logique, le groupe choisit de mettre l'accent sur la prévention plutôt que sur le contrôle, et souligne l'intérêt des solutions technologiques.

Bien que cette question excède la seule application de la directive 95/46/CE à la surveillance des e - mails, le groupe se prononce également sur l'absence de caractère raisonnable d'une interdiction absolue de l'utilisation d'Internet par les salariés à des fins privées, qui ne tiendrait pas compte de l'aide qu'Internet peut apporter dans la vie quotidienne. On peut souscrire à cette approche en particulier en raison de la difficulté de plus en plus grande de dissocier vie privée et vie professionnelle. De plus en plus d'employés mènent des activités personnelles sur le lieu de travail, ne fût-ce que pour réserver un billet de train, et vice-versa. Le développement du travail à domicile augmente encore la difficulté de tracer une ligne de démarcation claire entre vie privée et professionnelle. Dans ce contexte, optant résolument pour une approche pratique, le groupe propose de fournir aux salariés deux comptes de courrier électronique : un compte à usage uniquement professionnel qui pourrait être soumis à contrôle, et un compte à usage strictement privé qui ne serait dûment contrôlé que dans des cas exceptionnels d'abus. Cette position du groupe illustre bien la difficulté de l'approche. En effet, offrir un compte privé devrait permettre en théorie de distinguer les communications réellement « privées » des communications « professionnelles », et de répondre à l'attente évidente du respect par l'employeur de la confidentialité des communications de l'employé qui n'ont pas trait à sa vie professionnelle. Cela étant, la surveillance des communications est souvent justifiée sur la base de cas exceptionnels notamment des comportements gravement déloyaux de l'employé (divulgation de secret commerciaux ...). Or, si l'on garantit à l'employé une confidentialité de ses appels donnés à titre « privé », c'est sur la base de cette garantie de confidentialité qu'il pourrait être tenté d'effectuer les appels auxquels l'employeur voudrait précisément avoir accès. Hors ces cas, les comportements professionnels sont normalement basés sur la confiance réciproque et donc sur une transparence de la part de l'employé vis-à-vis de son employeur quant à ses activités. La surveillance des communications n'y est de ce fait pas nécessaire.

On terminera ce trop bref examen du droit communautaire par la mention de la procédure de consultation des partenaires sociaux initiée par la Commission européenne sur la protection des données à caractère personnel des travailleurs[15]. Il faut noter que tout instrument qui pourrait être proposé dans ce contexte se devrait de respecter les directives communautaires relatives à la protection des données.

14. Le groupe estime notamment que des données collectées à des fins de sécurité ne devraient dès lors pas être réutilisées à des fins de contrôle.
15. Le dialogue social est prévu aux articles 138 et 139 du traité CE, articles qui institutionnalisent le rôle des partenaires sociaux dans l'élaboration de la politique sociale communautaire.

## 3 Eléments de droit comparé

On soulignera d'emblée des différences d'approche entre pays. En outre, un aperçu du droit comparé illustre largement les difficultés juridiques que l'on retrouve en Belgique. Ainsi, certains pays choisissent de fonder leur approche sur une législation abordant spécifiquement la surveillance des employés[16] tandis que d'autres s'en remettent plutôt à la Convention européenne des droits de l'homme, à leurs principes constitutionnels[17], à l'application des réglementations relatives à la protection des données[18], au secret de la correspondance ou aux normes spécifiques au droit du travail, ou encore fréquemment à une combinaison de ces différentes sources. Par exemple en France, aucune réglementation spécifique ne semble à ce jour exister sur la question. On relèvera par ailleurs que dans un certain nombre de pays, l'approche se fonde également sur des avis, recommandations ou codes de conduite avec une intervention plus ou moins importante de l'autorité de contrôle chargée de la protection des données personnelles. Ainsi, au Royaume-Uni, un code de conduite a été élaboré en la matière[19].

Pour ce qui est de la jurisprudence, on relève une tendance des juridictions suprêmes à renforcer les conditions d'interception des correspondances sur la base de la protection des droits individuels[20]. Ainsi, les tribunaux français ont tendance à limiter le pouvoir de l'employeur en vue d'assurer la protection des droits fondamentaux des employés. En Allemagne, la jurisprudence de la Cour constitutionnelle protège les correspondances établies à partir du lieu de travail sur la base de la protection des droits de la personnalité des employés[21].

16. Voir notamment la législation finlandaise de mai 2001.
17. On relèvera que la possibilité d'invoquer directement la Convention européenne des droits de l'homme ou les dispositions constitutionnelles varie sensiblement d'un Etat à l'autre. En Belgique, cette invocation directe semble acceptée. Voy. par exemple l'arrêt de la Cour de cassation du 27 février 2001.
18. Ces législations se retrouvent dans bon nombre d'Etats européens que ce soit en tant que mesures de transposition de la directive 95/46/CE ou en tant qu'instruments adoptés pour se conformer à la Convention n° 108 du Conseil de l'Europe.
19. L'approche anglaise est fondée sur un code de conduite relatif à l'utilisation des données personnelles dans les relations de travail. Ledit code détermine les limites à la surveillance des communications des employés sur le lieu de travail, qu'il s'agisse de communications téléphoniques, d'e-mails ou d'accès à Internet. Dans ce contexte, l'autorité de protection des données britannique a soutenu la nécessité de consulter les employés ou leurs représentants avant la mise en place de méthodes de surveillance, ainsi que de procéder à l'information concernant les buts et les moyens de surveillance, et a rejeté les méthodes d'investigation cachées. Des dérogations sont toutefois admises par exemple si l'information est susceptible de causer préjudice à la prévention ou la détection d'actes criminels. Dans ce cas, la surveillance peut permettre de réunir les preuves nécessaires. Par ailleurs, les questions de surveillance des e-mails sont régies par le *Data Protection Act* de 1998 et par le *Regulation of Investigatory Powers Act* (RIPA) voté en 2000. Ce dernier texte prévoit qu'il est illégal pour un employeur d'intercepter des communications en cours sur un réseau de télécommunications privé, à moins que certaines conditions soient réunies, en particulier le consentement des deux parties, ou, de manière similaire à ce qui est prévu en droit américain, l'enregistrement de communications professionnelles ayant un rapport direct avec l'activité de l'entreprise.
20. Voy. en particulier les jurisprudences française et espagnole en ce sens. Ainsi, la jurisprudence française insiste sur la nécessaire information des employés. Dans un arrêt du 14 mars 2000 (Cass. Soc., 14 mars 2000, *Dujardin c/ Société Instinet France*, n° 98.42.090), la Cour de cassation française précise que si l'employeur est en droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail, il ne peut pas le faire dans n'importe quelles conditions et doit préalablement informer les salariés de l'entreprise de l'existence d'un système de surveillance. Dans un arrêt du 2 octobre 2001, la Cour de cassation française a reconnu que « le salarié a droit, même aux temps et lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur ».
21. Les juridictions inférieures allemandes ne semblent pas toujours suivre cette approche.

La jurisprudence hollandaise pour sa part semble, selon l'opinion de M. M.A.C. de Wit, laisser bien peu de place à la question des droits fondamentaux[22]. La situation américaine[23], qui se caractérise par l'existence de nombreux cas de plainte suite à des licenciements liés à la lecture de courriers électroniques par l'employeur, est quant à elle clairement éloignée d'une approche fondée sur les droits de l'homme. Si la législation offre une certaine protection, de nombreuses exceptions sont prévues au cas où le contrôle effectué par l'employeur est lié à l'activité de l'entreprise. L'interprétation donnée à cette dernière notion par les tribunaux est assez extensive. On citera la célèbre affaire Smyth v. Pillsbury[24] qui concerne un licenciement suite à un échange de courriers électroniques non professionnels. Or, les employés de la société en cause disposaient de la possibilité d'échanger des e - mails à l'intérieur d'une société. A plusieurs reprises, il avait été déclaré que la vie privée des employés serait respectée. Néanmoins, le juge a écarté la protection dans la mesure où, d'une part, une personne raisonnable ne pourrait admettre que l'interception des communications constitue une intrusion importante dans sa vie privée et, d'autre part, que l'intérêt de l'employeur qui procède à la prévention d'activités illicites et non professionnelles l'emporte sur celui de l'employé. On retrouve une approche similaire dans un autre cas (lié au harcèlement sexuel) tranché par la Cour d'appel du Texas (McLaren v. Microsoft)[25], dans lequel un employé se plaignait de l'atteinte à sa vie privée découlant de l'accès aux e-mails stockées sur son ordinateur, ou dans l'affaire United States v. Simons[26], affaire concernant le fait qu'un gestionnaire de système avait retracé l'accès à des sites web pornographiques à partir de l'ordinateur du défendeur.

## 4 Le cadre juridique en droit belge

Les dispositions de droit belge s'inscrivent largement dans la continuité des dispositions internationales qui viennent d'être évoquées, avec lesquelles elles doivent être en conformité.

Ainsi, le droit à la vie privée sur le lieu de travail, tel qu'il a été reconnu par les textes du Conseil de l'Europe et la jurisprudence de la Cour européenne des droits de l'homme susvisés (voy. supra), est consacré également en droit interne par différentes dispositions juridiques.

### 1. Le contexte du lieu de travail

On évoquera en particulier les textes suivants :

- la loi du 8 avril 1965 instituant les règlements de travail (article 6) prévoit que « le règlement de travail doit indiquer (...):

22. M.A.C. DE WIT, « Privacy van Werknermers in het informatietijdperk », *Sociaal maandblad arbeid*, nr. 6, 2002, pp. 351-360.
23. Sur la situation canadienne, voir M. GEIST, « Surveillance des ordinateurs et du courrier électronique en milieu de travail au Canada : de l'attente raisonnable en matière de respect de la vie privée à la surveillance raisonnable », mars 2002, http://www.cjc-ccm.gc.ca/francais/publications/Geist_Fr.pdf
24. *Michel A. Smith v. The Pillsbury Company*, District Court for the Easter District of Pennsylvanie,1996.
25. Cour d'appel du Texas, 28 mai 1999, Cas n° 05-97-00824.
26. Cour d'appel de Virginie, *United States v. B. Simmons*, 1998.

5° les droits et obligations du personnel de surveillance » ;

- 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, prévoit une information préalable et une consultation des employés en ce qui concerne l'utilisation par l'employeur de nouvelles technologies ayant des conséquences notamment dans l'organisation du travail[27].

Dans le prolongement de ces dispositions, le Conseil national du travail a adopté deux conventions collectives visant à instaurer un équilibre entre les droits de l'employeur et ceux des employés dans le contexte de la surveillance par caméras sur le lieu du travail[28] ainsi que dans le contexte du contrôle des données de communications électroniques en réseau (ce dernier texte fera l'objet d'un examen spécifique au point 4).

## 2. La protection des données de télécommunication

Deux dispositions légales visent plus spécifiquement la protection, d'une part, du contenu des communications et d'autre part, des données de communication au sens large. Il s'agit de l'article 314bis du Code pénal et de l'article 109terD de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.

L'article 314bis du Code pénal réglemente l'interception du contenu des communications ou télécommunications en ces termes:

« Est puni d'un emprisonnement de six mois à un an et/ou d'une amende de deux cent à dix mille francs celui qui, intentionnellement, à l'aide d'un appareil quelconque, écoute (...) prend connaissance (...) enregistre (...) pendant leur transmission, des communications ou télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications ».

L'article 109terD de la loi du 21 mars 1991 protège de façon générale les données transmises par voie de télécommunications[29].

« 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

27. Article 2, § 1er : « 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. »

28. Respectivement la convention collective de travail n° 68 rendue obligatoire par arrêté royal le 20 septembre 1998, et la convention collective de travail n° 81 rendue obligatoire par arrêté royal le 12 juin 2002.

29. L'article 109*ter*D réglementait également à l'origine la prise de connaissance du contenu des télécommunications. La suppression du terme « contenu » du libellé de l'article pourrait laisser penser que celui-ci n'est plus réglementé que par l'article 314*bis* du Code pénal, et que l'article 109*ter*D voit son champ d'application limité aux données connexes, tels que numéros appelant et appelé, heure d'appel, localisation de l'appelant, etc. On note toutefois que l'article 109*ter*D protège toujours les écrits et les images, qui peuvent être considérés comme du contenu... ce qui laisse à notre sens à cet article un champ d'application particulièrement large, qui télescope dans une certaine mesure celui de l'article 314*bis* du code pénal.

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. »

Il convient de s'arrêter sur la notion de communication privée, telle qu'elle est protégée par l'article 314bis du Code pénal. Est privé – et donc protégé par la loi – « ce qui n'est pas destiné à être entendu par d'autres que les participants à la communication. Il ne s'agit donc pas de savoir si la communication est professionnelle ou non »[30]. « Une communication professionnelle, mais non destinée à être entendue par d'autres personnes que les partenaires à la conversation, est une communication privée au sens de la loi »[31]. Bien que le critère retenu soit différent de celui de la Cour européenne des droits de l'homme, le résultat obtenu n'est pas très différent dans la mesure où il conduit à reconnaître une protection aux communications émises ou reçues sur le lieu de travail. Alors que dans la jurisprudence évoquée ci-dessus, la Cour de Strasbourg opte pour une interprétation dynamique du concept de vie privée auquel elle rattache son interprétation[32], la loi belge préfère quant à elle se fonder sur les caractéristiques propres à la communication, évitant à juste titre d'exclure du champ de la protection les communications professionnelles. En droit belge, une communication est privée dans la mesure où elle n'est pas publique, et non pas dans le sens où elle ne serait pas professionnelle.

Cette distinction est importante dans la mesure où, comme nous le verrons, certaines pratiques de contrôle sur le lieu de travail utilisent ce critère de la communication privée ou professionnelle pour exclure les communications professionnelles du bénéfice de la protection que leur accorde la loi.

En principe, toute prise de connaissance des données de communication (qu'il s'agisse du contenu ou des données de « trafic ») est interdite, sauf consentement des parties à la communication, ou utilisation de l'une des exceptions prévues à l'article 109terE de la loi du 21 mars 1991 - l'on relève que, pour ajouter à la complexité des rapports entre les articles 314bis du Code pénal et 109terD de la loi du 21 mars 1991, les exceptions prévues à l'article 109terE de cette dernière s'appliquent également à l'article 314bis du Code pénal.

### *a. Le consentement des parties*

L'interdiction prévue à l'article 109terD de la loi du 21 mars 1991 s'applique « sous réserve de l'autorisation de toutes les autres personnes directement ou indirectement concernées». La question qui se pose

30. Travaux préparatoires de la loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, *Doc. parl.*, Sén., sess. 1992-1993, n° 843-2, p. 36.
31. *Doc. parl.* Sén., sess. 1992-93, n° 943/1 p.7, et 843/2 p. 36.
32. En ce qui concerne la protection des données personnelles, la Cour choisit généralement une interprétation dynamique de l'article 8 de la Convention européenne des droits de l'homme (article qui lui a souvent servi de base pour des avancées jurisprudentielles importantes) plutôt que de se fonder sur la protection des autres droits et libertés protégés par la Convention.

d'emblée est de savoir si un consentement général et préalable peut être considéré comme valable. Certains auteurs[33] ont ainsi suggéré qu'une icône pourrait s'afficher, de façon répétitive ou non, sur l'écran d'ordinateur de l'employé qui se connecte à Internet ou qui utilise le logiciel de courrier électronique. L'employé devrait ainsi cliquer sur cette icône afin d'accepter ou de refuser la surveillance dont il va faire l'objet.

La question du caractère libre du consentement de l'employé doit toutefois être soulevée : « L'on peut se demander si l'employé aura dans une telle hypothèse réellement le choix de refuser la surveillance, sous peine de se voir refuser l'accès à l'outil informatique. L'autorité de l'employeur qui s'exerce à son égard risque en tout état de cause de l'inciter à ne pas contrarier ce dernier, et nous fait douter du caractère réellement libre d'un consentement donné dans de telles circonstances »[34].

Ajoutons que les travaux préparatoires de la loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées indiquent que « l'employeur ne peut obtenir le consentement de son employé, par exemple, pour écouter de manière générale ses communications »[35]. Une négociation globale et à caractère trop général ne serait donc pas non plus valable. Par ailleurs, se pose en tout état de cause la question du consentement du tiers à la communication.

La Commission de la protection de la vie privée a abordé, dans une recommandation récente[36], la question des conditions d'obtention du consentement des employés parties à la communication.

Elle a à cet égard considéré que « en ce qui concerne les employés, une note de service ou le règlement de travail seuls ne sont pas suffisants pour garantir le consentement libre de l'employé. Il s'agit de combiner le consentement individuel de l'employé avec la négociation d'un texte général à laquelle seront associés les représentants des employés.(...)

Le consentement obtenu par la mention des conditions d'enregistrement dans le règlement de travail ou le code de conduite, qui font l'objet d'une discussion au sein du Conseil d'entreprise et contribuent ainsi au caractère libre du consentement, pourra par exemple être complété via un avenant au contrat de travail ou la signature d'un formulaire ad hoc par l'employé, garantissant ainsi le caractère individuel du consentement ».

### *b. Les exceptions de l'article 109terE*

La prise de connaissance pourrait être autorisée, même en l'absence de consentement de l'employé, lorsque les actes visés sont accomplis dans le but exclusif d'assurer le bon fonctionnement du réseau.

33. TH. VERBIEST, « La surveillance de l'usage de l'Internet dans l'entreprise : quelle légalité ? », *Droit et nouvelles technologies*, http://www.droit-technologie.org, 25.01.00.
34. A.C. LACOSTE, « Données personnelles et contrôle de l'Internet et de l'e-mail »,in *Manuel de la vie privée*, Politeia, 2001.
35. *Doc. parl., Sén.*, sess. 1992-1993, n°843-2, pp. 35 et 943-1, p. 8.
36. Recommandation n° 1/2002 du 22 août 2002 relative à l'enregistrement des télécommunications effectuées dans le cadre des services bancaires.

On pense aux interventions techniques sur le réseau de l'entreprise, qui peuvent parfois nécessiter une identification de certaines données de télécommunication lorsque par exemple des courriers trop volumineux (comportant des annexes sous forme de fichiers exécutables ou d'images) ou des virus bloquent le système informatique. Le fonctionnement général des systèmes de gestion de la sécurité du réseau (logiciels de filtrage, ...) devrait pouvoir bénéficier de l'exception prévue à l'article 109terE.

Parmi les autres exceptions prévues par l'article 109terE, figure la possibilité d'une prise de connaissance des données de communication lorsque la loi la permet ou l'impose. La consécration légale de l'autorité de l'employeur (article 17, § 2 de la loi du 3 juillet 1978 relative aux contrats de travail), ou encore son obligation d'assurer le respect des convenances et des bonnes mœurs au sein de l'entreprise (article 16 de la même loi) ont parfois été interprétées comme permettant un tel contrôle. Nous rejoignons néanmoins la doctrine qui considère que, pour justifier l'ingérence de l'employeur dans un échange de communications, des dispositions légales plus précises sont nécessaires[37].

Nous examinerons dans la dernière partie de cet article la question de savoir si la récente Convention collective de travail n° 81, qui traite spécifiquement du contrôle des communications électroniques en réseau, peut être considérée comme une loi au sens de l'article 109terE.

### c. *Cas particuliers*

Certaines situations concrètes peuvent être envisagées, dans lesquelles un employeur pourrait faire valoir un besoin urgent de prendre connaissance de certaines communications, sans qu'aucune des conditions des articles 314bis, 109terD et 109terE ne soit remplie.

Quelles sont par exemple les possibilités d'action d'un employeur, qui n'a pas négocié de politique de surveillance des communications avec ses employés, à l'égard d'un employé qu'il soupçonne fortement d'avoir commis une infraction d'une gravité extrême, telle que la réception ou la distribution d'images pédophiles ou la divulgation de secrets de fabrique ?

Selon certains auteurs, « la commission par le travailleur d'une infraction d'une gravité extrême pourrait justifier que l'employeur enfreigne l'article 109terD de la loi du 21 mars 1991 en vue d'empêcher la réalisation de l'infraction du travailleur. Il est bien entendu que l'employeur ne pourra procéder de la sorte que s'il a épuisé tous les autres moyens de prévenir ou d'interrompre la réalisation de l'infraction »[38].

37. Dans le même sens : O. RIJCKAERT, « Le contrat de travail face aux nouvelles technologies », *Orientations*, n° 11, novembre 2000, p. 207 ; P. LEDUC, cité par O. RIJCKAERT, *ibidem* ; *contra*, Trib. trav. Bruxelles (12e ch.), 22 juin 2000, inéd., R.G. n° 88 187/98, *ibidem*.
38. O. RIJCKAERT, *op. cit.*, p. 208.

Il devra être procédé à une mise en balance des droits fondamentaux de l'employé et des intérêts ainsi que de la responsabilité propre de l'employeur. L'état de nécessité, caractérisé par la doctrine comme une « situation de crise exceptionnelle » [39], pourrait justifier que l'employeur enfreigne l'article 109terD de la loi du 21 mars 1991 et/ou l'article 314bis du Code pénal, en vue d'empêcher la réalisation de l'infraction du travailleur ou de préserver sa propre responsabilité. Il faudrait en outre que « l'employeur dispose d'éléments suffisamment précis et concordants lui permettant de soupçonner l'extrême gravité de l'infraction. L'état de nécessité ne peut être invoqué pour justifier des interceptions généralisées et systématiques »[40].

C'est en dernier ressort au juge qu'il appartiendra d'apprécier si la balance des intérêts en présence et la gravité de la situation justifiaient la violation de la loi.

### 3. La protection des données à caractère personnel

Toute donnée de communication se rapportant à une(des) personne(s) identifiée(s) ou identifiable(s) constitue une donnée à caractère personnel. Outre le respect des dispositions légales spécifiques aux communications, toute personne traitant de telles données devra respecter les principes de la loi du 8 décembre 1992 relative à la protection de la vie privée, loi qui assure la transposition de la directive communautaire 95/46/CE évoquée plus haut.

Les principes de la loi du 8 décembre 1992 visent à assurer un traitement légitime des données à caractère personnel, dans le respect des droits et libertés fondamentaux ainsi que des intérêts en présence. On relève en particulier les obligations suivantes :

- la proportionnalité et le caractère nécessaire des données collectées ;
- la transparence du traitement vis-à-vis de la personne dont les données sont traitées ;
- une durée de conservation des données limitée et des conditions strictes d'accès et de stockage de ces données.

La Commission de la protection de la vie privée a interprété, dans un avis du 3 avril 2000[41], l'application de ces principes au contexte de la surveillance par l'employeur de l'utilisation de l'outil informatique sur le lieu de travail. Dans l'avis mentionné, la Commission a fourni certaines orientations concrètes concernant notamment le degré d'intrusion que peut revêtir la surveillance, en fonction du contexte et de la nature des données concernées,

39. Tel que décrit par C. HENNEAU et J. VERHAEGEN, *Droit pénal général* , Bruxelles, Bruylant, 1991, p. 161.
*Contra* : F. HENDRICKX, *Privacy en arbeidsrecht* , Brugge, Die Keure, 1999 ; Trib. trav. Bruxelles, (12e ch.), 22 juin 2000, inéd., A.R. n° 1.471/99, http://www.droit-technologie.org : « Overwegende dat artikel 109*ter*E van de wet van 21 maart 1991 bepaalt dat het verbod tot kennisname van telecommunicatie vervat in de bepalingen van artikel 109*ter*D van deze wet en van artikel 314*bis* van het strafwetboek niet van toepassing zijn wanneer de wet het stellen van de bedoelde handelingen toestaat of oplegt;
Verder is de noodsituatie een algemeen aanvaarde uitzondering in het strafrecht, die zou toelaten om zonder medeweten of toestemming van de gesprekspartners een gesprek af te luisteren of van een e-mail bericht kennis te nemen op voorwaarde dat de overtreding van het verbod het enige middel is om hogere rechtsbelangen te beschermen zoals en fysische of psychische integriteit. [...]
Overwegende dat op de werkgever de wettelijke verplichting rust overeenkomstig artikel 126 van de wet van 3 juli 1978 de goede zeden in acht te nemen en te doen nemen gedurende de uitvoering van de arbeidsovereenkomst ».
40. A.C. LACOSTE, *op. cit.*, p. 270.
41. Avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, n° 10/2000 du 3 avril 2000.

ainsi que les informations concrètes[42] qui devraient être fournies aux employés.

Depuis lors, une deuxième initiative visant à interpréter et concilier les différents droits en présence a vu le jour. La Convention collective de travail n°81[43] a ainsi pour objectif de fournir tant aux employeurs qu'aux employés un instrument clair afin que tout contrôle sur le lieu de travail soit effectué dans le respect du droit.

C'est à l'analyse de cette Convention, au regard des dispositions juridiques explicitées ci-avant, que nous nous attachons maintenant.

## 4. La convention collective de travail n° 81

La Convention collective n° 81 (ci-après la CCT), vise à établir un équilibre entre, d'une part, la protection de la vie privée du travailleur sur le lieu de travail et, d'autre part, les prérogatives de l'employeur qui lui permettent d'assurer le bon fonctionnement de l'entreprise[44]. Elle ne vise pas à régler les modalités d'accès et/ou d'utilisation des moyens de communication électronique en réseau, qui restent la prérogative de l'employeur.

### *a. Traitement de données à caractère personnel*

A priori, le contrôle visé par la section I de la CCT (les modalités de contrôle des données de communications électroniques) ne viserait pas le traitement de données à caractère personnel puisqu'il n'y aurait pas d'individualisation des données[45]. Toutefois, selon les termes des commentaires de la Convention, la collecte des données relatives à la durée de connexion à Internet se fait par « poste de travail »[46]. Or il va de soi que dans la majorité des entreprises un poste de travail correspond à une personne déterminée. Il y a donc traitement de données à caractère personnel entraînant l'application de la loi du 8 décembre 1992. Le contrôle visé par la section II de la Convention implique par contre, par essence même, une attribution des données à une personne identifiée et donc un traitement de données à caractère personnel.

Pour autant qu'il y ait traitement de données à caractère personnel, les principes de finalité, proportionnalité et transparence tels que définis dans la loi du 8 décembre 1992 s'appliquent sans pour autant être identiques à ceux définis dans la Convention. En effet, dès lors que des données à caractère personnel sont traitées, le respect de cette loi s'impose. Cela sera le cas en ce qui concerne les informations concernant la collecte de données relatives

42. La Commission a ainsi identifié les éléments suivants comme devant être portés à la connaissance des employés :
« 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 ».
43. Arrêté royal du 12 juin 2002 rendant obligatoire 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, *M.B.*, 29.06.2002, 29489.
44. CCT n° 81, p. 13. Pour une analyse de ce texte, voy. M.A.C. DE WIT, « Privacy van werknemers in het informatietijdperk », *op.cit.* ; X, « New national agreement on electronic communication », *E.I.R.R.*, 2002,342 25.
45. CCT, p. 17.
46. Ibidem.

à l'utilisation du courrier électronique pour autant qu'on puisse identifier directement ou indirectement le travailleur, de même que, en ce qui concerne les données relatives aux visites de sites, à partir du moment où l'employeur peut faire le lien entre les adresses des sites et un employé déterminé. Il ne faut donc pas s'y méprendre : le respect de la Convention n'entraîne pas d'office le respect des principes de finalité, proportionnalité et de transparence tels que définis dans la loi du 8 décembre 1992.

### b. *Notion de données de communications électroniques en réseau*

La Convention porte uniquement sur les « données de communications électroniques », notion qui est décrite de manière extrêmement large, indépendamment du support par lequel les données sont transmises ou reçues par un travailleur dans le cadre de la relation de travail. En ce qui concerne les données relatives aux courriers électroniques, la notion vise les données dites « de trafic » qui entourent la communication (expéditeur, destinataire, date, heure,...) et non pas le contenu du courrier lui-même[47]. Elle vise les communications électroniques en réseau tant interne (intranet) qu'externe (internet). Contrairement à l'avis de la Commission de la protection de la vie privée[48], la C.C.T. ne fait pas de distinction dans les principes applicables selon que le contrôle porte sur les courriers électroniques ou les sites internet visités.

### c. *Engagement réciproque des parties*

La C.C.T. se base sur un engagement réciproque des parties[49] en vertu duquel les travailleurs reconnaissent à l'employeur un droit de contrôle sur l'utilisation des moyens de télécommunications mis à leur disposition par l'employeur, que ceux-ci soient utilisés à des fins professionnelles ou à des fins privées. Par ailleurs, les employeurs reconnaissent le respect du droit à la vie privée des travailleurs dans le cadre de leur relation de travail, ainsi que les droits et obligations que celle-ci implique pour chacune des parties.

La question se pose de savoir si cet engagement réciproque présent dans la Convention peut être considéré comme valant un consentement du travailleur au sens de l'article 109ter D de la loi du 21 mars 1991 (supra). Une telle approche va à l'encontre de l'avis de la Commission de la protection de la vie privée qui préconise, outre une négociation avec les représentants des employés, un consentement individuel de l'employé.

A supposer que l'on considère que cela équivaut à un consentement au sens de l'article 109terD de la loi du 21 mars 1991, encore faut-il obtenir le consentement de la personne ayant envoyé ou reçu l'e-mail dans le cas d'échanges de courriers électroniques avec des personnes externes à l'entreprise.

47. L'on se trouve dès lors hors du champ de l'article 314*bis* du Code pénal.
48. Avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, n° 10/2000 du 3 avril 2000.
49. Article 3 de la C.C.T.

### d. Modalités de contrôle général des données

Les modalités de contrôle de la C.C.T. se divisent en deux selon que le contrôle se fait de manière générale ou que l'on procède à une individualisation des données.

Selon les termes de l'article 4 de la Convention, le contrôle des données de communications électroniques en réseau n'est autorisé que pour autant qu'il satisfasse aux principes de finalité, de proportionnalité et de transparence que les conditions de procédure définies dans la Convention visent à établir.

#### 1. *Principe de finalité*

Le contrôle des données de communication ne peut viser que l'une des finalités définies à l'article 5 de la Convention. Celui-ci énumère donc de façon exhaustive les finalités pour lesquelles le contrôle des données de communication par l'employeur est permis[50]. L'employeur devra déterminer de façon concrète et précise, et selon le contexte de travail, les finalités de contrôle poursuivies. D'emblée, on peut émettre certaines réserves par rapport à la formulation trop large de certaines de ces finalités (telles que « la protection des intérêts économiques, commerciaux et financiers de l'entreprise 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 de l'entreprise, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise ; le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise ») qui ne permet pas de garantir leur détermination suffisante. Ces mêmes réserves avaient d'ailleurs été émises dans l'avis d'initiative de la Commission de la protection de la vie privée 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[51].

Comme nous l'avons déjà précisé, si les données permettent d'identifier une personne physique, il convient également de respecter la loi relative à la protection des données à caractère personnel. Cela implique notamment que la finalité soit considérée comme étant « légitime » au sens de l'article 4 de la loi de 1992. On peut alors se demander si le fait que la finalité soit prévue dans la C.C.T. implique en soi la légitimité de celle-ci[52]. L'examen de la légitimité de la finalité fait appel à une pondération des intérêts qui devrait se faire au cas par cas. Citons à ce propos la Commission de protection de la vie privée qui dans son avis 10/2000 précise : qu' «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'em-

50. Aucune dérogation ne peut être apportée à la liste sauf à la limiter en faveur de l'employé. En effet, la Convention précise qu'elle ne porte pas préjudice à des dispositions plus favorables (C.C.T., p. 6).
51. Avis d'initiative 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, 8 octobre 2001.
52. Sur le principe de légitimité voir TH. LEONARD et Y. POULLET, « Les libertés comme fondement de la protection des données nominatives », in F. RIGAUX, *La vie privée, une liberté parmi les autres ?*, Travaux de la Faculté de droit de Namur, n°17, Bruxelles, Larcier, 1992, pp. 231 et s.

ployeur 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».

Par ailleurs, le respect de la loi de 1992 implique que les données ne soient pas traitées pour une finalité incompatible avec la finalité pour laquelle elles ont été initialement collectées, et qu'un fondement puisse être trouvé au sein de l'article 5 de la loi. A ce titre, la Commission de protection de la vie privée rappelle « qu'il ne suffit pas, pour qu'une finalité réponde au prescrit de la loi relative à la protection de la vie privée, qu'elle soit prévue par un texte réglementaire. Toute finalité, pour être légitime, doit répondre à l'une des conditions de l'article 5, dont notamment, le consentement indubitable de la personne concernée, le respect d'une obligation à laquelle le responsable du traitement est soumis en vertu d'une loi, d'un décret ou d'une ordonnance, ou la réalisation de l'intérêt légitime poursuivi par le responsable du traitement (...) 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. Un examen de proportionnalité doit donc être effectué, afin de mettre en balance la finalité poursuivie et les droits et libertés fondamentaux des personnes sujettes à surveillance»[53].

### 2. *Principe de proportionnalité*

Le principe de proportionnalité, selon les termes de la C.C.T., signifie que l'on ne peut collecter, en vue du contrôle, que les données de communications électroniques qui sont nécessaires au contrôle, c'est-à-dire les données qui, compte tenu de la finalité poursuivie par le contrôle, entraînent l'ingérence la plus réduite dans la sphère privée du travailleur. Il s'agit plus particulièrement de collecter des données globales de l'entreprise et non de procéder à une individualisation par travailleur[54]. Le contrôle doit donc revêtir un caractère adéquat, pertinent et non excessif.

La Commission de protection de la vie privée a déduit de ce principe que le contrôle doit 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 de ces données apparaît disproportionné par rapport à l'objectif poursuivi[55]. Ce principe de l'interdiction de la surveillance constante du lieu de travail s'est d'ailleurs trouvé explicitement repris dans l'article 6 de 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[56].

Il est regrettable dès lors que la C.C.T. n'ait pas limité le contrôle permanent des données. En effet, le rapport précise : « Il y a lieu d'attirer l'attention sur le fait qu'aucune distinction n'est opérée selon que le contrôle poursuivi a ou non un caractère permanent. La fonction de contrôle étant quasi indissociable des systèmes de réseau véhiculant des données de communications électroniques, il est apparu que cette distinction risquait d'être artificielle et la préférence s'est portée sur le

53. Avis d'initiative 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, 8 octobre 2001.
54. *Ibidem*, p. 17.
55. Avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, n° 10/2000 du 3 avril 2000, p. 6.
56. Rendue obligatoire par l'Arrêté royal du 20.09.1998, *M.B.*, 2 octobre 1998.

traitement lui-même dont la Convention fixe clairement les limites par rapport au contenu des données »[57].

### 3. *Principe de transparence*

Le principe de transparence est essentiel puisqu'il établit que le contrôle ne peut avoir lieu que si les travailleurs ont été préalablement informés de la nature du contrôle et de la finalité de la mesure envisagée. La Commission de protection de la vie privée avait préconisé cette même transparence dans son avis d'initiative : « 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 (...); 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 »[58].

L'employeur qui souhaite installer un système de contrôle des données de communications électroniques en réseau doit informer le conseil d'entreprise sur tous les aspects du contrôle (voy. infra le contenu de l'information), conformément aux dispositions de la C.C.T. n° 9 du 9 mars 1972 coordonnant les accords nationaux et les conventions collectives de travail relatifs aux conseils d'entreprise. A défaut de conseil d'entreprise, cette information est fournie au comité pour la prévention et la protection au travail ou, à défaut, à la délégation syndicale ou, à défaut, aux travailleurs.

Lors de l'installation du système de contrôle des données de communications électroniques en réseau, l'employeur informe les travailleurs concernés sur tous les aspects du contrôle visé à l'article 9, §§ 1er et 2 de la Convention. L'information fournie doit être effective, compréhensible et mise à jour. Le choix de son support est laissé à l'employeur. L'information pourra dès lors être fournie par exemple dans le cadre d'instructions générales (circulaires, affichage, etc.), par mention dans le règlement de travail , par mention dans le contrat de travail individuel ou par des consignes d'utilisation fournies à chaque utilisation de l'outil (mention sur écran de messages à l'allumage du poste de travail et/ou lors de l'activation de certains programmes).

L'information collective et individuelle porte à la fois sur la politique de contrôle ainsi que sur les prérogatives de l'employeur et du personnel de surveillance , la ou les finalités poursuivies, le fait que des données personnelles soient ou non conservées, le lieu et la durée de conservation et le caractère permanent ou non du contrôle.

En outre, l'information individuelle porte sur l'utilisation de l'outil mis à la disposition des travailleurs pour l'exécution de leur travail, en ce compris les limites à l'utilisation fonctionnelle (durée de connexion, nombre de messages,...) , les droits, devoirs, obligations des travailleurs et les interdictions éventuelles prévues dans l'utilisation des moyens de communication électronique en réseau de l'entreprise et les sanctions prévues au règlement de travail en cas de manquement.

Le contenu de l'information correspond dès lors à ce que la loi relative à

57. C.C.T., p. 7.
58. Avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, n° 10/2000 du 3 avril 2000, p. 5.

la protection des données et la Commission de la protection de la vie privée préconisent.

### e. *L'individualisation des données*

#### 1. *Champ d'application*

La section II de la Convention vise à définir la procédure à suivre en cas d'individualisation des données de communication[59].

Notons de prime abord que les règles définies dans la Convention concernant l'individualisation des données ne s'appliquent toutefois pas lorsque l'objet et le contenu des données de communications électroniques ont un caractère professionnel non contesté par le travailleur. Dans ce cas, l'employeur pourra consulter les données sans autre procédure[60]. Le contenu de la communication privée ne pourra pas être connu de l'employeur, et les courriers électroniques devront être clairement intitulés comme étant à caractère privé afin de s'assurer de l'application de la procédure établie dans la Convention.

Cette distinction entre données ayant un caractère professionnel ou privé, qui n'est pas opérée par la Commission de protection de la vie privée, est a priori regrettable. En effet, comme nous l'avons déjà indiqué, une communication, même à titre professionnel peut également bénéficier de la protection de l'article 314bis du Code pénal.

L'individualisation des données de communications électroniques en réseau est opérée soit dans le cadre d'une procédure directe, soit dans le cadre d'une procédure indirecte selon le type de finalité poursuivie. La procédure d'individualisation sera directe, c'est-à-dire sans phase d'information au préalable, si elle vise 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 de l'entreprise auxquels est attaché un caractère de confidentialité, ainsi que la lutte contre les pratiques contraires à la sécurité et/ou au bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise. Lorsque le contrôle vise des atteintes aux règles d'utilisation des technologies en réseau, fixées dans l'entreprise, l'individualisation des données de communication sera précédée d'une phase d'information par le biais d'un entretien avec le travailleur ayant pour objectif d'avertir le travailleur d'une anomalie et de lui permettre de faire part de ses objections. En pratique cet entretien est instauré lorsque le travailleur responsable d'une anomalie est identifié et est donc concomitant à l'individualisation des données[61].

L'individualisation des données devra se faire dans le respect des principes de finalité et de proportionnalité tels qu'ils sont définis dans la Convention mais également tels qu'ils sont consacrés dans la loi du 8 décembre 1992.

#### 2. *Principe de finalité*

Selon l'article 13, § 1er de la Convention, l'employeur individualise les données de communications électroni-

59. Par « individualisation » il convient de comprendre l'opération consistant à traiter les données de communications électroniques en réseau collectées lors d'un contrôle installé par l'employeur en vue de les attribuer à un travailleur identifié ou identifiable (article 12, § 1er).
60. C.C.T. n° 81, p. 9.
61. C.C.T. n° 81, p. 24.

ques en réseau « de bonne foi » et « en conformité avec la ou les finalités que poursuit ce contrôle ». On peut penser que la notion de bonne foi fait appel à la notion de traitement loyal tel que défini dans la loi du 8 décembre 1992. Il s'agit d'individualiser les données dans le respect du principe de transparence. Or, précisément lors d'une procédure d'individualisation directe, l'employeur qui constate une anomalie peut retracer directement, à partir de données globales, l'identité du responsable de l'anomalie et ce sans en avertir préalablement le travailleur. On peut donc remettre en question l'équivalence de la notion de loyauté dans la loi et la Convention collective.

L'article 13, § 2 précise que si les données de communication sont traitées en vue d'une finalité autre que celle pour laquelle le contrôle a été installé, l'employeur doit s'assurer que ce traitement est compatible avec la finalité initiale. Ce même principe de compatibilité est décrit à l'article 4, § 1er, 2°, de la loi du 8 décembre 1992. Si aucun des deux textes ne définit précisément ce qu'il faut entendre par une finalité « compatible », la loi du 8 décembre 1992 indique que le fait que l'intéressé puisse raisonnablement s'attendre à ce que ces données soient traitées à telle fin est un critère permettant d'apprécier le caractère compatible ou non des différentes finalités poursuivies. Le fait que la finalité soit prévue dans un texte légal permet également d'en apprécier la compatibilité[62].

Comme nous l'avons déjà précisé, le principe de finalité tel que défini dans les articles 4 et 5 de la loi du 8 décembre 1992 devra par ailleurs être respecté.

### 3. *Principe de proportionnalité*

L'article 14 de la Convention précise que l'on ne peut individualiser les données de communications électroniques collectées lors d'un contrôle que d'une manière compatible avec la ou les finalités poursuivies à l'article 5, § 1er. Il s'agit, selon nous, d'un rappel du principe de finalité plutôt que de proportionnalité.

Le paragraphe 2 de l'article 14 précise que seules les données de communications électroniques nécessaires à la ou les finalités poursuivies pour le contrôle peuvent être individualisées, et que les données doivent être adéquates, pertinentes et non excessives au regard de cette ou ces finalités. Il s'agit bien du principe de proportionnalité tel qu'il est énoncé dans l'article 4 de la loi du 8 décembre 1992. A ce propos, il convient de rappeler que seules les données de communication à savoir les données qui entourent la communication, pourront être traitées (expéditeur, destinataire, date, heure,...) et non pas le contenu lui-même du courrier qui ne pourra être attribué à un travailleur identifié ou identifiable à moins d'obtenir l'accord exprès et préalable de tous les participants à la communication en vertu de l'article 314bis du Code pénal.

62. M.-H. Boulanger, C. De Terwangne, T. Leonard, S. Louveaux, D. Moreau, Y. Poullet, « La protection des données à caractère personnel en droit communautaire », *J.T.D.E.* , 1997, p. 146.

Au terme de l'examen de la C.C.T., on soulignera en premier lieu que ce texte a le mérite de fournir des lignes directrices en ce qui concerne les modalités des contrôles, et à ce titre, offre des orientations utiles aux employeurs tout en énonçant certaines garanties en faveur des employés.

Toutefois, la C.C.T. ne suffit pas à elle seule à assurer que les contrôles opérés sur le lieu de travail sont effectués en conformité avec l'ensemble des dispositions légales applicables. La Convention collective s'inscrit en effet dans un cadre plus large, comportant notamment des dispositions de droit international, des dispositions constitutionnelles et légales consacrant la protection des données à caractère personnel et le secret des communications. On évoquera en particulier l'obligation pour l'employeur de déterminer de façon concrète et précise et selon le contexte de travail les finalités de contrôle poursuivies, ainsi que d'évaluer au cas par cas la légitimité de chacune de ces finalités.

On insistera également sur les exigences de concertation préalable entre employeurs et employés qui sont indispensables à l'adoption d'une politique de contrôle au sein de l'entreprise ainsi que sur l'exigence prévue par le code pénal, de l'obtention du consentement des parties à une communication, sauf si toutes les parties à la communication entendent donner à cette communication un caractère public.

Or, lorsqu'il est indiqué dans le rapport préliminaire à la C.C.T. qu'« il faut cependant admettre des aménagements mais stricts quant à [la] mise en œuvre [des principes constitutionnels et légaux de protection de la vie privée et de secret des télécommunications] sur le lieu de travail »[63], il semble que la C.C.T. entende déroger aux dispositions de droit international, et aux dispositions constitutionnelles et légales susvisées, ce qui conduit à s'interroger sur le respect des normes supérieures par la Convention collective.

Précisément, en vertu des principes constitutionnels et en vertu de la Convention européenne des droits de l'homme, toute ingérence dans un droit fondamental tels que la vie privée doit, pour être licite, être prévue par une loi[64].

La question de savoir si une convention collective de travail peut être considérée comme une loi au sens de la Convention européenne des droits de l'homme et de la Constitution a été examinée par la doctrine, sans qu'il existe à ce sujet de position unanime.

On retiendra de la jurisprudence de la Cour européenne des droits de l'homme qu'une norme ne doit pas nécessairement revêtir la forme d'une loi au sens formel pour pouvoir être prise en considération[65]. Une certaine jurisprudence belge se fondant sur cette jurisprudence en déduit qu'il suffit que « la norme de droit interne, écrite ou non, soit suffisamment accessible aux justiciables et que le champ d'application et le contenu normatif soient suffisamment précis pour pouvoir en pré-

63. Page 9.
64. Voyez l'article 8, § 2 C.E.D.H.
65. CLAEYS, TOUSSAINT, DEJONGHE, « L'utilisation des nouvelles technologies, de l'e-mail durant le contrat de travail, la notion de faute et son évolution dans l'exécution du contrat de travail », *Le contrat de travail et la nouvelle économie* , pp. 264-265.

voir les conséquences raisonnablement prévisibles »[66].

On relève néanmoins, avec d'autres auteurs, que cette interprétation de la notion de norme ne remet pas en cause les exigences légales plus précises qui doivent être respectées lorsqu'un texte prévoit une ingérence dans la vie privée de l'individu. Seul le législateur dispose du pouvoir d'apporter une restriction à une liberté fondamentale reconnue à l'article 22 de la Constitution. « En l'occurrence, l'intérêt d'une telle exigence serait d'autant plus manifeste que les délibérations donnant lieu à l'élaboration des conventions collectives de travail, à la différence des débats parlementaires donnant lieu à l'adoption d'une norme législative, ne sont pas publiques, et que le principe de la transparence des documents administratifs, consacré par la loi du 11 avril 1994 relative à la publicité de l'administration, ne leur est pas applicable, ce qui exclut qu'un véritable contrôle démocratique puisse s'exercer sur les arguments invoqués pour mettre en place tel ou tel régime de restriction »[67].

En définitive, nous nous interrogeons sur la sécurité juridique qui découlerait de dérogations à des droits et libertés fondamentaux, prises sur la seule base d'une convention collective de travail sans contrôle parlementaire. Pour cette raison, nous recommandons d'interpréter la C.C.T. comme fournissant des orientations utiles mais qui devraient toujours être interprétées en conformité avec les instruments internationaux de protection des droits de l'homme[68], les principes constitutionnels ainsi que les lois de protection des données à caractère personnel et des télécommunications qui les exécutent.

66. Trib. trav. Nivelles, 8 février 2002, *J.T.T.*, 2002 p. 182.
67. DE HERT, DE SCHUTTER ET SMESTERS, « Emploi, vie privée et technologies de surveillance », *J.T.T.*, 2001, pp. 9 et 10.
68. En s'inspirant de la technique de l' « interprétation conformée » dégagée par la Cour de Justice des Communautés européennes notamment dans l'affaire *Marleasing*, 13 novembre 1990 (C106-89).